Ю.С. Тарасенко, Ю.В. Савченко,
О.О. Шаповал, М.М. Мороз

ОСНОВИ МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ ЛОГІСТИЧНОЇ ДІЯЛЬНОСТІ

Монографія

Кременчук
NOVABOOK
ВИДАВНИЦТВО
2026

УДК 658.528:004.056.5:338.24
О 72

Друкується за рекомендацією вченої ради
Кременчуцького національного університету імені Михайла
Остроградського (протокол № 5 від 20.02.2026 р.)
Рецензенти:

КУХАР Володимир Валентинович – доктор технічних наук, професор, проректор з науково-дослідної роботи, ТОВ «ТЕХНІЧНИЙ УНІВЕРСИТЕТ «МЕТІНВЕСТ ПОЛІТЕХНІКА», м. Запоріжжя, Україна;
ПРИТЧИН Сергій Емільович – доктор технічних наук, професор, професор кафедри автоматизації та інформаційних систем, Кременчуцький національний університет імені Михайла Остроградського, м. Кременчук, Україна.

О 72 **Основи менеджменту інформаційної безпеки в умовах логістичної діяльності** / Ю.С. Тарасенко, Ю.В. Савченко, О.О. Шаповал, М.М. Мороз. – Кременчук : Видавництво «НОВАБУК», 2026. – 478 с.
ISBN 978-617-639-578-2

В монографії розглядаються теоретичні і методологічні основи управління процесами інноваційного та інвестиційного розвитку господарюючих суб'єктів. Значна увага приділена питанням прогнозування, планування і забезпечення досягнення бажаних результатів, що сприяють інвестиційному та інноваційному розвитку фірм та організацій з обліком зовнішніх і внутрішніх факторів середовища. Наприкінці кожного розділу наводяться питання для самоконтролю, приклади розрахункових завдань та завдання для самостійного опрацювання. У монографії також вміщено тести для перевірки знань здобувачів вищої освіти та термінологічний словник. Метою даної монографії є сприяти підготовці фахівців галузі знань D «Бізнес, адміністрування та право», спеціальності D3 «Менеджмент», галузі знань F «Інформаційні технології», спеціальностей F5 «Кібербезпека та захист інформації», галузі знань K «Безпека та оборона», спеціальності K3 «Національна безпека», а також розраховано на студентів вищих навчальних закладів, аспірантів, викладачів вищих навчальних закладів, підприємців і керівників-практиків, яких цікавлять проблеми захисту даних, інноваційного та інвестиційного менеджменту, спеціалістів науково-дослідних організацій, а також широкого кола ділових людей. Монографія складається з вступу, восьми розділів, списку використаних джерел і додатків. Повний обсяг становить 478 сторінок, 78 рисунків, 15 таблиць, 2 додатків, списку використаних джерел із 37 найменувань.

УДК 621.396.96

ISBN 978-617-639-578-2

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

AI/ES (artificial inteligence/expert systems) – штучний інтелект / експертна систем
BC (barcoding) – штрихове кодування
CALS – концепція «безперервного розвитку та підтримки життєвого циклу»
DM (datamanagment) – управління даними
ED (electronic data interchange) – електроний обмін даними
ETL – репозиторій
GDSN (Global Data Synchronisation Network) – всесвітня мережа синхронізації даних
GPRS – General Packet data Radio Service 76
LTE – Long-Term Evolution
RA&C (remote accessand communication) – дистанційний доступ та комунікації
WAP – Wireless Application Protocol
ISO/OSI (The Open Systems Interconnection model) – мережева модель стека (магазину) мережевих протоколів
LAN (Local Area Network) – локальна комп'ютерна мережа
КСЗІ – комплексна система захисту інформації

ПЕРЕДМОВА

Автори монографії зосереджують увагу на особливостях підготовки фахівців, здатних вирішувати практичні проблеми та складні спеціалізовані задачі інформаційного напрямку у господарської діяльності, що характеризуються комплексністю та невизначеністю умов у сфері управління організаціями та їх підрозділами за спеціальностями D3 Менеджмент (згідно освітньо-професійною програмою (ОПП) «Логістика») *,[1] з урахуванням концептуально-гносеологічних*,[2] та правових аспектів щодо створення комплексних систем захисту інформації (КСЗІ) та F5 Кібербезпека та захист інформації*,[3], наприклад, об'єктів критичної інфраструктури (ОКІ), як наглядно домінуючою складовою синергетичного ефекту у сфері **логістики та менеджменту підприємництва***,[4]**.** Також автори наголошують на тому факті, що сьогодні процес забезпечення навчального процесу державною (українською) мовою в цьому напрямку ускладнений відсутністю строгої, позбавленої різночитання, наукової термінології, що потребує детальнішого розтлумачення усіх понять та термінології у даному навчальному процесі. Наприклад, щойно згаданий термін **«концепція»** (від лат. *conceptio* – «система розуміння») може бути використаний як: - або комплекс поглядів чого-небудь, пов'язаних між собою і таких, що випливають один з іншого; - або певний спосіб розуміння, трактування яких-небудь явищ; основна точка зору, керівна ідея для їх висвітлення; - або система поглядів на явища в світі, природі, суспільстві; - або провідний задум, конструктивний принцип у науковій, художній, технічній, інших

*[1] ОПП «Логістика» розроблена на основі Закону України «Про освіту» від 05.09.2017 № 2145-VIII, Закону України «Про вищу освіту» від 01.07.2014 № 1556-VII та Стандарту вищої освіти за спеціальністю 073 «Менеджмент», затвердженого наказом МОН України від 29.10.2018 № 1165.

*[2] Гносеоло́гія (від грец. γνώσις — «пізнання» і λόγος — «вчення, наука») — теорія пізнання.

*[3] Закон України № 2163-VIII «Про основні принципи забезпечення кібербезпеки України». 2018р.

*[4] Карпов В.Е., Карпов А.В. Менеджмент-логістики. Навч. посібник. м. Кіровоград. 2013.– 493 с.

видах діяльності; - або система шляхів вирішення задачі; - або спосіб розуміння, розрізнення і трактування будь-яких явищ, що породжує властиві тільки йому міркування і висновки.

Фактично виходить, що концепція визначає стратегію дій, однак, залежно від області застосування (використання), різним концепціям відповідатиме свій термінологічний апарат. Крім того, виправдано вважається, що основою забезпечення безпеки інформаційної системи є три складові у вигляді конфіденційності, цілісності, доступності, а сам процес успішного захисту інформації в інформаційній системі, наприклад ОКІ, **залежить від рівня розвитку апаратного забезпечення, програмного забезпечення і рівня комунікації (забезпечення зв'язку).** При цьому процедури (механізми) захисту, що використовуються, поділяють на фізичний рівень захисту, на рівень захисту персоналу та організаційний рівень, а саме поняття **«інформаційна безпека»** вводять із точки зору або **діяльності,** спрямованої на забезпечення захищеного стану об'єкта (в цьому значенні частіше використовується термін «захист інформації»), або **стану** (як якості) певного об'єкту (де об'єкт може бути як інформація, так і дані, і ресурси автоматизованої системи, і сама автоматизована система, і інформаційна система підприємства, суспільства, держави і т. п.).

Очевидно, що інформаційна безпека – це стан захищеності інформаційного середовища, а захист інформації – являє собою діяльність щодо запобігання витоку інформації, що захищається, несанкціонованих і ненавмисних дій щодо інформації, яка підлягає захисту, тобто процес, спрямований на досягнення цього стану.

Прийнято розрізнять **інформаційну безпеку організації,** як стан захищеності інформаційного середовища організації, що забезпечує її формування, використання і розвиток, та **інформаційну безпека держави**, – як стан збереження інформаційних ресурсів держави і захищеності законних прав особистості і суспільства в інформаційній сфері. *,[5]

---

*[5] Алпеев А.С. Термінологія безпеки: кібербезпека, інформаційна безпека. Журнал: «Питання кібербезпеки». Випуск №5 (8) / 2014.

У сучасному соціумі інформаційна сфера має дві складові: інформаційно-технічну (у вигляді створеного людиною світу техніки, технологій тощо) та інформаційно-психологічну (світ живої природи, що включає і саму людину). Тому в загальному випадку інформаційну безпеку суспільства (держави) можна представити двома складовими частинами: інформаційно-технічною безпекою та інформаційно-психологічною (психофізичною) безпекою. Залежно від застосування діяльності соціуму із захисту інформації заведено виокремлювати такі галузі забезпечення інформаційної безпеки: − законодавчу, нормативно-правову та наукову, що включають нормативно-правові акти, нормативно-методичні документи та стандарти в області інформаційної безпеки; −структурну, із затвердженням органів та підрозділів по виконанню технічних і організаційних вимог і завдань інформаційної безпеки; −організаційно-технічну із зазначенням заходів і методів політики інформаційної безпеки; − програмно-технічну із зазначенням способів та засобів забезпечення інформаційної безпеки.

В даному навчальному посібнику викладено концептуально-правові аспекти щодо створення комплексних систем захисту інформації (КСЗІ). Наведено концепцію забезпечення інформаційної безпеки, основи політики безпеки в області інформації та методологічні основи створення комплексної системи захисту інформації (розділи 1-3). Деталізована вразливість інформації, що захищають, і наведено аналіз джерел і каналів несанкціонованого доступу (розділи 4 і 5). У наступних розділах розглянуті питання моделювання, архітектури побудови комплексної системи захисту інформації та її кадрово-інтелектуальна безпека в процесі експлуатації. Розглянуто алгоритм створення кодексу корпоративної поведінки. Викладені кадрові та нормативно-правові аспекти забезпечення комплексної системи захисту інформації та її управління ОКІ. При цьому загалом об'єкти критичної інфраструктури доцільно розглядати не тільки з позицій конкретної логістичної системи, а й з позиції сучасного аналізу та реалізації безпечної життєдіяльності більшості видів соціуму.

ВСТУП

Сучасний світ жорсткої конкуренції на світовому ринку праці стрімко підвищує вимоги до рівня вузівського формування професійної компетенції випускника у сфері інформаційного менеджменту та інформаційних систем управління на підприємствах або компаній різного профілю діяльності.

Даний посібник є спробою авторів акцентувати навчання, (згідно освітньою програмою «Логістика» за спеціальністю D3 Менеджмент), на підвищення рівня професійній підготовки фахівців у галузі ***логістики*** шляхом реалізації мети отримання ***синергетичного ефекту*** підвищення конкурентоспроможності національних підприємств та компаній різного профілю діяльності, де навчально-методичним об'єктом дослідження є аспекти безпеки та захищеності їхньої критичної інфраструктури. Останнє притаманне виробничому менеджменту у вигляді сукупності принципів, методів, засобів і форм управління виробництвом, що має на меті підвищення його ефективності та збільшення прибутку, а логістика, як менеджмент усіх видів діяльності, сприяє руху та координації попиту та пропозиції на товари різних сфер виробництва у визначеному місці і в заданий час*,[6].

Залежно від ресурсів підприємства, що підлягають інтеграції, виділяють операційну, фінансову, управлінську, інвестиційну та інформаційну форму ***синергії****,[7]**.***

Від напрямку бізнесу компанії виділяють політичну, маркетингову, фінансову, виробничу, кадрову та інноваційну. Залежно від напрямку інтеграції компаній виділяють системну

---

*[6] Карпов В.Е., Карпов А.В. Менеджмент-логістики. Навчальний посібник. м. Кіровоград. 2013.– 493 с. (укр. мова).

*[7] Синергія (від грец. Synergos – (syn) разом; (ergos) діючий, дія) – це сумуючий ефект, який полягає у тому, що при взаємодії двох або більше факторів їх дія суттєво переважає ефект кожного окремого компонента у вигляді простої їх суми. Однака дана мова йдеться про явище посилення дії одного каталізатора додаванням іншого.

синергію та синергію від перенесення компетенцій*,[8].

Очевидно, що з позицій позитивного синергетичного ефекту у сфері **менеджменту підприємництва** (наприклад, при диверсифікації, створенні концернів, кооперації тощо) не слід нехтувати безпекою сучасної інформаційної форми синергії, яка, залежно від його (підприємства) ресурсів, що підлягають інтеграції, є особливо актуальною, наприклад, для об'єктів критичної інфраструктури (ОКІ) з комплексної системою захисту інформації (КСЗІ). При цьому, на таких об'єктів реалізація системи управління, навіть за наявністю власної критичної інформаційної інфраструктури (КІІ), не може формуватися відірвано від внутрішніх та зовнішніх чинників впливу на штатний режим їх життєдіяльності.

Таким чином, і не тільки у даному випадку, наша освітня життєдіяльність та і уся супутня сфера буття суттєво залежать від/та безпосередньо впливають на інформаційну область сучасного соціуму на фоні природніх, тобто фізичних (від давньогрецької – «природа») та інших соціально-економічних та виробничих процесів, у тому числі і традиційного побуту у тривимірному просторі. У зв'язку з чим безпосереднє викладення даного навчального матеріалу доцільно починати з понятійного трактування використовуваних сигнальних ознак. У їх основі закладено семантичний (від давньогрецької – «означаючий») та/або математичний опис процесу життєдіяльності сучасної спільноти. Так, саме поняття «сигнал» у кожного з нас формувалося з перших днів життя, а далі уточнювало на наступних її етапах. Фактично воно (це поняття) уточнювало у процесі виникнення та оцінки умовних знаків у оточуючому нас світі: на початку у вигляді жестів, поведінки, комунікації за допомогою слів, яке удосконалювалося, і на даний момент є базовим елементом сучасних інформаційних технологій (ІТ).

Різноманіття сигналів очевидно і у зв'язку із природою свого виникнення виявляються у вигляді акустичних, електричних, магнітних, корпускулярних, променевих, електромагнітних та

---

*[8] Верхоглядова Н.І., Лисенко Ю.В. Методичний підхід до визначення синергетичних ефектів інтеграційних угод. Східна Європа: економіка, бізнес та управління. Випуск 1 (01) 2016 с.48-54.

інших впливів на соціум. Тому їх (сигналів) форми виявлення (регулярні, випадкові), представлення (аналогові, дискретні), обробки (оцінки), зберігання та передачі (комутації) є базовими у ІТ – інформаційних технологій.

Тем не менш до цього часу, через необмежене різноманіття сигнальних ознак відсутнє єдине формулювання самого поняття інформації. У нашому випадку під інформацією розуміємо як дещо пізнавально-загальне, насамперед з освітньої та наукової областей буття, що забезпечує достовірність та цілісність у процесі науково-практичної, виробничої, побутової та інших сферах життєдіяльності людини*,[9]. Будь-яке її (інформації) спотворення, випадкове (несвідоме) та навмисне (заздалегідь продумане) доцільно класифікувати як повідомлення. Причому у останньому випадку можна такі дії вважати хакерською атакою на інформацію*,[10]. Також, є очевидним, що не кожне повідомлення необхідно вважати інформацією. З точки зору оптимальної фільтрації обробленого (досліджуваного) сигналу вагомими факторами у процесі оцінювання його, наприклад, захищеності від завад та надійності є форми регулярності виявлення (постійні або випадкові) та представлення (аналогові та дискретні) різноманітних видів інформації: телеграфних, телекодових, факсимільних, телевізійних та будь-яких інших кодувань.

Як правило, сигнал або його ж сигнальна функція у вигляді математичного представлення підлягають різноманітному виду перетворень у інформаційних технологіях. Причому прийнято вважати, що ІТ – це сукупність методів і інструментарію для збору, обробки, зберіганню і комутації інформації (повідомлень) про об'єкт дослідження. Тому ІТ (як можливість оптимізації, а часто і руйнування життєдіяльності соціуму) рідка обходяться

---

*[9] Ю.С.Тарасенко. Методологія набуття професійної компетенції за вивчення дисципліни «Схемотехніка та архітектура комп'ютера», Збірник матеріалів міжнародної наукової конференції «Інноваційні технології, моделі управління кібербезпекою ІТМК-2022», Part 2/ December 12-14. 2022. Київ. С.66-68.

*[10] Хакерська атака на інформацію - це навмисний і несанкціонований доступ до інформаційних систем та даних, який має на меті порушити їх конфіденційність, цілісність або доступність, або ж змінити чи знищити їх.

без засобів обчислювальної техніки. Останні, у залежності від аналітичного або цифрового представлення та обробки запису сигналу, розробляють у відповідності з вибором їхньої схемотехнічної реалізації (СТР) у вигляді конкретного технічного пристрою, наприклад ноутбука або планшета, що забезпечують можливість оцінювання і аналізу отримуваної інформації з наступним перетворенням, зберіганням або комутацією з новим споживачем.

Описані процеси прийнято оптимізувати, аналізуючи конкретні потенційно-схемотехнічні рішення (схемотехніку) комп'ютерів та ЕОМ, відповідно до вибору більш прогресивної архітектури. Причому при виборі як архітектури, так і її СТР, спочатку прийнято проводити їх структурно-лінгвістичне обґрунтування як за призначенням, так і за відповідної технології створення, із врахуванням яких у майбутньому забезпечують розробку структурно-логічних і функціональних схем (СЛС і СФС) конкретного обчислювального пристрою (ОП). Ці схеми призначені для наступного створення принципових електричних схем, або, як прийнято говорити, їх (ОП) схемотехніку. При цьому використовують сучасне поняття «архітектури» ОП у вигляді її (комп'ютера) концептуальної моделі, за якою прийнято вивчати принципи проектування та перспективи їх розвитку (стиль), з урахуванням взаємодії як складових блоків між собою, так і можливим оточенням.

Відтак, при викладання навчального матеріалу автори навчального посібника дотримувались алгоритму вивчення дисципліни у відповідності до принципу пізнання «від легкого до складного» з акцентуванням не тільки значимості та актуальності матеріалу, що вивчається, а й наведенням структурно-функціональних схем, що пояснюють не лише ***обьект, предмет та послідовність*** **викладу** (етапи пізнання) **матеріалу** (див. рис. В.1) з урахуванням потоково-семестровий та сесійний звітності, а також динамічне ускладнюванних реалізацій комплексних систем захисту інформації (КСЗІ) згідно їїх структурно-функціональних схем. При цьому підсумкова СФС методології побудови розширеної системи захисту та безпеки об'єктів

критичної інфраструктури (див. рис. В.2) *,[11] переконливо демонструє повноту та значимість дисципліни, що вивчається, та додатково орієнтує і дисциплінує студента до професійного освоєння обраної спеціальності.

Оскільки цей навчальний посібник призначений для студентів молодших курсів (які ще слабко володіють методикою пізнання), то саме в таких випадках необхідно акцентувати увагу того, хто навчається, на можливих причинах виникнення потенційних помилок у його пізнавальній діяльності з метою вчасного їх коригування. Як показує практика*,[12], прийнято виокремлювати такі основні причини помилкових відповідей: або через незнання матеріалу, або через відсутність зв'язків між поняттями, або через плутанину з термінами та визначеннями, або через помилкове подання (сприйняття) екзаменаційного матеріалу. Очевидно, що для ліквідації їх негативного прояву в освітньому процесі передбачено семінарсько-практичні заняття. Однак і тут, незважаючи на природне збільшення навчального матеріалу, зростання ролі викладача і важливості його безпосереднього контакту зі студентами, чітко прослідковується тенденція до скорочення так званого «голосового навантаження» у вигляді лекційних та семінарських занять, залишаючи непорушним сам процес екзаменаційної сесії.

Оскільки цей навчальний посібник призначений для студентів молодших курсів (які ще слабко володіють методикою пізнання), то саме в таких випадках необхідно акцентувати увагу того, хто навчається, на можливих причинах виникнення потенційних помилок у його пізнавальній діяльності з метою вчасного їх коригування.

*[11] Ю.С.Тарасенко, Ю.В.Савченко. Ризик-орієнтовані процеси забезпечення безпеки об'єктів критичної інфраструктури // Системи та технології, 2023, 65 (1). С. 66-76.

*[12] Taber K. S. Student thinking and learning in science: perspectives on the nature and development of learner's ideas. Oxford: Routledge, 2014. 2018p

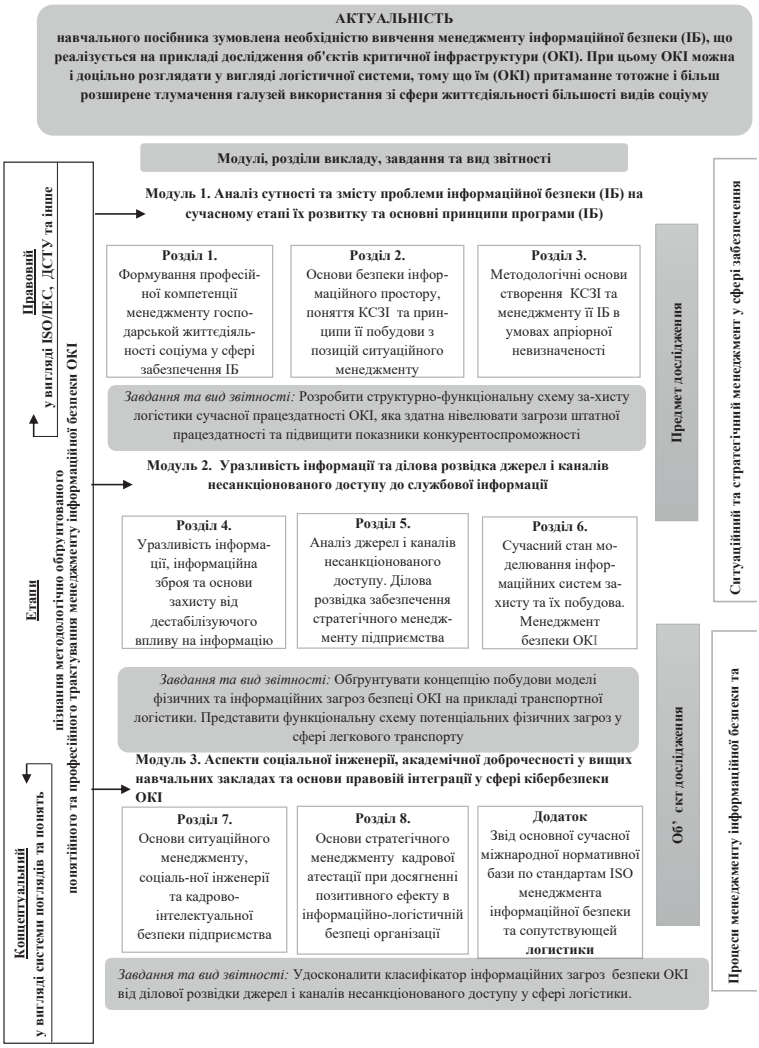

Рис. В.1. Структурно-пізнавальна схема етапів викладення концептуально – методологічних і правових основ менеджменту інформаційної безпеки підприємства

Як показує практика*,[13], прийнято виокремлювати такі основні причини помилкових відповідей: або через незнання матеріалу, або через відсутність зв'язків між поняттями, або через плутанину з термінами та визначеннями, або через помилкове подання (сприйняття) екзаменаційного матеріалу. Очевидно, що для ліквідації їх негативного прояву в освітньому процесі передбачено семінарсько-практичні заняття. Однак і тут, незважаючи на природне збільшення навчального матеріалу, зростання ролі викладача і важливості його безпосереднього контакту зі студентами, чітко прослідковується тенденція до скорочення так званого «голосового навантаження» у вигляді лекційних та семінарських занять, залишаючи непорушним сам процес екзаменаційної сесії.

Фактично тільки в процесі іспиту (заліку) у викладача з'являється адекватна можливість коригувати в пізнавальній діяльності кожного студента причини виникнення можливого їхнього помилкового сприйняття фахової термінології та понять. У зв'язку з цим доцільно, особливо для складних дисциплін, безпосередньо сам екзаменаційний процес трансформувати в режим відкритого іспиту*,[14]. Причому, єдиною відмінністю від загальноприйнятого процесу прийому іспиту у студента є доказовий захист (озвучування) його (відповідно до екзаменаційного квитка) підготовленого матеріалу перед усією студентською групою.

Таким чином, багато апріорі помилкових уявлень через не зовсім чітке сприйняття матеріалу в тих, хто складає іспит, нівелюються, що і сприяє формуванню підсумкового цілісного уявлення про предмет і його подальшу професійну значущість у всієї групи.

---

*[13] Taber K. S. Student thinking and learning in science: perspectives on the nature and development of learner's ideas. Oxford: Routledge, 2014. 2018p

*[14] Тарасенко Ю.С. Аспекти формування професійної компетенції студентів вузу. // International scientific conference "Innovative technologies, models Cyber Security Management, ITCSM-2020 Annual Scientific Conference ITCSM-2020 Dnipro, Ukraine Book of Abstracts. Pp 98-100.

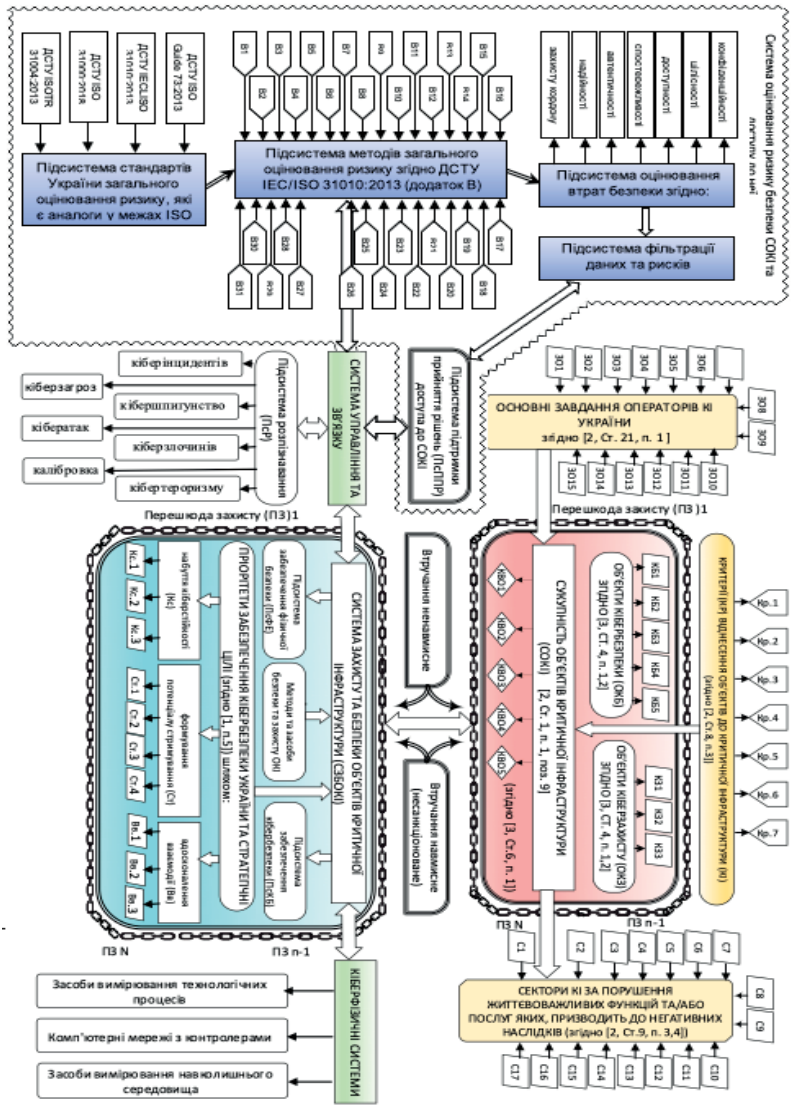

Рис. В.2. Схема методології побудови розширеної системи захисту та безпеки об'єктів критичної інфраструктури

Монографія складається з вступу, восьми розділів, списку використаних джерел і додатків. Повний обсяг становить 478 сторінок, 78 рисунків, 15 таблиць, 2 додатку, список використаних джерел із 37 найменувань.

1. ФОРМУВАННЯ ПРОФЕСІЙНОЇ КОМПЕТЕНЦІЇ МЕНЕДЖМЕНТУ ГОСПОДАРСЬКОЇ ЖИТТЄДІЯЛЬНОСТІ СОЦІУМА У СФЕРІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1. Концептуально-гносеологічні та правові аспекти формування понятій з інформаційної безпеки соціума

Очевидно, що поняття інформації у кожного з нас складалося індивідуально в процесі пізнання навколишнього світу та сучасного соціума*,[15]. На даний момент (розуміючи, що з латини information – «відомості, роз'яснення, викладення»)

*[15] «Суспільство як соціум характеризує суспільний світ як саму абстрактну, в певному смислі невизначену всезагальність людського суспільного буття, яка охоплює весь суспільний світ без будь-яких виключень. Саме завдяки своїй абстрактності, у певній мірі невизначеності, соціум виступає як «чисте», концентроване втілення суті суспільного буття людини», згідно Воронкова В.Г. Співвідношення людини і соціуму як своєрідна іманентна суперечливість самої людини. Гуманітарний вісник ЗДІА. Філософія. Випуск 42. 2010. Стор. 14-24.

кожен з нас вкладає у це слово власне понятійне трактування, сформовану у процесі життєдіяльності (учбової, виробничої, культурної, соціальної тощо), яку розширює по мірі свого професійного і культурного зростання, не зменшуючи значення діючої парадигми. У якості додаткового підтвердження її актуальності цілком достатньо прикладу розвитку сучасних телекомунікаційних систем з гарантованою якістю обслуговування QoS (Quality of Service). Причому зі створення цифрових мереж інтегрального обслуговування і технології асинхронного методу передачі (ATM – Asynchronous Transfer Mode) почалася реалізація транспортного механізму для передачі (**логистики**) усіх видів інформації з QoS. Їх представлення у єдиному цифровому форматі з виділенням потрібних ресурсів мережі, які гарантують QoS перед початком передачі інформації користувача, є обов'язковими компонентами технологій IP/MPLS (Internet Protokol / Multiprotocol Label Switching – мульти-протокольна комутація за мітками) і ATM. З 2003 року, коли озвучено «Архітектуру безпеки для систем, що забезпечують зв'язок між кінцевими пристроями», фактично вперше було визначено методологію організації інформаційної безпеки телекомунікаційних систем*,[16].

Дана Архітектура безпеки передбачувала розподілення усіх ресурсів телекомунікаційних систем (канали зв'язку, програмно-апаратні комплекси і т.д.) на незалежні модулі захисту інформації, де кожен модуль повинен задовольняти задекларованим параметрам інформаційної безпеки.

Відповідно, у рамках державної політики забезпечення безпеки інформаційних ресурсів, при створенні і розвитку сучасної методології ефективного забезпечення безпеки інформації необхідно використовувати загальновизнану парадигму захисту інформації. Реалізацію останньої прийнято забезпечувати у відповідності до державних (на рівні ДСТУ) і міжнародних (на рівні ISO/IEC) правовими документами.

*[16] UTI-T Recommendation X.805 Security Architecture for Systems providing end-to-end Communications, 2003.

У наш час існує більше кілька десятків міжнародних стандартів ISO/IEC 2700*,[17], що пов'язані з інформаційною безпекою (ІБ) та кібербезпекою України*,[18],. Слід зауважити, що ці європейські стандарти не є обов'язковими, однак їх значимість у вітчизняному соціумі складно переоцінити. Вони відображають особливості сучасного рівня інформаційних технологій (принципи, підходи реалізації), але, нажаль не містять наскрізних шкал цінності і переліків

вимог безпеки до використовуваних систем захисту інформації. Реалізація же безпеки останніх, як правило, починається з побудови моделі пізнання гіпотетичних інформоб'єктів з апріорним їх захистом від можливих кібератак і інцидентів, тобто від різноманітних загроз природнього та штучного походження. Фактично парадигма інформації і її безпеки, як вихідної концептуальної схеми і моделі постановки проблем, зводиться до реалізації алгоритмів їх рішень і оптимізації запропонованих методів і засобів захисту інформації. При цьому, відносно тенденції розвитку ІБ, можна стверджувати, що поняття інформації немислиме без поєднання об'єкта її виникнення, засобів зв'язку і підтримуючої інфраструктури, захищених від навмисних або випадкових впливів природнього або штучного походження. Очевидно, що від характеру таких впливів можливими є негативні наслідки як безпосередньо для самої інформації і об'єктів її первинного виникнення, так і відповідної підтримуючої інфраструктури. Навіть при використанні стандарту ISO/IEC 15408, який визначає профіль захисту для підтримуючої інфраструктури з необхідним її рівнем, ймовірні втрати виражаються лише у лінгвістичній формі вигляду «ризик середній».

Викладене вище дає підставу також у лінгвістичній формі озвучити і своє понятійне трактування «інформації», не дивлячись на те, що список існуючих варіантів є вагомим. Тим не менш, без чіткого понятійного трактування інформації

*[17] Дивись Додаток 1. Сімейство стандартів ISO/SEC 27000 як джерело для створення національного стандарту з кібербезпеки.

*[18] Закон України № 2163-VIII «Про основні принципи забезпечення кібербезпеки України». 2018р.

ускладнено побудову будь-якої моделі пізнання (забезпечення) безпеки інформаційної системи. Отже, у нашій редакції інформація – це результат опосередкованого впливу у вигляді пізнавально-нематеріального вихідного представлення (субстанції) у фундаменті буття соціуму, що забезпечує достовірність і цілісність в науково-технічній, виробничій, побутовій та інших сферах життєдіяльності людини. Будь-яке її (інформації) перетворення або спотворення, випадкове (несвідоме) або не випадкове (завчано продумане) доцільно розглядати як **повідомлення.**

Очевидно, що наступні трансформації (перетворення) інформації до вигляду **повідомлень** потребують відповідних фіксацій (від лат. fixus – міцний, закріплений), реалізованих за допомогою поля (у першу чергу електромагнітного, що забезпечує телекомунікацію різноманітних видів повідомлень) або за допомогою матеріально-речових носіїв, наприклад, у вигляді газет, документів, дискет, флешек і тому подібних. При цьому будь-яку особистість можна також розглядати з позицій як джерела, так і носія інформації. Відповідно, саме матеріальні носії потребують, у першу чергу, захисту від несанкціонованого допуску до них. Тому, як правило, інформаційну безпеку ототожнюють із захистом її носіїв. Причому, як було озвучено у Введення, прийнято вважати, що основою забезпечення безпеки інформаційної системи є три складові у вигляді конфіденційності, цілісності, доступності, а сам процес успішного захисту інформації в інформаційній системі залежить від рівня апаратного забезпечення, програмного забезпечення і рівня комунікації (забезпечення зв'язку). Використовувані процедури (механізми) захисту від потенційних загроз розділяють на фізичний рівень захисту, на рівень захисту персоналу і організаційний рівень. Саме ж поняття «інформаційна безпека» використовують як вид або діяльності, що направлена на забезпечення захищеного стану об'єкту (у цьому значенні частіше за все використовується термін «захист інформації»), або стану (як якості) конкретного об'єкту. При цьому, у якості об'єкта може виступати і інформація, і дані, і ресурси автоматизованої системи, і сама автоматизована система, і інформаційна система підприємства, суспільства, держави і т.д.

Звідси, інформаційна безпека – це стан захищеності інформаційного середовища, а захист інформації являє собою діяльність по запобіганню витоку інформації, що захищається, тобто є процес, який направлений на досягнення цього стану.

Нажаль, першоджерело виникнення (появи) безпосередньо самої інформації, на відміну від процесу її поширення і обробки, прийнято замовчувати. Хоча наступні її (інформації) сприйняття, поширення, обробка, зберігання і оцінка як змісту пізнавальної корисності і об'єму, тобто якості і кількості, завжди затребувані і досить важливі при виборі засобів безпеки і захисту від випадкових і навмисних загроз безпосередньо як для самої інформації, так і для відповідної підтримуючої інфраструктури (див. рис. 1.1 [1]). Фактично маємо стійку взаємну кореляцію між об'єктом-джерелом інформації, безпосередньо самою інформацією і об'єктом сприйняття і наступної обробки інформації. Даний процес є аналогічним методам радіолокаційного виявлення, виміру, дозволу, розпізнавання об'єкту спостереження з додатковою інфраструктурою безпеки. Ось і в нашому випадку, розмірковування о виникненні поняття інформації не доцільно здійснювати у відриві від першоджерела (об'єкта), що створює цю інформацію.

Залишаючи біологічну сторону виникнення інформації біонікам, методи яких [2], наприклад уже привели до рівня розробки моделей штучних нейронних мереж, зазначимо тільки матеріальні аспекти появи і наступної реалізації безпеки інформації.

Очевидно, що в основі даного процесу лежать фізіологічні (зорове, слухове, дотику і т.д.) сприйняття будь-якого впливу (включаючи і інформаційні загрози), який йде від оточуючого нас світу, у тому числі і соціуму, у якому ми знаходимося. При цьому кожна адекватна людина такий вплив оцінює на основі порівняльної характеристики з раніше існуючими асоціаціями, що були отримані ним у процесі своєї життєдіяльності.

Таким чином створюється підсумковий опосередкований результат, який виступає у вигляді першоджерела інформації, оскілки був отриманий безпосередньо у процесі порівняльної лінгвістичної оцінки тих «впливів», які людина набуває протягом свого життя. Звідси, будь-яка первинна інформація є

суб'єктивною, а її об'єктивність встановлюють відповідними (у тому числі і метрологічними) експертизами. Подальша обробка первинної інформації (її оцінка, зберігання, поширення і т.д.) у процесі трансформації у вторинну потребує (див. рис. 1.1) адекватних захисних заходів.

Відповідно, запропоноване лінгвістичне трактування інформації, (яке має невизначеність за аналогією з радіолокаційною [3]), без уточнювального прив'язування до об'єкту або суб'єкту, (що створив її з наступною реалізацією над нею дій у вигляді: розпізнавання, розповсюдження, зберігання, додаткової обробки з метою трансформації у інші види представлення і захисту від випадкових або навмисних загроз її існуванню), є цілком виправданим. Завдяки цьому сутність поняття (терміну) «інформація» доцільно розглядати з позицій критично важливого об'єкта, і, відповідно, до неї (інформації) може бути застосовано увесь арсенал технічних і програмно-апаратних засобів захисту як гіпотетично критичному об'єкту пізнання.

Нині, характерний не тільки неминучістю інформаційних війн, аспекти безпеки проявляються в усіх сферах соціуму: від побутових до науково-виробничих, де домінантною прийнято вважати безпеку держави, суспільства, людини. У такому контексті значущість оцінювання стану безпеки будь-яких сучасних об'єктів, передусім **критично-важливих (КВО)** з їхніми інформаційними інфраструктурами (ІІ) та забезпеченням повноти й достовірності інформації в задіяних комп'ютерних мережах, завжди актуальна й необхідна. Останнє вагомо підтверджується прийняттям Законів України «Про основні засади забезпечення кібербезпеки України» [4] та «Про критичну інфраструктуру» [5].

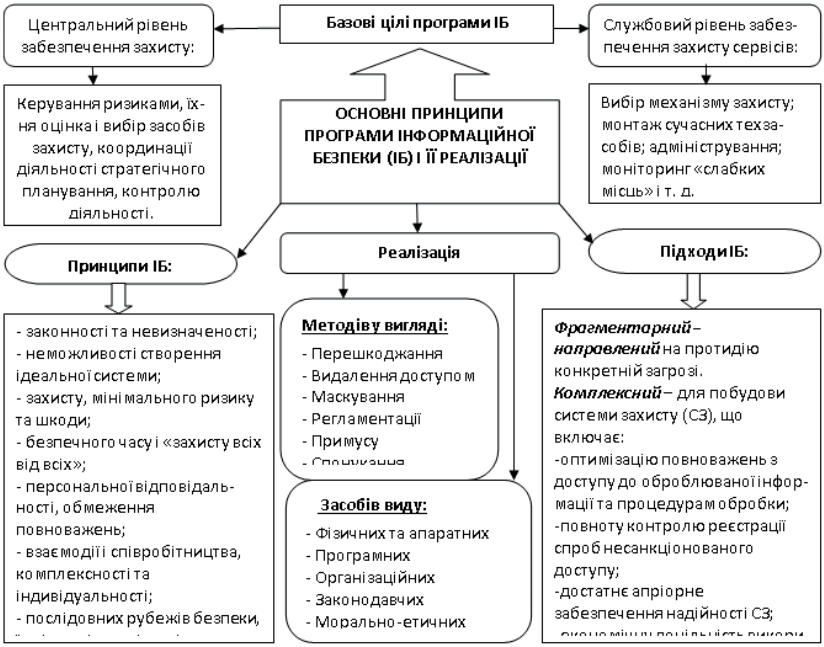

Рис. 1.1. Формування та забезпечення процесу реалізації програми інформаційної безпеки

Так Закон України № 2163-VIII 2018 р. «Про основні засади забезпечення кібербезпеки України» набув чинності з 9 травня 2018 року, де правову основу забезпечення кібербезпеки України становлять Конституція України, Кримінальний кодекс України, Кодекс України про Адміністративні правопорушення, непосредственно сам закон № 2163-VIII та інші закони України, міжнародні договори, згода на обов'язковість яких надана Верховною Радою України, а також видані на виконання законів інші акти України.

Закон № 2163-VIII визначає об'єкти і суб'єкти забезпечення кібербезпеки. При цьому основними суб'єктами Національної системи кібербезпеки є: Державна служба спеціального зв'язку та захисту інформації України, Національна поліція України, Служба безпеки України, Міністерство оборони України та Генеральний штаб Збройних Сил України, розвідувальні органи,

Національний банк України. Фактично Національна система кібербезпеки «являє собою сукупність суб'єктів забезпечення кібербезпеки і взаємопов'язаних заходів політичного, науково-технічного, інформаційного, освітнього характеру, організаційних, правових, оперативно-розшукових, розвідувальних, контррозвідувальних, оборонних, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформаційних ресурсів, кіберзахисту об'єктів критичної інформаційної інфраструктури».

Законом «Про критичну інфраструктуру» [5] від 16.11.2021 року фактично нівелюється неузгодженість у термінологічному сприйнятті використовуваних термінів. Зокрема, «Віднесення **об'єктів до критичної інфраструктури (ОКІ)** здійснюється за сукупністю критеріїв, що визначають їх соціальну, політичну, економічну, екологічну значущість для забезпечення оборони країни, безпеки громадян, суспільства, держави і правопорядку, зокрема для реалізації життєво важливих функцій та надання життєво важливих послуг, що свідчать про існування загроз для них, можливість виникнення кризових ситуацій через несанкціоноване втручання в їх функціонування, припинення функціонування, людський фактор чи природні лиха, тривалість робіт для усунення таких наслідків до повного відновлення штатного режиму» [Ст.8, п.2]. Причому для організації ефективного гарантування безпеки та непорушності такої структури визначено її сімнадцять секторів, зокрема електронні комунікації та інформаційні послуги [Ст. 9, п. 4], паспорти безпеки на кожний об'єкт критичної інфраструктури (КІ) з урахуванням конкретизації існуючих загроз [Ст. 12, п. 1-3], чотири режими їхнього функціонування: штатний; готовності та запобігання реалізації загроз; реагування на виникнення кризової ситуації; відновлення штатного функціонування [Ст. 15, п. 1], а також передбачено операторів КІ [Ст. 15, п. 1], а також операторів КІ [Ст. 15, п. 1]. Серед різноманіття основних (із 15) завдань для цих операторів [Ст.21, п.1], акцентуємо увагу на необхідності «проведення навчань і тренінгів, підготовки та перевірки персоналу, який відповідає за охорону, безпеку та захист об'єктів критичної інфраструктури; та захист інформації про системи управління, зв'язку, фізичну безпеку та кібербезпеку». Крім того,

ОКІ зобов'язані розробляти вимоги як щодо організації захисту критичної інфраструктури, так і посадові інструкції для осіб, відповідальних за її забезпечення та організацію [Ст.21, п.2].

Таким чином, надійна працездатність об'єктів, у світлі вищевказаної сукупності критеріїв, неможлива без успішного здійснення інформаційної боротьби за потенційну безпеку перерахованих послуг і об'єктів, що, по суті, і ототожнюється з поняттям кібербезпеки. У зв'язку з чим у цикл професійної підготовки з формуванням та забезпечення процесу реалізації програми інформаційної безпеки багатьох ВНЗ вводиться навчальна дисципліна «Комплексні системи захисту інформації» та їй аналогічні. При цьому безпосередньо поняття «система», «комплексність», «захист» та «інформація» у кожного з'явилося в процесі пізнання навколишнього світу через його оцінку (так і хочеться сказати, - інформаційну) проявів цього світу, що послідовно відображалося у свідомості людини шляхом зорового, тактильного і слухового сприйняття. Так, поняття «захисту» у кожного із Вас, хто читає даний посібник, винікло дуже рано: – у одних це пов'язано із захистом від больового відчуття (наприклад, у вигляді гарячого або холодного), у інших, – з протидією будь-якому виду агресії (наприклад, від тваринного або сильнішого супротивника), у третіх, – з проявом природних явищ (наприклад, у вигляді дощу, снігу і т. д.), у четвертих, – та Ви самі можете продовжити цей перелік. Вперше з поняттям «системи» Ви зустрічалися, вирішуючи алгебраїчні системи рівнянь, а з науковим поняттям «комплексність», – при вивченні комплексних чисел. Ці поняття в перебігу подальшого освітнього циклу значно розширилися і на даний момент у кожного з Вас ототожнюються у вигляді певної філософської категорії. Так, з точки зору діалектичного визначення системи розуміють систему як частину об'єктивної реальності, обмежену ціллю (цілями) та ресурсами. Системно у світі все: практика та практичні дії, знання і процес пізнання, навколишнє середовище та зв'язки з нею (в ній). Процес пізнання структурує системи, оточуючий нас світ. Все, що не пізнане в даний момент часу, утворює "хаос у системі", змушує шукати нові структури, нову інформацію, нові форми подання та опису знань, призводить до появи нових гілок знання. Тому комплексність – це цілеспрямоване і планомірне

встановлення і застосування системи взаємопов'язаних вимог до об'єкту матеріальної або нематеріальної сфери та його складових частин, а також до інших матеріальних і нематеріальних чинників, що впливають на об'єкт, шляхом узгодження їх взаємних вимог. Як бачимо, у кожного процес пізнання навколишнього світу був індивідуальним, але тим не менше реалізований за єдиним сценарієм у вигляді «від простого до складного». Це характерно і для поняття «інформація». Термін ***«інформація»*** походить від латинського слова ***informatio,*** що означає «відомості, роз'яснення, виклад». Інформація – це настільки загальне і глибоке поняття, що його не можна пояснити однією фразою. У це слово вкладається різний зміст у техніці, науці і в життєвих ситуаціях. У побуті інформацією називають будь-які дані або відомості, які кого-небудь цікавлять, наприклад повідомлення про які-небудь події, про чию-небудь діяльність і т. п. «Інформувати» в цьому сенсі означає «повідомити щось, невідоме раніше». При цьому одне і теж саме інформаційне повідомлення (стаття в газеті, оголошення, лист, телеграма, довідка, розповідь, креслення, радіопередача і т. п.) може містити різну кількість інформації для різних людей залежно від їх накопичених знань, від рівня розуміння цього повідомлення та інтересу до нього. Так, повідомлення, складене японською мовою, не несе ніякої нової інформації людині, що не знає цієї мови, але може бути високоінформативним для людини, що володіє японською. Ніякої нової інформації не містить і повідомлення, викладене знайомою мовою, якщо його зміст незрозумілий або вже відомий. Отже, інформація є характеристика не повідомлення, а співвідношення між повідомленням і його споживачем. Без наявності споживача, хоча б потенційного, говорити про інформацію безглуздо.

Таким чином, можна констатувати, що у поняття «інформація» закладені відомості про об'єкти і явища навколишнього середовища, їх параметри, властивості та стан, які сприймають у процесі життєдіяльності та роботи інформаційних систем.

Останнім часом прийнято розуміти, що ***інформаційна система (ІС)*** – це система, яка реалізує інформаційну модель предметної області, найчастіше – якої-небудь сфери людської

діяльності. ІС повинна забезпечувати: отримання (введення або збір), зберігання, пошук, передачу та обробку (перетворення) інформації.

Інформаційна система (або інформаційно-обчислювальна система) – сукупність взаємопов'язаних апаратно-програмних засобів для автоматизації накопичення та обробки інформації. У той же час ***інформаційна система*** – сукупність інформації, яка міститься в базах даних (відомості/повідомлення/дані незалежно від форми їх подання), та інформаційних технологій, які забезпечують її обробку (процеси, методи пошуку, збору, зберігання, обробки, надання, поширення інформації та способи здійснення таких процесів і методів) і технічних засобів. В інформаційну систему дані надходять від джерела інформації. Ці дані відправляють на зберігання або вони зазнають в системі деяку обробку і потім передаються споживачеві. Між споживачем і власне інформаційною системою може бути встановлений зворотній зв'язок. У цьому випадку інформаційну систему називають замкнутою. Канал зворотного зв'язку необхідний, коли потрібно врахувати реакцію споживача на отриману інформацію. Інформаційна система складається із баз даних, в яких накопичується інформація, джерела інформації, апаратної частини ІС, програмної частини ІС, споживача інформації.

Очевидно, що використання інформаційних систем (ІС), як правило, здійснюється на тлі певної сукупності ***ризиків****,[19] під час її експлуатації, - особливо якщо в ІС відсутні технічні сучасні засоби перероблення інформації, але використовується персонал, «людський фактор» якого складно оцінити, навіть застосовуючи ***методи соціальної інженерії***. У зв'язку з чим, на думку низки фахівців, такі ІС доцільно відносити до ***ручних інформаційних систем.*** Зокрема, про діяльність менеджера*,[20] у

---

*[19] Інформаційні ризики – це ризики втрати, несанкціонованої зміни інформації через перебої у функціонуванні ІС або за їх виходу з ладу, що призводить до втрати інформації.

*[20] Походження слова «менеджмент» є від латинського слова «manus» – рука, що означало вміння вести домашнє господарство та вправно працювати. На даний момент поняття «менеджмент» трансформувався і він охоплює види

фірмі, де відсутні комп'ютери, можна говорити, що він працює з ручною ІС.

Автоматизовані інформаційні системи (АІС), як найбільш популярний клас ІС, передбачають участь у процесі накопичення та обробки інформації, у створенні баз даних та програмного забезпечення, в експлуатації технічних засобів обслуговуючим персоналом і т. д. Автоматичні інформаційні системи здатні виконувати всі операції з переробки інформації без участі людини, що значне нівелює ***ризики.***

- інформаційно-пошукові системи, тобто системи для накопичення, обробки, пошуку і видачі інформації, що цікавить користувача;

- інформаційно-аналітичні системи, як клас інформаційних систем, призначених для аналітичної обробки даних із використанням баз знань і експертних систем;

- інформаційно-вирішувальні системи, тобто системи, що здійснюють накопичення, обробку та переробку інформації з використанням прикладного програмного забезпечення;

- керуючі інформаційні системи з використанням баз даних і прикладних пакетів програм;

- дорадчі експертні інформаційні системи, що використовують прикладні бази знань, накопичені ситуаційними центрами у вигляді інформаційно-аналітичних комплексів.

Інформаційні системи можна класифікувати за архітектурою:

- локальні ІС (працюють на одному електронному пристрої, не взаємодіючому з сервером або іншими пристроями);

- клієнт- серверні ІС (працюють у локальній або глобальній мережі з єдиним сервером);

- розподілені ІС (децентралізовані системи у гетерогенній мультисерверній мережі).

За сферою застосування інформаційні системи класифікуються на:

діяльності та реалізує загальні та спеціальні функції, у процесі яких відбувається формування і досягнення різного роду цілі.

- інформаційні системи організаційного управління, призначені для забезпечення автоматизації функцій керуючого персоналу;
- інформаційні системи управління технічними процесами, призначені для забезпечення керування механізмами, технологічними режимами на автоматизованому виробництві;
- автоматизовані системи наукових досліджень у вигляді програмно-апаратних комплексів, призначених для наукових досліджень і випробувань;
- інформаційні системи автоматизованого проектування, тобто програмно-технічні системи, призначені для виконання проектних робіт із застосуванням математичних методів;
- автоматизовані навчальні системи у вигляді комплексів, що складаються з програмно-технічного оснащення, навчально-методичної літератури та електронних підручників, які забезпечують навчальну діяльність;
- інтегровані інформаційні системи, що забезпечують автоматизацію більшості функцій підприємства;
- економічні інформаційні системи, призначені для забезпечення автоматизації збору, зберігання, обробки та видачі необхідної інформації, для виконання функцій управління;
- модельні інформаційні системи, що дозволяють встановити діалог із моделлю в процесі її дослідження (надаючи при цьому відсутню для прийняття рішення інформацію). Як правило, вони складаються з математичних, статистичних, фінансових та інших моделей, використання яких полегшує подальше вироблення стратегії і видачу об'єктивної оцінки серед результатів альтернативних рішень;
- експертні інформаційні системи, пов'язані з обробкою знань для вироблення та оцінки можливих альтернатив прийняття рішення користувачем. При цьому, такі системи реалізують на двох рівнях. На першому рівні (концепція «типового набору альтернатив»), здійснюється збір і оцінка відомостей про проблемні

ситуації з метою з'ясування до якого класу рішень можна віднести досліджувану ситуацію. Використання такої експертної підтримки на даному рівні сприяє створенню інформаційного фонду зберігання для подальшого аналізу типових альтернатив. На другому рівні провадиться генерація можливих альтернатив на основі правил перетворення і процедур оцінки синтезованих альтернатив, використовуючи базу наявних в інформаційному фонді даних. Очевидно, що такі експертні системи базуються на сукупності фактів, відомостей і даних та безпосередньо використовують багатопрофільні системи правил логічного виведення інформації на підставі логічних моделей баз даних і баз знань. При цьому ***бази даних*** містять сукупність конкретних даних, а ***бази знань*** – сукупність конкретних і узагальнених відомостей в рамках логічної моделі бази знань.

У випадках, коли говорять про автоматизовану роботу з інформацією за допомогою будь-яких технічних пристроїв, зазвичай, в першу чергу, цікавляться не базою даних і не змістом повідомлення, а тим, скільки символів це повідомлення містить.

Стосовно комп'ютерної обробки даних під ***інформацією*** розуміють деяку ***послідовність символічних позначень*** (букв, цифр, закодованих графічних образів і звуків і т. п.), що несе смислове навантаження і представлену в зрозумілому комп'ютеру вигляді. Кожен новий символ у такій послідовності символів збільшує інформаційний обсяг повідомлення.

Очевидно, що інформація може існувати у вигляді: текстів, малюнків, креслень, фотографій; світлових або звукових сигналів; радіохвиль; електричних і нервових імпульсів; магнітних записів; жестів і міміки; запахів і смакових відчуттів; хромосом, за допомогою яких передаються у спадок ознаки і властивості організмів, і т. д.

Предмети, процеси, явища матеріальної чи нематеріальної природи, що розглядаються з точки зору їх ***інформаційних властивостей***, прийнято називати ***інформаційними об'єктами*** (про них трохи пізніше).

Як правило, у сучасному світі одержання і аналіз інформаційних властивостей об'єктів природи та природного походження здійснюють радіофізичними системами, які об'єднують радіофізичні методи і способи вилучення, передачі, вирішення і руйнування інформації про цей об'єкт пізнання.

Такі системи включають в себе не тільки радіотехнічні системи, що їх реалізують, а і пристрої радіоуправління як об'єктом, так і безпосередньо самою радіотехнічною системою.

Відмітною ознакою радіосистеми є наявність одного або декількох радіоканалів, які об'єднують: джерело радіохвиль; середовище, в якому ці радіохвилі поширюються, і приймач, що забезпечує обробку радіохвиль з метою вилучення інформації про об'єкт – джерело радіохвиль.

Радіохвилі, що несуть ту чи іншу інформацію, називають радіосигналами.

Прийнято класифікувати радіосистеми виходячи із способів і методів обробки інформації, які в свою чергу, породжують свої різновиди функціональної належності ***систем***.

Так, до ***систем вилучення інформації*** відносять радіолокаційні та радіонавігаційні системи, системи радіоастрономії, радіоспостереження поверхні Землі та інших космічних об'єктів, радіорозвідки, митного радіоконтролю і т. д.

Серед ***систем передачі інформації*** розрізняють системи радіозв'язку, телеметрії, передачі команд, радіомовлення і телебачення.

До ***систем дозволу (розподілу) інформації*** можуть бути віднесені технічні пристрої, що забезпечують фільтрацію корисної інформації від активних або пасивних супутніх сигналів і перешкод і призначені для підвищення рівня надійності інформаційних засобів вилучення і передачі повідомлень.

Системи руйнування інформації призначені для створення умов, в яких функціонування протиборчої сторони стає неможливим.

Очевидна необхідність високої завадостійкості всіх перерахованих вище систем, аж до застосування в таких системах ***спеціальних засобів захисту інформації.***

На ринку захисту інформації пропонується багато окремих інженерно-технічних, програмно-апаратних, криптографічних

засобів захисту інформації. Зрозуміло, що засоби захисту інформації нерозривно пов'язані із засобами отримання інформації. Вони зазвичай об'єднані в єдину систему, де ключовим елементом є людина, яка вважається важко формалізованою і потенційно слабкою її ланкою.

Така комплексна система зобов'язана забезпечувати належним чином дієвий захист інформаційних ресурсів підвідомчих структур і об'єктів від усіх можливих реальних загроз природного і штучного походження.

При цьому самі комплексні системи реалізуються технічними засобами, в основі побудови яких лежать як традиційні (оптичні, радіаційні, рентгенівські), так і сучасні (електромагнітні) методи і засоби одержання, аналізу та захисту інформації від об'єктів спостереження і контролю.

Найчастіше поняття «інформаційної безпеки», а надалі і «кібербезпеки», використовують як синоніми, оскільки їх родовий зв'язок визначений через поняття «безпека». Однак обидва ці терміни, м'яко кажучи, можуть підлягати критиці.

Дійсно, саме поняття «безпека» у сучасному світі відіграє чи не найголовнішу роль в усіх життєвих процесах: біологічних, політичних, економічних, соціальних, технічних, територіальних та ін. Тому дуже важливо не тільки коректно визначати це поняття і його похідні, але і правильно застосовувати їх за призначенням.

Цілком коректно вибирати визначення «безпека» за аналогією з публікації [6], де прийнято, що ***«безпека»*** – область науки, що вивчає природні, техногенні, соціальні, економічні та інші процеси освіти, розвитку і взаємодії суб'єктів, об'єктів навколишнього середовища і їх комбінацій з метою виявлення джерел небезпек, визначення їх характеристик та формування законів та інших нормативних актів, що встановлюють поняття, вимоги, рекомендації та методики, виконання яких повинно гарантувати захищеність інтересів окремої особистості і суспільства в цілому від усіх виявлених і вивчених джерел небезпеки». У такому випадку, ***кібербезпека*** – розділ безпеки, що вивчає процеси формування, функціонування та еволюції кібероб'єктів, з метою виявлення джерел кібернебезпеки, які можуть завдати їм шкоди, і формування законів та інших

нормативних актів, що регламентують терміни, вимоги, правила, рекомендації та методики, виконання яких повинно гарантувати захищеність ***кібероб'єктів*** від усіх відомих та вивчених джерел ***кібернебезпеки.*** Під ***кібероб'єктом*** тут розуміється, будь-який об'єкт, функціонування якого здійснюється за участю програмованих засобів.

Зауважимо, що визначення терміну «кібербезпека» [7] базується на понятті «***кіберпростір***»: «кіберпростір – сфера діяльності в інформаційному просторі, утворена сукупністю комунікаційних каналів Інтернету та інших телекомунікаційних мереж, технологічної інфраструктури, що забезпечує їх функціонування, і будь-яких форм людської активності (особистості, організації, держави), яка здійснюється за допомогою їх використання».

У визначенні терміну «кіберпростір» також родовий термін «сфера» обраний не логічно. Цей термін був би доречний, якби визначався термін «кіберсфера». Отже, більш коректно визначити поняття «кіберпростір» через поняття «кібероб'єкт» наступним чином: ***кіберпростір*** – простір, у якому здійснюється функціонування і взаємодія кібероб'єктів. Тоді ***кібербезпека об'єкту*** – властивість об'єкта, що характеризує його внутрішні можливості не бути причиною утворення збитку для зовнішнього середовища або обмежувати його величину допустимими нормами.

При цьому слід розуміти, що збиток кібероб'єкту наноситься в результаті спеціально організованих кібератак. Під кібератакою розуміють навмисно організовану сукупність дій за участю програмно-технічних засобів (ПТЗ), яка спрямована на нанесення економічного, технічного або інформаційного збитку. Наприклад, одержання секретних відомостей з різних аспектів.

За джерелом організації кібератаки можна поділяти на дві групи: зовнішні, відносно об'єкту кібератаки та внутрішні.

Повертаючись до поняття «інформаційна безпека», будемо надалі його, як правило, використовувати, за аналогією з [8], у наступному вигляді: ***«інформаційна безпека»*** – захист конфіденційності, цілісності та доступності інформації, або ***«інформаційна безпека»*** – стан захищеності особистості, організації та держави і їх інтересів від загроз, деструктивних та

інших негативних впливів у інформаційному просторі. Складність цього поняття полягає в тому, що сам предмет, безпека якого визначається, не визначений як за внутрішньою структурою, так і за внутрішніми властивостям, які необхідні для формування вимог щодо його безпеки.

Навіть саме визначення інформації, в даний час вельми неоднозначне і суперечливе. Таким чином сформувати поняття безпеки такого предмета на підставі його внутрішньої структури і внутрішніх властивостей не видається можливим. Тим більше, що у вище наведених визначеннях використовують термінологію, понятійне трактування якої раніше не було чітко деталізоване.

Надалі будемо вважати, що:

конфіденційність інформації – це такий стан інформації, при якому доступ до неї тільки у об'єктів з наявністю прав на неї;

цілісність інформації – це блокування несанкціонованих змін інформації;

доступність інформації – це запобігання приховування інформації від користувачів з правами доступу.

Звертає увагу те, що всі складові являють собою тільки зовнішні дії по відношенню до інформації: призначення прав доступу до інформації; блокування несанкціонованих змін інформації; запобігання приховування інформації від користувачів з правами доступу. Більш того, обидва взятих для уточнення поняття фактично встановлюють еквівалентність термінів «безпека» та «захищеність». Така ситуація в термінології іменується порочним колом: «безпека це захищеність», а «захищеність це безпека».

Як правило, захищеність об'єкта це його захист від зовнішніх джерел небезпеки, в той час як безпека об'єкта це внутрішня властивість об'єкта не бути джерелом небезпеки для навколишнього середовища.

З цієї точки зору потрібно розрізняти два терміни: **«кібербезпека об'єкта»** і **«кіберзахищеність об'єкта»**, що відповідає англійській інтерпретації **«cyber safety object»** та **«cyber security object»**.

Перший термін визначено вище, другий термін може бути уточнено таким чином: ***кіберзахищеність об'єкта*** **–** це

властивість об'єкта, що характеризує його зовнішні можливості запобігати утворенню збитку від кібератак або обмежувати його величину допустимими нормами.

Що стосується терміну «інформаційна безпека», то має сенс поки міркувати про інформацію як про чорний ящик, тобто тільки про захищеність інформації. Тому термін «безпека інформації», наразі визначається тільки намірами її власника і ні чим іншим.

Це дає підстави стверджувати, що термін «інформаційна безпека» на даний момент часу (поки не визначено коректно, що таке інформація і яка її внутрішня структура і властивості) не коректний за своєю суттю. Замість нього можна запропонувати термін «інформаційна захищеність» і використовувати для нього визначення викладене раніше, тобто:

- ***«інформаційна захищеність»*** – захист конфіденційності, цілісності та доступності інформації, що коректніше відповідає реальному стану розглянутої проблеми.

Очевидно, що наведена аргументація допоможе деяким чином просунути розуміння термінології безпеки на якісно новий рівень. У подальшому викладі будемо свідомо відходити від застосування поняття у вигляді «інформаційна безпека», використовуючи термін «захист інформації».

Таким чином, ***інформаційну безпеку*** будемо розглядати як забезпечення стану захищеності:

1) особи, суспільства, держави від впливу недоброякісної інформації;

2) інформації та інформаційних ресурсів від неправомірного і несанкціонованого впливу сторонніх осіб;

3) інформаційних прав і свобод громадянина і людини, тобто, не розглядаючи питання захисту від впливу недобросовісної інформації, і в подальшому будемо віддавати перевагу більш «вузькому» терміну у вигляді ***захисту інформації.***

1.2. Домінуючі аспекти форм створення, передачі, обробки та етапи обігу інформації в інформаційних системах

Отже очевидно, що існує множина визначень поняття інформації від найзагальнішого, – філософського (де інформація

є відображенням реального світу за допомогою різного роду повідомлень), до найбільш вузького, – практичного, де під інформацією розуміють будь-які відомості, що є об'єктом зберігання, передачі та перетворення. Поняття інформації пов'язано з деякими моделями реальних речей, що відображають їх сутність у тій мірі, у якій це необхідно для практичних цілей.

Як правило, така інформація в сучасному соціумі призначена для виконання конкретних функцій життєдіяльності суспільства, основними з яких є:

- ***пізнавальна,*** мета якої - отримання нової інформації через реалізацію основних етапів обігу інформації у вигляді її синтезу (виробництва), подання, зберігання і сприйняття (споживання);

- ***комунікативна***, яка використовується в процесі спілкування людей, реалізуючи етапи обігу інформації через її розподіл (за допомогою фіксації на різних носіях даних) і передачу в просторі та в часі;

- ***управлінська,*** мета якої, під час отримання та після опрацювання інформації, полягає у формуванні доцільної поведінки як представників соціуму, так і сфер оптимальної взаємодії підвідомчих об'єктів і виробництв, спільно об'єднаних з їхніми пізнавальними та комунікативними функціями.

Це узгоджується і з філософською концепцією відображення речей один в одному і в живих організмах.

Таким чином, під інформацією потрібно розуміти не самі предмети і процеси, а їх представницькі характеристики відображення або відображення у вигляді чисел, формул, описів, креслень, символів, образів і інших абстрактних характеристик. Зокрема, в теорії інформації розрізняють три основні підходи (і подальшого аналізу) до поняття інформація та її форм:

- структурний, де представником інформації є повідомлення, що складається із символів;

- статистичний, де представлення інформації, як міри невизначеності (ентропії) події, забезпечується в рамках повідомлення з конкретно реалізованою невизначеністю у вигляді різних записів на папері, плівці та інших матеріалах, та динамічних (в процесі передачі, прийому і обробки) форм існування;

- семантичний*,[21] де подання інформації в текстовій формі повідомлення залежить від реалізованого контексту пізнання.

Тому сама по собі інформація може бути віднесена до області абстрактних категорій, подібних, наприклад, до математичних формул і може виявляється в матеріально-енергетичній формі у вигляді сигналів (інформаційних). Зокрема, згідно зі структурним підходом до інформації як її носії в матеріально- енергетичній формі можуть виступати не тільки її тверді представники у вигляді книжок, малюнків, дискет тощо, а й електричні, магнітні, хімічні та біологічні носії, а також електромагнітні, акустичні, тектонічні та іншого типу імпульси, хвилі, фізичні та культурно-виробничі прояви соціуму, міміка як мова жестів і ще багато чого, що можна сприйняти й усвідомити.

Також очевидно, що в наш час з передачею і обробкою інформації пов'язані дії будь-якого автоматизованого пристрою, творча діяльність людини, розвиток науки і техніки, економічні та соціальні перетворення у суспільстві. При цьому сам же процес формування, передачі, прийому і обробки інформації, реалізований в системах телемеханічних, радіотехнічних та системах зв'язку, вимагає серйозної кваліфікації обслуговуючого персоналу і часто піддається серйозним супутнім спотворенням, у тому числі і не завжди доброзичливим. Зазвичай інформаційне сприйняття об'єкта забезпечується на етапі виявлення через його розпізнавання. При цьому необхідно відокремити корисну інформацію від пасивних шумів і активних спотворень, що в ряді випадків пов'язане зі значними труднощами.

На етапі підготовки інформації здійснюються такі операції, як нормалізація, квантування, кодування і модуляція носія (сигналу) інформації. Передача інформації полягає у перенесенні її на відстань за допомогою сигналів різної фізичної природи відповідно електричними, електромагнітними та оптичними каналами. Прийом інформації на іншій стороні каналу має характер вторинного сприйняття з властивими йому операціями боротьби з шумами. Обробка інформації полягає у вирішенні задач, пов'язаних з її перетворенням, незалежно від їх

*[21] семантика – изучение текста с точки зрения его смысла.

функціонального призначення. Перетворення інформації здійснюється або засобами інформаційної техніки, або людиною. Якщо процес обробки піддається формалізації, він може виконуватися технічними засобами. У сучасних складних автоматизованих системах (АС) ці функції покладаються на ЕОМ і мікропроцесори, де до основних етапів обігу інформації в АС відносять: збирання (сприйняття) і підготовку (перетворення) інформації від об'єкта (процесу, явища) спостереження або спілкування; передання й оброблення (перетворення) інформації; зберігання і відображення (відтворення) інформації (див. Рис.1.2.).

Рис. 1.2. Структурна схема створення, передачі та обробки інформації

На етапі сприйняття інформації здійснюється цілеспрямоване вилучення й аналіз інформації про якийсь об'єкт (процес), унаслідок чого формується образ об'єкта, здійснюються його впізнання й оцінка. Найпростішим видом сприйняття є розрізнення двох протилежних станів: наявності («так») і відсутності («ні»), складнішим - вимірювання.

На етапі підготовки інформації здійснюється її первинне перетворення. На цьому етапі проводяться такі операції, як нормалізація, аналого-цифрове перетворення, шифрування. Іноді етап підготовки розглядають як допоміжний на етапі сприйняття. У результаті сприйняття і підготовки отримують сигнал у формі, зручній для передання, зберігання або обробки.

На етапі передання інформація пересилається з одного місця в інше (від відправника одержувачу-адресату). Передача здійснюється каналами різної фізичної природи, найпоширенішими з яких є електричні, електромагнітні та оптичні. Вилучення сигналу на виході каналу, схильного до дії шумів, має характер вторинного сприйняття.

На етапах опрацювання інформації виявляються її загальні та суттєві взаємозалежності, що становлять інтерес для системи. Перетворення інформації на етапі обробки (як і на інших етапах) здійснюється або засобами інформаційної техніки, або людиною.

У загальному випадку під опрацюванням інформації розуміють будь-яке її перетворення, яке проводять за законами логіки, математики, а також за неформальними правилами, що ґрунтуються на «здоровому глузді», інтуїції, узагальненому досвіді, усталеними поглядами та нормами поведінки. Результатом опрацювання є та сама інформація, але або подана в інших формах (наприклад, упорядкована за якимись ознаками), або така, що містить відповіді на поставлені запитання (наприклад, розв'язання певної задачі). Якщо процес опрацювання формалізований, його можуть виконувати технічні засоби. Кардинальні зрушення в цій царині відбулися завдяки створенню ЕОМ - універсального перетворювача інформації, у зв'язку з чим з'явилися поняття даних і обробки даних.

На етапі зберігання інформацію записують у запам'ятовувальний пристрій для подальшого використання. Для зберігання інформації використовують переважно напівпровідникові, магнітні та оптичні носії. Розв'язання завдань вилучення збереженої інформації (пошуку інформації) пов'язане з розробленням класифікаційних ознак і схем розміщення інформації, що зберігається, систематизацією, правилами доступу до неї, порядком її поповнення і поновлення, тобто всім тим, що визначає можливість цілеспрямованого пошуку й оперативного вилучення інформації, що зберігається.

Етап відображення інформації має передувати етапам, пов'язаним з участю людини. Мета цього етапу - надати людині потрібну їй інформацію за допомогою пристроїв, здатних впливати на її органи чуття.

При цьому послідовність дій, що виконуються з інформацією, називають інформаційним процесом, а якщо процес обробки не піддається формалізації і вимагає творчого підходу, обробка інформації здійснюється людиною.

Таким чином, інформація надходить в систему утворення інформаційного сигналу в формі повідомлень як сукупності знаків або первинних сигналів, що містять інформацію (див. Рис. 1.3).

Розрізняють дискретні і безперервні повідомлення. Дискретні повідомлення формуються в результаті послідовної видачі джерелом окремих елементів - знаків. Множину різних знаків називають алфавітом джерела повідомлень, а кількість знаків – об'ємом алфавіту. Безперервні повідомлення нероздільні на елементи і описуються функціями часу, які приймають безперервну множину значень. У ряді випадків безперервні повідомлення з метою підвищення якості передачі перетворюються у дискретні.

В автоматизованих інформаційних системах виокремлюють:

- структурну (перетворювальну) інформацію об'єктів системи, що міститься в структурах системи, її елементів управління, алгоритмів і програм переробки інформації;

- змістовну (спеціальну, головним чином таку, що інформує, вимірювальну та керувальну, а також науково-технічну, технологічну та ін.) інформацію, яку витягують з інформаційних масивів (повідомлень, команд тощо) відносно індивідуальної моделі предметної області одержувача (людини, підсистеми).

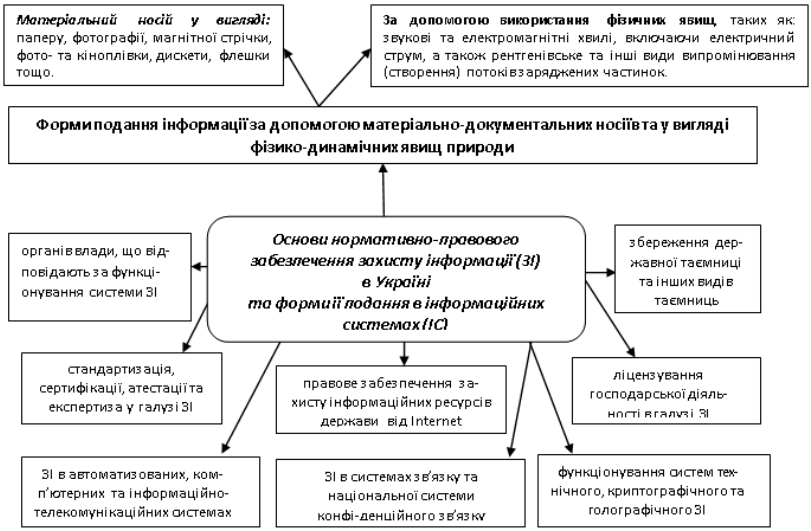

Рисунок.1.3. Форми подання інформації в інформаційних системах та основи нормативно-правового забезпечення захисту інформації в Україні

Перша пов'язана з якістю інформаційних процесів у системі, з внутрішніми технологічними ефектами, витратами на переробку інформації. Друга - як правило, із зовнішнім цільовим (матеріальним) ефектом.

Під час реалізації інформаційних процесів передача інформації (повідомлення) від джерела до приймача може здійснюватися за допомогою будь-якого матеріального носія (паперу, магнітної стрічки тощо) або фізичного процесу (звукових чи електромагнітних хвиль). Залежно від типу носія заведено розрізняти документальний, акустичний (мовленнєвий) і телекомунікаційний види інформації.

Документальна інформація подається в графічному або буквено-цифровому вигляді на папері, а також в електронному вигляді на магнітних та інших носіях.

Мовна інформація виникає під час ведення розмов, а також під час роботи систем звукопідсилення і звуковідтворення. Носієм мовленнєвої інформації є акустичні коливання (механічні

коливання частинок пружного середовища, що поширюються від джерела коливань у навколишній простір у вигляді хвиль різної довжини) у діапазоні частот від 200-300 Гц до 4-6 кГц.

Телекомунікаційна інформація циркулює в технічних засобах обробки і зберігання інформації, а також у каналах зв'язку під час її передачі. Носієм інформації під час її обробки технічними засобами та передачі дротовими каналами зв'язку є електричний струм, а під час передачі радіо- та оптичними каналами - електромагнітні хвилі.

Таким чином, найчастіше повідомлення може мати форму, не пристосовану для передачі, зберігання і обробки. У зв'язку з цим застосовують різні способи перетворення повідомлення у сигнал. До них відносяться дискретизація, кодування і модуляція. Під кодуванням розуміється процес перетворення дискретних або квантованих безперервних повідомлень в складний дискретний сигнал, що являє собою набір елементарних сигналів. Під модуляцією розуміється процес зміни параметрів носія під дією повідомлення.

Оскільки в інформаційних системах під сигналом розуміється фізичний процес, що несе повідомлення, то операцію відновлення повідомлення за прийнятим сигналом називають демодуляцією і декодуванням, технічна реалізація яких здійснюється демодулятором і декодером відповідно. Під лінією зв'язку розуміють фізичне середовище, яке забезпечує надходження сигналів від передавального пристрою до приймального.

Сигнали, що на виході ліній зв'язку, можуть відрізнятися від переданих внаслідок загасання, спотворення і впливу завад. Завадами називають сторонні збурення, що спотворюють корисний сигнал. Ефект впливу завад на різні блоки системи намагаються врахувати еквівалентним зміною характеристик лінії зв'язку. Тому джерело завад умовно відносять до лінії зв'язку.

Міру відповідності прийнятого повідомлення до надісланого називають достовірністю передачі, що позначає ступінь надійності та правдивості переданих відомостей. Прийняте повідомлення з виходу системи зв'язку надходить до одержувача,

а сукупність технічних засобів, призначених для передачі повідомлень, називають каналом зв'язку.

У сучасній практичній діяльності людини під час обміну інформацією використовують певну систему знаків у вигляді або природної, або штучної (формалізованої) мови. У зв'язку із цим проблеми передачі такої інформації поділяють на синтаксичні, семантичні та прагматичні проблемні рівні.

Проблеми синтаксичного рівня стосуються створення теоретичних основ побудови систем зв'язку, основні показники функціонування яких були б близькі до гранично можливих. При цьому, існує цілий ряд проблем щодо підвищення ефективності їх використання, і, перш за все, в технічній галузі вдосконалення методів передачі повідомлень і сигналів. На цьому рівні рішення проблем доставки одержувачу повідомлень забезпечується шляхом реалізації через сукупність знаків, повністю абстрагуючись від їх смислового і прагматичного змісту. Воно (рішення) спирається на поняття кількість інформації, що є мірою частоти вживання знаків, яка ніяк не відображає ні сенсу, ні важливості переданих повідомлень. У зв'язку з цим іноді говорять, що теорія інформації знаходиться на синтаксичному рівні.

Проблеми семантичного рівня пов'язані з формалізацією змісту переданої інформації, наприклад, введенням кількісних оцінок близькості інформації до істини, тобто оцінок її якості. Ці проблеми надзвичайно складні, так як смисловий зміст інформації більше залежить від одержувача, ніж від семантики повідомлення, представленого якою-небудь мовою. При цьому ми ще не вміємо вимірювати семантичну інформацію. Все, що раніше стосувалося підходів щодо її виміру, поки мали дуже приватний характер.

На прагматичному рівні, як правило, цікавлять наслідки від отримання і використання даної інформації абонентом. Проблеми цього рівня – це проблеми ефективності. Основна складність тут полягає в тому, що цінність або споживча вартість інформації може бути абсолютно різною для різних одержувачів. Крім того, вона істотно залежить від істинності інформації, своєчасності її доставки та використання. Відтак, у зв'язку зі створенням інформаційно-обчислювальних мереж, ведуться

інтенсивні дослідження в області оцінки старіння інформації, тобто втрати її цінності в процесі доставки. Однак, на думку багатьох фахівців, поняття «старіння» не точно відображає сенс цього процесу, особливо в технічній галузі передавання повідомлень та їх документування, оскільки, якщо носій інформації містить об'єктивну істину, то він не може застаріти.

1.3. Загальні положення концепції забезпечення інформаційної безпеки організації[22]*

На підставі вище викладеного під інформаційною безпекою (ІБ) потрібно розуміти захищеність інформації і підтримуючої інфраструктури від випадкових і навмисних впливів природного або штучного характеру, що можуть призвести до нанесення збитку власникам або користувачам інформації і підтримуючій інфраструктурі.

Незалежно від розмірів організації і специфіки її інформаційної системи, роботи щодо забезпеченню режиму ІБ у тому чи іншому вигляді повинні містити наступні етапи [9]:

a) Визначення політики ІБ.
b) Визначення сфери (меж) системи управління інформаційною безпекою та конкретизація цілей її створення.
c) Постановка задачі та оцінка ризиків, пов'язаних з порушенням ІБ.
d) Управління ризиками, які пов'язані з порушенням ІБ.
e) Вибір контрзаходів, що забезпечують режим ІБ.
f) Аудит системи управління ІБ.

а) Визначення політики ІБ

---

* Аспекти використання понять організація, підприємство, об'єкти та їх менеджмент (управління) викладено у п.1.5.

Визначення політики ІБ має зводитися до наступних практичних кроків:

1. Визначення використовуваних керівних документів і стандартів в області ІБ, а також основних положень політики ІБ, включаючи: управління доступом до засобів обчислювальної техніки (ЗОТ), програм і даних, антивірусний захист та питання резервного копіювання; проведення ремонтних і відновлювальних робіт та інформування про інциденти в області ІБ.

1. Визначення підходів щодо управління ризиками: чи є достатнім базовий рівень захищеності або потрібно проводити повний варіант аналізу ризиків;

3. Структуризація контрзаходів за рівнями;

4. Порядок сертифікації на відповідність стандартам в області ІБ. Повинна бути визначена періодичність проведення нарад за тематикою ІБ на рівні керівництва, включаючи періодичний перегляд положень політики ІБ, а також порядок навчання усіх категорій користувачів інформаційної системи з питань ІБ.

b) Визначення сфери (меж) системи управління ІБ і конкретизація цілей її створення

Необхідно визначити межі системи, для якої повинен бути забезпечений режим ІБ. Відповідно, система управління ІБ повинна будуватися саме в цих межах.

Опис меж системи рекомендується виконувати за таким планом:

1. Структура організації. Опис існуючої структури та змін, які передбачається внести у зв'язку з розробкою (модернізацією) автоматизованої системи.
2. Розміщення засобів ЗОТ і підтримуючої інфраструктури.
3. Ресурси інформаційної системи, що підлягають захисту.

Рекомендується розглянути ресурси автоматизованої системи наступних класів: ЗОТ, дані, системне і прикладне ПЗ. Всі ресурси представляють цінність з точки зору організації. Для їх оцінки повинна бути обрана система критеріїв і методологія отримання оцінок за цими критеріями.

4. Технологія обробки інформації та задачі, що вирішуються. Для чого

повинні бути побудовані моделі обробки інформації у термінах ресурсів. У результаті має бути складений документ, в якому зафіксовані межі системи, перераховані ресурси, які підлягають захисту, надана система критеріїв для оцінки їх цінності.

с) Постановка задачі та оцінка ризиків, пов'язаних з порушенням ІБ

На даному етапі повинна бути поставлена задача оцінки ризиків та обґрунтовані вимоги до методики оцінки ризиків. Існують різні підходи щодо оцінки ризиків. Вибір підходу залежить від рівня вимог, що пред'являються в організації до режиму інформаційної безпеки, характеру загроз, які беруться до уваги (спектру дії загроз) і ефективності потенційних контрзаходів.

1. Мінімальні вимоги до режиму ІБ.

Мінімальним вимогам до режиму ІБ відповідає базовий рівень ІБ. Звичайною областю використання цього рівня є типові проектні рішення. Існує ряд стандартів і специфікацій, в яких розглядається мінімальний (типовий) набір найімовірніших загроз, таких як віруси, збої устаткування, несанкціонований доступ і т. д. Для нейтралізації цих загроз обов'язково повинні бути прийняті контрзаходи незалежно від ймовірності їх здійснення і уразливості ресурсів. Таким чином, характеристики загроз на базовому рівні розглядати не обов'язково.

2. Підвищені вимоги до режиму ІБ.

У випадках, коли порушення режиму ІБ загрожують важкими наслідками, базовий рівень вимог до режиму ІБ є недостатнім. Для того, щоб сформулювати додаткові вимоги, необхідно: визначити цінність ресурсів; додати до стандартного набору список загроз, актуальних для досліджуваної інформаційної системи; оцінити ймовірності загроз; визначити вразливості ресурсів.

d). Управління ризиками, які пов'язані з порушенням ІБ

Повинна бути розроблена стратегія управління ризиками різних класів. Можливо кілька підходів: 1. *Зменшення ризику*; 2. *Ухилення від ризику*; 3. *Зміна характеру ризику;* 4. *Прийняття ризику*.

1. *Зменшення ризику від порушення ІБ*.

Багато ризиків можуть бути істотно зменшені шляхом використання досить простих і дешевих контрзаходів. Наприклад, грамотне управління паролями знижує ризик несанкціонованого доступу.

2. *Ухилення від ризику*.

Від деяких класів ризиків можна ухилитися. Наприклад, винесення Web-сервера організації за межі локальної мережі дозволяє уникнути ризику несанкціонованого доступу в локальну мережу з боку Web-клієнтів.

3. *Зміна характеру ризику від порушення ІБ.*

Якщо не вдається ухилитися від ризику або ефективно його зменшити, можна прийняти деякі заходи страховки. Приклади: обладнання може бути застраховане від пожежі; можуть бути укладені договори з постачальниками ЗОТ щодо супроводу та компенсації збитку, викликаного позаштатними ситуаціями.

4. *Прийняття ризику*.

Багато ризиків не можуть бути зменшені до нехтовно малої величини. На практиці, після прийняття стандартного набору контрзаходів, ряд ризиків зменшується, але залишається все ще значущим. Необхідно знати залишкову величину ризику.

В результаті підсумком виконання етапу d є стратегія управління ризиками.

е). Вибір контрзаходів, що забезпечують режим ІБ

Повинен бути запропонований комплекс заходів, структурованих за рівнями (організаційному, програмно-технічному) і окремим аспектам безпеки. Запропонований комплекс будується відповідно до обраної стратегії управління ризиками. Якщо проводиться повний варіант аналізу ризиків, для кожного ризику оцінюється ефективність комплексу контрзаходів.

f). Аудит системи управління ІБ

Метою проведення аудиту є перевірка відповідності обраних контрзаходів декларованим у політиці безпеки цілям. В результаті має бути створений документ «Відомість відповідності», в якому міститься аналіз ефективності контрзаходів. Основні розділи цього документа: - межі проведеного аудиту;

- методика оцінки;
- відповідність існуючого режиму ІБ вимогам організації і використовуваним стандартам;
- невідповідності та їх категорії;
- загальні зауваження, висновки, рекомендації.

1.4. Затребуваність комплексного захисту інформації та його зміст

Об'єктивна необхідність постановки проблеми комплексного захисту інформації, в тому числі і в

автоматизованих системах (АС), зумовлена системним характером впливу на її безпеку великої сукупності різних обставин, що мають до того ж різну фізичну природу і різні цільові посилки. Очевидно, що в цих умовах адекватним сучасним потребам і умовам захисту інформації може бути тільки комплексний підхід до вирішення даних проблем.

Нагадаємо раніше дане визначення комплексного захисту. Під комплексним захистом інформації будемо розуміти цілеспрямоване застосування в системах її обробки різних засобів, методів і заходів з метою підтримки заданого рівня захищеності інформації за всією сукупністю показників і умов, які є суттєво важливими з точки зору її безпеки. При цьому саме поняття комплексності є складним і включає в себе, принаймні, наступні аспекти:

- захист за всією сукупністю і показників захищеності інформації та всією сукупністю факторів, що на неї впливають (цільова комплексність);
- безперервний захист інформації протягом усього часу і на всіх етапах життєвого циклу АС (часова комплексність);
- реалізація проблем захисту в загальній сукупності всіх проблем розвитку, побудови та використання АС (концептуальна комплексність).

При цьому часова комплексність передбачає безперервність здійснення заходів щодо захисту інформації та до того ж не тільки в процесі її безпосередньої автоматизованої обробки, але і на всіх інших етапах життєвого циклу АС. Зауважимо, що ця обставина сама собою передбачає організацію і забезпечення цілеспрямованого управління всією сукупністю цих заходів.

Концептуальна комплексність інтерпретується в тому сенсі, що потреби, можливості і умови захисту інформації повинні органічно враховуватися в концепціях побудови та організації функціонування АС, а в більш широкому сенсі – в цілому при вирішенні проблем інформатизації суспільства.

З викладеного випливає, що на систему комплексного захисту інформації покладається [9]:

- забезпечення фізичної цілісності, тобто заданої синтаксичної структури інформації, що захищається;

- забезпечення логічної цілісності, тобто семантичних характеристик інформації та встановлених взаємозв'язків між її елементами;

- забезпечення довіри до інформації в прагматичному плані, тобто попередження її несанкціонованої модифікації навіть при збереженні синтаксичних і семантичних характеристик;

- попередження несанкціонованого отримання інформації, що захищається, особами, які не мають на це спеціальних повноважень, тобто, забезпечення встановленого статусу її конфіденційності;

- попередження несанкціонованого копіювання інформації, оголошеної чиєюсь власністю.

Отже такою, що підлягає захисту, може бути будь-яка інформація, що знаходиться в системі обробки: документи, масиви (бази) даних, алгоритми, програми і т. п., представлені як на машинних, так і на традиційних носіях. При цьому комплексний захист повинен передбачати нейтралізацію негативного впливу на інформацію всіх потенційно можливих ***дестабілізуючих факторів***, а саме:

- ***стихійних лих***, які можуть відбуватися в межах системи обробки або у навколишньому середовищі;

- ***злочинних дій людей***, причому як сторонніх осіб, так і осіб, що входять до складу системи обробки;

- ***побічних явищ***, які можуть мати місце в навколишньому середовищі і при цьому впливати на інформацію, що захищається.

Звісно, що всі задачі, покладені на систему комплексного захисту інформації, повинні реалізовуватися при неухильному дотриманні вимоги щодо забезпечення відповідного рівня її доступності. Інакше найзахищенішою буде та АС, до якої ніхто не має фізичного доступу.

Слід відмітити, що складність висвітлення проблеми безпеки інформації пов'язана з відсутністю до теперішнього часу загальноприйнятого тлумачення термінів, які використовуються для опису даної предметної області за винятком визначення термінів, які у Законі № 2163-VIII «Про основні засади забезпечення кібербезпеки України» від 2018 р. [4] вживаються у такому значенні:

1) **кібератака** – несанкціоновані дії, що здійснюються за допомогою інформаційно-комунікаційних технологій та спрямовані на порушення конфіденційності, цілісності і доступності інформації, яка обробляється в інформаційній (автоматизованій), телекомунікаційній, інформаційно-телекомунікаційній системі, або порушення сталого функціонування такої системи;

2) **кібербезпека** – стан захищеності життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі;

3) **кіберзагроза –** наявні та потенційно можливі явища і чинники, що загрожують кібербезпеці;

4) **кіберзахист** – сукупність заходів організаційного, нормативно-правового, воєнного, оперативного, технічного та іншого характеру, спрямованих на забезпечення кібербезпеки;

5) **кіберзлочин** – суспільно небезпечне винне діяння у кіберпросторі, передбачене законодавством України про кримінальну відповідальність;

6) кіберзлочинність – сукупність кіберзлочинів;

7) **кіберінцидент** – надзвичайна подія, пов'язана з реалізацією або можливістю реалізації кібератаки;

8) **кібероборона** – сукупність політичних, економічних, соціальних, воєнних, наукових, науково-технічних, інформаційних, правових, організаційних та інших заходів, спрямованих на захист інформаційного суверенітету та забезпечення обороноздатності держави у кіберпросторі;

9) **кіберпростір –** середовище, яке виникає в результаті функціонування на основі єдиних принципів і за загальними правилами інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем;

10) **кібертероризм** – терористична діяльність, що провадиться у кіберпросторі або з його використанням;

11) **критична інформаційна інфраструктура** – сукупність об'єктів критичної інформаційної інфраструктури держави;

12) національний сегмент кіберпростору (**кіберпростір України**) – кіберпростір, що належить до юрисдикції України;

13) **об'єкт критичної інформаційної інфраструктури** – інформаційна (автоматизована), телекомунікаційна,

інформаційно-телекомунікаційна система, порушення сталого функціонування якої матиме негативний вплив на стан національної безпеки і оборони України;

14) **суб'єкти забезпечення кібербезпеки** – державні органи, органи

місцевого самоврядування, органи управління Збройних Сил України та інших військових формувань, утворених відповідно до законів України, правоохоронні органи, а також підприємства, установи та організації незалежно від форми власності, які провадять діяльність, пов'язану із забезпеченням безпеки національного сегмента кіберпростору, у тому числі забезпеченням кіберзахисту в рамках надання інформаційних та/або телекомунікаційних послуг;

15) **суб'єкти забезпечення кібербезпеки постійної готовності** – державні органи або їх підрозділи, що входять до складу національної системи кібербезпеки, сили та засоби яких спеціально виділені для перебування у постійній готовності до реагування на кіберзагрози та оперативного виконання завдань забезпечення кібербезпеки.

Крім того, нижче наведені поняття будемо використовувати у загальноприйнятому тлумаченні [9]:

- безпека інформації – стан захищеності інформації, що зберігається і обробляється в автоматизованій системі, від негативного впливу на неї з точки зору порушення її фізичної і логічної цілісності (знищення, спотворення) або несанкціонованого використання;

- загрози безпеки інформації – події або дії, які можуть викликати порушення функціонування автоматизованої системи, пов'язане зі знищенням або несанкціонованим використанням оброблюваної в ній інформації;

- вразливість інформації – можливість виникнення на будь-якому етапі життєвого циклу автоматизованої системи такого її стану, при якому створюються умови для реалізації загроз безпеки інформації;

- захищеність інформації – підтримання на заданому рівні тих параметрів інформації, яка знаходиться в автоматизованій системі, які характеризують встановлений статус її зберігання, обробки та використання;

- захист інформації – процес створення і використання в автоматизованих системах спеціальних механізмів, що підтримують встановлений статус її захищеності;

- комплексний захист інформації – цілеспрямоване регулярне застосування в автоматизованих системах засобів і методів, а також здійснення заходів з метою підтримки заданого рівня захищеності інформації за всією сукупністю показників і умов, які є суттєво важливими з точки зору забезпечення безпеки інформації;

- автоматизована система – організована сукупність засобів, методів і заходів, які використовуються для регулярної обробки інформації в процесі вирішення певного кола прикладних задач;

- початково захищена інформаційна технологія – інформаційна технологія, яка, з одного боку, є уніфікованою в широкому спектрі функціональних додатків, а з іншого, – початково містить всі необхідні механізми для забезпечення необхідного рівня захисту як основного показника якості інформації;

- якість інформації – сукупність властивостей, які обумовлюють придатність інформації задовольняти певні потреби відповідно до її призначення.

1.5. Основи менеджменту господарської життєдіяльності соціуму та об'єктів критичної інфраструктури

Відповідно до загальноприйнятої системи поглядів, оцінок та образних уявлень про світ і місце в ньому людини, тобто відповідно до її світогляду, поняття діяльності (наприклад, господарської) можна озвучити як «діяльність особи, що пов'язана з виробництвом (виготовленням) та/або реалізацією товарів, виконанням робіт, наданням послуг, спрямована на одержання доходу і проводиться такою особою самостійно та/або через свої відокремлені підрозділи, а також через будь-яку іншу особу, що діє в інтересах першої особи, зокрема за договорами комісії, доручення та агентськими договорами» [10]. Згідно з емпіричним досвідом діяльність таких людей однозначно

корелює з їхньою активністю з досягнення поставлених цілей, що визначаються потребами соціуму, де безпосередньо сам об'єкт і процес усвідомленої реалізації прийнято називати **підприємством** (*виробництвом або іншими формами організації виробництва*) та **підприємництвом**, а задіяних людей - **підприємцями**.

Зазвичай для успішної підприємницької діяльності насамперед приділяють увагу адекватній реалізації основних функцій підприємництва, а саме [11]:

- **фінансова** - ведення фінансів й обліку (передбачає мобілізацію необхідного капіталу й управління його використанням і доходами);
- **кадрова** - прийом працівників на роботу, розстановка, навчання, стимулювання працівників, вирішення трудових конфліктів та ін.;
- **матеріально-технічне постачання й інформаційне забезпечення** - придбання обладнання, матеріалів, інформації тощо;
- **виробнича (операційна)** - процес перетворення сировини у продукцію (послуги);
- **маркетингова** - дослідження ринку та управління процесами прасування та збуту продукції (послуг).

Крім основних функцій періодично виконуються додаткові функцій підприємництва:

- ***інноваційна*** - науково-дослідні і проектні роботи щодо розробки нових технологій і нової продукції, розповсюдження ідей і досвіду управління підприємницькою діяльністю;
- ***зв'язки із громадськістю*** (англ. public relations) - управління відносинами між підприємством та громадськими структурами, засобами масової інформації.

Слід зазначити, що багаторічний досвід господарювання різних суб’єктів у країнах із розвиненою ринковою економікою вказує на те, що підприємницька діяльність зазвичай здійснюється за класичною або інноваційною моделлю [11]. При цьому, успішність підприємств під час безпосередньої жизнедіяльності за зазначеними моделями багато в чому залежить як від рівня їхнього **менеджменту,** так і, адекватної сучасним вимогам, реалізації засобів захисту та безпеки об’єктів

підприємницької діяльності у вигляді матеріальних, нематеріальних, людських та фінансових ресурсів, продукції і послуг, більш яких за своїми характеристиками, (відповідно до ст. 55 ГК України [12]), доцільно відносити до **об'єктів критичної інфраструктури (ОКІ).**

Зазначимо, що ще в п. 1.1. «Концептуально-гносеологічні та правові аспекти формування понять з інформаційної безпеки» Розділу 1 вже було озвучено алгоритм "Віднесення об'єктів до критичної інфраструктури" за сукупністю критеріїв, що визначають їхню соціальну, політичну, економічну, екологічну значущість об'єктів для забезпечення оборони країни, безпеки громадян, суспільства, держави і правопорядку, зокрема для реалізації життєво важливих функцій та надання життєво важливих послуг (див. Ст.8, п.2. [5]). Оскільки ж будь-який гіпотетичний об'єкт, залежно від потенційних загроз його штатному функціонуванню, вже на етапах проєктування і створення зобов'язаний відповідати апріорним вимогам безпеки, а в процесі експлуатації (починаючи з контрольних, так званих, «обкаток») послідовно модернізуватися з позицій оптимізації впроваджуваних захисних заходів, то і критично важливі об'єкти (КВО), і їхні інформаційні інфраструктури (ІІ), і навіть безпосередньо та персонал повинні відповідати вимогам з успішного відсікання будь-яких загроз. При цьому збиток від таких загроз, за аналогією з деструктивними наслідками (тіньовими сторонами) соціальної інженерії [13] у вигляді хакерства в ІІ, цілком прогнозовані.

Отже, людський фактор і потенційно залежні від нього заходи з безпеки об'єктів критичної інфраструктури з урахуванням особливостей життєдіяльності їхнього штатного персоналу (досить вельми переконливого трагічного прикладу чорнобильської катастрофи) стають одним із вирішальних чинників у всіх сферах реалізації методів і засобів захисту КВО. Тому, навіть у рамках оптимізації ділової професійної поведінки та етики сучасного соціуму, виникає об'єктивна доцільність розроблення структурно-логічної схеми реалізації штатних заходів (у вигляді кодексу) для конкретних секторів критичної інфраструктури (КІ), в якому має бути викладено чітке формулювання професійно-етичних обов'язків працівників і

алгоритмів їхніх захисних дій за будь-яких режимів функціонування КІ, що й буде озвучено в завершальному розділі цього навчального посібника.

Відтак, рівень сучасної життєдіяльності соціуму на тлі великого різноманіття об'єктів критичної інфраструктури багато в чому вже визначається політикою **управління** останніми, де **менеджмент** потенційно-динамічних ризиків для яких, постійно потребує вчасного нівелювання з метою зниження невизначеності у сфері безпеки та захищеності ОКІ [14].

Нарешті, слід уточнити різницю між поняттями ***управління та менеджмент***, які часто сприймають як синоніми. Згідно з [11, стор.28]: «**управління** дослідники визначають як цілеспрямовану **дію на об'єкт** з метою змінити його поведінку або стан в зв'язку зі змінами певних обставин. Воно як явище об'єктивного світу дуже різноманітне. Характеризуючи оточуюче середовище, дослідники виділяють три основні сфери управління: нежива природа, жива природа й соціальне управління.» Основні форми та рівні управління включають відповідні підвиди (див. рис. 1.4, адаптований згідно [15], с. 30).

Отже сутність поняття «менеджмент» часто розглядають як сукупність функцій і форм управління організаціями, засобів, принципів, методів з метою реалізації конкретних стратегічних планів (див. рис.1.5, адаптований*,[23] з [11], стор.38].

Характерною особливістю менеджменту є зв'язок із конкретними емпіричними дослідженнями організації, психологією та соціологією. З наукової точки зору, менеджмент – це уміння використовувати об'єктивні закони й закономірності, які використовуються в галузі управлінської діяльності. Своєю чергою, у сфері практичної діяльності социума менеджмент розглядає підприємство не тільки як технологічну ланку суспільного виробництва, а й як соціально-виробничу підсистему

*[23] Тут і в наступних аналогічних випадках застосована технічна адаптація тексту, завдяки якій можлива зміна формату, структури або способу подання інформації першоджерела з метою її понятійної доступності. Нагадаємо, що існують різні види адаптації, такі як компресія (скорочення тексту), експлікація (додавання пояснень), сильна, середня і слабка адаптація, які відрізняються ступенем змін у тексті.

ринкових відносин, системно реалізуючи для кожного індивідуального підприємства з конкретної сфери життєдіяльності свої специфічні функції. Фактично, реалізація спеціальних функції менеджменту охоплюють велике різноманіття конкретної управлінської діяльності, в тому числі пов'язані з:

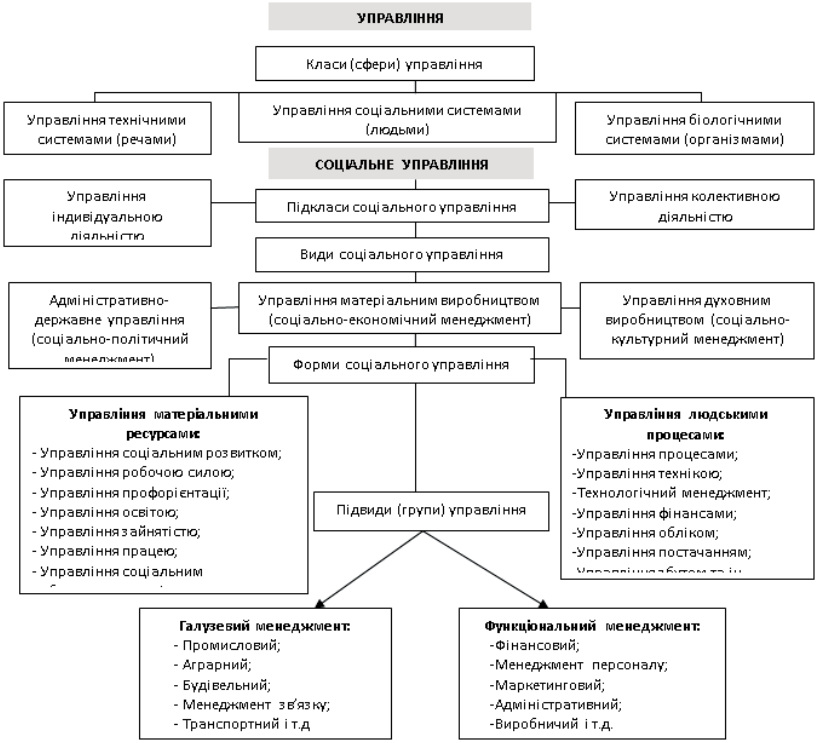

Рис. 1.4. Класифікація (типологія) управління

- управління технічною та технологічною підготовкою виробництва;

- управління економічною підготовкою виробництва;

- оперативне управління виробництвом та трудовими ресурсами;

- управління матеріально-технічною забезпеченням і збутом;

- управління якістю праці і продукції;

- управління маркетингом та зовнішньоекономічними зв'язками;

- управління обліком та фінансовою діяльністю;

- управління капітальним будівництвом і реконструкцією виробництва;

- управління охороною праці і технікою безпеки виробництва.

Це різноманіття конкретної управлінської діяльності, як правило, систематизують і ототожнюють їх у вигляді типових для спеціальних галузей, включно зі сферою виробництва. У результаті «залежно від сфери дії виділяються різні види менеджменту: загальний або адміністративний, галузевий, організаційний, функціональний, підприємницький, міжнародний та інші. Зокрема, можна вести мову про маркетинговий менеджмент, фінансовий, кадровий, виробничий (операційний), транспортний, **ситуаційний**, стратегічний менеджмент тощо» (рис. 1.6, адаптований з [11], стор. 65).

Рис. 1.5. Суть менеджменту

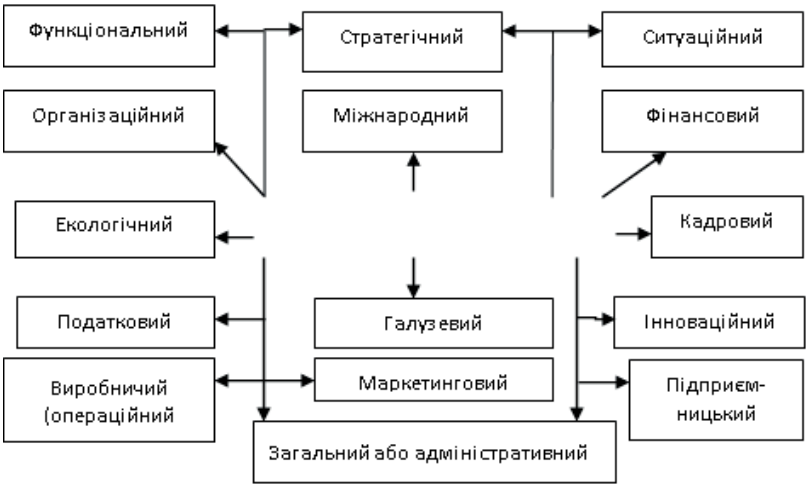

Рис. 1.6. Види менеджменту

На жаль менеджмент ризику штатної життєдіяльності як у сфері безпеки підприємств, включно з ОКІ, так і у сфері захисту буття соціуму, у наведеній типізації рис.1.6, не озвучений. Хоча, крім традиційної наявності керівних інструкцій з охорони праці та техніки безпеки у сфері виробництва, вже навіть існують навчальні посібники в галузі ситуаційного менеджменту, наприклад [16], де викладено сучасну концепцію ситуаційного управління організацією, що функціонує в умовах ринкової економіки, розглянуто методологію та практичне застосування деяких методів управління за проблемними ситуаціями, які складаються в організації на різних етапах її життєвого циклу. При цьому очевидно, що успішність ситуаційного управління підприємством (організацією) багато в чому залежить від методів соціальної інженерії [17-19], які засновані на особливостях психології людей. Зокрема кінцевим результатом цих методів є отримання доступу до конфіденційної інформації, паролів, банківських даних та іншого роду інформації, яка циркулює в системі, що охороняється від стороннього кібернетичного впливу у вигляді ворожої

кібернетичної розвідки з послідующій реалізацій кібернетичних атак або кібернетичного тероризму.

Контрольні запитання до Розділу 1

1. Сформулюйте своє понятійне трактування «інформації» та «повідомлення».
2. У чому відмінність поняття «інформаційна безпека» від терміну «захист інформації»?
3. Яки базові цілі програми Інформаційна безпека (ІБ)?
4. Поясніть основні методи та засоби реалізації ІБ.
5. Що прийнято розуміти під інформаційними інфраструктурами (ІІ) та КВО?
6. Що являє собою Національна система кібербезпеки України?
7. Що прийнято розуміти під інформаційній системою (ІС)?
8. Що таке конфіденційність інформації, цілісність інформації, доступність інформації?
9. Що прийнято розуміти під інформаційними ризиками?
10. У чому відмінності ручних інформаційних систем від автоматизованих (АІС)?
11. Перелічіть основні види АІС залежно від галузі використання та архітектури побудови.
12. Назвіть три основні форми теоретичного аналізу інформації.
13. Які існують основні етапи обігу інформації в АІС?
14. Які існують форми подання інформації в інформаційних системах.
15. Назвіть та поясніть етапи роботи щодо забезпеченню режиму ІБ АІС
16. Перелічіть основні види дестабілізуючих факторів (негативного) впливу на інформацію.
17. Які основні терміни, згідно Закону № 2163-VIII «Про основні засади забезпечення кібербезпеки України», використовують для опису забезпечення безпеки інформації.

18. Перелічіть основні функції підприємництва і сучасні вимоги щодо реалізації засобів захисту та безпеки об'єктів підприємницької діяльності.
19. Уточнити різницю між поняттями управління та менеджмент. Якою є їхня суть.
20. Перелічіть основні форми та рівні управління у сфері підприємницької діяльності.
21. Перелічіть основні форми соціального управління.
22. Назвіть основні види менеджменту.

Список використаних джерел під час підготовки тексту розділу 1

1. Пізнавальні аспекти інформації та її безпеки. О.І.Панченко, П.А.Стеблянко, Ю.С.Тарасенко Збірник матеріалів міжнародної наукової конференції «Інноваційні технології, моделі управління кібербезпекою - «ІТМК-2023», Дніпро, 18–20 квітня 2023 р. С. 11 – 15.
2. Субботін С.О., Олійник А.О., Олійник О.О. Неітеративні, еволюційні та мультиагентні методи синтезу нечітко логічних і нейромережних моделей: Монографія / Під заг. Ред.. С.О.Субботіна. – Запоріжжя: ЗНТУ, 2009. – 375 с.
3. Тарасенко Ю.С. Фізичні основи радіолокації [Текст]: навч. посіб. Т 19 / Ю.С. Тарасенко. – Д.: «Пороги», 2011.– 487с.
4. Закон України «Про основні засади забезпечення кібербезпеки України». Документ 2163-VIII. Відомості Верховної Ради (ВВР). 2017. № 45.
5. Закон України Про критичну інфраструктуру № 1882-IX від 16.11.2021р. Голос України. 2021. № 236
6. Алпеев А.С. Терминология безопасности: кибербезопасность, информационная безопасность. Журнал: «Вопросы кибербезопасности». Выпуск №5 (8) / 2014
7. Ежемесячное приложение к журналу «Стандарты и качество». Экологические аспекты проблем надёжности *и безопасность технических систем. «Основные понятия безопасности». М., 1994 (7).*

8. Клим, В., & Тарасенко, Ю. (2022). Методология построения познавательной модели безопасности критической инфраструктуры. European Science, 1(sge11-01), 38–50. https://doi.org/10.30890/2709-2313.2022-11-01-009. Выпуск № sge11-01 (2022): Перспективные мировые научные тренды ‘2022.
9. А.А.Малюк, С.В.Пазизин, Н.С.Погожин. Введение в защиту информации в автоматизированных системах. _ М.: Горячая линия _ Телеком. 2001. _ 148 с.
10. Податковий Кодекс України. Підпункт 14.1.35 пункту 14.1 статті 14. Визначення понять. https://kodeksy.com.ua/ka/dictionary/h/hozyajstvennaya_deyatel_nost.htm
11. Т.І.Балановська. О.П.Гогуля. А.В.Троян. Основи менеджменту, маркетингу та підприємництва. Навч. посібник. - Київ: ЦП «КОМПРИНТ», 2018. – 518с.
12. Господарський кодекс України. Стаття 55. Поняття суб'єкта господарювання. Докладніше: https://kodeksy.com.ua/gospodars_kij_kodeks_ukraini/statja-55.htm
13. Тарасенко Ю.С., Соляннiков В.Г., Бруй І.І. Тіньові сторони соціальної інженерії. Інноваційні технології, моделі управління кібербезпекою: зб. матеріалів міжнар. наук.-практ. інтернет-конф., м. Дніпро, 14 – 16 квіт. 2021р. Дніпро, 2021р.
14. Ю.С.Тарасенко, В.Ю.Клим, С.В.Гарагатая, В.Г.Солянников. Аспекты безопасности и защищённости критической инфраструктуры. "Innovative technologies, models Cyber Security. Management, ITCSM-2021. Part 2. December 13-15, 2021. Dnipro, Ukraine.. P.12-14.
15. Щекин Г.В. Теория социального управления: Монография / Щекин Г.В. К.: МАУП, 1996. 408 с.
16. Василенко В.О., Шостка В.І. Ситуаційний менеджмент. Навч. посібник. - К.:ЦУЛ, 2003. - 285 с.
17. ИСО/МЭК 17007:2009 «Оценка соответствия. Методические указания по разработке нормативных документов, предназначенных для применения при оценке соответствия» (ISO/IEC 17007:2009 «Conformity assessment — Guidance for drafting normative documents suitable for conformity assessment»).

18. ИСО/МЭК 17000:2004 Оценка соответствия. Словарь и общие принципы (ISO/IEC 17000:2004, Conformity assessment — Vocabulary and general principles).

19. Концептуально-гносеологічні аспекти інформаційної безпеки (захищеності) з позицій соціальної інженерії [Текст] / Ю.С.Тарасенко, Соляннiков В.Г., Калюжний О.Е. // Системи та технології. – 2020. – № 2(60). С. 89-98.

20. Зниження стороннього деструктивного кібернетичного впливу за допомогою соціальної інженерії. / Тарасенко Ю.С. Кузьменко Д.С. // International scientific conference "Innovative technologies, models Cyber Security Management, ITCSM-2020 ANNUAL SCIENTIFIC CONFERENCE ITCSM-2020 Dnipro, Ukraine Book of Abstracts p. 96-98.

2. ОСНОВИ БЕЗПЕКИ ІНФОРМАЦІЙНОГО ПРОСТОРУ, ПОНЯТТЯ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ ТА ПРИНЦИПИ ЇЇ ПОБУДОВИ З ПОЗИЦІЙ СИТУАЦІЙНОГО МЕНЕДЖМЕНТУ

2.1. Структурування аспектів пізнання у сфері інформаційної життєдіяльності соціуму

Нині світовій спільноті у своїй життєдіяльності притаманне прогресивне використання інформаційних і комунікаційних технологій, де в сучасних дослідженнях інтелекту замість понять «увага», «пам'ять», «мислення», які характеризують пізнавальну діяльність людини, використовується термін «когнітивні здібності» *,[24], що фіксуються у психометричних тестах інтелекту, або когнітивні технології (КТ), такі як когнітивний менеджмент чи когнітивний маркетинг. З одного боку, на тлі

*[24] У перекладі з латинської мови «cognitio» означає “пізнання”.

таких технологій і подальшого вдосконалення персональних комп'ютерів з їхньою можливою майбутньою реалізацією на рівні квантових операцій, (останнє доказово підтверджено в системах зв'язку), уже розробляють спеціалізовані функціональні системи з елементами штучного інтелекту. З іншого боку, на жаль, у реаліях наявної політичної моделі устрою світу продовжують радикалізуватися релігійні, анархістські та інші соціальні течії, які є джерелом негативних форм соціального протесту у вигляді терактів, диверсій і навіть призводять до міждержавних конфліктів. Так, наприклад, останні події в Іраку, Лівії, Сирії та інших країнах показують, що стратегія дій учасників, втягнутих у конфлікти на тлі зростаючої кількості нетрадиційних, асиметричних загроз, визначається потенціалом цих країн, де більш слабка сторона обирає шлях асиметричного протиборства, зазвичай, за сценарієм (концепцією) мережево-центричного управління [1]. При цьому, для підтримання господарської стабільності життєдіяльності соціума, когнітивний менеджмент (КМ) [*,25], стосуються способів та алгоритмів реалізації (досягнення) різних цілей людьми, фірмами, політичними організаціями через інструменти пізнання світу, комунікації, оброблення інформації. Причому від самого початку когнітивні технології управління розвивалися у тісному взаємозв'язку з гуманітарними та інформаційними технологіями, використовуючи синергетичний підхід до управління різними господарсько-економічними системами. Отже, найважливіші чинники запровадження когнітивних технологій та КМ – наявність потрібних знань, фінансове та організаційне забезпечення їх поширення у суспільстві, зокрема через когнітивні підсистеми менеджменту та маркетингу підприємств [2] та їхньої безпеки.

[*25] Когнітивний менеджмент – це управління пізнанням, пізнавальними можливостями людини, що застосовуються до конкретного контексту – організаційному та інституційному (т.е. офіційно встановлений, закріплений у своєму суспільному статусі). Когнітивний менеджмент – це менеджмент побудований на знаннях або менеджмент знань, що формується в межах тієї чи іншої соціальної системи.

Таким чином доцільно реалізовувати способи трансформації пізнавальної поведінки людини через покращення їхнього інтелектуального потенціалу, використовуючи сучасні долучення до когнітивних технології навчання, в основі яких, як правило, використовують структурно-лінгвістичні схеми об'єктів пізнання.

В контексті викладеного вище та на підставі наведених у Введенні як структурно-пізнавальної схеми етапів викладення концептуально-методологічних і правових засад КСЗІ ОКІ (див. рис. В.1), так і схеми методології побудови розширеної системи захисту та безпеки об'єктів критичної інфраструктури (див. рис. В.2), реалізованих згідно позицій стандартів України, що мають аналоги в межах ISO щодо оцінювання супутніх ризиків фізичної та інформаційної безпеки, приведена адаптована из [3] структурно-лінгвістична функціональна схема (СЛФС) безпеки інформаційного простору (іносфери) з акцентом на захист інформаційнії життєдіяльністі соціума (див. рис. 2.1).

Ці СЛФС наочно й переконливо окреслюють межі забезпечення інформаційної безпеки соціуму. Зокрема, безпосередній захист і безпека мирної життєдіяльності суспільства реалізується (див. рис. В.1) за допомогою скоординованих дій з керівництва та управління організацією в галузі ризику, оцінювання ризику безпеки сукупності об’єктів критичної інфраструктури (СОКІ) та доступу до неї з позицій зниження результативності ризиків [4]. При цьому, із врахуванням вибору критеріїв ризику та «ступеню реалізації запланованих робіт і досягнення запланованих результатів» (тобто результативності [5, п.3.7.11]) необхідно оптимізувати (розглянути) підсистеми: стандартів України [6 - 9] загального оцінювання ризику, які є аналоги у межах ISO; методів загального оцінювання ризику згідно IEC/ISO 31010 2013 (Додаток В); оцінювання втрат безпеки згідно ДСТУ ISO/IEC 27000:2019 (конфіденційності, цілісності, доступності, спостережності, автентичності, надійності [10] та стійкості

рубежів захисту [11]); фільтрації даних ризиків, згідно ДСТУ ISO/IEC 27001:2013 та підтримки прийняття рішень (ПсППР) доступа до СОКІ [12, Ст.1, п.1, поз.9]. Крім того (див. рис. 2.1), необхідне практичне забезпечення сучасних умов і заходів зі створення технічних (виробничих) та апаратно-обчислювальних комплексів і засобів, адекватних політиці та концепції безпеки інформації під час схеми реалізації відносно різноманітних елементів захисту від несанкціонованого проникнення у корпоративну мережу, витіку інформації по каналам зв'язку, від критичних ресурсів мережі, від несанкціонованого доступу (НСД) до робочих місць і ресурсів та криптографічного захисту інформаційних ресурсів і розмежування потоків інформації між сегментами мережі. При цьому доцільно уточнити, відповідно до рис. 2.1, використовуване понятійне трактування таких термінів як: ***«політика», "концепція"*** та ***"принципи".***

Зокрема, ***«політика»*** (від грец. πολιτικά (politiká) «справи міст») - це сукупність видів діяльності, пов'язаних з ухваленням рішень у групах або іншими формами владних відносин між людьми, такими як розподіл статусу або ресурсів. Вона, як правило, в контексті захисту інформації як системи, включає: правове забезпечення; організаційне забезпечення; апаратне забезпечення; інформаційне забезпечення; програмне забезпечення; математичне забезпечення; лінгвістичне забезпечення та нормативно-методичне забезпечення.

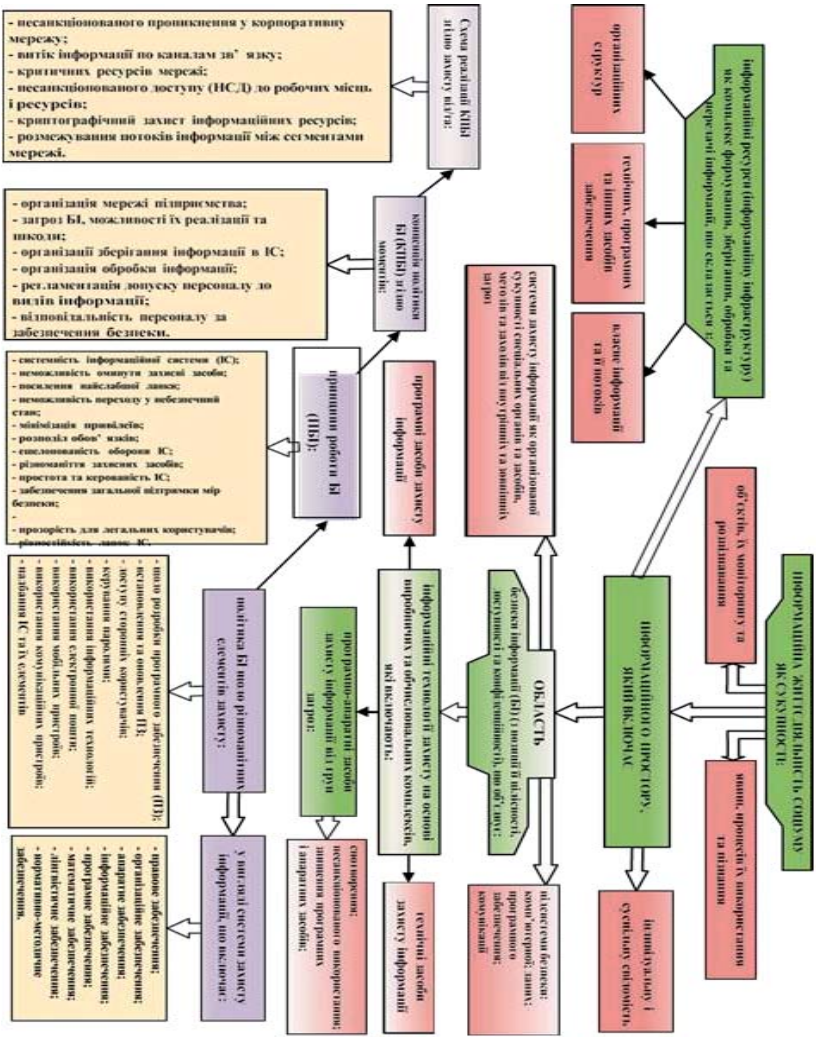

Рис. 2.1. СЛФС безпеки іносфери (інформаційного простору) з акцентом на захист інформаційнії життєдіяльності соціума

Отже, можна стверджувати, що політика БІ щодо різноманітних елементів захисту, - це сукупність видів діяльності щодо:

- розробки програмного забезпечення (ПЗ);
- встановлення та оновлення ПЗ;
- доступу сторонніх користувачів;
- керування паролями;
- використання інформаційних технологій;
- використання електронної пошти;
- використання мобільних пристроїв;
- використання комунікаційних пристроїв;
- надбання ІС та їх елементів та інши.

Своєю чергою **«принцип»** (лат. principium - початок, основа) — це твердження, яке сприймається як головне, важливе, суттєве, неодмінне або, принаймні, бажане. При цьому, згідно рис.2.1, в основу принципів роботи систем та засобів захисту інформації покладено: системність інформаційної системи (ІС); неможливість оминути захисні засоби; посилення найслабшої ланки; неможливість переходу у небезпечний стан; мінімізація привілеїв та розподіл обов'язків; ешелонованість оборони ІС; різноманіття захисних засобів; простота та керованість ІС; забезпечення загальної підтримки мір безпеки; адекватність; прозорість для легальних користувачів; рівностійкість ланок ІС.

Термін **«концéпція»** (від лат. conceptio – осягати, сприймати) – система поглядів, понять про ті чи інші явища або процеси, спосіб їхнього розуміння, тлумачення; основна ідея будь-якої теорії, головний задум; ідея чи план нового, оригінального розуміння; конструктивний принцип технічної та інших видів діяльності. Вона (згідно концепції політики БІ) реалізується відносно моментів:

- організації мережі підприємства;
- загроз БІ, можливості їх реалізації та шкоди;
- організації зберігання інформації в ІС;
- організації обробки інформації;
- регламентації допуску персоналу до видів інформації;
- відповідальності персоналу за забезпечення безпеки.

Отже, наведений вище структурований (за посередництвом рис. 2.1 та рис. В.1 і В.2) матеріал свідчить про подальший напрямок поетапного лекційного викладення основних аспектів пізнання в сучасній сфері інформаційної життєдіяльності соціуму

з позицій менеджменту її безпеки та захисту на рівні нормативних державних і міжнародних стандартів

2.2. Стратегія в області захисту інформації та парадигма інформаційної безпеки: від прийнятного ризику до ефективності інвестицій

Очевидно, що багатогранність життєдіяльності суспільства в різних галузях свого буття поетапно формувалася з присутніми даному соціуму стратегіями і науковими парадигмами. З часом більш гостріше ставало питання «деструктивного впливу» на різного роду інформаційні структури, включаючи телекомунікаційні, структури державного рівня та недержавного сектору, в тому числі і критично важливі об'єкти інфраструктури країни. Такий деструктивний вплив найчастіше пов'язаний із порушенням їх системи безпеки життєдіяльності (СБЖД) на тлі ослаблення (нівелювання) стратегії захисту інформації, а також її технічних та інтелектуальних засобів використання, передавання та накопичення.

Відзначимо, що під ***стратегією*** прийнято розуміти загальну спрямованість в організації відповідної діяльності, що розробляється з урахуванням об'єктивних потреб у даному виді діяльності та оцінкою потенційно можливих умов її здійснення і можливостей подальшої реалізації самого алгоритму організації (вдосконалення) обраної діяльності. Щоб успішно будувати та реалізовувати стратегію в будь-якій обраній сфері діяльності, необхідно мати значний досвід роботи в цій галузі діяльності, адекватно оцінювати будь-які зміни, що впливають безпосередньо на реалізацію стратегії, і вчасно «включати» зворотний зв'язок з метою подальшої її (стратегії) оптимізації.

Завдання стратегії полягає у створенні конкурентної переваги, в усуненні негативного ефекту нестабільності навколишнього середовища, в забезпеченні прибутковості, в урівноваженні зовнішніх вимог і внутрішніх можливостей. Через її призму розглядаються всі ділові ситуації, з якими доводиться стикатися у повсякденному житті.

Здатність будь-якої організації проводити самостійну стратегію у всіх областях робить таку організацію (компанію, підприємство, організацію, фірму і т. п., – в подальшому будемо намагатися використовувати єдиний термін у вигляді «підприємство») більш гнучкою, стійкою, своєчасно дозволяє їй адаптуватися до вимог часу і обставин. Стратегія формується під впливом внутрішнього і зовнішнього середовища, постійно розвивається, бо завжди виникає щось нове, на що потрібно реагувати.

Фактори, які можуть мати для фірми вирішальне значення в майбутньому, називаються стратегічними. Вони (фактори), впливаючи на стратегію любого підприємства, надають їй специфічні властивості. До таких факторів перш за все можна віднести:

- ***організаційні фактори***, серед яких виділяється внутрішня

структура підприємства та її очікувані зміни, система управління, ступінь інтеграції і диференціації внутрішніх процесів;

- ***конкурентні переваги***, якими володіє підприємство у своїй

сфері діяльності в порівнянні з суперниками або до яких воно (підприємство) прагне. Вважається, що конкурентні переваги будь-якого типу мають на стратегію найбільший вплив, забезпечуючи більш високу ефективність використання ресурсів організації;

- ***характер продукції***, що випускається, особливості її збуту,

після продажного обслуговування, ринки та їх межі;

- ***наявні ресурси*** (матеріальні, фінансові, інформаційні,

кадрові та ін.). Чим вони більші, тим масштабніші можуть бути інвестиції в майбутні проекти. Сьогодні для розробки і реалізації стратегії велике значення мають, перш за все, структурні, інформаційні та інтелектуальні ресурси. Порівнюючи значення параметрів наявних і потрібних ресурсів, можна визначити ступінь їх відповідності стратегії;

- ***потенціал розвитку підприємства***, вдосконалення

діяльності, розширення масштабів, зростання ділової активності, інновацій;

- ***культуру, етичні погляди і компетентність керівників***,

рівень їх домагань і підприємливості, здатність до лідерства, внутрішній клімат в колективі, – все, що відображає філософію організації і її призначення.

На стратегічний вибір впливають: ризик, на який готове йти підприємство; досвід реалізації діючих стратегій; позиції власників та наявність часу.

За ступенем регламентованості особливості стратегічних рішень відносяться до контурних, тобто надають широку свободу виконавцям у тактичному відношенні, а за ступенем обов'язковості дотримання головних установок – до директивних.

За функціональним призначенням такі рішення найчастіше бувають організаційними або розпорядчими щодо способу здійснення в певних ситуаціях тих чи інших дій.

З точки зору визначеності, це рішення запрограмовані. Вони приймаються в нових, неординарних обставинах, коли необхідні кроки важко заздалегідь точно розписати.

З точки зору важливості, стратегічні рішення кардинальні, оскільки стосуються основних проблем і напрямків діяльності фірми та визначають основні шляхи розвитку її в цілому, включаючи окремі підрозділи або види діяльності на тривалу перспективу. Вони випливають насамперед із зовнішніх, а не з внутрішніх умов, і повинні враховувати тенденції розвитку ситуації, а також інтереси множини суб'єктів.

Практична незворотність стратегічних рішень обумовлює необхідність їх ретельної та всебічної підготовки і їм властива комплексність.

Стратегія зазвичай являє собою не одне, а сукупність взаємопов'язаних рішень, об'єднаних спільною метою, узгоджених між собою за термінами виконання та ресурсами.

Такі рішення визначають пріоритети і напрямки розвитку підприємства, його потенціалу, ринків, способи реакції на непередбачені події. ***Вироблення стратегічних рішень здійснюється із урахуванням наступних вимог*** [13]:

1. Реальності, яка передбачає відповідність ситуації, цілям, технічному та економічному потенціалу підприємства, досвіду і навичок працівників і менеджерів, культурі, існуючій системі управління;

2. Логічності, зрозумілості, прийнятності для більшості членів організації, внутрішня цілісність, несуперечність окремих елементів, підтримка ними один одного, що породжує синергетичний ефект;

3. Своєчасності (реалізація рішення повинна вчасно нівелювати негативний розвиток ситуації з метою збереження перспектив свого розвитку);

4. Сумісності з середовищем, забезпечуючи можливість взаємодії з ним, оскільки безпосередньо сама стратегія може бути схильна до різних змін середовища в оточенні підприємства;

5. Спрямованості на формування конкурентних переваг;

6. Збереження свободи тактичного маневру;

7. Усунення причин, а не наслідків існуючої проблеми;

8. Чіткого розподілу за рівнями організації роботи з підготовки та прийняття рішень, а також відповідальності за них конкретних осіб;

9. Обліку прихованих і явних, бажаних і небажаних наслідків, які можуть виникнути під час реалізації стратегії або відмови від неї для фірми, її партнерів; від існуючого законодавства, етичної сторони справи, допустимого рівня ризику та ін.

Розробка науково обґрунтованої системи стратегій підприємства як ключової умови її конкурентоспроможності та довгострокового успіху є однією з основних функцій її менеджерів, перш за все вищого рівня. Від них вимагається:

- виділяти, відстежувати і оцінювати ключові проблеми;
- адекватно і оперативно реагувати на зміни всередині і в оточенні організації;
- вибирати оптимальні варіанти дій з урахуванням інтересів основних суб'єктів, причетних до її діяльності;
- створювати сприятливий морально-психологічний клімат, заохочувати підприємницьку і творчу активність низових керівників і персоналу.

Очевидно, що за вихідний момент формування стратегії слід приймати момент постановки глобальних якісних цілей і параметрів діяльності, які організація повинна досягти в майбутньому. В результаті ув'язки цілей і ресурсів формуються альтернативні варіанти розвитку, оцінка яких дозволяє вибрати кращу стратегію.

Цілком зрозуміло, що єдиних рецептів вироблення стратегій не існує. В одному випадку доцільно стратегічне планування (програмування) в іншому – ситуаційний підхід.

Виходячи з великої різноманітності умов, при яких може виникнути необхідність захисту інформації, загальна цільова установка на вирішення стратегічних питань полягала в розробці множини стратегій захисту, і вибір такого мінімального їх набору, який дозволяв би раціонально забезпечувати необхідний захист в будь-яких умовах.

Відповідно до найбільш реальних варіантів поєднань значень розглянутих факторів виділено ***три стратегії захисту*** **[13]:**

- ***оборонна***, де захист від вже відомих загроз здійснюється автономно, тобто без істотного впливу на інформаційно-керуючу систему;
- ***наступальна***, де захист від усієї множини потенційно можливих загроз, при здійсненні якої в архітектурі інформаційно-керуючої системи і технології її функціонування повинні враховуватися умови, продиктовані потребами захисту;
- ***попереджуюча***, де при створенні інформаційного середовища потенційні загрози інформації не мали б підгрунтя (умов) для свого прояву.

Очевидно, що перш ніж пропонувати будь-які рішення щодо організації системи захисту інформації, необхідно аргументовано розробити алгоритми реалізацій конкретних (цілком предметних) методик безпеки, які в кінцевому підсумку утворюють фундамент побудови всієї політики безпеки.

Під політикою безпеки прийнято розуміти сукупність законів, правил і практичних рекомендацій, на основі яких будується управління, захист і перерозподіл інформації з метою її захисту від несанкціонованого доступу. Вона (політика)

повинна охоплювати всі особливості процесу обробки інформації, визначаючи поведінку системи в різних ситуаціях.

Політика безпеки реалізується за допомогою організаційних заходів та програмно-технічних засобів, що визначають архітектуру системи захисту, а також за допомогою засобів управління механізмами захисту.

Для конкретної організації політика безпеки повинна бути індивідуальною, залежною від конкретної технології обробки інформації, використовуваних програмних і технічних засобів, розташування організації і т. д.

Організаційно політика безпеки визначає порядок надання та використання прав доступу користувачів, а також вимоги звітності користувачів за свої дії в питаннях безпеки. При цьому система захисту інформації виявиться ефективною, якщо вона буде надійно підтримувати виконання правил політики безпеки, і навпаки.

Прийнято розрізняти такі **етапи побудови організаційної політики безпеки:**

- це внесення в опис об'єкта структури цінностей;
- це проведення аналізу ризику;
- це визначення правил для будь-якого процесу користування даним видом доступу до ресурсів об'єкта автоматизації, які мають даний ступінь цінності.

Як правило, спочатку складають деталізований опис загальної мети побудови системи безпеки об'єкта, який виражається через сукупність факторів або критеріїв, які уточнюють мету. Причому сукупність факторів є базисом для визначення вимог до системи (так званий, – вибір альтернатив). При цьому фактори безпеки, в свою чергу, можуть поділятися на правові, технологічні, технічні та організаційні.

Розробка політики безпеки організації, як формальної, так і неформальної, – безумовно, нетривіальне завдання. Експерт повинен не тільки володіти відповідними стандартами і добре розбиратися в комплексних підходах щодо забезпечення захисту інформації організації, але і, наприклад, виявляти детективні здібності при виявленні особливостей побудови інформаційної системи та існуючих заходів по організації захисту інформації.

Аналогічна проблема виникає в подальшому при необхідності аналізу відповідності рекомендацій політики безпеки реальному стану речей: необхідно за деяким критерієм відібрати свого роду «контрольні точки» і порівняти їх практичну реалізацію з еталоном, що задається політикою безпеки.

У загальному випадку можна виділити цілий **комплекс заходів**, пов'язаний з розробкою і реалізацією **політики безпеки**, зокрема:

- це заходи з аналізу потенційних ризиків, що включає облік

матеріальних або інформаційних цінностей, і моделювання можливих загроз і їх наслідків для інформаційної системи;

- це заходи з оцінки відповідності мір щодо забезпечення захисту інформації системи деякого еталонному зразку, наприклад, у вигляді стандарту, профілю захисту і т. п..;
- це сукупність дій, пов'язаних з розробкою різного роду

документів, зокрема звітів, діаграм, профілів захисту, визначених у переліку вимог щодо безпеки;

- це дії, що забезпечують збір, зберігання і обробку необхідних даних для подальшої статистичної обробки за апріорними та апостеріорними подіями безпеки конкретної організації.

Очевидно, що для вивчення властивостей обраного способу управління доступом доцільно створювати його формальний опис у вигляді математичної моделі, яка повинна відображати не лише стан всієї системи з її переходами з одного стану в інший, але також враховувати, які стани і переходи можна вважати безпечними в сенсі даного управління. Без цього говорити про які-небудь властивості системи, а тим більше гарантувати їх, щонайменше некоректно.

У даний час найкраще вивчені два види політики безпеки: вибіркова і повноважна, засновані, відповідно, на вибірковому і повноважному способах керування доступом. Крім того, існує набір вимог, що підсилюють дію цих політик і призначений для управління інформаційними потоками в системі. Необхідно відзначити, що засоби захисту, призначені для реалізації будь-якого з названих способів управління доступом, тільки надають

можливості надійного управління доступом або інформаційними потоками.

Основою вибіркової політики безпеки є вибіркове керування доступом, суть якого полягає в тому, що всі суб'єкти і об'єкти системи повинні бути ідентифіковані, а права доступу суб'єкта до об'єкта системи визначаються на підставі деякого правила (властивість вибірковості).

Для опису властивостей вибіркового управління доступом застосовується модель системи на основі матриці доступу, іноді її називають матрицею контролю доступу.

Така модель отримала назву матричної [13]. Матриця доступу являє собою прямокутну матрицю, в якій об'єкту системи відповідає рядок, а суб'єкту – стовпець. На перетині стовпця і рядка матриці вказується тип дозволеного доступу суб'єкта до об'єкта. Зазвичай виділяють такі типи доступу суб'єкта до об'єкта, як «доступ на читання», «доступ на запис», «доступ на виконання» та ін.

Множина об'єктів і типів доступу до них суб'єкта може змінюватися відповідно деяких правил, що існують в даній системі. Визначення і зміна цих правил також є задачею матриці доступу.

Рішення на доступ суб'єкта до об'єкта приймається відповідно до типу доступу, зазначеному у відповідній клітинці матриці доступу. Зазвичай вибіркове управління доступом реалізує принцип «що не дозволено, те заборонено», який передбачає явний дозвіл доступу суб'єкта до об'єкта.

Таким чином, матриця доступу є найбільш простим підходом до моделювання систем доступу і вона є домінуючою у вибірковій політиці безпеки, найбільш широко застосовується в комерційному секторі, так як її реалізація на практиці відповідає вимогам комерційних організацій щодо розмежування доступу і підзвітності, а також має прийнятну вартість і невеликі накладні витрати.

На відміну від вибіркової політики безпеки, основу повноважної політики безпеки складає повноважне управління доступом, що передбачає, що всі суб'єкти і об'єкти системи повинні бути однозначно ідентифіковані. При цьому кожному об'єкту системи привласнена своя мітка критичності, що

визначає цінність інформації, яка міститься в ньому, а кожному суб'єкту системи привласнений рівень прозорості, що визначає максимальне значення мітки критичності об'єктів, до яких суб'єкт має доступ. Коли сукупність міток має однакові значення, кажуть, що вони належать до одного рівня безпеки.

Організація міток має ієрархічну структуру, і, таким чином, у системі можна реалізувати ієрархічно висхідний потік інформації (наприклад, від рядових виконавців до керівництва). Чим важливіше об'єкт чи суб'єкт, тим вище його мітка критичності. Тому найзахищенішими виявляються об'єкти з найвищими значеннями мітки критичності.

Кожен суб'єкт крім рівня прозорості має поточне значення рівня безпеки, яке може змінюватися від деякого мінімального значення до значення його рівня прозорості.

Відтак, успішність реалізації системи інформаційної безпеки ІБ пов'язана з цілісністю, доступністю та конфіденційністю контрольованої інформації і залежить від ефективності інформаційної системи безпеки (ЕІСБ). Своєю чергою, стійкість ЕІСБ зумовлюється оптимальністю вибору видів контролю: логічних засобів управління, за допомогою використання, наприклад, кібер-фізичних систем; адміністративно-організаційних заходів, що забезпечують дотримання штатних процедур, стандартів і принципів, включно з персоналом з його політикою корпоративної безпеки; безпосереднього контролю комп'ютерно-обчислювальних засобів та допоміжного інженерного середовища проживання. При цьому ступінь захисту залежить від повноти перекриття каналів витоку інформації та можливих шляхів обходу засобів захисту, а також від міцності захисту. Під міцністю захисту (перепони) заведено розуміти величину ймовірності його неподолання порушником. Вважають, що міцність захисної перепони є достатньою, якщо очікуваний час подолання її порушником більший за час життя предмета захисту або більший за час виявлення і блокування доступу за відсутності шляхів обходу цієї перепони [14, с.80].

Як видно, ЕІСБ і СБЖД між собою корелюють передусім із позиції оцінки загроз безпеці [15], що кількісно залежить від багатьох, зазвичай змінюваних у часі, чинників технічного характеру впливу та соціально-психологічних механізмів

інформаційного впливу [16, с. 99-142]. Під загрозою безпеці інформації (інформаційною загрозою) заведено розуміти [17, с. 18-32] дію або подію, що може призвести до руйнування, спотворення або несанкціонованого використання інформаційних ресурсів, включно зі збереженою, переданою та оброблюваною інформацією, а також програмними та апаратними засобами. Одним із характерних проявів небезпеки руйнування є ризик, поняття якого не є однозначним, тому що джерелом небезпеки і ризику можуть бути суспільство, навколишнє середовище і техніка разом або кожен із цих факторів окремо. Можлива їх класифікація за фізичним, соціальним або природно-соціальним походженням і розвитком. У такому трактуванні ризик можна ототожнювати і з вчинком, який реалізовано в умовах невизначеності, хоча може бути і результатом пасивності та бездіяльності його творця.

За шкалою ступеня реалізації ризик може бути надмірним, гранично допустимим, припустимим і таким, яким слід знехтувати. На жаль, досягти нульового рівня ризику, тобто рівня абсолютної безпеки, на практиці не вдається.

Лімітуючим у встановленні прийнятного ризику прийнято вважати економічні витрати. Визначальним при цьому є прагнення до мінімізації прогнозованого матеріального збитку за апріорно врахованих загроз інформаційній безпеці. Фактично, під час оцінювання ефективності вкладень в інформаційну безпеку відбувається зіставлення витрат на створення системи захисту інформації (СЗІ) та на можливу компенсацію збитків через її відсутність. У переважній більшості будь-який метод оцінки ефективності інвестицій в ІБ базується на математичних співвідношеннях і логічних викладеннях, коректність застосування яких залежить від істинності обґрунтування. Тому їхня вразливість, як правило, пов'язана з достовірністю вихідних даних, їхньою якістю, подальшим опрацюванням і механізмами інформаційного впливу, в основі якого лежить соціальна інженерія [18, с.7-26].

Відтак, достовірність інформації, необхідна для ухвалення остаточного рішення щодо доцільності інвестицій за планованими варіантами реалізації СЗІ, насамперед, залежатиме від ступеня істинності вихідних даних. І якщо оцінку вразливості

різних систем інформаційної безпеки можна аналітично визначити, то «досі не розв'язано проблему оцінки ефективності реалізації функцій захисту шляхом розв'язання певної задачі захисту» [14, с.28]. Тому потрібне неухильне дотримання типових інструкцій з інформаційної безпеки (ІІБ). Сам же процес модернізації алгоритму ІІБ протягом усього терміну експлуатації СЗІ рідко обходиться без конкретних професійних доопрацювань, які потребують постійних інвестиційних вкладень із серйозним підвищенням ефективності із забезпечення захисту інформації на основі комплексного використання й удосконалення всіх відомих методів із розв'язання цієї проблеми.

Таким чином очевидно, що основне призначення повноважної політики безпеки, – це регулювання доступу суб'єктів системи до об'єктів з різним рівнем критичності і запобігання витоку інформації з верхніх рівнів посадової ієрархії в нижні, використовуючи блокування можливого проникнення з нижніх рівнів у верхні. Фактично повноважна політики безпеки функціонує на тлі вибіркової політики, надаючи її вимогам ієрархічно упорядкований характер (відповідно до рівнів безпеки). При цьому вибір безпосередньої політики безпеки – це прерогатива керівника системи захисту інформації.

2.3. Основи щодо проектування систем захисту інформації та оцінки її ефективності з позицій забезпечення надійності та невизначеності вимірювань

У життєдіяльності сучасного суспільства, схильного до різних впливів, часто далеко недружніми, бажано дуже уважно оцінювати інформацію, що надходить, оскільки вся сукупність інформаційних ресурсів, засобів і систем передачі та обробки інформації, а також засоби їх забезпечення, включаючи приміщення і об'єкти (будівлі, споруди, технічні засоби), в яких ці засоби і системи встановлені, можуть бути вдало або невдало використані відповідно до заданої (аж до ворожої) інформаційної технології. При цьому безпосередньо об'єкт інформатизації визначають як сукупність інформаційних ресурсів, засобів і

систем обробки інформації (використовуваних відповідно до заданої інформаційної технології), а також засобів їх забезпечення, включаючи приміщення і об'єкти (в тому числі будівлі, споруди, технічне обладнання), в яких ці засоби і системи встановлені, або безпосередньо самі приміщення і об'єкти, призначені для ведення конфіденційних переговорів [13].

Слово «сукупність» в даному визначенні вказує на те, що об'єкт інформатизації це єдина інформаційна система, що охоплює в цілому підприємство, установу, організацію і т. п.

У реальному житті всі ці окремі «об'єкти інформатизації», розташовані в межах одного підприємства, являють собою єдиний комплекс об'єктів, пов'язаних спільними цілями, завданнями, структурними відносинами, технологією інформаційного обміну і т. д. При цьому сучасне підприємство, як складне об'єднання великої кількості різнорідних компонентів, призначених для виконання конкретних цілей, у процесі свого функціонування, здатне модифікуватися. Тому, те різноманіття і складність впливу внутрішніх та зовнішніх факторів, які часто не піддаються строгій кількісній оцінці, производять до того, що безпосередньо сама складна інформаційна система часто набуває нових якостей, які не властиві складовим її компонентів. В цьому випадку слід зазначити, що найбільш характерною особливістю подібних інформаційних систем є насамперед наявність впливу людини на кожну зі складових її підсистем.

Дійсно, множина компонентів, що складають об'єкт інформатизації, інтегрально представляються у вигляді сукупності трьох підгруп (систем), що складаються з людей (що входять і утворюють біосоціальну систему), техніки, включаючи технічні системи та приміщення, в яких вони розташовані, і відповідне комп'ютерно-програмне забезпечення, що є інтелектуальним посередником між людиною і технікою (що утворюють інтелектуальну систему).

Сукупність цих трьох підгруп утворює соціотехнічну систему. Із самої назви **«соціотехнічна система»** випливає, що вона утворена з наступних підсистем:

- ***соціальної підсистеми***, включаючи зайнятих в організації службовців (їх знання, вміння, настрій,

ціннісні установки, ставлення до виконуваних функцій), управлінську структуру і систему заохочень;

- ***технічної підсистеми***, включаючи пристрої, інструменти і технології, що перетворюють вхід у вихід тим способом, який покращує економічну ефективність організації.

Якщо аналізувати організацію в ширшому контексті, тоді як фактори повинні додатково враховуватися зв'язки організації з навколишнім середовищем, тобто утворюючи підсистему «середовище». Остання включає соціальні цінності, соціальні і державні інститути, з якими взаємодіє організація, інші організації, які виступають конкурентами або знаходяться в інших відносинах.

Досягти високої ефективності функціонування всієї організації в цілому можливо оптимізуючи її підсистеми і їх взаємодію, тобто гармонізуючи їх роботу. Таке уявлення про соціотехнічні системи є досить об'ємним і може бути поширене на безліч об'єктів. Інформаційні операції і атаки в соціотехнічних системах добре описані [19], а ретроспектива **розвитку засобів захисту інформації** (ЗІ) дозволяє умовно виділити **три періоди**:

а) перший, – відноситься до часу, коли обробка інформації здійснювалася за традиційними (вручну, паперовим) технологіями;

б) другий, – коли обробка інформації на регулярній основі здійснювалася засобами електронної обчислювальної техніки перших поколінь;

в) третій, – коли використання засобів електронно-обчислювальної техніки, реалізованої на рівні персональних комп'ютерів, набрало масового і повсюдного характеру.

З появою сучасної комп'ютерної техніки реалізовані багатопрофільні локальні, глобальні, національні та транснаціональні інформаційні мережі, в яких реалізуються різні канали зв'язку з використанням як просунутих, так і нових стандартів стільникового зв'язку. Так, наприклад, стандарт першого покоління стільникового зв'язку з'явився в 1980-х – тоді сигнали були аналоговими і передавали тільки звук і голоси

абонентів. На якість сигналу сильно впливали завади, через що в 1990-ті ввели 2G – цифровий стандарт, який дозволив передавати не тільки звукові, а й текстові повідомлення, витіснивши пейджери з ринку мобільних пристроїв в першій половині 2000-х. До цього часу з'явилися технології WAP і GPRS*,[26], які дозволили отримувати користувачам зображення, аудіо та відео невеликих розмірів. Паралельно з технологіями передачі мультимедіа для 2G розроблявся стандарт 3G, який відкрив доступ для повноцінного інтернет-серфінгу на мобільних пристроях. 4G дозволив підняти швидкість передачі даних з 2 Мбіт/с до 100 Мбіт/с для рухомих і до 1 Гбіт/с для стаціонарних пристроїв. При розробці LTE*,[27] вдалося налагодити зв'язок так, що телефони двох абонентів знаходяться в одному діапазоні частот, що зменшує втрати трафіку і завади при звичайній розмові.

Якщо раніше сигнал від телефону передавався до базових станцій, контролерів і комутаторів, то в мережах 4G – від підстанцій безпосередньо до комутаторів. Впровадження стандарту 5G реалізує передачу даних з середньою швидкістю 1-2Гбіт/с і максимальною швидкістю до 25Гбіт/с [20]. Слід зауважити, що головна перевага цього формату – не в швидкості, а в багатофункціональності передачі даних. 5G включає в себе кілька форматів зв'язку, які розділять єдиний інформаційний потік на його складові (слайси - від англ. slice, - тонкий зріз, шар).Так, наприклад, один з цих слайсів, призначений для передавання даних мобільним пристроям, інший – для відстеження переміщення людини, ще один – для пристроїв з низьким, але постійним споживанням трафіку.

---

*[26] WAP (англ. Wireless Application Protocol - протокол бездротового доступу) - це засіб отримання доступу до ресурсів інтернету за допомогою тільки мобільного телефону, не вдаючись до допомоги комп'ютера та/або модему.

GPRS (General Packet data Radio Service) - технологія (вид зв'язку), створена для передавання так званих «пакетних» даних мережами стільникового зв'язку.

*[27] LTE (англ. Long-Term Evolution, - «довготривалий розвиток», часто позначається як 4G LTE) - стандарт бездротової високошвидкісної передачі даних в межах 4G.

Зазначені фактори дозволяють реалізувати можливості для так званого «тактильного інтернету» (ТІ) [21], технічні системи якого спрямовані не тільки на аудіовізуальну взаємодію, але і на участь роботизованих систем, які управляються з непомітним для користувача часом затримки. Основна ідея концепції ТІ полягає в тому, що кінцевому користувачеві дається можливість повністю «зануритися» в віртуальний світ, оскільки час затримки, який йде на обробку одного пакета, дуже малий і визначається як 1 мс. При цьому вважається, що цього цілком достатньо для реального «відчуття», так як час реакції людського організму до тактильного подразнення визначається як 0,15-0,8 с. Отже, користувачі не відчують затримку між зображенням на екрані і подією в реальному просторі, що є досить актуальним, наприклад, в хірургії при проведенні дистанційних операцій, або в авіації на етапі зльоту або посадки і т. д. На жаль, дані фактори не залишаються без уваги, особисто при створенні високоефективних систем розвідки з метою отримання інформації про сучасні підприємства або їх спотворення аж до знищення службової інформації.

Отже створення нових і поліпшення класичних методів і засобів інформаційних систем та технологій передачі повідомлень додатково посилюють вимоги щодо реалізації високого рівня потенційної захищеності їх штатних тактико-технічних характеристик. Однак, навіть завжди апріорна надійність працездатності кібер-фізичних систем - Cyber-Physical Systems (CPS - КФС) [22, с.34-38] може бути значно змінена не усвідомленими або свідомими діями (атаками) з боку порушників достовірності та цілісності вихідної інформації. При цьому, адресного впливу, на прикладі автоматизованої системи (АС) з КФС, може бути підданий як персонал, так і комплекс засобів її автоматизації (КСА).

Кібер-фізичні системи - це інтелектуальні системи, що включають в себе інженерно-взаємодіючі мережі фізичних та обчислювальних компонентів, тобто через комп'ютерні мережі і вбудовані контролери забезпечується (автономно або за участю людини) управління фізичними процесами за допомогою реалізації зворотних зв’язків. На даний момент КФС стрімко проникають у всі сфери життєдіяльності людини: при

дослідженні космосу, управлінні транспортом, виробництвом, в енергетичній та військовій сферах, медицині, при побудові сучасної інфраструктури і т.д. Основою розроблення різних моделей кібер-фізичних систем є наявність засобів вимірювання (ЗВ) та їх програмного забезпечення, де ЗВ необхідні для контролю параметрів технологічних процесів та навколишнього середовища. Як правило, КФС є системами з критичною областю застосування (критичними об'єктами). Тому, при проектуванні таких систем висувають підвищені забов`язання до надійності і безпеки ЗВ з метою виконання жорстких вимог з оцінки ризиків кібербезпеки в умовах реалізації **принципу невизначеності** [23] при забезпеченні метрологічної достовірності вимірювань за допомогою цих засобів вимірювання.

Безпосередньо концепція принципу достовірності підтвердження відповідності ЗВ побудована на основі оцінки прийнятних ризиків і аналізу функціонування комбінованої системи підтвердження відповідності в умовах невизначеності, де підсумкові результати вимірів традиційно вимагають наявності їх достовірності, що ототожнюється з їх апостеріорною похибкою. При чому, саме поняття "похибки результату вимірів" корелює з поняттям істинного значення, чого принципово неможливо досягти. Отже, належний метрологічній контроль ЗВ необхідно реалізовувати в умовах невизначеності згідно з міжнародними стандартами, що розробляються відповідно до Директив ISO / МЕК [23].

Проте, досі спостерігається не деяке сприйняття, а часто й протиріччя між традиційним використанням терміну "похибка виміру" і сучасним - "невизначеність виміру", що особливо проявляються при використанні нестандартних засобів вимірювання, які можуть бути і в арсеналі КФС. Фактично з терміном "невизначеність виміру", з'явився цілий напрямок в техніці вимірів, наприклад у радіолокації [24, с. 374], що використовує не стільки нові аналітичні вирази й обчислення, скільки реалізує трансформацію класичного погляду на парадигму вимірювання, обумовлених інтеграційнім процесом міжнародного співтовариства у напрямі гармонізації стандартів и других нормативних документів в області метрології. Саме тому, в ході сучасних подій та явищ безпосередній детальний аналіз

радіоелектронних вимірів (як технічної основи КФС) з позицій їх адекватності, достовірності і надійності дозволяє констатувати, що поняття "невизначеність виміру", за відсутності яких ось нових аналітичних виразів і обчислення, відображає деяку трансформацію накопичення знань і досвіду у сфері необхідних умов вимірів, а як достатня умова реалізації достовірності вимірів, - потрібна апостеріорна оцінка у вигляді деякої (наполягаємо, - імовірнісною) міри (сфери) розсіяння результатів виміру. При цьому, до цих результатів доцільно додавати детальні звіти по калібруванню і методам випробувань, які не заперечують міжнародним і національним стандартам і локальним регулюючим державним актам.

Відтак [25], надійність інформаційної системи з поєднанням засобів радіоелектронних вимірів та їхня адекватність і достовірність відповідності у рамках використання принципу невизначеності можна ототожнювати, як з видачою апостеріорних результатів вимірів, так і з виробленням рішення по приписаних їм похибок в можливих інтервалах їх змін у вигляді деяких мереж (сфер) розходження, що безпосередньо і буде відображати наявність обліку факту невизначеності вимірів. При цьому невизначеність проявів ризиків завжди присутній при будь-якому прийнятті рішень (виборі) з оцінки (недооцінки / переоцінці) важливості інформації і потенційних для неї загроз. Тому ІС, засоби захисту інформації (ЗЗІ) та процес оптимізації їх використання в залежності від співвідношення потенційних загроз і можливостей знищування них підлягають захисту и апріорі потребують серйозних економічних витрат. Величина таких витрат** зазвичай визначається на фоні невизначеності як при розділені інформаційних ресурсів на категорії, так і ЗЗІ по їх цінності при оцінюванні еквівалентної вартості експлуатації самих засобів, не виключаючи заходи щодо запобігання атак на них, наприклад, в процесі використання їх побічних електромагнітних випромінювань і наводок [27].

Таким чином, **сучасне підприємство**, в рамках якого здійснюється захист інформації, ***являє собою складну систему*** зі своїми основними особливостями у вигляді багатофакторної організаційної структури, багатоаспектності функціонування, високого технічного оснащення, широких зв'язків по кооперації,

необхідності розширення доступу до інформації, всезростаючої питомої ваги безпаперової технології обробки інформації, зростаючої питомої ваги автоматизованих процедур у загальному обсязі процесів обробки даних, важливості і відповідальності рішень, прийнятих в автоматизованому режимі, на основі автоматизованої обробки інформації, високої концентрації в автоматизованих системах інформаційних ресурсів, великої територіальної розподіленості компонентів автоматизованих систем, накопичення на технічних носіях величезних обсягів інформації, інтеграції в єдиних базах даних інформації різного призначення і різної приналежності, довготривалого зберігання великих обсягів інформації на машинних носіях, безпосереднього і одночасного доступу до ресурсів (в т. ч. і до інформації) автоматизованих систем великої кількості користувачів різних категорій і різних установ, інтенсивної циркуляції інформації між компонентами автоматизованих систем, в тому числі і віддалених один від одного. При цьому, реалізація індустрії переробки інформації, з одного боку, створює об'єктивні передумови для підвищення рівня продуктивності праці та життєдіяльності людини, а з іншого боку, породжує цілий ряд складних і великомасштабних проблем.

Однією з них є забезпечення збереження і встановленого статусу інформації, що циркулює і обробляється на підприємстві, за допомогою створення **комплексної системи захисту інформації**, до якої, як до системи, висуваються такі **вимоги**:

- вона (система) повинна бути прив'язана до цілей і задач захисту інформації на конкретному підприємстві;
- вона повинна бути цілісною, тобто містити всі її складові і мати структурні зв'язки між компонентами, що забезпечують її узгоджене функціонування;
- вона повинна бути всеохоплюючою, що враховує всі об'єкти і складові їх компоненти захисту, всі обставини і фактори, що впливають на безпеку інформації, і всі види, методи і засоби захисту;
- вона повинна бути достатньою для вирішення поставлених задач і надійною в усіх елементах захисту, тобто базуватися на принципі гарантованого результату;

- вона повинна бути «вмонтованою» в технологічні схеми збору, зберігання, обробки, передачі і використання інформації;
- вона повинна бути логічно, технологічно і економічно обґрунтованою;
- вона повинна бути реалізованою, забезпеченою всіма необхідними ресурсами;
- вона повинна бути простою і зручною в експлуатації і управлінні, а також у використанні законними споживачами;
- вона повинна бути безперервною, досить гнучкою, здатною до цілеспрямованого пристосування при зміні компонентів її складових частин, технології обробки інформації, умов захисту.

Таким чином, забезпечення безпеки інформації - це безперервний процес, який полягає в контролі її захищеності, у виявленні вузьких місць у системі її захисту, в обґрунтуванні та реалізації найбільш раціональних шляхів модернізації та використання прогресивних систем захисту. Причому в сучасних умовах буття належна безпека інформації фактично може бути забезпечена лише за умови комплексного використання всього арсеналу наявних засобів захисту, включно з високопрофесійною підготовкою користувачів і дотриманням ними всіх правил безпеки та захисту інформації, пам'ятаючи при цьому, що жодна система захисту не є абсолютно надійною.

2.4. Поняття комплексної системи захисту інформації та принципи її побудови з позицій ситуаційного менеджменту підвищення рівня захищеності в інформаційно-телекомунікаційних системах

З огляду на вищевикладене, можна стверджувати, що головний напрямок пошуку нових шляхів захисту інформації полягає не просто у створенні відповідних механізмів, а являє собою реалізацію регулярного процесу, здійснюваного на всіх етапах життєвого циклу систем обробки інформації при

комплексному використанні всіх наявних засобів захисту. При цьому всі засоби, методи і заходи, які використовуються для захисту інформації (ЗІ), найбільш раціональним чином об'єднуються в єдиний цілісний механізм, - причому не тільки від зловмисників, але і від некомпетентних або недостатньо підготовлених користувачів і персоналу, а також позаштатних ситуацій технічного характеру.

Основною проблемою реалізації систем захисту є забезпечення надійного захисту безпосередньо самої системи отримання, обробки та зберігання інформації, апріорі виключаючи будь-яке випадкове або навмисне отримання інформації сторонніми особами шляхом обмеження (аж до заборони) доступу до пристроїв і ресурсів інформаційної системи підприємства без винятку для всіх користувачів, адміністрації та обслуговуючого персоналу. З іншого боку, системи захисту не повинні створювати помітних незручностей користувачам в ході їх роботи з ресурсами системи.

Проблема забезпечення бажаного рівня захисту інформації досить складна, що вимагає для свого рішення не просто здійснення деякої сукупності наукових, науково-технічних і організаційних заходів і застосування спеціальних засобів і методів, а й створення цілісної системи організаційно-технологічних заходів і застосування комплексу спеціальних засобів і методів по ЗІ.

На основі теоретичних досліджень і практичних робіт в області ЗІ сформульований системно-концептуальний підхід щодо захисту інформації [13]. Концептуальний підхід спрямований на розробку єдиної політики впровадження науково-обґрунтованих поглядів, положень і рішень, необхідних і достатніх для оптимальної організації та забезпечення надійності захисту інформації, а також цілеспрямованої організації всіх робіт по ЗІ. Системний підхід включає аспекти цільової системності, в якій захищеність інформації розглядається як основна частина загального поняття якості інформації; просторової системності, що пропонує рішення всіх питань захисту у всіх структурах і підрозділах підприємства; тимчасової системності, що забезпечує безперервність роботи по ЗІ, що здійснюються відповідно до регламенту і стратегії

підприємства, і організаційної системності, націленої на єдність організації та управління всіх робіт по ЗІ.

Комплексний (системний - див. Введення) підхід до побудови будь-якої системи передбачає вивчення об'єкта впроваджуваної системи, оцінку загроз безпеки об'єкта, аналіз засобів, необхідних для побудови системи, оцінку економічної доцільності, безпосереднього вивчення самої системи, її властивостей, принципів роботи та можливості збільшення її ефективності, співвідношення всіх внутрішніх і зовнішніх факторів, а також можливості додаткових змін в процесі побудови системи з повною організацією всього процесу від початку до кінця.

Комплексний (системний) підхід – це принцип розгляду проекту, при якому аналізується система в цілому, а не її окремі частини. Його задачею є оптимізація всієї системи в сукупності, а не поліпшення ефективності окремих частин. Це пояснюється тим, що, як показує практика, поліпшення одних параметрів часто призводить до погіршення інших, тому необхідно намагатися забезпечити баланс протиріч вимог і характеристик.

Комплексний (системний) підхід не рекомендує приступати до створення системи до тих пір, поки не визначені такі компоненти як:

- вхідні елементи, тобто ті елементи, для обробки яких створюється безпосередньо сама система і де в якості вхідних елементів відображають види загроз безпеки, можливі на даному об'єкті;
- ресурси, тобто ті засоби, які забезпечують створення та функціонування системи (наприклад, матеріальні витрати, енергоспоживання, і тощо);
- параметри навколишнього середовища, оскільки будь-яка реальна система завжди взаємодіє з іншими системами, кожен об'єкт пов'язаний з іншими об'єктами. При цьому дуже важливо встановити межі області інших систем, що не залежать від сфери відповідальності розглянутого підприємства. Причому характерним прикладом важливості вирішення цього завдання є розподіл функцій по захисту інформації, яка передана сигналами по лініях зв'язку, що проходять по територіях різних об'єктів. Як би

не встановлювалися межі системи, не можна ігнорувати її взаємодію з навколишнім середовищем, бо в цьому випадку прийняті рішення можуть виявитися марними. Це справедливо як для меж об'єкта, що захищається, так і для меж системи захисту;

- цільове призначення і/або функції, тобто для кожної системи повинна бути сформульована мета або її функціональне призначення, до якої вона (ця система) прагне. Чим точніше і конкретніше вказано призначення або перераховані функції системи, тим швидше і правильніше можна вибрати кращий варіант її побудови. Так, наприклад, мета, сформульована в найзагальнішому вигляді як забезпечення безпеки об'єкта, змусить розглядати варіанти створення глобальної системи захисту. Якщо уточнити її, визначивши, наприклад, як забезпечення безпеки інформації, що передається по каналах зв'язку всередині будівлі, то коло можливих рішень істотно звузиться. Слід мати на увазі, що, як правило, глобальна мета досягається через досягнення множини менш загальних локальних цілей (підцілей). Побудова такого «дерева цілей» значно полегшує, прискорює і здешевлює процес створення системи;

− критерії ефективності, за якими оптимізують напрямки побудови системи, що

забезпечує задані цілі функціонування, використовуючи критерії ефективності як інструмент порівняння.. Такий інструмент повинен: характеризувати якість реалізації заданих функцій; враховувати витрати ресурсів, необхідних для виконання функціонального призначення системи; мати ясний і однозначний фізичний зміст; бути пов'язаним з основними характеристиками системи і допускати кількісну оцінку на всіх етапах створення системи.

Тому***, цілі успішного захисту службової інформації*** (як правило, в умовах жорсткого дефіциту часу та різноманіття потенційних, як внутрішніх так і зовнішніх різного роду загроз та інформаційних атак) на підприємстві, складність його структури, а також часто негативної участі людини в технологічному процесі обробки інформації, ***можуть бути досягнуті тільки***

шляхом створення сучасних надійних **засобів захисту інформації** (ЗЗІ) реализуя комплексный подход в виде безпрерывного циклу последовательности этапов:

1) визначення інформації, що підлягає захисту; 2) проведення оцінки вразлівості та ризиків інформації за наявною множиною загроз та каналів витоку; 3) виявлення множини потенційно можливих загроз, каналів витоку інформації та визначення вимог до системи захисту; 4) здійснення вибору засобів захисту інформації та їх характеристик; 5) впровадження та організація використання вибраних заходів, способів та засобів захисту; 6) здійснення контролю цілісності та управління системою захисту.

Кожному етапу в процесі свого напрацювання надано можливість брати участь в уточненні вимог щодо модернізації ЗЗІ в рамках отримання синергетичного ефекту у сфері логістики, менеджменту та підвищення конкурентоспроможності підприємств та компаній різного профілю діяльності.

Як уже було зазначено у Введенні, саме «з позицій позитивного синергетичного ефекту у сфері менеджменту підприємництва (наприклад, при диверсифікації, створенні концернів, кооперації тощо) не слід нехтувати безпекою сучасної інформаційної форми синергії, яка, залежно від його (підприємства) ресурсів, що підлягають інтеграції, є особливо актуальною, наприклад, для об'єктів критичної інфраструктури (ОКІ) з комплексної системою захисту інформації (КСЗІ). При цьому, на таких об'єктів реалізація системи управління з новітніми інформаційними технології, навіть за наявністю власної критичної інформаційної інфраструктури (КІІ), не може формуватися відірвано від внутрішніх та зовнішніх чинників впливу на штатний режим їх життєдіяльності», де процеси інформаційної підтримки прийняття рішень відображені на рис.2.2 (адаптовано згідно [28], с.23) з використанням інформаційно-телекомунікаційної системи (ІТС)

Таким чином, системи захисту інформації – це організована сукупність об’єктів і суб’єктів ЗІ, що забезпечує реалізацію способів і методів, здійснюваних засобами захисних заходів для вирішення завдань безпеки сучасних інформаційних технологій. При цьому компоненти ЗІ, з одного боку, є складовою частиною

системи, а з іншого – самі організовують систему, здійснюючи захисні заходи. Оскільки система може бути визначена як сукупність взаємопов'язаних елементів, то призначення ЗЗІ полягає в тому, щоб об'єднати всі складові захисту в єдине ціле, в якому кожен компонент, виконуючи свою функцію, одночасно забезпечує виконання функцій іншими компонентами і пов'язаний з ними логічно і технологічно шляхом отримання синергетичного ефекту.

Рис. 2.2. СЛФС процесів інформаційної підтримки прийняття рішень з використанням ІТС

Слід мати на увазі, що працездатність, а, отже, і надійність захисту інформації прямо пропорційна системності та її комплексності, так як при неузгодженості між собою окремих складових частота «відмов» в технології захисту збільшується. При цьому необхідність комплексності рішень полягає перш за все в об'єднанні в єдине ціле локальних (правових, організаційних, інженерно-технічних і т. п.) ЗЗІ з оптимально корельованими логічними і технологічними всіх реалізованих складових захисту.

Звідси якість і надійність захисту залежать не тільки від видів складових системи, але і від їх повноти, яка забезпечується при врахуванні всіх факторів і обставин, що впливають на захист. Саме повнота всіх складових системи захисту, що базується на аналізі таких факторів і обставин, є другим призначенням комплексності.

Зокрема, в 21 сторіччі, де електронно-цифрові прилади стали невід'ємною частинною нашого життя, дуже гостро ставиться питання інформаційної безпеки в частині нівелювання наслідків різного, як внутрішніх так і зовнішніх, роду атак. Такі атаки (наприклад, так звані «атаки по стороннім каналам зв'язку»), спрямовані на ураження цифрових пристроїв. Атака по стороннім каналах використовує інформацію в виді фізичних процеси в пристрої, які не розглядаються в теоретичному описі. Подібного роду атаки мають фізичний вплив на електронно-цифрові пристрої і мережі, що зв'язують їх. Атака по електромагнітному випромінюванню може бути віднесена як пасивна атака, де електронні шифрувальні пристрої випромінюють електромагнітне випромінювання під час своєї роботи. Пов'язуючи певні спектральні компоненти цього випромінювання з операціями виконуваними в пристрої, можна отримати достатньо інформації для визначення секретного ключа або самої оброблюваної інформації. Крім того, не варто забувати про електромагнітні перешкоди – небажане фізичне явище або вплив електричних, магнітних або електромагнітних полів, електричних струмів або напруги зовнішнього або внутрішнього джерела, яке порушує нормальну роботу технічних засобів, або викликає погіршення технічних характеристик та їхні параметри [29].

Для запобігання подібного роду атак, можливе використання класичного екранування як корпусу самого електронно-цифрового пристрою, в нашому випадку це персональний комп'ютер (ПК) чи сервер. Це (екранування) суттєво зменшить вірогідність ризику стосовно шкідливого впливу атак, тобто екранування є

ефективним способом боротьбі з побічними електромагнітними випромінюванні і наводками (ПЕВН).

На жаль, заходи по використанню екранування самого електронно цифрового пристрою (ПК чи сервера, а також самого приміщення, де вони розташовані) можуть бути недостатніми з точки зору необхідного рівня захисту. В цьому випадку можуть бути використана технологія безехових камер (БЕК), де замість звичного корпусу, ми розмішуймо всі комп'ютерні комплектуючи в так званий «модернізований корпус»,

розроблений по принципам безехових камер. Також можливо оснащувати серверні приміщення такими камерами, для запобігання шкідливого впливу і витоку інформації.

Найпростішою радіочастотної камерою є звичайна екранована камера, виконана за принципом клітки Фарадея. Вона являє собою якесь замкнуте обсяг з модульних конструкцій, (в попередні роки камери були зварними), який дозволяє захищати секретну інформацію щодо радіочастотного каналу. Основним призначенням таких конструкцій є фільтрація і виключення неналежних перешкод по мережі живлення. Радіосигнал не може піти з екранованої камери і потрапити всередину неї.

Подібні технології можна використовувати, як для захисту електронно-цифрових приладів від зовнішніх атак, так і для захисту від внутрішнього і зовнішнього прослуховування. В якості прикладу, запропоновано використовувати рупоробразну безехову камеру (БЕК), стінки якої є основним джерелом паразитних відбитів покрита радіопоглинаючим матеріалом (РПМ) (наприклад типу В2-Ф3 з коефіцієнтом відбиття по потужності Кп = 0,05 (-13 дБ) з підставою в виді фольгованого склопластику. Крім того такий РПМ забезпечує, екранування. В цьому випадку [24] при λ =4,3см коефіцієнт безеховості (КБЕ) камери склав -47дБ, а при λ =3см відповідно -50дБ. В інших точках робочого діапазону КБЕ був не гірше -35 дБ. Таким чином БЕК забезпечує певне середовище, в якій можна бути впевненим що інформація не буде перехвачено.

Таким чином можна зробити висновок, що екранування електронно-цифрових пристроїв (в тому числі ПК) є невід'ємним атрибутом інформаційної безпеки в цілом, а використання технологій безехових камер значно підвищує рівень інформаційної безпеки. Тим не менш повинні враховуватися всі інтегральні параметри уразливості інформації та потенційно можливі загрози її безпеки, охоплюватися всі необхідні об'єкти захисту, використовуватися всі можливі види, методи і засоби захисту, забезпечуючи захист штатних співробітників та здійснюватися усі, виходячи з цілей і завдань захисту, заходи. По-третє, тільки при комплексному підході система при будь-яких обставинах може забезпечувати безпеку всієї сукупності інформації, що підлягає захисту. Це означає, що повинні

захищатися всі носії інформації, у всіх компонентах її збору, зберігання, передачі і використання, в будьякий час і при всіх режимах функціонування систем обробки інформації. У той же час комплексність не виключає, а, навпаки, передбачає диференційований підхід до захисту інформації, в залежності від: складу її носіїв; видів таємниці, до яких віднесена інформація та ступеня її конфіденційності; засобів зберігання і обробки; форм і умови прояву уразливості та каналів і методів несанкціонованого доступу до інформації.

Таким чином, значимість комплексного підходу щодо захисту інформації полягає: в інтеграції локальних систем захисту; в забезпеченні повноти всіх складових системи захисту; в забезпеченні всеосяжності захисту інформації.

Виходячи з цього, можна стверджувати, що комплексна система захисту інформації – це така система, яка повно і всебічно охоплює всі предмети, процеси і фактори людського буття з метою безпечного отримання, обробки, використання і зберігання всієї інформації, що вимагає захисту.

При побудові будь-якої комплексної системи захисту інформації необхідно заздалегідь обумовлювати принципи її побудови. Як правило, КСЗІ – це складна система, яка функціонує ***в умовах невизначеності*** у сфері ***ситуаційного менеджменту*** (див. рис.2.3) та вимагає значних матеріальних витрат.

Зокрема, поняття ***невизначеності*** широко використовується в галузях освіти, науки, техніки та інших сферах життєдіяльності соціуму. Так, для забезпеченні метрологічної достовірності вимірювань за допомогою штатніх засобів вимірювання предусмотрені даже нормативніе мировіе стандарті в виде ISO/IEC Guide 98-1:2009 [23]. В квантовой физике используют ***принцип невизначеності*** Гейзенберга [30], в виде фундаментальной концепции, яка стверджує, що неможливо одночасно знати точне положення та імпульс елементарної частинки, що виникає через частинково-хвильовий дуалізм таких частинок у квантовій механіці. Це означає, що елементарні частинки можуть поводитися і як хвилі, і як частинки залежно від обставин. При цьому, одним із ключових наслідків цього

принципу невизначеності, є обмеження того, наскільки точно ми можемо виміряти властивості таких елементарних частинок.

Також зазначимо, що ***ситуаційний менеджмент*** [31] в процесі прийняття управлінських рішень в умовах глобалізації, цифрових технологій, економічних криз та деструктивних інформаційних війн - це в даний час є чи не єдиним підходом, який адекватно базується на здатності приймати управлінські рішення на основі конкретних обставин і контексту кожної ситуації. Він (ситуаційний менеджмент) являє собою підхід що дозволяє керівникам реагувати на динамічні зміни, швидко аналізувати ситуацію та приймати відповідні рішення в умовах інтенсивного розвитку технологій та наростання мало передбачуваних загроз життєдіяльності соціуму. Так, завдяки гнучкості ситуаційного менеджменту керівництво різних підрозділів та підприємств має змогу швидко приймати рішення, які відповідають поточним умовам, наприклад у бізнес-середовища або у процесі мережоцентричних війн, на основі реалізації його концептуальної моделі (рис. 2.3). Причому принципи ситуаційного підходу, такі як аналіз і класифікація управлінських ситуацій (див.п.7.1), а також використання релевантних методів для їх оцінки, відіграють важливу роль у підвищенні як безпеки, так и конкурентоспроможності підприємств.

Упевнено можна стверджувати, що ключовими факторами успішного застосування ***ситуаційного менеджменту*** в динамічному середовищі є гнучкість, інноваційність та адаптивність управлінських рішень в кризових умовах.

Тому якісне початкове визначення рівня (оцінки) основних принципів побудови КСЗІ завжди є актуальним і потребує професійної реалізації, акцентуючи увагу:

1) на принципі законності, який полягає у відповідності вжитих заходів згідно законодавства країни про захист інформації, а в разі відсутності відповідних законів – іншим державним нормативним документам щодо захисту;

2) на принципі повноти інформації, що захищається, де захисту підлягає не тільки інформація, яка становить державну, комерційну або службову таємницю, а й та частина несекретної інформації, втрата якої може завдати шкоди її власнику.

Реалізація цього принципу дозволяє забезпечити і охорону інтелектуальної власності;

3) на принципі обґрунтованості захисту інформації, який полягає у встановленні шляхом експертної оцінки доцільності засекречування та захисту тієї чи іншої інформації, ймовірних економічних та інших наслідків такого захисту виходячи з балансу життєво важливих інтересів держави, суспільства і громадян. Це, в свою чергу, дозволяє витрачати засоби на захист тільки тієї інформації, втрата або витік якої може завдати дійсну шкоду її власнику;

4) на принципі створення спеціалізованих підрозділів по захисту інформації, які є невід'ємною умовою організації комплексного захисту, оскільки тільки спеціалізовані служби здатні належним чином розробляти і впроваджувати захисні заходи і здійснювати контроль за їх виконанням;

5) на принципі участі в захисті інформації всіх дотичних з нею осіб, тому що захист інформації є службовим обов'язком кожної особи, що має за родом виконуваної роботи відношення до інформації, що захищається, і така участь дає можливість підвищити якість захисту

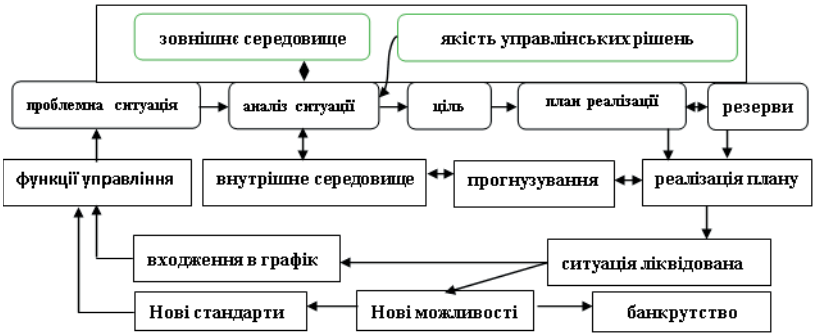

Рис. 2.3. Концептуальна модель ситуаційного менеджменту–адаптована з [31]

5) на принципі участі в захисті інформації всіх дотичних з нею осіб, тому що захист інформації є службовим обов'язком кожної особи, що має за родом виконуваної роботи відношення

до інформації, що захищається, і така участь дає можливість підвищити якість захисту.

6) на принципі персональної відповідальності за захист інформації, який вимагає, щоб кожна особа персонально відповідала за збереження і нерозголошення довіреної йому інформації, що захищається, а за втрату або поширення такої інформації вона несе кримінальну, адміністративну або іншу відповідальність.

7) на принципі наявності і використання всіх необхідних правил і засобів, в результаті чого КСЗІ вимагає, з одного боку, участі в ній керівництва підприємства і спеціальної служби захисту інформації та всіх виконавців, які працюють з інформацією, яка захищається, з іншого боку, використання різних організаційних форм і методів захисту, а з третього боку, наявність необхідних матеріально-технічних ресурсів, включаючи технічні засоби захисту.

8) на принципі превентивності вжитих заходів щодо захисту інформації, в якому передбачається апріорне випереджаюче завчасне вжиття заходів щодо захисту до початку розробки або отримання інформації. З цього принципу випливає, зокрема, необхідність розробки захищених інформаційних технологій.

Слід звернути увагу на те, що серед розглянутих принципів навряд чи можна виділити більш, або менш важливі, тому доцільно при побудові КСЗІ використовувати їх в сукупності як складових, що реалізують ***синергетичний ефект.***

Контрольні запитання до Розділу 2

1. Що прийнято розуміти під когнітивними технологіями (КТ), когнітивним менеджментом і когнітивним маркетингом?
2. Що таке результативність з позицій зниження інформаційних ризиків?
3. Дайте понятійне трактування таких термінів як: «політика», “концепція” та “принципи” відносно різноманітних систем та засобів захисту інформації.

4. Що прийнято розуміти під стратегією у створенні конкурентної переваги інформаційної безпеки?
5. Які основні фактори впливают на стратегію
6. Які основні чинники (фактори) впливають на стратегію будь-якого підприємства та надають йому специфічних властивостей?
7. Назвіть три основні стратегії захисту від відомих та можливих загроз на інформаційно-керуючу систему.
8. Перелічіть основні етапи побудови організаційної політики безпеки.
9. Поясніть, будь ласка, основне призначення повноважної політики безпеки підприємства (організації) або об'єкта критичної інфраструктури.
10. Що прийнято розуміти під соціотехнічною системою і з яких підсистем вона утворена?
11. Що прийнято розуміти під технологіями WAP та GPRS?
12. Що таке «тактильний інтернет» (TI) та що прийнято розуміти під стандартом LTE?
13. Що таке кібер-фізичні системи?
14. Що прийнято розуміти під принципом невизначеності під час забезпечення метрологічної достовірності вимірювань за допомогою засобів вимірювання?
15. Які основні вимоги щодо створення комплексної системи захисту інформації?
16. Поясніть, будь ласка, що таке системно-концептуальний підхід щодо захисту інформації?
17. Сфера ситуаційного менеджменту – що це?
18. Якіх основних принципів слід дотримуватися під час реалізації ситуаційного менеджменту?
19. Що таке принципі персональної відповідальності при застосуванні ситуаційного менеджменту?
20. Що прийнято розуміти під синергетичним ефектом.

Список використаних джерел під час підготовки тексту розділу 2

1. Панов М., Маневич В. Військові конфлікти межі 2030 року // Зарубіжний військовий огляд. 2008. № 1. С. 3-15.

2. Хром'як Й.Я., Слюсарчук Ю.М., Цимбал Л.Л., Цимбал В.М. Когнітивні технології та їх особливості у менеджменті й маркетингу // Вісник Національного університету „Львівська політехніка" Менеджмент та підприємництво в Україні: етапи становлення і проблеми розвитку. – № 739 (2012). – С.233–238.

3. Ю.С.Тарасенко, П.А.Стеблянко, Н.І.Максимчук Структурування аспектів пізнання. International conference mathematic problems of the technical mechanicannual scientific conference МРТМ 2024, (18-19 квітня 2024). Dnipro, Ukraine – 2024. С.120-123.

4. Тарасенко Ю.С. Ризик-орієнтовані процеси забезпечення безпеки об'єктів критичної інфраструктури //Ю.С.Тарасенко, Ю.В.Савченко// Системи та технології №1 (65), 2023. с.67-76.

5. ДСТУ ISO 9000:2015 (ISO 9000: 2015, IDT) Системи управління якістю. Основні положення та словник термінів. Київ ДП «УкрНДНЦ», 2016. 51 с.

6. ДСТУ ISO Guide 73:2013. Керування ризиком. Словник термінів (ISO Guide 73:2009, IDT). [Чинний від 2014–07–01]. Вид. офіц. Київ: Мінекономрозвитку України, 2014. 17с

7.. ДСТУ IEC/ISO 31010:2013 Керування ризиком. Методи загального оцінювання ризику (IEC/ISO 31010:2009, IDT). [Чинний від 2014–07–01]. Вид. офіц. Київ: Мінекономрозвитку України, 2015. 80 с.

8. ДСТУ ISO 31000:2018 Менеджмент ризиків. Принципи та настанови (ISO 31000:2018 Risk Management –

Principles and guidelines on implementation, IDT). [Чинний від 2019–01–01].

9. ДСТУ ISO/TR 31004:2013 Управління ризиками – Керівництво з впровадження ISO 31000 (Risk management – Guidance for the implementation of ISO 31000, IDT). [Чинний від 2019–01–01].

10. ДСТУ ISO/IEC 27000:2019 (ISO/IEC 27000:2018, IDT) Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Огляд і словник термінів. Київ ДП «УкрНДНЦ». Наказ від 16.10.2019 № 312.

11. ISO/IEC 27001:2013 Інформаційні технології - Методи забезпечення безпеки - Системи менеджменту інформаційної безпеки - Вимоги /Information technology — Security techniques — Information security management systems —Requirements/ Вторая редакція. 2013-10-01.

12. Закон України Про критичну інфраструктуру № 1882 - IX від 16.11.2021р. // Голос України. . – № 236 (14.12.2021).

13. Інформаційна безпека підприємства: Навчальний посібник / Н.В. Гришина. - 2-е изд., доп. - М.: Форум: НИЦ ИНФРА-М, 2015. – 240 с.

14. Вострецова Е. В. Основи інформаційної безпеки: навчальний посібник для студентів вузів/Є. В. Вострецова. - Єкатеринбург: Вид-во Урал. ун-ту, 2019. — 204 с.

15. Тарасенко Ю.С., Соляннiков В.Г., Бруй І.І. Paradigm of information security: from acceptable risk to efficiency of investment Матеріали міжнародної науково-практичної інтернет-конференції «Інноваційні рішення в економіці, бізнесі, суспільних комунікаціях та міжнародних відносинах» Секц. «Спрямування розвитку сучасних інноваційних технологій у сфері комп'ютерних наук та кібербезпеки» Дніпро 16 квітня 2021 р. С. 422-423.

16. Плющ А. Н. Соціально-психологічні механізми інформаційного впливу: монографія / А. Н. Плющ. - Ніжин: «Видавництво «Аспект-Поліграф», 2017. — 244 с.

17. Ясенев В.Н. Інформаційна безпека в економічних системах: навчально-методичний посібник/В.М. Ясенів. - Нижній Новгород. Вид-во «Нижегородський державний університет ім. Н.І. Лобачевського». 2017. 254с.

18. Кузнєцов, М. В. Соціальна інженерія та соціальні хакери / М. В. Кузнєцов, І. В. Симдянов. - СПб.: БХВ-Петербург, 2007. — 368 с.:

19. Волобуєв С. В. Безпека соціотехнічних систем. Обнінськ. Видавець: Вікінг. 2012. – 340 с.

20. І. Шахнович. Системи бездротового зв'язку 5G: телекомунікаційна парадигма, що змінить світ. Короткі тези. // ЕЛЕКТРОНІКА: НТБ. 2015. №7. С. 48-55.

21. Ястребова А. А., Виборнова А. І., Киричек Р. В. Огляд концепції тактильного інтернету та технологій для його реалізації // Інформаційні технології та телекомунікації. 2016. Том 4. № 4. С. 89-96

22. Кіберфізичні системи та їх програмне забезпечення / Ван Чунжі, С. П. Яцишин, О. В. Лиса, А.-В. В. Мідик // Вимірювальна техніка та метрологія: міжвідомчий науково-технічний збірник. — Львів: Видавництво Львівської політехніки, 2018. Том 79. № 1. С. 34–38.

23. ISO/IEC Guide 98-1:2009, Uncertainty of measurement - Part 1: Introduction to the expression of uncertainty in measurement, IDT. Невизначеність виміру. Частина 1. Введення в посібники з виразу невизначеності виміру. М. Стандартінформ. 2017.

24. Тарасенко Ю.С. Фізичні основи радіолокації. Дніпро: Пороги, 2011. 487 с

25. Тарасенко Ю.С., Соляніков В.Г. Інформаційні системи з позицій забезпечення надійності та невизначеності вимірювань. Збірник матеріалів міжнародної науково-практичної інтернет-конференції «Інноваційні технології, моделі управління кібербезпекою -

«ІТМК-2021», Дніпро, 14 – 16 квітня 2021 р. с.29-30

26. Щодо оцінки ефективності засобів захисту інформації / Ю.С.Тарасенко, Д.С.Кузьменко // Матеріали міжнародної наукової конференції «Математичні проблеми технічної механіки та прикладної математики». Інноваційні технології, прогнозування та моделювання в соціальній сфері, економіці. Моделі корпоративного управління кібербезпекою / - Дніпро, Кам'янське – 2019(2). С. 72-73

27. Кірєєва Н.В., Семенов А.В. Витік інформації по каналах ПЕМІ та способи їх захисту // Міжнародний журнал прикладних та фундаментальних досліджень.– 2016. – № 8-4. – С. 499-504].

28. Завгородня Г.А. Інформаційна система підвищення надійності потенційно небезпечних об'єктів. С.23-24 // Міжнародна наукова інтернет-конференція «Інформаційне суспільство:технологічні, економічні та технічні аспекти становлення (випуск 41)» / Збірник тез доповідей: випуск 41 (м. Тернопіль, 13 вересня 2019 р.). – Тернопіль. – 2019. – 100 с.

29. Кузьменко Д.С., студент Б16-1, Луценко В.В., студент Б16-1, Тарасенко Ю.С. Питання підвищення рівня захищеності в інформаційно-телекомунікаційних системах. С.71-73 // Комп'ютерна інженерія і кібербезпека : досягнення та інновації : матеріали Всеукр. Наук.-практ. Конф. Здобувачів вищої освіти й молодих учених (м. Кропивницький, 27–29 листоп. 2018 р.)

30. Величко С.П., Костенко Л.Д. Вивчення основ квантової фізики: Навчальний посібник для студентів вищих навчальних закладів. – Кіровоград: РВЦ КДПУ ім. В. Винниченка, 2002. – 274 с.

31. Бондар О. В. Ситуаційний менеджмент. Навч. посіб. Київ : Центр учбової літератури, 2012. 388 с.

3. МЕТОДОЛОГІЧНІ ОСНОВИ СТВОРЕННЯ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ ТА МЕНЕДЖМЕНТУ ЇЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ АПРІОРНОЇ НЕВИЗНАЧЕНОСТІ

3.1. Методологія захисту інформації, принцип емерджентності та основні положення теорії систем

Нагадаємо, що методологія – це вчення про методи і методики, способи і засоби пізнання навколишнього світу. У прикладному сенсі методологія – це система принципів і підходів в конкретній дослідницькій діяльності людини в ході отримання та розробки знань в рамках обраної області пізнання. В даному контексті викладу предметом вивчення є створення комплексної системи захисту інформації (СЗІ), головною метою якої, – досягнення максимальної ефективності захисту за рахунок одночасного використання всіх необхідних ресурсів, методів і засобів.

СЗІ відносяться до систем організаційно-технологічного (соціотехнічного) типу [1,2], тому що загальну організацію захисту та вирішення значної частини задач перш за все здійснюють люди (організаційна складова), а безпосередньо захист інформації реалізують паралельно з технологічними

процесами її обробки (так звана технологічна складова). Тут, як і раніше, використано поняття «організація», під яким прийнято розуміти деяку сукупність елементів (людей, органів, підрозділів), об'єднаних для досягнення будь-якої мети або вирішення якої-небудь задачі на основі поділу праці, розподілу обов'язків та ієрархічної структури.

Очевидно, що серйозним спонукальним мотивом до проведення перспективних досліджень в галузі захисту інформації послужили ті постійно наростаючі кількісні і якісні зміни в сфері інформатизації, які мають і мали місце останнім часом і які, безумовно, повинні бути враховані в концепціях захисту інформації. Захист інформації стає все актуальнішою для маси об'єктів (великих і малих, державної та недержавної власності) та об'ємнішою у зв'язку з істотним розширенням сфери різноманітності (державної, промислової, комерційної, персональної і т. п.), що підлягає захисту. В результаті чого вельми своєчасно поставлено питання про комплексний захист інформації, а саме здійснення заходів щодо захисту інформації носить масовий характер. Зрозуміло, що успішне здійснення заходів захисту (безпеки) при такій їх масштабності можливо тільки при наявності хорошого інструментарію у вигляді методів і засобів вирішення відповідних задач, а сама розробка такого інструментарію вимагає наявності розвинених науково-методологічних основ захисту інформації.

Тут під науково-методологічними основами комплексного захисту інформації (як рішення будь-якої іншої проблеми) розуміється сукупність принципів, підходів і методів (науково-технічних напрямків), необхідних і достатніх для аналізу (вивчення, дослідження) проблеми комплексного захисту, побудови оптимальних механізмів захисту і управління механізмами захисту в процесі їх функціонування.

При цьому під принципами розуміється основне вихідне положення якої-небудь теорії, вчення, науки, світогляду; під підходом – сукупність прийомів, способів вивчення і розробки будь-якої проблеми; під методом – спосіб досягнення будь-якої мети, вирішення конкретного завдання. Так, наприклад, при реалізації принципу розмежування доступу як підходу можна

вибрати моделювання, а в якості методу реалізації – побудову матриці доступу.

Загальне призначення методологічного базису полягає у формуванні: погляду на організацію і управління КСЗІ, що відображає найбільш істотні аспекти проблеми; повної системи принципів, дотримання яких забезпечує найбільш повне рішення основних задач; сукупності методів, необхідних і достатніх для вирішення всієї сукупності задач управління.

Оскільки предметом викладу є розгляд різних аспектів забезпечення безпеки соціотехнічної системи, характерним прикладом якої є сучасний об'єкт інформатизації, то до складу науково-методологічних основ організації, побудови та управління КСЗІ увійдуть основні положення теорії систем, загальні закони кібернетики (як науки про управління у системах будь-якої природи), а також принципи і методи моделювання великих систем і процесів їх функціонування.

Почнемо з уточнення поняття «системи», яке вже раніше було озвучено у Вступі. Так як система, – це деяка сукупність або множина пов'язаних між собою елементів, то в подальшому під системою будемо розуміти природне з'єднання складових частин, самостійно існуючих в природі, а також щось абстрактне, породжене уявою людини. Такий підхід до визначення поняття системи заздалегідь пропонує існування зв'язків між її елементами, тобто всяка система складається з взаємопов'язаних і взаємодіючих між собою та із зовнішнім середовищем частин. При цьому очевидно, що система взаємодіє із зовнішнім середовищем і, отже, може бути кількісно оцінена через свої входи і виходи. Входами, наприклад, можуть бути, в загальному сенсі, сировина, що переробляється, його кількість, склад, температура тощо., а в якості виходів можуть служити і кількість готового продукту, і його якість і т. п. Як правило, будь-яка система піддається конкретним впливам, включаючи і не доброзичливі. Для їх компенсації, тобто для того, щоб система працювала в заданому напрямку, використовують керуючі впливи.

Система – це досить складний об'єкт, який можна розчленувати (провести декомпозицію) на складові елементи або підсистеми. Безпосередньо елементи пов'язані один з одним і з

навколишнім середовищем об'єкта. Сукупність зв'язків утворює структуру системи. Очевидно, що будь-яка система має свій алгоритм функціонування, спрямований на досягнення певної мети. Всі системи можна умовно розділити на малі і великі. Малі системи однозначно визначаються властивостями процесу і зазвичай обмежені одним типовим процесом, його внутрішніми зв'язками, а також особливостями функціонування. Великі системи являють собою складну сукупність малих систем (підсистем) і відрізняються від них в кількісному і якісному відношеннях. Кожна система апріорі володіє конкретними властивостями і її, як правило, можна розчленувати на складові елементи, де під елементами розуміють обмежене число компонентів, частин і більш дрібних об'єктів системи. Під властивістю озвучених елементів прийнято розуміти якості елементів, що дають можливість кількісного опису системи, виражаючи її в певних значеннях, а під зв'язком, – те, що з'єднує елементи і властивості системи в ціле.

При аналізі систем значний інтерес представляє вивчення їх структури. Структура відбиває найбільш істотні, стійкі зв'язки між елементами системи і їх групами, які забезпечують основні властивості системи, тобто структура – це форма організації системи. Структура системи може зазнавати певних змін в залежності від факторів (причин) внутрішньої і зовнішньої природи та від часу.

Поняття «стан» зазвичай виявляють на підставі дослідження, ситуаційного аналізу, досліджуючи, наприклад, вхідні впливи і вихідні результати системи.

Поведінка системи характеризує можливість стійкого, контрольованого переходу системи з одного стану в інший. Поняття «рівновага» визначається як здатність системи за відсутності зовнішніх впливів зберігати заздалегідь заданий стан. Стійкість характеризується як здатність системи повертатися в стан рівноваги після того, як вона була виведена з нього під дією зовнішнього впливу. Реально стійкість систем може досягатися тільки в певних межах. Поняття «розвиток» характеризує вдосконалення структури і функцій системи під впливом внутрішніх факторів, у зв'язку з чим поведінка системи набуває більш впорядкований і передбачуваний характер.

Головна властивість системи в тому, що вона набуває особливості, які не властиві її елементам. Цю властивість прийнято називати принципом емерджентності. Емерджентність або емергентність (від англ. Emergent – виникаючий, що несподівано з'являється) в теорії систем – це наявність у будь-якої системи особливих властивостей, які не притаманні її елементам, а також сумі елементів, не пов'язаних особливими системо утворюючими зв'язками, тобто незвідність властивостей системи до суми властивостей її компонентів. Як синонім часто використовують поняття «системний ефект», хоча на перших порах термін «системний ефект» сприймався лише як зростання ефективності діяльності за рахунок з'єднання, інтеграції окремих частин в єдине з'єднання. В кінцевому підсумку об'єднання частин в систему породжує у такої системи якісно нові властивості, що не зводяться до властивостей частин, які не виводяться з властивостей частин, властиві тільки самій системі і існують тільки поки система становить єдине ціле. В цьому випадку система є щось більше, ніж проста сукупність елементів. Якості такої новоствореної системи, притаманні лише їй, і називають емерджентними [3].

Для більш детального пояснення можна привести досить прості приклади реалізації принципу емерджентності в різних областях пізнання, наприклад:

- з області фізики-механіки, де в результаті взаємодії з двома каменями можна висікати іскри, видавати стуки, колоти горіхи і т. д., в той час як при їх окремому використанні неможливо досягти подібних ефектів;
- з області хімії, де в результаті з'єднання водню з киснем, що володіють кожен рядом особливих властивостей, можна отримати нову речовину – воду, багато властивостей якої (пам'ять води, тала, намагнічена, лужна, кислотна і т. п. вода) до сих пір не вивчені до кінця і не є похідними від властивостей водню і кисню;
- з області біології, в якій чоловіча та жіноча особини двостатевої популяції володіють кожна своїми індивідуальними особливостями, але тільки при їх з'єднанні виникає можливість продовження роду, утворення соціуму і т. д.

Мабуть, властивість емерджентності більш всіх інших говорить про природу систем оскільки є безпосередньою властивістю системи. У результаті можна констатувати, що:

- якщо система володіє емерджентними властивостями, то вони не можуть бути виражені через властивості окремо взятих її частин;
- джерелом, носієм емерджентних властивостей є безпосередньо сама структура системи, оскільки при різних структурах у систем, утворених з одних і тих же елементів, виникають різні властивості;
- системи можуть мати і неемерджентними властивостями, зберігши притаманні властивості її частин (наприклад, для технічних систем перш за все це обсяг і маса);
- емерджентність є індикатором цілісності системи. При зникненні такої властивості можна констатувати, що її (системи) цілісність порушена, – якщо ж це властивість проявляється, – значить система ціла. Приклад: жодна з частин літака не може злетіти, а літак може.

Таким чином, емерджентності притаманна більш розвинена форма вираження закону діалектики про перехід кількості в якість, тобто виявляється, що для переходу в нову якість не обов'язково "накопичення" кількості (згадайте вислови: "остання крапля переповнила чашу" або "остання соломинка переламала хребет верблюдові"). Для появи нової якості досить об'єднати в ціле хоча б два елементи.

Нагадаємо, що динамічний аспект емерджентності характеризується окремим терміном – синергетичність, про що вже було згадано у Вступі. Основне поняття синергетики – визначення структури як стану, що виникає в результаті багатоваріантного і неоднозначного поводження таких багатоелементних структур або багатофакторних середовищ, що не деградують до стандартного для замкнутих систем усереднення термодинамічного типу, а розвиваються внаслідок відкритості, припливу енергії ззовні, нелінійності внутрішніх процесів, появи особливих режимів з загостренням і наявності більше ніж одного стійкого стану.

Вище відзначили, що до складу науково-методологічних основ організації, побудови та управління КСЗІ входять основні

положення теорії систем і загальні закони кібернетики. При цьому в задачі загальної теорії систем, як міждисциплінарної галузі наукових досліджень, входить: розробка узагальнених моделей систем; побудова методологічного апарату; опис функціонування і поведінки системних об'єктів; розгляд динаміки систем, їх поведінки, розвитку, ієрархічної будови і процесів управління в системах. Теорія систем оперує такими поняттями, як системний аналіз і системний підхід.

Системний аналіз – це стратегія вивчення складних систем. В якості методу дослідження в ньому використовується математичне моделювання, а основним принципом є декомпозиція складної системи на простіші підсистеми (принципи ієрархії системи). У цьому випадку математична модель будується за блоковим принципом: загальна модель підрозділяється на блоки, яким можна дати порівняно прості математичні описи. Системний аналіз дозволяє організувати наші знання про об'єкт таким чином, щоб допомогти вибрати потрібну стратегію або передбачити результати однієї або декількох стратегій, які здавалися доцільними для тих, хто повинен приймати рішення. В основі ***стратегії системного аналізу*** лежать такі загальні положення: чітке формулювання мети дослідження; постановка задачі для реалізації цієї мети і визначення критерію ефективності виконання задачі; розробка розгорнутого плану дослідження з зазначенням основних етапів і напрямів рішення задачі; послідовне просування по всьому комплексу взаємопов'язаних етапів і можливих напрямків; організація послідовних наближень і повторних циклів досліджень на окремих етапах; принцип спадної ієрархії аналізу і висхідної ієрархії синтезу в рішенні складених задач і т. п.

З позицій системного аналізу вирішуються задачі моделювання, оптимізації, управління та оптимального проектування систем. Особливий внесок (важливість) системного аналізу у вирішенні різних проблем полягає в тому, що він дозволяє виявити фактори і взаємозв'язки, які згодом можуть виявитися вельми істотними, висвітлює слабкі місця гіпотез і припущень, дає можливість спланувати методику спостережень і побудувати експеримент так, щоб ці фактори були включені в розгляд. Як науковий підхід системний аналіз

створює інструментарій пізнання фізичного світу і об'єднує його в систему гнучкого дослідження складних явищ. Системний підхід орієнтує дослідження на розкриття цілісності об'єкта, на виявлення різних особистих типів зв'язків у ньому і відомості в єдину теоретичну картину. Він заснований на уявленні про систему як про щось цілісне, шо володіє новими властивостями (якостями) в порівнянні з властивостями складових її елементів. Нові властивості при цьому розуміються дуже широко. Вони можуть виражатися, зокрема, в здатності вирішувати нові проблеми або досягати нові цілі. Для цього потрібно визначити межі системи, виділивши її з навколишнього світу, і потім відповідним чином змінити (перетворити), або, кажучи математичною мовою, перевести систему в бажаний стан.

Прийнято в ***системному підході*** виділяти ***етапи:***

- постановки задачі (проблеми), включаючи визначення об'єкта дослідження, постановку цілей, конкретизації критеріїв для вивчення об'єкта та управління ним;
- встановлення меж досліджуваної системи і її (первинна) структуризація, тобто всю сукупність об'єктів і процесів, що мають відношення до поставленої мети, розбивають на два класи у вигляді власне досліджуваної системи і зовнішнього середовища;
- складання математичної моделі досліджуваної системи, включаючи параметризацію системи, задання області визначення параметрів, встановлення залежностей між введеними параметрами;
- дослідження побудованої моделі, в тому числі прогноз розвитку досліджуваної системи на основі її моделі та аналіз результатів моделювання;
- оцінки і вибору оптимального управління.

Вибір оптимального управління якраз і дозволяє перевести систему в бажаний (цільовий) стан і тим самим вирішити проблему. Однак, незважаючи на чітке математичне трактування системного підходу, він не отримав однозначної практичної інтерпретації. Проте розвиваються кілька напрямків його практичної реалізації в області вдосконалення систем управління: проводиться їх обстеження (діагностичний аналіз), виявляються недоліки та шляхи усунення останніх, формуються

заходи щодо вдосконалення систем і розробляються проекти систем, впровадження яких розглядається як спосіб перетворення існуючих систем управління. Значну роль в цих методах відіграють поняття системи, підсистеми, навколишнього середовища, класифікація основних властивостей і процесів в системах, класифікація систем і т. д.

Зупинимося на узагальненому визначенні системи. Система, з одного боку, може бути описана динамічно як процес, а з іншого – статично, з точки зору або зовнішніх, або внутрішніх характеристик. Крім того, внутрішня будова системи може бути представлена у вигляді функціональних залежностей і у вигляді структури, що реалізує ці залежності. Таким чином, можна виділити **п'ять основних системних представлень [3]: процесуальне, функціональне, макроскопічне, ієрархічне і мікроскопічне.**

У процесуальному плані система розглядається динамічно як процес, інші системні представлення відображають її статичний аспект. У макроскопічному поданні описуються зовнішні характеристики системи, у функціональному, ієрархічному і мікроскопічному – внутрішні. Мікроскопічне подання системи засноване на розумінні її як сукупності взаємопов'язаних елементів, нерозкладних далі «цеглинок».

Центральним поняттям мікроскопічного системного представлення є поняття елемента. Звичайно, у загальному вигляді елемент лише відносно неподільний, проте для даної системи він є абсолютно неподільним. Елементи також можуть бути розглянуті як системи, але це будуть системи іншого типу, відносно досліджуваної.

Крім того, система розуміється як сукупність різнорідних елементів, які можуть відрізнятися за принципом дії, за технічним виконанням і за рядом інших характеристик. Система може зводиться до ансамблю простих частин. Елементи системи мають зв'язками, які об'єднують їх в цілісну систему. Елементи можуть існувати тільки в «пов'язаному» вигляді, тобто між елементами обов'язково встановлюються зв'язки. Елементи в системі обов'язково взаємодіють, у результаті одні властивості змінюються (інтерпретуються як змінні), інші залишаються незмінними (константи).

Важливу роль в системних дослідженнях відіграє пошук системоутворюючих зв'язків, завдяки яким всі елементи системи виявляються пов'язаними воєдино.

Функціональне представлення системи пов'язане з розумінням системи як сукупності функцій (дій) для досягнення певної мети. Кожен елемент в системі виконує певну функцію.

Синонімом поняття «структура» для функціонального подання служить поняття функціональної структури, або організація. Організація може бути реалізована різними структурами (при цьому функціональна сутність системи залишається тією ж, змінюється тільки спосіб реалізації). Для макроскопічного подання характерне розуміння системи як нероздільного цілого. Тут важливо поняття системного оточення.

Під навколишнім середовищем системи розуміється сукупність всіх об'єктів, зміна властивостей яких впливає на систему і на які впливає зміна властивостей системи. Жодна система об'єктів не може бути розглянута поза системного оточення.

Системне оточення дозволяє охарактеризувати систему множиною зовнішніх зв'язків (або зовнішньою структурою), так і сукупністю зовнішніх відносин.

Ієрархічне представлення системи (як ієрархічної впорядкованості) засновано на понятті підсистеми, або одиниці, які слід відрізняти від поняття «елемент». Одиниця володіє функціональною специфікою цілого (системи). Система може бути представлена у вигляді сукупності одиниць, що складають системну ієрархію.

Можна виділити два типи функціональних зв'язків між одиницями системної ієрархії у вигляді горизонтальних (між одиницями одного рівня) і вертикальних (між одиницями різних рівнів), тобто одиниці кожного рівня описуються набором вертикальних і горизонтальних зв'язків.

Процесуальне представлення системи передбачає розуміння системного об'єкта як сукупності процесів, що характеризуються послідовністю станів у часі. Основним поняттям тут є поняття періоду життя – тимчасового інтервалу, протягом якого функціонує даний процес.

Дуже важливо, розглядаючи теорію систем, не забувати про її зв'язки з проектуванням. Навіть добре працюючі компоненти, з'єднані разом, не обов'язково складають добре функціонуючу систему. У складній системі часто виявляється, що навіть якщо окремі компоненти задовольняють всім необхідним вимогам, система як ціле не буде працювати.

Таким чином, комплексна система захисту інформації (КСЗІ) – це система організаційно-технологічного типу. Вона створюється людиною, тобто штучна і, матеріальна, – останнє підкреслює не тільки об'єктивність її існування, але і рівень матеріальних і фінансових витрат при її реалізації. Вона відкрита, оскільки можливе її розширення, динамічна (схильна до старіння, розвитку, руху, прогресу і регресу, поділу, злиття і т. д.) та імовірнісна, що особливо проявляється і характерно при виробленні оцінки працездатності системи в цілому і при поблочному її розгляді.

3.2. Управління та загальні закони кібернетики

Вищесказане дозволяє стверджувати, що КСЗІ – це складна і багатогранна система, а для забезпечення її ефективного функціонування необхідно грамотне управління, - тобто аспекти менеджменту.

Так як процес управління можливий тільки в організованому середовищі, потрібно було створити відповідні умови і позначити виконавчі органи, між якими відбувається обмін інформацією у вигляді інформаційних сигналів, що транслюються через спеціальні давачі. Таким чином, обмін інформацією – постійний процес, а для його управління створені і створюються новітні розробки в сфері кібернетики.

Існує безліч визначень поняття кібернетика. І всі вони по-своєму правильні. Так що таке кібернетика? Взагалі вважається, що кібернетика – це наука, що представляє закони взаємодії машин з живими організмами. Але основне поняття кібернетики зводиться до мети управління. Адже управління – це завжди цілеспрямований процес, для якого і існує створена система. Так як будь-які процеси управління пов'язані з прийняттям рішень на

основі отриманої інформації, то кібернетику часто визначають ще й як науку про загальні закони одержання, зберігання, передачі і перетворення інформації в складних керуючих системах. У сферу кібернетики входить вивчення основної структури і принципів роботи систем управління, здатність сприймати і переробляти необхідну інформацію. Методика кібернетики ґрунтується на використанні математичного апарату для побудови математичних моделей структур.

Таким чином, кібернетика (від грец. – мистецтво управління), як область науки про загальні закони одержання, порівняння, передачі і переробки інформації, має керуючі системи. Для того щоб в системі могли відбуватися процеси управління, вона повинна мати певний ступінь складності. З іншого боку, здійснення процесів управління в системі має сенс тільки в тому випадку, якщо ця система змінюється, рухається, тобто якщо мова йде про динамічну систему. Тому можна уточнити, що об'єктом вивчення кібернетики є складні динамічні системи, в тому числі КСЗІ. Зауважимо, що до складних динамічних систем відносяться і живі організми (тварини і рослини), і соціально-економічні комплекси (організовані групи людей, бригади, підрозділи, підприємства, галузі промисловості, держави), і технічні агрегати (потокові лінії, транспортні засоби, системи агрегатів). Однак, розглядаючи складні динамічні системи, кібернетика не ставить перед собою задач всебічного вивчення їх функціонування. Наприклад, розглядаючи роботу складного електронного автомата, зазвичай не цікавляться на основі яких елементів (електромеханічні реле, лампові або транзисторні тригери, феритові сердечники, напівпровідникові інтегральні схеми) функціонують його арифметичні і логічні пристрої, пам'ять та ін. Як правило, цікавить які логічні функції виконують ці пристрої, як вони беруть участь в процесах управління. Предмет кібернетики становлять лише ті сторони функціонування систем, якими визначається перебіг у них процесів управління, тобто процесів збору, обробки, зберігання інформації та її використання для цілей управління. Однак коли ті чи інші приватні фізико-хімічні процеси починають істотно впливати на процеси управління системою, кібернетика повинна включати їх в сферу свого дослідження, але не всебічного, а саме

з позицій їх впливу на процеси управління. Таким чином, предметом вивчення кібернетики є процеси управління в складних динамічних системах, в нашому випадку КСЗІ.

Системи в кібернетиці вивчаються по їх реакціях на зовнішні впливи, інакше кажучи, за тими функціями, які вони виконують. Поряд з матеріальним і структурним підходами, кібернетика ввела в науковий обіг функціональний підхід як варіант системного підходу в широкому сенсі слова. Застосування системного та функціонального підходів при описі та дослідженні складних систем відноситься до основних методологічних принципів кібернетики.

Основна мета кібернетики як науки про управління – домагатися побудови на основі вивчення структур і механізмів управління таких систем, такої організації їх роботи, такої взаємодії елементів всередині цих систем і такої взаємодії із зовнішнім середовищем, щоб результати функціонування цих систем були найкращими, тобто приводили б найшвидше до заданої мети функціонування при мінімальних витратах тих чи інших ресурсів (сировини, людської праці, машинного часу, пального і т. д.). Все це можна визначити коротко терміном «оптимізація». Таким чином, основною метою кібернетики є оптимізація систем управління, що для нашого випадку є вельми актуальним для побудови організаційно-функціональної структури національної системи кібербезпеки.

Для дослідження систем кібернетика використовує три принципово різних методи та підходів: математичний аналіз, фізичний експеримент і обчислювальний експеримент [4, стор.66-73].

Перші два з них широко застосовуються і в інших науках. Сутність першого методу полягає в описі досліджуваного об'єкта в рамках того чи іншого математичного апарату (наприклад, у вигляді системи рівнянь) і подальшого здобуття різних результатів з цього опису шляхом математичної дедукції (наприклад, шляхом вирішення відповідної системи рівнянь).

Сутність другого методу полягає у проведенні різних експериментів або з самим об'єктом, або з його реальною фізичною моделлю.

Досягненням кібернетики є розробка і широке використання нового (третього) методу дослідження, який отримав назву обчислювального або машинного експерименту, інакше званого математичним моделюванням. Суть його в тому, що експерименти проводяться не з реальною фізичною моделлю досліджуваного об'єкта, а з його математичним описом, реалізованим на комп'ютері.

У дослідженні способів зв'язку і моделей управління кібернетики знадобилося ще одне поняття, яке було давно відоме і добре нам зрозуміле, але вперше одержало фундаментальний статус у природознавстві, – поняття інформації (з латинського – ознайомлення) як міри організованості системи на противагу поняттю ентропії як міри неорганізованості. У даному поданні кібернетика виявляє залежності між інформацією та іншими характеристиками систем. Існує обернено-пропорційна залежність між інформацією та ентропією. З підвищенням ентропії зменшується інформація, і навпаки – зниження ентропії збільшує інформацію. Зв'язок інформації з ентропією свідчить і про зв'язок інформації з енергією, оскільки енергія (від грецького energeia – діяльність) характеризує загальну міру різних видів руху і взаємодії в формах: механічної, теплової, електромагнітної, хімічної, гравітаційної, ядерної. У той час як детермінованість сигналу, – «носія» інформації, не залежить від кількості енергії, яка використовується для передачі сигналу незважаючи на те, що енергія та інформація пов'язані між собою.

Отже, в рамках кібернетики запропоновані загальні принципи будь-якого управління, а саме: будь-яке управління є цілеспрямований інформаційний безперервний процес, що полягає в зборі, обробці та передачі інформації, де управління здійснюється в замкнутому контурі, утвореному керуючим і керованими об'єктами (органами), об'єднаними в єдину систему з прямою і зворотною лініями зв'язку (див. п.2.4, рис. 2.2).

Зазначені принципи, сформульовані у вигляді фундаментальних законів, утворюють систему, яка повинна розглядатися в сукупності і взаємозв'язку, і носять загальний характер, так як вони справедливі для систем будь-якої природи: біологічних, технічних, соціальних.

Таким чином, для кібернетики як науки предметом дослідження є системи будь-якої природи, а в якості методу дослідження – математичне моделювання, що дозволяє аналізувати і синтезувати досліджувані системи, прогнозувати їх оптимальну поведінку, виявляти канали та алгоритми управління такими системами. Завдяки сучасному розвитку обчислювальної техніки методи моделювання стали основним інструментом кібернетики, незважаючи на те, що використовувані моделі стають все більш масштабними і розгалуженими. При цьому методи кібернетики не тільки дозволяють створювати процес або систему, що оптимально функціонує, а й вказують конкретні шляхи вибору і використання оптимального режиму безпосередньої реалізації самого процесу оптимального управління

3.3. Рішення та методологія його прийняття в умовах існування різних видів невизначеності суб'єктів господарювання

Очевидно, що суть управління полягає в прийнятті конкретного рішення при аналізі будь-якої проблеми, розглядаючи завжди кілька шляхів, що ведуть до мети. Щоб зрозуміти, який з можливих шляхів краще, слід спочатку визначити, де проходить межа між системою і зовнішнім середовищем, які цілі ставляться перед системою, як оцінювати ефективність майбутньої системи і які витрати ресурсів необхідні на всіх етапах життєвого циклу майбутньої системи. Фактично для прийняття остаточного рішення зі створення системи необхідно заздалегідь затвердити критерії ефективності планованої до реалізації системи конкретного призначення. Пошук і розробка варіантів залежать від наявних обмежень на час, ціну та ресурси. Крім цього, пошук варіантів обмежується багажем знань проектувальників системи і тим фактом, що для вибору найкращого варіанта можна порівняти лише невелике число варіантів.

Пропоновані системи завжди повинні порівнюватися на основі системного підходу, тобто мають бути розглянуті всі ті учасники, які впливають на проектну систему або зазнають її впливу.

Для того щоб оцінити перевагу одного варіанта перед іншим, необхідно виявити результати і наслідки всіх допустимих варіантів; бажано враховувати при цьому ймовірності появи певних ситуацій в роботі системи.

Особа, яка приймає остаточне рішення, повинна володіти відповідним рівнем знань і досвіду, які допомагають йому при розгляді наявних варіантів. Варіанти – це різні стратегії або технічні рішення, за допомогою яких можуть бути реалізовані наявні наміри. Кожен варіант веде до одного або декількох заздалегідь відомих результатів.

Поняття «рішення» дуже багатозначне. Рішення є певний процес, що складається з ряду окремих актів і процедур, а його вольовий фактор є одним із моментів, що направляють процес вироблення і прийняття рішення. Залежно від вольового фактору рішення може бути різним, отже, воно неоднозначне. Тому призначення вольового фактора в тому і полягає, щоб вибрати один варіант. Рішення передбачає попереднє усвідомлення цілей і засобів дії. Усвідомлення – це процес, який базується на інформації про ціль і засоби дії. Однак це – не просте перетворення інформації, а більш складний процес, який передбачає ув'язку цілей і засобів. Якщо ціль задана, то процес усвідомлення полягає в сприйнятті і осмисленні того, що задано разом з встановленням взаємозв'язків між ціллю і засобами. Якщо ціль не задана і її треба визначити (або, принаймні, уточнити), тоді в усвідомлення включається вольовий акт. Кількість можливих цілей може бути також дуже велика, так що не існує точного способу визначити чи вибрати найкращий варіант. У цьому випадку вирішальне значення набуває вольовий вибір. Точно так же вольовий

момент набуває вирішального значення, коли немає строгого способу однозначно вибрати між конкуруючими альтернативами, навіть якщо їх скінченне або невелике число.

Отже, під рішенням розуміється і знаходження певного варіанту дій, і сам процес діяльності, і її кінцевий результат, тобто для розгляду управлінського процесу доцільно використовувати модель, в основу якої покладено три складники процесу управління: розробка, ухвалення та реалізація управлінського рішення.

Таким чином, управлінське рішення (у тому числі згідно [5, стор.31] (Таблиця 1. Деякі приклади визначення понять “управління”, “рішення” та “управлінське рішення” у спеціальній літературі) — це результат творчого цілеспрямованого аналізу проблемної ситуації, вибору шляхів, методів і засобів її вирішення у відповідності з ціллю системи менеджменту, - тобто результат вибору альтернативи з багатьох варіантів досягнення конкретної цілі. При цьому варто акцентувати увагу на три пов'язаних між собою аспекти управлінського рішення. По-перше, управлінське рішення – це вид діяльності, який здійснюється суб'єктом управління і пов'язаний з підготовкою, знаходженням, вибором і прийняттям певних варіантів дій. В цьому аспекті управлінське рішення – вид роботи суб'єкта управління, певний етап процесу управління. По-друге, управлінське рішення – це варіант впливу суб'єкта управління на об'єкт. У цьому сенсі управлінське рішення є опис передбачуваних дій керуючої системи по відношенню до керованої, формула впливу суб'єкта управління на об'єкт. По-третє, управлінське рішення – це організаційно-практична діяльність, спрямована на втілення рішення в життя.

Крім того управлінські рішення повинні відповідати певним вимогам, ігнорування яких, повне або часткове, може привести до помилок і незадовільних результатів. Зокрема:

1. Рішення повинно відображати об'єктивні закономірності розвитку організації і системи управління нею. Якщо ця вимога не виконується, то таке рішення буде блокуватися або відхилятися працівниками;

2. Рішення повинно ґрунтуватися на повній та достовірній інформації;

3. Рішення повинно враховувати можливість прояву потенційного ризику. Якою би повною і достовірною не була інформація, рішення, що приймаються керівником, спрямовані в майбутнє, яке завжди містить елементи невизначеності;

4. Кожне управлінське рішення має врівноважувати суперечливі цілі, цінності, критерії. Будь-яке рішення має якісь негативні наслідки – це треба розуміти і сприймати як факт. У практиці зустрічається дуже мало настільки однозначних ситуацій, що результатом найкращого рішення буде тільки благо для всіх. З позицій системного підходу приймається таке рішення, яке буде найкращим з точки зору кінцевих результатів, тобто для всієї організації та ефективним в перспективі;

5. Рішення повинно бути реальним у виконанні, тобто виходити з реально наявних ресурсів і часу, а також містити механізм реалізації;

6. Рішення повинно задовольняти вимогу оперативності. Воно повинно готуватися, прийматися і виконуватися в реальному масштабі часу тих процесів, якими управляють, з урахуванням можливих швидкостей розвитку ситуації;

7. Рішення повинно бути економічним і ефективним, тобто поставлені цілі повинні бути досягнуті при мінімальних витратах;

8. Рішення повинно задовольняти умові повноважності. Це означає, що воно повинно прийматися органом або особою, яка має право приймати саме це рішення. Перевищення повноважень створює передумови невиконання рішення;

9. Рішення повинно бути несуперечливим. Приймаючи рішення, необхідно враховувати, що воно буде здійснюватися не ізольовано, а має розвивати і доповнювати раніше прийняті рішення;

10. Рішення повинно бути своєчасним. Своєчасність прийняття управлінського рішення означає, що з моменту виникнення проблемної ситуації до прийняття рішення в організації не повинно статися незворотних процесів, що роблять це рішення непотрібним. Своєчасність означає також своєчасність реалізації управлінського рішення.

Очевидно також що поведінка людини, яка приймає рішення, і саме рішення багато в чому залежать від структури і об'єктивних характеристик ситуації, стосовно якої особа приймає рішення. Ситуації є частиною навколишнього середовища, в якій діє людина, і для їх аналізу потрібне попереднє знання характеристик цього середовища.

У навколишньому середовищі, як правило, відбуваються події, які не можна передбачити з повною визначеністю. Тому **ступінь невизначеності** з точки зору прийняття рішення є вельми важливим. Крім того, середовищу властива певна ступінь динаміки, так як з плином часу воно піддається модифікації і перетворенню.

Нарешті, саме середовище характеризується певним ступенем складності, а середовище людської діяльності та

поведінки тим складніше, чим більше змінних факторів (ситуації) в ній міститься.

Особливо непередбачуваними можуть бути, наприклад, ступінь конфліктності інтересів осіб, що діють в соціумі та належать до сфери (галузі) соціальної інженерії, що і буде розглянуто в розділі 7. Зазначимо тільки, що з погляду методики прийняття рішень у так званих прикордонних ситуаціях [6] можливі як недетерміновані, так і детерміновані ситуації, в яких (в останніх) рішення приймаються в умовах визначеності і які прийнято називати неризикованими ситуаціями (задачами).

У цих (останніх) ситуаціях кожна альтернатива приводить до однозначно визначених наслідків. Детерміновані ситуації можуть бути простими і статичними, складними і статичними, простими і динамічними або складними і динамічними. Навпаки, у ризикованих (імовірнісних) ситуаціях особа, яка приймає рішення, не знає напевно, який результат досягнутий після прийняття того чи іншого рішення.

Ризиковані ситуації можуть бути простими і статичними, складними і статичними, простими і динамічними або складними і динамічними.

Таким чином, ситуації можуть бути класифіковані, як:

1) ***стандартні проблеми***, які мають чітку структуру, причинно-наслідкові зв'язки, аналоги;

2) ***добре структуровані проблеми***, які можуть бути розчленовані на підпроблеми, блоки питань, для кожного з яких зазвичай є набір рішень;

3) ***слабо структуровані проблеми***, в яких далеко не завжди проглядаються причинно-наслідкові зв'язки, а самі проблеми не окреслюються досить чітко;

4) ***неструктуровані проблеми***, які зазвичай не мають аналогів, їх причинно-наслідкові зв'язки не завжди зрозумілі, способи вирішення не визначені. Класичний

приклад – катастрофи природні і техногенні з великими соціальними наслідками.

До **методів аналізу і вирішення проблем** можуть бути віднесені:

1) ***інструкції та керівництва***, які чітко і виразно обґрунтовують послідовність аналізу системи і рішення проблем;

2) ***економіко-математичні моделі і методи***, що формалізують взаємозв'язки процесів і явищ;

3) ***системний аналіз,*** що дозволяє виявити напрямки взаємодії підсистем, стратегію їх розвитку;

4) ***експертні оцінки і судження***, що дозволяють авторитетним фахівцям оцінити питомі ваги подій, явищ, факторів, прогнози розвитку систем і підсистем, співвідношення детермінованих і імовірнісних факторів.

Цілком очевидно, що важливе значення в процесі прийняття управлінського рішення відіграє психологічна теорія рішень – система мотивованих тверджень, які розкривають внутрішній зміст діяльності осіб в процесі підготовки і прийняття рішень.

Досвід показує, що структура задачі значною мірою визначає поведінку людини, що вирішує її. Хоча задачі, з якими доводиться стикатися керівнику, дуже різні, але в них можна виділити ряд спільних рис, що дозволяють описувати їх структуру.

Психологічна теорія рішень поряд зі структурою задач враховує риси особистості, які відіграють важливу роль в процесі прийняття рішень. Одним з найважливіших при цьому є те, що дії особи, яка приймає рішення, завжди спрямовані на досягнення певних цілей. У процесі підготовки і прийняття рішення відіграють істотну роль такі пізнавальні якості, як короткочасна і довгострокова пам'ять, швидкість переробки інформації.

Загально прийнято сам **процес психологічних тверджень в теорії рішень розбивати за класами [6]:**

1. **Перший клас** стосується того, як у людей виникає, уявлення про ситуацію прийняття рішень. Таке уявлення є суб'єктивним образом цієї ситуації. Психологи виявили, що дуже часто той, хто приймає рішення спрощує ситуацію, забуваючи або ігноруючи деякі альтернативи або їх наслідки;

2. **Другий клас** описує процес оцінки суб'єктивної цінності того чи іншого варіанту дії, званої корисністю. Це найважливіший клас тверджень, оскільки корисність наслідків альтернатив у значній мірі визначає характер прийнятого рішення;

3. До **третього класу** належать твердження, що стосуються суб'єктивної оцінки ймовірностей обставин, що визначають наслідки прийнятого рішення. Так, наприклад, психологи виявили, що люди переоцінюють ймовірності настання малоймовірних подій і одночасно недооцінюють ймовірності настання дуже правдоподібних подій;

4. **Четвертий клас** стосується стратегій вибору поведінки. Вони описують, як особи, що приймають рішення, інтерпретують інформацію про корисність результатів і їх ймовірності і те, які правила вибору альтернатив вони при цьому використовують. Психологи виявили, що в простих задачах, пов'язаних з ризиком, люди зазвичай вибирають стратегії, максимізує суб'єктивно очікувану корисність, яку вони представляють як лінійну комбінацію суб'єктивної ймовірності фіналів і їх корисності;

5. **П'ятий клас** описує фактори, що керують процесом прийняття рішень. До їх числа належать вплив навколишнього середовища, особистісні особливості того, хто приймає рішення і вплив соціальної групи.

Зазвичай, в ***психологічних дослідженнях процесів прийняття рішень використовуються три методи:***

- *перший метод у вигляді лабораторного експерименту*. Якщо в економіці цей метод розглядається як допоміжний, то в психології він є домінуючим;

- *другий метод – це процес формалізації*. Він полягає в тому, що на першому етапі створюється сукупність аксіом, що стосуються будь-яких об'єктів, наприклад ризику або переваги, на другому етапі за допомогою формальних міркувань виводяться нові твердження, які є наслідками прийнятих аксіом, і на третьому етапі проводиться експериментальна перевірка дослідницьких гіпотез;

- *третій метод заснований на моделюванні діяльності щодо прийняття рішень, зокрема машинному.* Результати моделювання зіставляються з діями людини в аналогічній обстановці.

Отже, якісні та ефективні управлінські рішення повинні, з одного боку, спиратися на об'єктивні закони і закономірності суспільного розвитку, а з іншого боку, управлінські рішення істотно залежать від множини суб'єктивних факторів, таких, як: логіки розробки рішень, якості оцінки ситуації, структуризації задач і проблем, певного рівня культури управління, механізму реалізації рішень, виконавчої дисципліни і т. п. При цьому необхідно завжди пам'ятати, що навіть ретельно продумані рішення можуть виявитися неефективними, якщо вони не зможуть передбачити можливих змін у ситуації, стані виробничої системи.

Таким чином, процес прийняття і реалізації рішень представляється як послідовна зміна взаємопов'язаних стадій, етапів різних дій керівника, пошук істини і аналіз помилок, шляхів рухів до цілі та засобів її досягнення в процесі прийняття рішень в умовах невизначеності. При

цьому кількісно невизначеність може виступати як можливість відхилення результату від очікуваного (або середнього) значення як у меншу, так і в більшу сторону (“спекулятивна” невизначеність), або можливість тільки негативних відхилень кінцевого результату події (“чиста” невизначеність) [7].

Наприклад економіка ринкового типу передбачає існування різних видів невизначеності для всіх суб'єктів господарювання, а саме:

1) залежно від способів визначення ймовірності це:

- статистична невизначеність, де ймовірність розглядається як об'єктивна можливість настання події та визначається на основі реальних даних за відносною частотою (часткою);
- нестатистична (апріорна, суб'єктивна) невизначеність, де ймовірність розглядається як ступінь впевненості, що дана подія відбудеться, тобто це суб'єктивна ймовірність, тому що визначається на основі опитувань ймовірності.

2) за ступенем ймовірності настання події:

- повна невизначеність, тобто повністю відсутня можливість яким-небудь чином прогнозувати перспективи розвитку як підприємства, так і ринку в цілому, де міра прогнозованості (ймовірність) настання події прагне до 0;
- повна визначеність, тобто реалізується можливість із 100%-ою ймовірністю прогнозувати не лише стратегію підприємства на ринку, але і ситуацію, тенденції розвитку і т. ін., де міра прогнозованості (ймовірність) настання події наближається до 1;
- часткова невизначеність, тобто є конкретний практичний характер у порівнянні з попередніми видами, що являють собою теоретичні припущення про можливості суб'єктів господарювання, а міра прогнозованості (ймовірність) настання події знаходиться в межах від 0 до 1.

3) за об'єктом невизначеності:

- людська невизначеність, що обумовлена неможливістю точного передбачення поведінки людини в процесі роботи із-за відмінностей в рівні освіти, емоційно-психологічному настрої та поглядів кожної людини;

- технічна невизначеність, що обумовлена мірою надійності устаткування, непередбаченістю виробничих процесів, складністю технології, рівнем автоматизації, темпами оновлення та обсягами виробництва;

- соціальна невизначеність, що обумовлена прагненням людей створювати соціальні зв'язки (профспілки) та поводитися відповідно до загальноприйнятих норм, традицій і взятих на себе зобов'язань.

Очевидно, що розвиток фірми в умовах ринкової економіки на кожному етапі повинен формуватися з урахуванням різних видів невизначеності. Чинники невизначеності, що впливають на будь-який ринковий суб'єкт, також наявні безпосередньо в процесі управління ним.

За місцем виникнення невизначеність в управлінні підприємством (фірмою) може бути наслідком:

- невизначеності у встановленні планового періоду і, зокрема, періоду, на який розробляється стратегія розвитку підприємства;

- невизначеності формування цілей підприємства та вибору пріоритетів у визначених цілях, що може бути зумовлено наявністю ряду альтернативних цілей;

- помилок в оцінках дійсного стану справ усередині самого підприємства і його місця на ринку, до чого, у свою чергу, може призвести ряд причин об'єктивного та суб'єктивного характеру;

- неповної або помилкової інформації стосовно перспектив розвитку даного підприємства і ринку в цілому, рішень, прийнятих на її підставі;

- можливих перебоїв у розробці чи реалізації стратегії розвитку підприємства;

- невизначеності контролю й оцінки результатів діяльності підприємства.

Таким чином, невизначеність виступає невід'ємним атрибутом прийняття господарських рішень. Але слід зазначити, що вона не завжди є негативним фактором, оскільки усвідомлення факту її існування мотивує до самостійного розв'язання господарських завдань, веде до ініціативності та творчого пошуку.

Далі, у контексті викладеного вище (зокрема з огляду на матеріал п.2.4, де було озвучено принципи побудови комплексної системи захисту інформації (КСЗІ), яка функціонує в умовах невизначеності і вимагає значних матеріальних витрат, рівень яких також залежить від когнітивних підсистем менеджменту та маркетингу підприємств [8] і так часто званих «об'єктів інформаційної діяльності» (ОІД) або «ключових систем інформаційної інфраструктури» (КСІІ), що відповідає Critical infrastructure systems (використовуваний як європейсько-англійський термін) або Mission critical information systems, [9]), **продовжимо** ***розглядати методологію побудови пізнавальної моделі безпеки об'єктів критичної інфраструктури в умовах апріорної невизначеності потенційних інформаційних загроз їхньому (об'єктам) штатному функціонуванню.***

3.4. Організаційно-нормативні питання стосовно комплексної системи інформаційної безпеки та основи побудови її моделі з акцентом на захист інформаційної життєдіяльності соціуму

Зазвичай під термінами «об'єктів інформаційної діяльності» (ОІД) та «ключових систем інформаційної інфраструктури» (КСІІ) розуміють інженерно-технічні споруди з визначеною контрольованою зоною, де здійснюється адміністративна, фінансово-економічна, виробнича, науково-технологічна та інша діяльність, яка пов'язана з інформацією, що підлягає захисту від витоку технічними каналами та спеціальних впливів (будівлі, приміщення, транспортні засоби в яких обробляється мовна або електронна інформація). КСІІ - це інформаційно-керуюча або інформаційно-телекомунікаційна система, яка здійснює управління критично важливим об'єктом (процесом), або інформаційне забезпечення управління таким об'єктом (процесом), або офіційне інформування громадян о деструктивних інформаційних впливів, через які може скластися надзвичайна ситуація або будуть порушені функції управління зі значними негативними наслідками. Тому, будь-яка КСЗІ в будь якому підприємстві також повинна відповідати вимогам інформаційної захищеності від загроз та можливих ризиків.

Значимість стану безпеки у всіх сферах соціуму, включаючи критичні інфраструктури (КІ), особливо актуальна та значно зростає під час загострення гарячих фаз інформаційних війн, які найчастіше реалізують і тероризм. Як правило, терористичні мотиви загроз і нападу багатогранні, а особи, які їх планують і вчиняють, досить винахідливі і прагнуть уникати свого упізнання (переконливим доказовим підтвердженням чого – терористичні акти від 11 вересня 2001 року, скоєні в США,

внаслідок яких крім 19 терористів загинуло 2977 людей, ще 24 зникли безвісти.). Для забезпечення гідної антитерористичної безпеки сучасного суспільства на міжнародному рівні було створено Цільову Групу ООН із Здійснення Контр терористичних Заходів – ЦГЗКЗ, у складі якої передбачено 38 міжнародних організацій та Інтерпол. Крім того, залучено робочу групу із захисту критично важливої інфраструктури, у сфері інтересів якої «уразливі цілі, безпека інтернету та туризму». Мандат такої групи виписаний відповідно до глобальної контр-терористичної стратегії Організації Об'єднаних Націй (A/RES60/288) [10]. На державному рівні значущість стану безпеки будь-яких сучасних об'єктів, насамперед критично-важливих (КВО) з їх інформаційними інфраструктурами та забезпеченням повноти та достовірності інформації, підтверджується прийняттям Закону України [11. Вочевидь, що різноплановий прояв тероризму, як по критичним так і по звичайним об'єктам, ускладнює систематизацію загроз та мінімізацію вразливості, як об'єктів, так і задіяного штатного персоналу. Для операторів критичної інфраструктури (ОКІ) [11, Ст.14, п.1. поз.16] визначені завдання, права та їх обов’язки [11, Ст.21], які свідчать про значну роль ОКІ в забезпеченні безпеки від потенційно можливих загроз природного, виробничого та соціального характеру проявів.

Отже, процес вироблення рекомендацій з безпеки КІ лежить у площині прояву загроз, пов'язаних як з людським фактором, так і в площині проявів техногенних аварій, включаючи їх природне походження. За тяжкістю наслідків - загрози, пов'язані з людським фактором, є найбільш непередбачуваними, тоді як результати прогнозування впливів інших проявів загроз можна змоделювати, змакетувати і, навіть, провести натурні випробування. У цьому разі, необхідно починати зі створення пізнавальної

моделі (ПМ), здатної відображати конкретику побудови і функціональні здібності (можливості) критично важливого об'єкта (КВО).

В такому випадку прийнято починати з лінгвістичного опису об'єкта пізнання, у якому повинні бути відображення його внутрішніх та зовнішніх причинно-наслідкових зв'язків, врахуючи існуючи загрози з імовірнісною оцінкою їх виникнення, що дозволяють далі забезпечити побудову структурно-логічних і функціональних схем (СЛС та СФС) ПМ.

Зазначимо, що відмінність СЛС від СФС, головним чином у тому, що перша дозволяє проводити аналіз статичної картини об'єкта пізнання із зазначенням прив'язки (локації) функціональних елементів (ланок), а друга, тобто СФС, дозволяє оцінити динамічні можливості об'єкта пізнання, оскільки, крім вказівки локації задіяних елементів і вузлів з них, відображає їхню взаємодію. Завдяки цьому існує можливість побудови конструктивних моделей для стохастичних систем з кінцевою множиною дискретних станів, що цілком і відповідає нашому гіпотетичному об'єкту у вигляді КІ з потенційними загрозами та атаками на адресу його штатного функціонування, оскільки фактично не існує обмежень щодо їх лінгвістичного опису [12]. Побудова конструктивних моделей таких стохастичних систем, лінгвістичний опис яких у процесі дослідження (пізнання) реалізовано, зводиться до системного аналізу схеми послідовного переходу від загальносистемної моделі функціонування до системної моделі, а від системної – до конструктивної. При цьому результат побудови конструктивної моделі системи з кінцевою множиною дискретних станів є синтез графа реалізації та взаємодії системних процесів, методика яких сформована на основі застосування імовірнісно-статистичних методів [13].

Таким чином, на підставі Указу Президента України

№447/2021 [14, п.5] на рис. 3.1. приведені цілі "нової якості національної системи кібербезпеки" з позицій "формування потенціалу стримування" (Ст), "набуття кіберстійкості" (Кс) та "вдосконалення взаємодії" (Вв), що мають бути досягнуті протягом періоду реалізації Стратегії Кібербезпеки України.

Згідно [11, Ст.8, п.2], "віднесення об'єктів до критичної інфраструктури здійснюється за сукупністю критеріїв, що визначають їх соціальну, політичну, економічну, екологічну значущість для забезпечення оборони країни, безпеки громадян, суспільства, держави і правопорядку, зокрема для реалізації життєво важливих функцій та надання життєво важливих послуг, свідчать про існування загроз для них, можливість виникнення кризових ситуацій через несанкціоноване втручання в їх функціонування, припинення функціонування, людський чинник чи природні лиха, тривалість робіт для усунення таких наслідків до повного відновлення штатного режиму".

На рис. 3.2) наведена, згідно Закону України №1882 [ЗУ №1882, Ст.8, п.3], деталізація належності критеріїв до ОКІ. Нажаль, критеріям властивий ймовірнісний характер, що заважає вибору оптимального варіанту захисту ОКІ, залежного від багатопрофільних аспектів експлуатації, включаючи і нечітку передбачуваність (невизначеність) довкілля. Тому зазвичай прийнято оцінювати безпеку будь-якого об'єкту з позиції його штатної експлуатаційної надійності, безвідмовності, довговічності та інших площин експлуатаційної технологічності, в основі яких, як правило, закладені конкретні багатоцільові метрологічні методики дослідження, більшість з яких задекларовані державними або галузевими стандартами, наприклад, як в [15, стор.176] та [16, стор.11], включаючи і область менеджменту інформаційної безпеки з аспектами захисту інформації через формування загальних понять і етапів управління.

На рис. 3.2) наведена, згідно Закону України №1882 [ЗУ №1882, Ст.8, п.3], деталізація належності критеріїв до ОКІ. Нажаль, критеріям властивий ймовірнісний характер, що заважає вибору оптимального варіанту захисту ОКІ, залежного від

багатопрофільних аспектів експлуатації, включаючи і нечітку передбачуваність (невизначеність) довкілля.

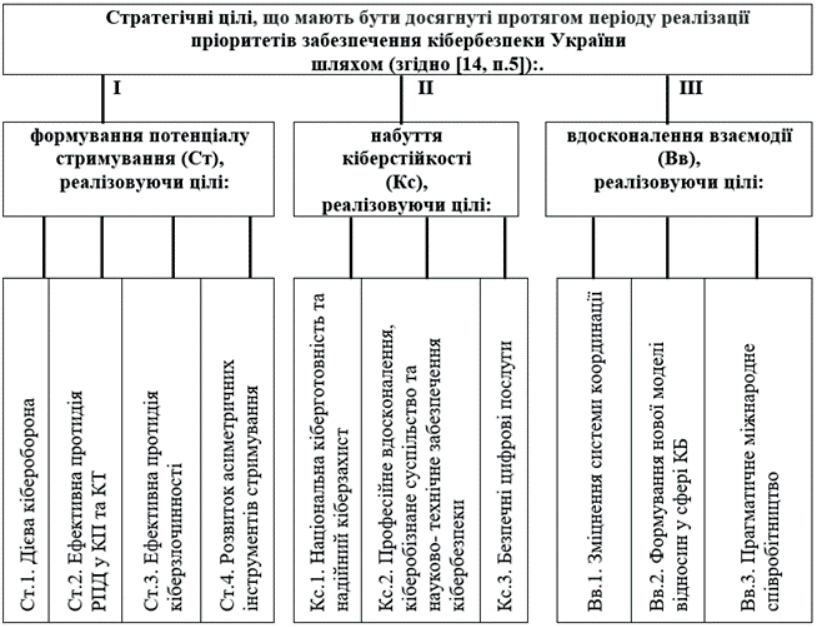

Рис. 3.1. Структурно-лінгвістична схема "Пріоритети забезпечення кібербезпеки України та стратегічні цілі," де: РПД – розвідувально-підривна діяльність, КП - кіберпростір, КТ – кібертероризм

Тому зазвичай прийнято оцінювати безпеку будь-якого об'єкту з позиції його штатної експлуатаційної надійності, безвідмовності, довговічності та інших площин експлуатаційної технологічності, в основі яких, як правило, закладені конкретні багатоцільові метрологічні методики дослідження, більшість з яких задекларовані державними або галузевими стандартами, наприклад, як в [15, стор.176] та [16, стор.11], включаючи і область менеджменту інформаційної безпеки з аспектами захисту інформації через формування загальних понять і етапів управління

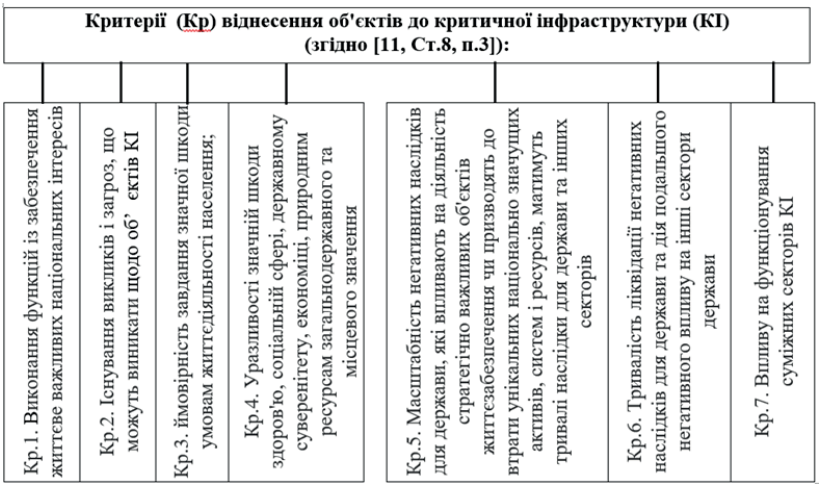

Рис. 3.2. СЛС "Критерії віднесення об'єктів до критичної інфраструктури (КІ)"

В межах організації ефективного забезпечення безпеки і непорушності системи захисту критичної інфраструктури (СЗКІ), введені сектори (С) [ЗУ №1882, Ст.9, п.3, 4] (дивись табл.3.1) та передбачено чотири режими функціонування СЗКІ: штатний; готовності та запобігання реалізації загроз; реагування на виникнення кризової ситуації; відновлення штатного функціонування [ЗУ №1882, Ст.15, п.1].

Серед основних завдань для операторів (ЗО) КІ (ОпКІ) [11, Ст.21, п.1] акцентуємо увагу на необхідність "захисту інформації про системи управління, зв'язку, фізичну безпеку та кібербезпеку" (див. табл.3.2).

Відтак, реальна безпека КВО як "Сукупності об'єктів критичної інфраструктури" (СОКІ) [ЗУ №1882, Ст.1, п.1, поз.9] залежить від штатної працездатності реалізованих систем у вигляді об'єктів кібербезпеки (ОКБ) і киберзахисту (рис.3.3) та критичної інфраструктури (рис. 3.4) з відповідним з боку ОпКІ контролем [ЗУ №1228, Ст.4, п.1, 2 та Ст.6, п.1] по отриманню,

обробці, зберіганню і передачі інформації по виділених сегментах (перешкодам) захисту із задекларованою їх експлуатаційною надійністю в умовах апріорної неоднозначності поведінки довкілля.

Таблиця 3.1 - СЛС "Сектори КІ, за порушення життєве важливих функцій та/або послуг яких, призводить до негативних наслідків"

Позначення	Зміст секторів КІ згідно [11, Ст.9, п.3, 4]
С1	Урядування та надання найважливіших адміністративних послуг
С2	Енергозабезпечення (у тому числі постачання теплової енергії)
С3	Водопостачання та водовідведення
С4	Продовольче забезпечення
С5	Охорона здоров'я
С6	Фармацевтична промисловість
С7	Виготовлення вакцин, стале функціонування біолабораторій
С8	Інформаційні послуги
С9	Електронні комунікації
С10	Фінансові послуги
С11	Транспортне забезпечення
С12	Оборона, державна безпека
С13	Правопорядок, здійснення правосуддя, тримання під вартою
С14	Цивільний захист населення та територій, служби порятунку
С15	Космічна діяльність, космічні технології та послуги
С16	Хімічна промисловість
С17	Дослідницька діяльність

Таким чином, викладений матеріал безперечно актуальний для розроблення конкретних СЛС і СФС засобів

захисту з подальшою їх реалізацією в напрямку мінімізації наслідків негативних впливів на штатну діяльність ОКІ. У зв'язку з чим нижче розглянемо методологію побудови пізнавальної гіпотетичної моделі безпеки об'єктів критичної інфраструктури з метою вивчення ефективності їх штатної діяльності та штатної секторальної життєдіяльності как сукупністі об'єктів критичної інфраструктури (СОКІ) залежно від безперервних розвідувальних (і не лише ворожих) вторгнень в непосредственную сферу кіберпростору, що захищається [18, с.38-50].

Отже, завдяки задекларованій нормативно-правовій інформації, приведеній вище, послідовно реалізуємо (згідно СЛС рис.3.1 – 3.4 та табл.3.1, 3.2) сегментарну побудову системи захисту та безпеки об'єктів критичної інфраструктури (СЗБОКІ), в якій передбачені підсистеми забезпечення фізичної безпеки (ПсФБ) та кібербезпек (ПсКБ), і система управління та зв'язку за наявності підсистеми підтримки прийняття рішень (ПсППР).

Таблиця 3.2 - СЛС " Основні завдання операторів КІ України "

Позначення	Зміст ЗО згідно [11, Ст.21, п.1]
ЗО1	Забезпечення захисту ОКІ, зокрема створення, налагодження та підтримання функціонування ефективної системи фізичної безпеки, безпеки операційних систем та кібербезпеки
ЗО2	Розроблення, оновлення та забезпечення виконання об'єктових планів заходів щодо забезпечення безпеки і стійкості критичної інфраструктури, правил управління ризиками безпеки, планів локалізації та ліквідації наслідків аварій, а також заходів кіберзахисту
ЗО3	Проведення оцінки ризиків на об'єктах критичної інфраструктури та обмін інформацією про ризики та загрози з іншими суб'єктами національної системи захисту критичної інфраструктури, а також створення умов для належного виконання правоохоронними, розвідувальними та контррозвідувальними органами своїх завдань щодо захисту критичної інфраструктури
ЗО4	Створення окремого структурного підрозділу або визначення відповідальної особи за організацію захисту критичної інфраструктури та забезпечення постійного зв'язку з відповідними суб'єктами національної системи захисту критичної інфраструктури
ЗО5	Оперативне реагування на протиправні дії, фізичні атаки, спрямовані на відключення або пошкодження роботи операційних систем чи систем забезпечення фізичної безпеки об'єкта критичної інфраструктури
ЗО6	Організація заходів з реагування на інциденти, кризові ситуації, а також ліквідації їх наслідків

Позначення	Зміст ЗО згідно [11, Ст.21, п.1]
	на ОКІ у взаємодії з іншими суб'єктами національної системи захисту критичної інфраструктури (СЗКІ)
ЗО7	Забезпечення відновлення функціонування ОКІ в разі виникнення аварій та інших небезпечних подій, вчинення протиправних дій
ЗО8	Участь у заходах із захисту повітряного простору над визначеними об'єктами критичної інфраструктури
ЗО9	Інформування органів у сфері захисту КІ про загрози та ризики диверсій, терористичних актів, актів КТ, надзвичайних ситуацій або інших подій, які небезпечни на державних об' єктах
ЗО10	Забезпечення постійного зв'язку з відповідальними за реагування на протиправні дії та з іншими компетентними організаціями та установами
ЗО11	Забезпечення постійної взаємодії з підприємствами: централізоване водопостачання, постачання теплової енергії, енергопостачання, функціонування електронних комунікаційних мереж, транспортне обслуговування, медичну допомогу, безпеку та інші послуги, від яких залежить процес реагування на кризові ситуації та відновлення функціонування ОКІ
ЗО12	Створення і використання необхідних резервів фінансових та матеріальних ресурсів для реагування на кризові ситуації та ліквідації їх наслідків
ЗО13	Проведення навчань та тренінгів, підготовка та перевірка персоналу, який відповідає за охорону, безпеку та захист ОКІ
ЗО14	Захист інформації про системи управління,

Позначення	Зміст ЗО згідно [11, Ст.21, п.1]
	зв'язку, фізичну безпеку та КБ, забезпечення відповідно до встановлених законодавством вимог конфіденційності інформації під час оброблення даних про ОКІ
ЗО15	Забезпечення захисту персоналу ОКІ, організація та здійснення евакуаційних заходів у разі виникнення надзвичайних ситуацій

Відповідно до методології побудови пізнавальної моделі КВО з СЗБОКІ також доцільне введення підсистеми розпізнавання (ПсР): кіберзлочину, кібершпигунства, кібертероризма та інших киберінцидентів, тобто подій "або ряд несприятливих подій ненавмисного характеру (природного, технічного, технологічного, помилкового, у тому числі внаслідок дії людського чинника) та/або таких, що мають ознаки можливої (потенційної) кібератаки, які становлять загрозу безпеці систем електронних комунікацій, систем управління технологічними процесами, створюють імовірність порушення штатного режиму функціонування таких систем (у тому числі зриву та/або блокування роботи системи, та/або несанкціонованого управління її ресурсами), ставлять під загрозу безпеку (захищеність) електронних інформаційних ресурсів" [17, ст.1, п.3].

Останнє свідчить про багатофакторний характер безпеки кіберпростіру (тобто середовища − "віртуальний простір, яку надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних" [17, ст.1, п.11]), де прояв різних

критерійних імовірнісних аспектів кіберзагроз істотно впливає на кінцевий вердикт людини, що приймає рішення. В такому разі "кіберзагроза − наявні та потенційно можливі явища і чинники, що створюють небезпеку життєве важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об'єктів" [17, ст.1, п.6]).

Проте, незалежно від того, що з прийняттям вище наведених нормативних документів України фактично знівелювала нев'язка в термінологічному сприйнятті використовуваних термінів, тлумачення понять «кібербезпека» і «кіберзахист» ще додатково вимагає уточнення, оскільки існує деяка відмінність між поняттями «безпека» і «захист». Зокрема, інформаційна безпека − це стан захищеності інформаційного середовища, а захист інформації − є діяльність по запобіганню просочуванню інформації, що захищається, у вигляді несанкціонованих і неумисних дій на інформацію, що захищається, тобто процес, спрямований на досягнення цього стану. Тому безпосереднє поняття захищеності об'єкту вказує на його (об'єкту) захист від зовнішніх джерел небезпеки, тоді як безпека об'єкту − це внутрішня властивість об'єкту не бути джерелом небезпеки для довкілля [19]

Очевидно, що СЛС та СФС об'єктів КЗ (ОКЗ) і КБ (ОКБ) можуть мати схожу за побудовою інформаційну схему підтримки прийняття рішень (ІСППР), оскільки відомо, що схема −це своєрідний графічний план, який визначає місце розташування основних компонентів конструкції та їх зв'язок. При цьому, процес вироблення рекомендацій з безпеки КІ лежить у площині прояву загроз, пов'язаних як з людським чинником, так і в площині проявів техногенних аварій, включаючи їх природне походження.

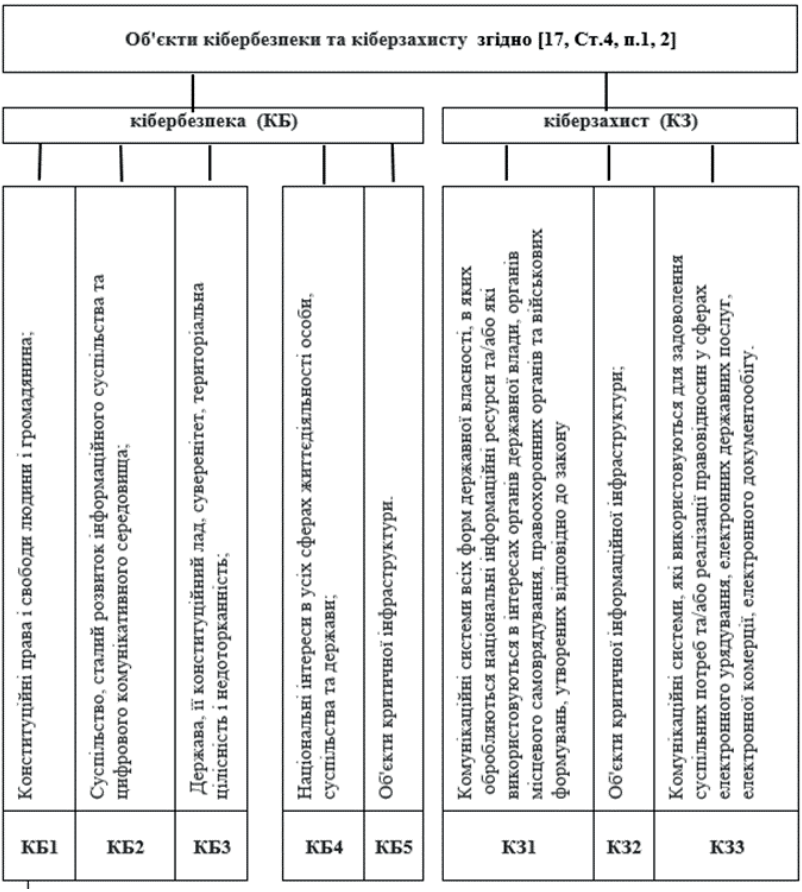

Рис. 3.3. СЛС "Об'єкти кібербезпеки та кіберзахисту"

Управління системою забезпечення захисту інформації критичної інфраструктури (ІКІ), як і у разі управління будь-якою соціально-технічною структурою [20, с.11], також пов'язане зі значними труднощами, спричиненими неповнотою інформації, конфліктами інтересів та цілей, швидкими та численними змінами у різних галузях, включаючи і здійснення інформаційної боротьби за потенційну безпеку КІ. Тому алгоритм прийняття рішень на всіх рівнях ієрархії з управління захистом ІКІ, за

аналогами з [21], має відповідати сучасним математичним моделям щодо оптимізації ієрархічних структур.

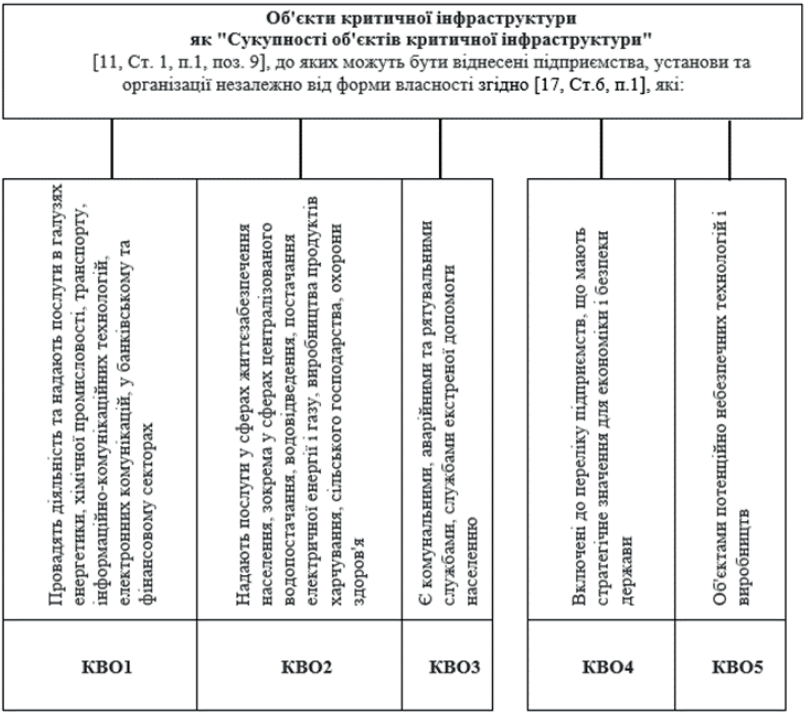

Рис. 3.4. СЛС "Сукупність об'єктів критичної інфраструктури"

Отже, основою побудови СЛС та СФС для випадку оцінювання КІ дійсно може бути лінгвістичний опис об'єкта пізнання з відображенням його внутрішніх та зовнішніх причинно-наслідкових зв'язків та врахування існуючих загроз з їхньою імовірнісною гіпотетичною оцінкою. Причому, відмінність СЛС від СФС, головним чином у тому, що перша дозволяє проводити аналіз статичної картини об'єкта пізнання із зазначенням прив'язки (локації) функціональних елементів (ланок). Друга ж, тобто СФС, дозволяє оцінити динамічні

можливості об'єкта пізнання, оскільки, крім вказівки локації задіяних елементів і вузлів з них, відображає їхню взаємодію. Завдяки цьому для стохастичних систем, лінгвістичний опис яких у процесі дослідження (пізнання) реалізовано, існує можливість побудови конструктивних моделей з елементами інтелектуальної кіберфізичної системи, що включають інженерно - взаємодіючі мережі фізичних та обчислювальних компонентів, тобто через комп'ютерні мережі і вбудовані контролери забезпечується (автономно або за участю людини) управління фізичними процесами за допомогою реалізації зворотних зв'язків [22, стор. 34].

Отже, доцільно застосування ймовірнісне-статистичних методів для оцінки стану безпеки об'єктів КІ в умовах конкретизації ймовірності випадкових недружніх для них впливів (наприклад, у вигляді ймовірності правильного виявлення або у вигляді ймовірності пропуску загрози), а їх конкретне використання може бути обрано після детального аналізу щодо аналізу СЛС та СФС побудови (у нашому випадку стану безпеки) КІ.

Очевидно, що міцність захисту залежить від тактико-технічних даних (ТТД) і тактико-технічних характеристик (ТТХ) перешкоди і вважається прийнятною, якщо вартість очікуваних витрат на її подолання порушником (хакером) перевищує вартість інформації, що захищається при дотриманні затребуваних реальних тимчасових умов з її подолання [23, с. 80-82]. Отже, якісна побудова цілісної системи захисту вже на етапі створення безпосередньої пізнавальної моделі гіпотетичного захисту від можливих інцидентів і кібератак вимагає встановлення тотожності ТТХ та механізмів функціонування об'єкта, що охороняється, до і після будь-яких нештатних (несанкціонованих) впливів на об'єкт. У подальшому аналіз такої ідентифікації (розпізнавання відмінностей до і після) доцільно використовувати при нівелювання проблем незахищеності об'єктів, що охороняються, і оптимізації при їх експлуатації.

З таких позицій в пізнавальній моделі безпеки ОКІ спільно з ПсР кіберзагроз, кіберінцидентів та кібератак необхідно передбачати як режим захисту від потенційно ворожих дій на СОКІ, так і режим представлення інформації у структурованому,

систематизованому та закодованому вигляді за допомогою системи управління і зв'язку з СЗБОКІ у вигляді символічних, графічних, візуальних, словесних та інших знаків. А оскільки кількість перешкод захисту залежить від апріорних (заздалегідь очікуваних) атак, то на противагу кожній з них мають бути передбачені свої схемотехнічні рішення, що забезпечують адекватну реалізацію відповідних перешкод захисту. Більше того, така схема методології побудови системи безпеки та захисту ОКІ (рис.3.5), має передбачати захист від передбачуваних (очікуваних) видів випадкових впливів, наприклад: у вигляді стихійних відважний та аварій; збоїв та відмов технічних засобів; навмисних та неусвідомлених помилок персоналу та користувачів, включаючи і руйнівні дії зловмисників, що використовують найширший спектр шляхів обходу та методів доступу до даних у процесі обробки та обміну інформацією. При цьому професійний аналіз апріорних видів вразливостей, включаючи безпосередньо і саму систему фізичної охорони, адекватно повинні відповідати рівню необхідної (достатньої) безпеки, методики розрахунку ефективності захисних заходів яких дуже різноманітні від рангу (ступеня допуску) інформації, що захищається, і моделі порушника

Отже, правильно побудована (адекватна реальності) модель СОКІ з його СЗБОКІ, а також модель порушника, в якій відображаються його практичні та теоретичні можливості, апріорні знання, час і місце дії та інші характеристики, є важливою складовою успішного проведення аналізу ризику та визначення вимог до складу та характеристик інтегральної системи захисту.

Проте, навіть в умовах багаторівневої системи перешкод жодна пізнавальна модель не може одночасно виконувати велику кількість завдань "захисного напрямку". Тому доцільно оцінювати ефективність будь-якої позновальної моделі в конкретному обраному аспекті її реалізації, основи більшості з яких розглянемо в наступних розділах. Зокрема, виявлення несанкціонованих повітряних атак зловмисників до підриву конкретної захисної оболонки об'єкта можливо шляхом реалізації радіолокації ближньої взаємодії (РБВ) [24, с. 66]

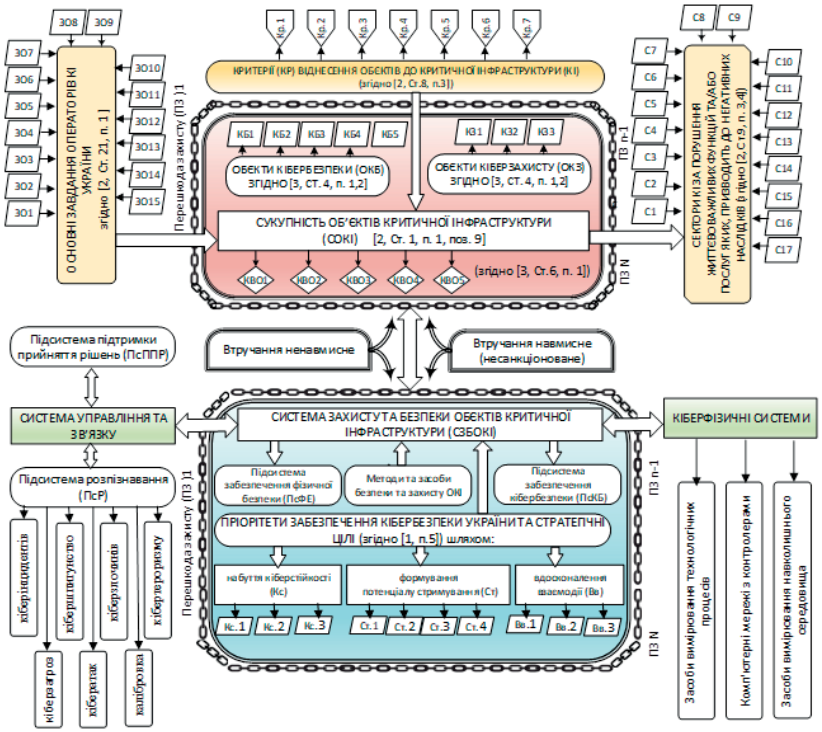

Рис. 3.5. СЛС методології побудови системи захисту та безпеки об'єктів критичної інфраструктури згідно [18, с. 38-50]

При цьому завдання загальної та параметричної ідентифікації розпізнавання потенційного втручання за допомогою дослідження гіпотетичної сигнальної аналогової дії можна звести до кореляційної обробки зондувальних та відбитих сигналів [24, с. 403], наприклад, від дронів, які вторглись у повітряну область КВО, що охороняється. В даному випадку, оптимальність вибору зондувального сигналу залежить, з одного боку, від результату апріорного аналізу його сигнальної функції та відповідного об'ємного тіла невизначеності, а з іншого боку –

від вимог забезпечення скритності самого процесу виявлення (дронів) із високою роздільною здатністю за двома параметрами −його дальності та швидкості. На закінчення вищевикладеного зазначимо, що за рахунок схемотехнічної реалізації ідеології кореляційного аналізу доцільно навіть здійснювати моніторинг кіберпростору або , що охороняється, використовуючи, наприклад, взаємно-кореляційні пристрої РБВ із безперервним шумоподібним (для приховування режиму штатного спостереження) надвисокочастотним зондувальним сигналом із будь-якою модуляцією.

Контрольні запитання до Розділу 3

1. Сформулюйте, будь ласка, своє визначення (трактування і використання) понять «організація», «система», «стан» і «емерджентність».
2. Емерджентность і синергетичність, - це синоніми чи як?
3. Що прийнято розуміти під системним аналізом та його стратегією?
4. Які прийнято виділяти етапи в системному підході?
5. Які можна виділити п'ять основних системних представлень?
6. Що таке кібернетика та у чому сенс (мета) керування (управління)?
7. Поясніть, будь ласка, що таке «рішення», «управлінське рішення»?
8. Що таке ступінь невизначеності з точки зору прийняття рішення?
9. Як можуть бути класифіковані ризиковані ситуації?
10. На які класи прийнято розбивати процес аналізу з питань ухвалення рішень?
11. Які використовуються методи в психологічних дослідженнях процесів прийняття рішень?
12. Перелічіть основні види невизначеності для суб'єктів господарювання в процесі прийняття та реалізації рішень?

13. За сукупністю яких критеріїв можуть віднести об'єкти до критичної інфраструктури?
14. Що таке лінгвістичний опис об'єкта пізнання, наприклад ОКІ?
15. Що прийнято розуміти під СЛС і СФС ОКІ?
16. Що таке сфера менеджменту інформаційної безпеки з аспектами захисту інформації шляхом реалізації юридично обґрунтованих і дозволених заходів та етапів управління?
17. Які є чотири режими функціонування СЗКІ?
18. Поясніть, будь ласка, що таке забезпечення безпеки та непорушності системи захисту критичної інфраструктури?
19. Що прийнято розуміти під моделью порушника?
20. Яке місце в системі управління підприємством посідають підсистеми забезпечення фізичної безпеки (ПсФБ), кібербезпеки (ПсКБ) і система управління та зв'язку за наявності підсистеми підтримки ухвалення рішень (ПсПППУР).

Список використаних джерел під час підготовки тексту глави 3

1. Волобуєв З. У. Безпека соціотехнічних систем. Обнінськ. Видавець: Вікінг. 2012. – 340 с.
2. Інформаційна безпека підприємства: Навчальний посібник/Н.В Гришина. - 2-е вид., Дод. - М.: Форум: НІЦ ІНФРА-М, 2015. – 240 с
3. Тарасенко Ф. П. Прикладний системний аналіз (наука та мистецтво вирішення проблем): Підручник. - Томськ; Видавництво Томського університету, 2004.186с.
4. І. Діордіца. Методологія дослідження кібербезпекової політики: кібернетичний, системний та матричний підходи. / Юридичний вісник, 2020/4, стор. 66-73.
5. О.А. Хименко, І.Ю. Єгоров. Деякі аспекти управлінського рішення в інноваційній діяльності суб’єкта підприємництва. / Наука, технології, інновації • 2019, № 3. Стор.29-41

6. Корнілова Т.В. Психологія ризику та прийняття рішень. Навчальний посібник для вишів. - М.: Аспект Прес, 2003. – 286 с.

7. Семенова К. Д. Обґрунтування господарських рішень та оцінювання ризиків: Навчальний посібник. – Одеса: ОНЕУ, ротапринт, 2013 р. – 194 с.

8. Хром'як Й.Я., Слюсарчук Ю.М., Цимбал Л.Л., Цимбал В.М. Когнітивні технології та їх особливості у менеджменті й маркетингу // Вісник Національного університету „Львівська політехніка" Менеджмент та підприємництво в Україні: етапи становлення і проблеми розвитку. – № 739 (2012). – С.233–238.

9. Організаційно термінологічні питання стосовно комплексної системи інформаційної безпеки. / Кузьменко Д.С., Тарасенко Ю.С., Луценко В.В. // Міжнародна наукова інтернет-конференція «Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення (випуск 41)». Секція «Інформаційні системи і технології». / Збірник тез доповідей: випуск 41 (м. Тернопіль, 13 вересня 2019 р.). – Тернопіль 2019. – 100 с. С.32-35.

10. Захист критично важливих об'єктів інфраструктури від терористичних атак: Збірник передового досвіду. Контртерористичне управління Організації Об'єднаних Націй (КТУ ООН) та Виконавчий директорат Контртерористичного комітету Ради Безпеки ООН (ІДКТК) Складено ІДКТК та КТУ ООН 2018.– 152 с.

11.Закон України "Про критичну інфраструктуру". Інформаційне управління Апарату Верховної Ради України. м. Київ 16 листопада 2021 року № 1882-IX. Голос України від 14.12.2021 — № 236, Урядовий кур'єр від 17.12.2021 — № 243.

12.Тарасенко Ю.С., Смірнов В.В., Соляніков В.Г. Критичні інфраструктури з позицій антитерористичної безпеки. Збірник матеріалів міжнародної наукової конференції «Інноваційні технології, моделі управління кібербезпекою - «ІТМК-2021», Дніпро, 13 – 15 грудня 2021 р. С. 27 – 29

13. Зайцев В.М. Системотехніка та системний аналіз мікросистем: метод. посібник із виконання практичних робіт для студ. спец. 1-55 01 02 «Інтегральні сенсорні системи»/В.М. Зайцев. – Мн.: БНТУ, 2005. – 50 с.

14. Указ Президента України №447/2021 «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України"

15. Барченко Н. Л., Ободяк В. К.. Система стандартів комплексних систем захисту інформації та управління інформаційною безпекою. Сучасні інформаційні технології в кібербезпеці : монографія за ред. В. К. Ободяка, І. В. Шелехова. Суми. Держ. університет 2021. С.176-193.

16. Toliupa S., Nakonechny V., Brailovskyi N.. Building cyber-security systems of information networks based on intellectual technologies. // Scientific and Practical Cyber Security Journal (SPCSJ) 1(1):10-19. Scientific Cyber Security Association (SCSA), 2017. p.11.

17. Закон України «Про основні засади забезпечення кібербезпеки України». Документ 2163-VIII. Відомості Верховної Ради (ВВР). 2017. № 45.

18.Тарасенко Ю.С., Клим В.Ю. Методологія побудови пізнавальної моделі безпеки критичної інфраструктури. стр. 38-50. Monographic series «European Science». / Prospective global scientific trends' 2022": sge11-01, Chapter 15. ScientificWorld-NetAkhatAV Karlsruhe Germany 2022 (DOI, ISBN, IndexCopernicus, Карлсруэ, Германия).

19.Тарасенко Ю.С., Соляніков В.Г., Калюжний О.Е. Концептуально-гносеологічні аспекти інформаційної безпеки (захищеності) з позицій соціальної інженерії // Системи та технології. 2020. № 2(60). С. 92-101.

20.Гітман М.Б., Столбов В.Ю., Гілязов Р.Л. Управління соціально-технічними системами з урахуванням нечітких переваг. М.: ЛЕНАНД,2011. 272 с.

21. Губко М.В. Математичні моделі оптимізації ієрархічних структур. М.: ЛЕНАНД, 2006. 264с.,

22. Ван Чунжі, Яцишин С. П., Лиса О. В., Мідик А. В. Кіберфізичні системи та їх програмне забезпечення // Вимірювальна техніка та метрологія: міжвідомчий наук.-техн. збірник. Львів: вид-во Львівської політехніки, 2018. Т. 79. № 1. С. 34-38.

23.Вострецова, Є. В. Основи інформаційної безпеки: навчальний посібник для студентів вишів. Єкатеринбург: вид-во Урал. ун-ту, 2019. 204 с

24.Тарасенко. Ю.С. Фізичні основи радіолокації: навч. посіб. Дніпро: «Пороги», 2011. 487с.

4. УРАЗЛИВІСТЬ ІНФОРМАЦІЇ, ІНФОРМАЦІЙНА ЗБРОЯ ТА ОСНОВИ ЗАХИСТУ ВІД ДЕСТАБІЛІЗУЮЧОГО ВПЛИВУ НА ІНФОРМАЦІЮ

4.1. Основи інформаційного забезпечення менеджменту, поняття інформаційного простору і складу інформації, що захищається та її класифікація за видами таємниці і ступенями конфіденційності

4.2. Визначення об'єктів захисту інформації та джерела дестабілізуючого впливу на них

4.3. Інформаційна зброя як загроза безпеці інформації в умовах дестабілізуючого впливу на неї

4.4. Основи менеджменту інформаційної безпеки та його правові аспекти

Контрольні запитання до Розділу 4

Список використаних джерел під час підготовки тексту Розділу 4:

4.1. Основи інформаційного забезпечення менеджменту, поняття інформаційного простору і складу інформації, що захищається та її класифікація за видами таємниці і ступенями конфіденційності

З вищевикладеного очевидно, що для успішної діяльності підприємств і організацій будь-якої організаційно-правової форми слід використовувати не тільки сучасні науково-технічні, соціальні та господарські методи і засоби їхньої реалізації, а й передові технології із забезпечення адекватних і надійних засобів управління на основі володіння відповідною актуальною, достовірною та захищеною службовою інформацією, що й притаманне сфері безпеки інформаційного менеджменту. При цьому сучасні форми інформаційної взаємодії в системі об’єктивного інформаційного забезпечення менеджменту передусім формують на основі документальних повідомлень або недокументованими повідомленнями, які відповідно утворюють бази даних під конкретну на даному виробництві систему

управління базами даних (СУБД), що представляє комплекс програмних і лінгвістичних засобів, які призначені для створення, зберігання, управління, використання баз даних в структурі єдиного інформаційного простору (ЄІП).

Єдиний інформаційний простір являє собою «сукупність автоматизованих інформаційних ресурсів (АІР), інформаційно-комунікаційних технологій їх формування, ведення та використання, а також організаційних механізмів, що забезпечують технологічну взаємодію учасників проекту та задоволення їх інформаційних потреб» [1, с. 75]. Побудова ЄІП здійснюється відповідно до концепції «безперервного розвитку та підтримки життєвого циклу» – CALS (Continuous Acquisition and Life cycle Support), що передбачає автоматизацію інформаційної підтримки з використанням інтелектуальних підсистем для життєвих етапів просування конкретного виробу.

На рис.4.1 наведена функціональна схема ЄІП (або структура, яка адаптовано з [1, с.76 та 2, с. 21]), в основі якої закладено процес набору баз даних (БД) і реалізації супутніх інформаційних потоків у вигляді автоматизованої системи управління технологічними процесами (АСУ ТП). Отже, під АІР доцільно розуміти бази та банки, актуалізацію доступу[*,28] та бази даних[*,29] відповідно до встановленого регламенту за допомогою інформаційно-комунікаційних технологій (ІКТ). Причому, програмні продукти джерел і приймачів даних (див. рис.4.1) принципово відрізняються один від одного, незважаючи на збіг назв використовуваних підсистем, де:

1. САПР – система автоматизованого проектування, що використовується для проектування об'єктів АСУ ТП;

2. ДУ і ЗД − підсистема диспетчерського управління і збору даних від SCADA (Supervisory Control And Data Acquisition – диспетчерське управління і збір даних);

---

*[28] Актуалізація доступу (або актуалізація прав доступу з метою підтримки безпеки та ефективності системи) – це процес, при якому користувачі мають можливість доступу до ресурсів системи тільки в тому обсязі, який їм необхідний для виконання своїх завдань.

*[29] Актуалізація бази даних – це уточнення наявних даних, як правило, про клієнтів та отримання нової інформації, необхідної для подальшої комунікації з ними.

3. ПЛК – підсистема програмованого логічного контролера;

4. Експертна система – програмний продукт підтримки прийняття рішень за даними або імітаційної моделі, або за фактичними даними, отриманими за допомогою модуля збору інформації в реальному часі;

5. Імітаційне моделювання (реалізоване за допомогою модуля імітації, що створює програмні засоби (базу апріорних знань) щодо формування вхідних/вихідних сигналів і завдання вихідних умов моделювання), призначене для подальшого апробування (порівняння) з експериментально отриманими сигналами з метою індикації попереджувальних повідомлень або рекомендацій до дії штатному оператору SCADA;

6. API (Application Programming Interface) – це програмний інтерфейс, що дозволяє використовувати внутрішні бібліотеки програм джерел і приймачів даних для формування файлів вивантаження необхідного формату і завантаження даних в програму-приймач.

Розробка інформаційної технології забезпечення взаємодії всередині ЄІП може бути забезпечена за рахунок створення механізмів, спрямованих на формування баз даних (БД) єдиного інформаційного простору. Роль таких механізмів виконують службові модулі підсистеми зберігання та обміну проектно-конструкторськими даними (ПКД):

- адміністрування;
- імпорту/експорту даних;
- конвертації ПКД;
- зберігання ПКД;
- перевірки цілісності та несуперечливості даних;
- обміну даними в реальному часі;
- журналізації;
- архівування;
- ведення службових даних проекту (дані користувачів, інформація про проект, набір правил, набір подій).

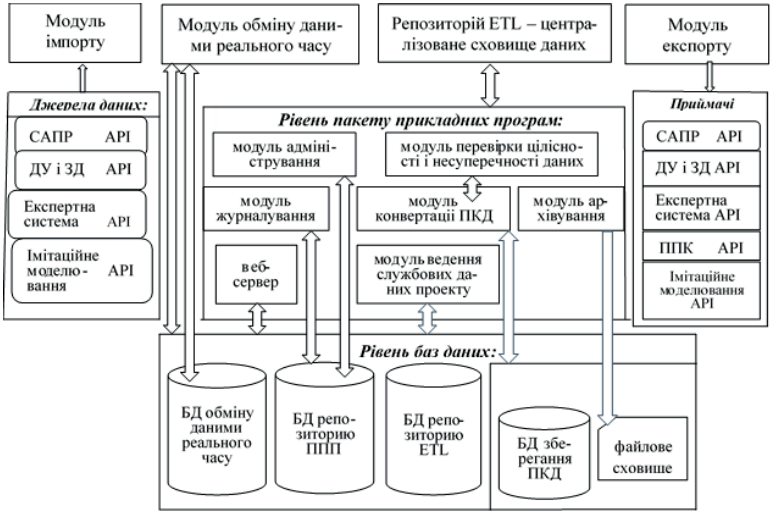

Рисунок 4.1. Структурна схема єдиного інформаційного простору з набором баз даних

Файлове сховище, зображене на рис. 4.1, призначене для зберігання вихідних файлів, отриманих з джерел даних, графічних даних та архіву журналу модуля журналювання, де пакет прикладних програм (ППП) забезпечує штатну роботу операторів SCADA з наступними базами даних (БД): − БД обміну даними в реальному часі; − БД зберігання ПКД; − БД репозиторію пакета прикладних програм[*,30] (ППП); − БД репозиторію програм обміну даними[*,31] (ETL).

[*30] Репозиторій — це універсальний термін, який може описувати різні типи сховищ даних, але найчастіше він відноситься до централізованого сховища, що використовується для зберігання та управління кодом і файлами проектів. У контексті розробки програмного забезпечення, репозиторій служить для зберігання вихідного коду, документації та інших ресурсів проекту, а також для відстеження історії змін і спільної роботи над проектом.

[*31] Репозиторій ETL (Extract, Transform, Load) – це централізоване сховище даних, призначене для зберігання інформації, отриманої з різних джерел і підготовленої для подальшого аналізу. Він (репозиторій) потім використовується для аналітики, звітності та прийняття рішень, оскільки дозволяє об'єднати дані з різних джерел, підготувати їх для аналізу та надати єдине джерело інформації для прийняття рішень.

Очевидно, що безпосередньо сам процес ухвалення рішення, як правило, реалізується в умовах дефіциту часу і на тлі потенційної вразливості використовуваної апостеріорної інформації. Оскільки процес управління – це процес планування, організації, мотивації та контролю, то при інформуванні фахівців різних рівнів (наприклад, менеджерів) у ритмі виробництва застосовується так звана технологія інформаційного забезпечення менеджменту (у вигляді обов'язкового використання інтегрованих ресурсів, як інформаційних моделей, об'єктів електронного бізнесу, а також елементів і процедур їх передання) яка звичайно включає три режими:

- ***автоматичний***, де у спеціальному масиві регламентуючої інформації, який виконує роль диспетчера, тобто направляє користувачам вихідні форми (як показник критерії втручання) з результатною інформацією в % відношенні величину можливого відхилення фактичних показників від планових, договірних, нормативних тощо, що і встановлюється за тим чи іншим об’єктом інформації для кожного менеджера з урахуванням його рангу і міри відповідальності;

- ***автоматизований***, де у спеціальному масиві регламентуючої інформації замість ознаки критерії втручання використовується ознака в який строк відповідна інформація передаватиметься на екран ПЕОМ конкретного користувача, що фактично характеризує графік інформування того або іншого менеджера чи фахівця з будь-якого об’єкта інформації. У цьому випадку в зазначений час відповідальний оператор, котрий щодня формує меню-підказку, в якій зазначається код ПЕОМ (кому), дата і час (коли), об’єкт інформації (про що), а інколи й ідентифікатори масивів, у яких містяться необхідні для інформування дані, в установленим порядком формує підсумкову (вихідну) форму у вигляді результативної інформації, яка і надсилається користувачеві на екран його ПЕОМ або на інший носій, що зазвичай зазначено в графі вид носія;

- ***консультативний,*** де у разі необхідності на екран ПЕОМ у діалоговому режимі за запитанням користувача або в змішаному режимі послідовно використовуються зазначені вище режими. Такий собі режим консультацій дозволяє здійснювати діалог користувача з ПЕОМ (сервер), який формує інформацію

про зовнішнє середовище або використовувати змішаний метод інформування, де менеджер змушений використовувати всі три режими — автоматичний (за ознакою критерії втручання), автоматизований (за ознакою в який строк) та ще режим консультацій.

Слід зауважити, що дану технологію інформаційного забезпечення вже давно використовують в системах автоматизованого проектування (САПР або CAD -Computer-Aided Design) з додатковим залученням систем автоматизації інженерних розрахунків і аналізу (CAE - Computer-aided engineering) для обробки деталей на верстатах з ЧПУ. Причому попередньо дані з CAD-систем насамперед передають в CAM (Computer-aided manufacturing) - систему автоматизованої розробки програм, а далі на виконавчі механізми по реалізації програмних продуктів для подальшого забезпечення штатної роботи верстатів.

У сучасних умовах завдання забезпечення функціонування виробничих комплексів з використанням автоматизованих робочих місць на основі застосування засобів обчислювальної техніки та контролю стану всієї системи з боку оператора (менеджера) в автоматичному, напівавтоматичному або ручному режимах вимагає надійних і ефективних рішень в частині створення вітчизняних засобів автоматизованих систем управління роботою технологічного обладнання їх об'єктів і систем (АСУ ТП). При цьому, як правило, обов'язково використовують інтегровані ресурси як інформаційних моделей елементів електронного бізнесу, і навіть елементів і процедур передачі. Тому, з урахуванням досвіду використання кращих рішень, що існують у світовій практиці в даній предметній області [2, с. 16], необхідно також розглядати комплекс систем та процедур реалізації бізнес-процесів.

На рис. 4.2 (адаптованому з [2, с. 17]) наведено структурну схему управління реалізацією бізнес-процесів, де:

− PDM (Product Data Management - управління даними про продукт) – це система, яка зберігає і управляє всією інформацією про вироби, від розробок до виробництва, що допомагає забезпечити цілісність даних, контролювати версії, поліпшити ефективність роботи і знизити витрати;

−CAD (Computer-Aided Design - управління проектуванням) - це технологія, яка використовує комп'ютерні системи для створення, модифікації, аналізу та оптимізації проектів, тобто це автоматизований процес, який використовує комп'ютерне програмне забезпечення для розробки та виготовлення різних об'єктів;

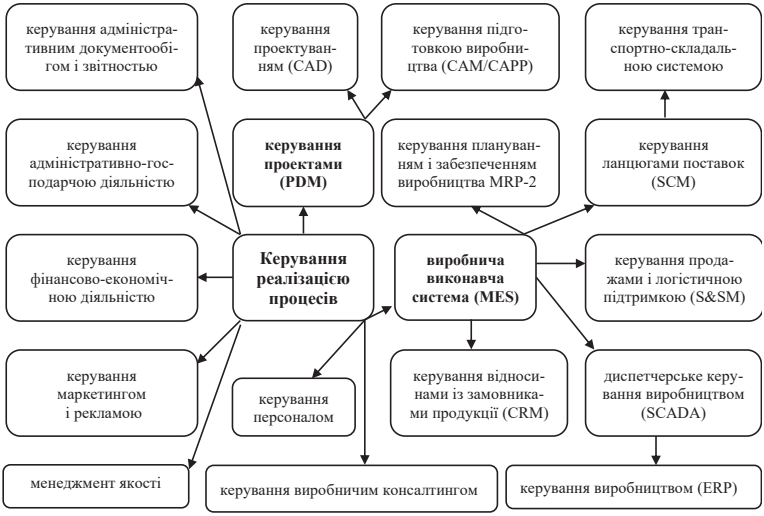

Рисунок 4.2. Структурна схема управління реалізацією бізнес-процесів

−CAM/CAPP (Computer-Aided Process Planning - комп'ютерне планування процесів) – це програмні продукти, які допомагають автоматизувати процес технологічної підготовки виробництва, тобто: проектування (планування) технологічних процесів і оформлення відповідної технологічної документації і є основою автоматизованої системи технологічної підготовки виробництва;

−MES (Manufacturing Execution System - система управління виробництвом) − це виконавча система, до завдань якої входять такі функції управління:

- ланцюгами поставок SCM (Supply Chain Management);
- транспортно-складською системою;

• плануванням і забезпеченням виробництва MRP-2 (Manufacturing

Resource Planning);

• виробництвом класу ERP (Enterprise Resource Planning) − це програмне забезпечення, яке допомагає компаніям автоматизувати та інтегрувати свої бізнес-процеси: тобто підвищити ефективність роботи підприємства, спростити процеси управління, прискорити прийняття рішень і поліпшити співпрацю між відділами;

• відносинами з замовниками продукції CRM (Customer Relationship

Management);

• продажами та логістичною підтримкою S&SM (Sales and Service

Management);

− SCADA (Supervisory Control And Data Acquisition — диспетчерське управління і збір даних) — програмний пакет, призначений для розробки або забезпечення роботи в реальному часі систем збору, обробки, відображення та архівування інформації про об'єкт моніторингу або управління. SCADA-системи використовують у всіх галузях господарства, де потрібно забезпечувати операторський контроль за технологічними процесами в реальному часі.

Таким чином, сучасна інформаційна система менеджменту кожної організації повинна бути пов'язаною з характером підприємства і політикою її загальної та інформаційної безпеки (ІБ). Останню, тобто ІБ, почнемо розглядати з уточнення поняття вразливості інформації та її класифікації за видами таємниці і ступенями конфіденційності.

Так, поняття вразливості як деякого параметра об'єкта дослідження або дії на нього характеризує можливість нанесення описуваній системі ушкоджень будь-якої природи тими чи іншими зовнішніми засобами або факторами. Уразливість нерозривно пов'язана з характеристикою «живучість», яка, згідно Б.2.2. ДСТУ 2860-94 [3], визначає «властивість об'єкта зберігати обмежену працездатність в умовах зовнішніх діянь, що призводять до відмов його складових частин. Примітка. Живучість характеризує властивість об’єкта протистояти

розвитку критичних відмов при будь-яких умовах експлуатації, включаючи і ті, що не передбачені документацією». Крім того, згідно [3]: «Живучість — це властивість, в першу чергу, як наслідок відмовостійкості об'єкта, що забезпечує здатність виконання потрібних функцій при наявності визначених відмов його складових частин. Живучість визначається «часом життя», інтервалом наробітку до виникнення критичної відмови аналогічно безвідмовності, довговічності, збережуваності». При цьому терміни «відмовостійкість» (fault tolerance) та «живучість» (survivability) «характеризують властивості об'єкта, які забезпечують надійність та безпеку об'єкта. Відмовосгійкість — це якісна характеристика об'єкта, яка забезпечується проектуванням і конструюванням, головним чином за рахунок резервування».

Відтак, ***живучість об'єкта***, – це його здатність до збереження працездатності в умовах зовнішніх впливів з боку навколишнього середовища, що виходять за межі нормальних умов експлуатації, на які був розрахований об'єкт. Серед зовнішніх впливів можна виділити особливий клас, пов'язаний з навмисними діями людини, наприклад, диверсіями. При цьому внутрішня властивість об'єкта витримувати зовнішні впливи характеризується стійкістю. Живучість же характеризує здатність функціонувати в оточуючій сфері взаємодій при заданих умовах не дивлячись на небезпеку зовнішніх впливів на розміщений об'єкт у цій сфері. Якщо об'єкт перемістити в іншу область сфери, то стійкість його залишиться незмінною, а ось живучість зміниться. Фактично ***вразливість характеризує слабкість, незахищеність об'єкта***. Оскільки вразливість проявляється за умови впливу навантаження, вона може бути названа умовною вразливістю.

Отже, для стійкості протилежною властивістю є умовна уразливість, а для живучості – безумовна уразливість (або просто вразливість). Під ***стійкістю розуміють властивість об'єкта зберігати свої параметри*** в межах встановлених допусків і виконувати свої функції під час і після зовнішніх навантажень. Залежно від виду впливу розрізняють і різні види стійкості, наприклад: електромагнітну, радіаційну, корозійну, сейсмостійкість та ін.

Характеристикою стійкості та умовної уразливості є ***критичне навантаження***, при якому, з одного боку, долається кордон стійкості, а з іншого – досягається поріг уразливості і настає руйнування. Таким чином, можна стверджувати, що у момент досягнення критичного навантаження значення стійкості збігається зі значенням уразливості.

Уразливість – слабке місце в інформаційній системі, що може привести до порушення безпеки. Розрізняють людську вразливість і технічну вразливість, що виникає в результаті несправності технологічного компонента інформаційної системи, тобто в процесі появи загроз. Загалом під загрозою прийнято розуміти потенційно можливу подію, дію (вплив), процес або явище, які можуть нанести збиток чиїмось інтересам. Під загрозою інтересам суб'єктів інформаційних відносин розуміють потенційно можливу подію, процес або явище, яке за допомогою впливу на інформацію або інші компоненти інформаційної системи може прямо або побічно призвести до нанесення шкоди інтересам даних суб'єктів.

Отже, **загроза інформаційній безпеці, – це сукупність умов і факторів, що створюють небезпеку порушення інформаційної безпеки**. На даний момент відома велика кількість різнопланових загроз безпеки інформації різного походження. Першим етапом побудови системи захисту з метою нівелювання загроз, – це визначення складу інформації, що захищається, її класифікації за видами таємниці і ступенями конфіденційності. Від того, наскільки даний етап буде виконано коректно і точно, залежить результат функціонування розроблюваної системи захисту.

Прийнято [4] всю інформацію, яка підлягає захисту, розчленовувати на відкриту (яка визначається безпосередньо власником цієї інформації), на службову (як правило, становить комерційну таємницю) та конфіденційну інформацію, тобто інформацію, що становить державну таємницю.

Нагадаємо, що тлумачення поняття «таємниця», як чогось невідомого і забороненого, що є об'єктом пізнавального інтересу, містить в собі парадокс, – для того, щоб проявляти інтерес, треба мати уявлення про об'єкт інтересу. Вирішення даного феномена в людській культурі відбувається, як правило, завдяки тому, що

таємниця зв'язується з чим-небудь відомим як його підґрунтя або пояснення. Цей принцип знаходить своє вираження у традиційному слововживанні: слово «таємниця» (а також близькі за значенням слова у вигляді «загадка», «секрет» і т. п.) вживається разом з позначенням феномена, поясненням якого повинна служити розгадка таємниці, наприклад, «таємниця матерії», «таємниця буття» і т. д. У сфері природничих наук поняття «таємниця» фактично може бути застосовано до будь-якого об'єкта дослідження, у той час як завданням гуманітарних наук іноді є модифікація або перекомпонування інформації, уже відомої соціуму і тому вона не може вважатися таємничою.

Багатовікові роздуми про причини існування і ступеня доступності таємничого привели до формування ***трьох основних підходів до розуміння таємниці:***

1) як ще непізнаного, тобто такого, що є предметом можливих майбутніх досліджень для науки, яка прогресивно розвивається, далекої перспективи пізнання;

2) як непізнаваного, тобто такого, що принципово знаходиться за межами можливостей людського пізнання, як переважаючого потенціал людського розуму в силу надмірної складності, принципової абсурдності, або відокремленості непереборними перешкодами.

3) як прихованого, тобто в принципі (комусь) відомого, але свідомо прихованого, засекреченого, зашифрованого.

Уявлення про таємницю як ще непізнанне стали буденними в наш час, як складова частина концепції позитивного прогресу знання. Сучасні традиційні погляди на перспективи природних наук містять в собі поєднання уявлень про непізнанне і непізнаване. Хоча будь-який наявний у Всесвіті порядок буття є в принципі пізнаваним, увесь Всесвіт в цілому, будучи нескінченним, принципово пізнати.

У нашому випадку, саме розуміння терміну «таємниця» як «прихованого» і буде використано у подальшому викладі матеріалу даного навчального посібника.

Таким чином можна констатувати, що державна таємниця, – це захищені державою відомості в області її військової, зовнішньополітичної, економічної, розвідувальної, контррозвідувальної і оперативно-розшукової діяльності,

поширення яких може завдати шкоди безпеці України. Очевидно, що необхідність захисту інформації пов'язана з її цінністю у сучасному соціумі. Тому конфіденційна інформація підлягає захисту від витоку і втрати, а відкрита тільки від втрати. Існує думка, що будь-яка відкрита інформація не може бути предметом захисту. Не всі згодні навіть з включенням інформації, віднесеної до державної таємниці, до складу конфіденційної. У зв'язку з чим приділимо цьому аспекту більше уваги.

Отже, захист відкритої інформації існував завжди і проводився шляхом реєстрації її носіїв, обліку їх руху і місцезнаходження, тобто створювалися безпечні умови зберігання.

Відкритість інформації не зменшує її цінності і часто потребує захисту від втрати. Цей захист не повинен бути спрямований на обмеження загальнодоступності інформації, тобто не може бути відмови в доступі до інформації, але доступ повинен здійснюватися з дотриманням вимог по її збереженню (сохранности) відповідно до вимог обробки та використання (наприклад, в бібліотеці).

Стосуючись поділу інформації з обмеженим доступом на конфіденційну і таку, що складає державну таємницю, слід зазначити наступне: 1) інформацію, віднесену до державної таємниці, прийнято називати секретною, тому що безпосередньо термін «конфіденційний» перекладається з латинської як «секретний», «довірчий»; 2) в «Конвенції про заборону розробки, виробництва, накопичення і застосування хімічної зброї та про її знищення» [5], до якої приєдналася і Україна, мова йде про інформацію, що становить державну таємницю, але її прийнято називати конфіденційною; 3) у більшості матеріалів про міжнародний інформаційний обмін [6, 7] інформація, яка може бути віднесеною до державної таємниці, поставлена в один ряд з «іншою конфіденційною інформацією».

Таким чином, буде справедливим віднести всю ту інформацію з обмеженим доступом, яка становить будь-який вид таємниці, до **конфіденційної інформації**.

Викладене вище встановлює лише межі інформації, що захищається, в межах яких повинен визначатися її склад. При вирішенні питання про віднесення конкретної інформації до

інформації, що захищається, потрібна оцінка основних критеріїв, тобто певних ознак, при наявності яких інформація може бути віднесена до інформації, що захищається.

Очевидно (як раніше вже відзначали), що спільною основою для віднесення інформації до інформації, що захищається, є її цінність, оскільки саме цінність інформації диктує необхідність її захисту. Тому критерії віднесення інформації до інформації, що захищається, є по суті **критеріями визначення її цінності**. Стосовно до відкритої інформації такими критеріями можуть бути:

- необхідність інформації для правового забезпечення діяльності підприємства. Це відноситься до документованої інформації, яка регламентує статус підприємства, права, обов'язки і відповідальність його працівників;

- необхідність інформації для виробничої діяльності (що стосується інформації, що відноситься до науково-дослідницької, проектної, конструкторської, технологічної, торгової і інших сфер виробничої діяльності);

- необхідність інформації для управлінської діяльності, сюди відноситься інформація, яка потрібна для прийняття управлінських рішень, а також для організації виробничої діяльності та забезпечення її функціонування;

- необхідність інформації для фінансової діяльності;

- необхідність інформації для забезпечення функціонування соціальної сфери;

- необхідність інформації як доказового джерела на випадок виникнення конфліктних ситуацій;

- важливість інформації як історичного джерела, що розкриває напрямки та особливості діяльності підприємства.

Ці критерії обумовлюють необхідність захисту відкритої інформації від втрати. Вони ж викликають потребу в захисті від втрати і конфіденційної інформації.

Головним, визначальним критерієм віднесення інформації до конфіденційної і захисту її від витоку є можливість отримання переваг від використання інформації за рахунок невідомості її третім особам. Цей критерій має як би дві складові: невідомість інформації третім особам і отримання переваг в силу цієї невідомості.

Дані складові взаємопов'язані і взаємозумовлені, оскільки, з одного боку, невідомість інформації третім особам сама по собі нічого не означає, якщо не забезпечує отримання переваг, а з іншого – переваги можна отримати тільки за рахунок такої невідомості.

Конфіденційність є правовою формою і одночасно інструментом забезпечення невідомості інформації.

Переваги від використання інформації, невідомої третім особам, можуть полягати в отриманні вигоди або запобіганні збитку, мати, залежно від областей і видів діяльності, політичні, військові, економічні, моральні та інші характеристики, виражатися кількісними і якісними показниками.

Очевидно, що захист державної таємниці є одним з найважливіших в реалізації її інтересів, а від правильного розуміння і понятійного визначення самого терміну багато в чому залежить і політика керівництва країни в цій галузі захисту секретів. Тут же лише викладені понятійні уявлення і основні методологічні аспекти побудови КСЗІ, зайвий раз підтверджуючи, що процес утворення відповідає принципу від простого до складного. Відповідно до законодавства країни до державної таємниці відносять відомості в області військової, зовнішньополітичної, економічної, розвідувальної, контррозвідувальної і оперативно-розшукової діяльності держави, поширення яких може завдати шкоди безпеці України, а також органів виконавчої влади та інших організацій (далі іменуються державними органами), наділених повноваженнями щодо розпорядження цими відомостями.

До переліку основних ***відомостей конфіденційного характеру*** включені:

- відомості про факти, події і обставини приватного життя громадянина, що дозволяють ідентифікувати його особу (персональні дані), за винятком відомостей, що підлягають поширенню у засобах масової інформації у встановлених законами випадках;
- відомості, що становлять таємницю слідства і судочинства;

- службові відомості, доступ до яких обмежений органами державної влади відповідно до законів держави (службова таємниця);

- відомості, пов'язані з професійною діяльністю, доступ до яких обмежено відповідно до Конституції і державними законами (лікарська, нотаріальна, адвокатська таємниця, таємниця листування, телефонних переговорів, поштових відправлень, телеграфних або інших повідомлень і так далі);

- відомості про сутність винаходу, корисної моделі чи промислового зразка до офіційної публікації інформації про них;

- відомості, пов'язані з комерційною діяльністю, доступ до яких обмежено відповідно до державних законів про комерційну таємницю.

У свою чергу, **комерційна таємниця** це:

- інформація конфіденційного рівня, що дозволяє її власникові при існуючих і/або можливих обставинах збільшити доходи, уникнути невиправданих витрат, зберегти положення на ринку товарів, робіт, послуг або отримати іншу комерційну вигоду, а також інформація, що становить комерційну таємницю;

- науково-технічна, технологічна, виробнича, фінансово-економічна або інша інформація (у тому числі та, що складає секрети виробництва), яка має дійсну або потенційну комерційну цінність у силу невідомості її третім особам, до якої немає вільного доступу на законній підставі й у відношенні якої власником такої інформації введений режим комерційної таємниці.

Причому право віднесення інформації до комерційної таємниці, як і встановлення режиму захисту комерційної таємниці в цілому, надається власникові комерційної таємниці. Процедура захисту інформації, що становить комерційну таємницю, повинна здійснюватися її володарем, а безпосередньо склад відомостей, що відображають дану таємницю і будь-яку сферу економічної діяльності, визначається тим же володарем комерційної таємниці або, згідно з договором, конфідентом комерційної таємниці.

4.2. Визначення об'єктів захисту інформації та джерела дестабілізуючого впливу на них

З викладеного вище напрошується висновок про те, що захист інформації має бути системним, що містить різні взаємопов'язані компоненти і функції управління життєвими циклами соціуму в інформаційному просторі (див. рис.4.3, **адаптованому з [2, с.15])** В контексті подальшого викладу найважливішим із цих компонентів є об'єкти захисту, бо від їхнього складу залежать і методи, і засоби захисту, і розв'язання адекватних завдань щодо захисних заходів від апріорних надзвичайних пригод, вельми деструктивних для штатної роботи підприємства.

Інформація є предметом захисту, але захищати її як таку неможливо, оскільки вона не існує сама по собі, а фіксується (відображається) у певних матеріальних об'єктах або пам'яті людей, які виступають в ролі її носіїв і складають основний, базовий об'єкт захисту. Отже, носієм інформації може виступати або фізична особа або матеріальний об'єкт, у тому числі фізичне поле, в яких інформація знаходить своє відображення у вигляді символів, образів, сигналів, технічних рішень і процесів. З носія інформації можливо (але не обов'язково) читання наявної (записаної) інформації. Для запису як секретної, так і несекретної інформації використовуються одні й ті ж носії.

Як правило, носії секретної та конфіденційної інформації охороняються власником цієї інформації. Найчастіше сам носій інформації розміщується в захисну оболонку, яка підвищує його збереження і, відповідно, надійність збереження інформації.

Носії інформації, що захищається, можна реалізувати у вигляді: документів; виробів (предметів); речовин і матеріалів; електромагнітних, теплових, радіаційних та інших випромінювань; акустичних, електромагнітних, гравітаційних та інших полів і т. п.

Особливим носієм інформації є людина, мозок якої представляє виключно складну систему, що зберігає і переробляє інформацію, що надходить із зовнішнього світу. Властивість мозку відображати і пізнавати зовнішній світ, накопичувати в

пам'яті колосальні обсяги інформації ставлять людину на особливе місце як носія інформації. Людина має можливість генерувати нову інформацію. І як носій інформації він володіє позитивними і негативними рисами.

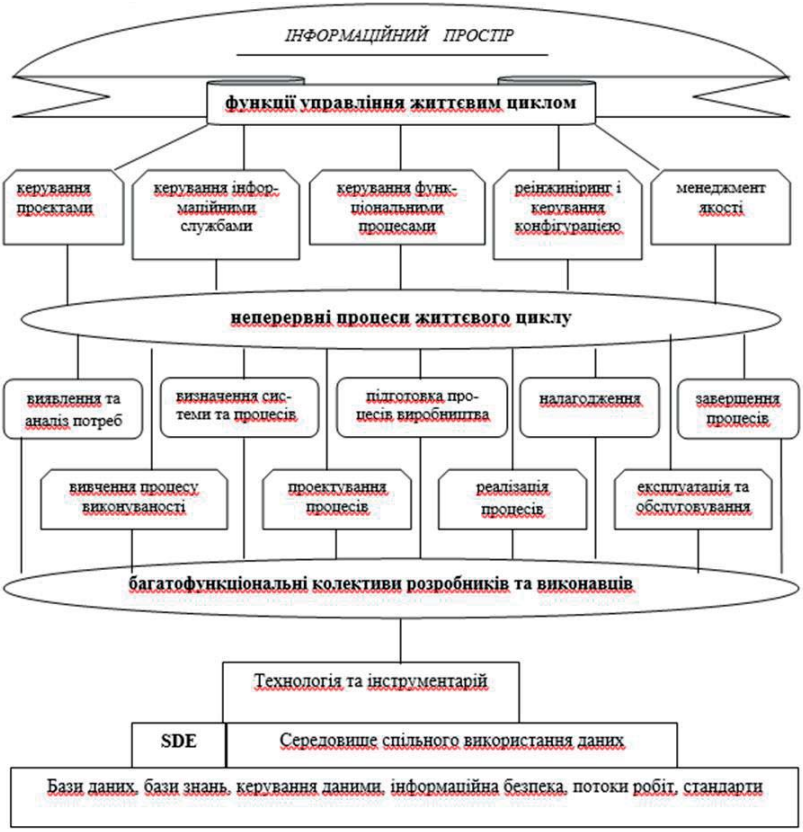

Рисунок 4.3. Структурно-функціональна схема забезпечення адекватного керівництва з реалізації штатного функціонування підприємством через зміну конфігурації підвідомчих виробничих об'єктів і соціальних процесів в них

Позитивні – без згоди суб'єкта-носія інформації, що захищається, з його пам'яті, як правило, ніяка інформація не може

бути вилучена. Він може оцінювати важливість наявної у нього інформації і відповідно до цього поводитися з нею. Він може ранжувати споживачів інформації, що захищається, тобто знати, кому і яку інформацію він може довірити.

Негативні – він може помилятися щодо істинності споживача інформації, що захищається, або навмисне не зберігати довірену йому інформацію.

Серед найбільш поширених ***видів носіїв конфіденційної інформації*** можна виділити наступні:

- паперові носії, в яких інформація, що відображається у вигляді символів і образів, фіксується рукописним, машинописним, електронним, типографським та іншими способами у формі тексту, креслення, схеми, формули і т. п.;

- магнітні носії у вигляді відеокасет (відеоплівок) або аудіокасет (аудіоплівок) для магнітофонів і диктофонів. Для відеомагнітофонів та деяких відеокамер можуть використовувати жорсткі (тверді) диски, дискети, магнітні стрічки. У цих носіях інформація фіксується (наноситься) за допомогою магнітного накопичення (запису сигналів), що здійснюється магнітним пристроєм, а відображається у вигляді символів. Відтворення (зчитування) інформації здійснюється також магнітним пристроєм за допомогою відновлення сигналів;

- магнітооптичні і оптичні носії (лазерні диски, компакт-диски). Запис даних у них виконується лазерним променем (у магнітооптичних і магнітним полем), інформація відображається у вигляді символів, а її зчитування (відтворення) здійснюється за допомогою лазерного променю.

Крім того, продукція, що випускається (назвемо це як вироби), виконуючи своє пряме призначення, одночасно може бути носієм інформації, що захищається. Не слід забувати, що безпосередньо самі технологічні процеси виготовлення продукції включають у себе як технологію виробництва продукції, так і компоненти, що застосовуються при її виготовленні (засоби виробництва): обладнання, прилади, матеріали, речовини, сировину, паливо та інше також є носіями інформації. У цьому випадку інформація відображається у вигляді технічних процесів (перша складова) і технічних рішень (друга складова). Перспективним носієм інформації є фізичні поля, у яких

інформація фіксується шляхом зміни їх інтенсивності, кількісних характеристик і відображається у вигляді сигналів, а в електромагнітних полях, – у вигляді образів.

Носії конфіденційної інформації як об'єкти захисту повинні захищатися, у залежності від їх видів, від несанкціонованого доступу до них, від втрати і від витоку інформації, яка міститься в них.

Але, щоб забезпечити захист, необхідно захищати і об'єкти, які є підступами до носіїв, і їх захист виступає в ролі певних рубежів захисту носіїв. І чим таких рубежів більше, чим складніше їх подолати, тим надійніше забезпечується захист носіїв.

В якості першого рубежу прийнято розглядати прилеглу до підприємства територію, яка повинна бути захищеною від несанкціонованого проникнення осіб до будівель підприємства і відходів виробництва (при наявності відходів). Наступним об'єктом захисту є будівлі підприємства. Їх захист здійснюється тими ж способами і переслідують ту ж мету, що і охорона території. Захист будівель є другим рубежем захисту носіїв. Наступний об'єкт захисту – це приміщення, в яких розташовані сховища носіїв інформації, їх обробка, а також здійснюється управлінсько-виробнича діяльність з використанням цих носіїв. Ці приміщення повинні бути захищені від несанкціонованого проникнення, від візуального спостереження за носіями, а також, у разі необхідності, від прослуховування конфіденційних розмов, що ведуться у них. Захист забезпечується працюючими в приміщеннях співробітниками, різними технічними засобами, у тому числі в неробочий час, – засобами охоронної сигналізації.

Крім того, ***об'єктами захисту*** повинні бути:

- ***засоби відображення, обробки, відтворення і передачі конфіденційної інформації,*** в тому числі ЕОМ, які повинні захищатися від несанкціонованого підключення, побічних електромагнітних випромінювань, зараження вірусом, електронних закладок, візуального спостереження, виведення з ладу, порушення режиму роботи;

- ***копіювально-розмножувальна техніка***, що захищається від візуального спостереження і побічних електромагнітних випромінювань під час обробки інформації; засоби відео-

звукозаписувальної та відтворювальної техніки, які вимагають захисту від прослуховування, візуального спостереження і побічних електромагнітних випромінювань;

- засоби транспортування носіїв конфіденційної інформації, що підлягають захисту від проникнення сторонніх осіб до носіїв або їх знищення під час транспортування;

- засоби радіо- і кабельного зв'язку, радіомовлення і телебачення, які використовуються для передачі конфіденційної інформації, які захищаються від прослуховування, виведення з ладу, порушення режиму роботи;

- системи забезпечення функціонування підприємства (електро та водопостачання, кондиціонування та ін.), які повинні захищатися від використання їх для виведення з ладу засобів обробки і передачі інформації, прослуховування конфіденційних розмов, візуального спостереження за носіями;

- технічні засоби захисту інформації та контролю за ними, що вимагають захисту від несанкціонованого доступу з метою виведення їх з ладу.

Очевидно, що говорити про безпеку об'єкта (системи) можна, лише маючи на увазі, що за допомогою цього об'єкта або над цим об'єктом відбуваються якісь дії. У цьому сенсі, якщо об'єкт не діє, а саме не функціонує (не використовується, не розвивається і т. д.), або, кажучи іншими словами, не взаємодіє з зовнішнім середовищем, то і розглядати його безпеку безглуздо. Отже, об'єкт необхідно розглядати в динаміці та у взаємодії із зовнішнім середовищем.

У деяких випадках можна говорити про безпеку системи при її збереженості. Але навіть при збережуваності системи взаємодія з зовнішнім середовищем неминуча. При функціонуванні об'єкта завжди переслідуються певні цілі. Сукупність дій, що здійснюються об'єктом, для досягнення певної цілі реалізується у вигляді результатів, які мають значення для самого об'єкта. Якщо ціль операції або сукупності цілеспрямованих дій досягнута, то безпеку операції, а отже, і інформації, що циркулює в системі, забезпечено.

Проблема дослідження критичних ситуацій і факторів, які можуть становити певну небезпеку для інформації, а також пошуку та обґрунтування комплексу заходів і засобів щодо їх

виключення або зниження, характеризується наступними особливостями:

- великою кількістю факторів небезпечних ситуацій і необхідністю виявлення джерел і причин їх виникнення;

- необхідністю виявлення і вивчення повного спектру можливих заходів і засобів нівелювання небезпечних факторів з метою забезпечення безпеки.

Фактично [8, 9], загроза інформації обумовлена цілком визначеними факторами, сукупністю явищ і умов, які можуть скластися у конкретній ситуації.

Носіями загроз безпеці інформації є **джерела загроз**. Як джерела загроз можуть виступати як суб'єкти (особистість), так і об'єктивні прояви, наприклад, конкуренти, злочинці, корупціонери, адміністративно-управлінські органи. Джерела загроз переслідують при цьому наступні цілі: ознайомлення з охоронюваними відомостями, їх модифікація в корисливих цілях і знищення для нанесення прямих матеріальних збитків.

Таким чином, по відношенню до інформаційної системи **всю множину загроз можна розбити на дві групи:** *зовнішні та внутрішні*, кожна з яких, у свою чергу, ділиться на *умисні й випадкові загрози*, які можуть бути *явними і прихованими.*

Виявлення та аналіз загроз інформації, що захищається, є відповідальним етапом при побудові системи захисту інформації на підприємстві. Більшість фахівців вживають термін «загрози безпеки інформації». Але безпека інформації – це стан захищеності інформації від впливів, що порушують її статус.

Отже, безпека інформації означає, що інформація знаходиться у такому захищеному вигляді, який здатний протистояти будь-яким дестабілізуючим впливам.

Будь-яка загроза не зводиться до чогось однозначного, вона складається з певних взаємопов'язаних компонентів, кожен з яких сам по собі не створює загрозу, але є невід'ємною частиною її, загроза ж виникає лише при сукупному їх взаємодії. Загрози інформації, якій необхідний захист, як було зазначено вище, пов'язані з її вразливістю, тобто нездатністю інформації самостійно протистояти дестабілізуючим впливам, таким, що порушує її статус.

Реалізація загроз призводить, в залежності від їх характеру, до однієї або кількох форм прояву уразливості інформації. При цьому кожній з форм прояву уразливості (або декільком з них) притаманні певні, що мають відношення тільки до них загрози з набором відповідних компонентів, тобто структура конкретної загрози зумовлює конкретну форму.

Однак повинна існувати і загальна, як би типова структура загроз, яка складає основу конкретних загроз. Ця загальна структура повинна базуватися на певних ознаках, характерних для загрози інформації, що захищається.

Перш за все, загроза повинна мати якісь сутнісні прояви. А будь-який прояв, виявлення чогось прийнято називати явищем. Отже, однією з ознак і разом з тим однією зі складових загрози повинні бути явища. Але в основі будь-якого явища лежать відповідні причини, які є його рушійною силою і які, в свою чергу, обумовлені певними обставинами або передумовами. Ці причини і обставини (передумови) відносяться до факторів, що створюють можливість дестабілізуючого впливу на інформацію. Таким чином, фактори є ще однією ознакою і другою складовою загрози.

Разом з тим фактори можуть стати спонукальною силою для явищ, а останні можуть «спрацювати» лише при наявності певних умов (обстановки) для цього. Наявність умов для дестабілізуючого впливу на інформацію є третьою ознакою і ще однієї складовою загрози.

Визначальною ознакою загрози є її спрямованість, результат, до якого може привести дестабілізуючий вплив на інформацію. Цим результатом у всіх випадках реалізації загрози є порушення статусу інформації.

Таким чином, загроза інформації, що захищається, – це сукупність явищ, факторів і умов, що створюють небезпеку порушення статусу інформації.

До явищ, тобто до ***сутнісних проявів загрози***, відносяться:

- *джерела дестабілізуючого впливу* на інформацію (від кого або від чого виходить дестабілізуючий вплив);

- *види дестабілізуючого впливу* на інформацію (яким чином (за якими напрямами) відбувається дестабілізуючий вплив);

- *способи дестабілізуючого впливу* на інформацію (якими прийомами, діями здійснюються (реалізуються) види дестабілізуючого впливу).

До факторів, крім причин і обставин, слід віднести наявність каналів і методів реалізації несанкціонованого доступу до конфіденційної інформації для впливу на інформацію з боку осіб, які не мають до неї дозволеного доступу (див. Розділ 5).

Що стосується складу структурних частин загрози, то необхідно підкреслити: стрижневими, вихідними є джерела дестабілізуючого впливу на інформацію, від їх складу залежать і види, і способи, і кінцевий результат впливу. Хоча склад інших структурних частин загрози також грає істотну роль, він на відміну від джерел не носить визначального характеру і прямо залежить від джерел. Разом з тим ще раз слід зазначити, що джерела самі по собі не є загрозою, якщо від них не відбувається тих чи інших впливів, але їх різноманіття вражає.

Всі **джерела загроз** інформаційній безпеці можна розділити на **три основні групи** [4, 9]:

- обумовлені діями суб'єкта (антропогенні джерела) – суб'єкти, дії яких можуть призвести до порушення безпеки інформації, дані дії можуть бути кваліфіковані як умисні або випадкові злочини. Джерела, дії яких можуть призвести до порушення безпеки інформації можуть бути як зовнішніми так і внутрішніми. Дані джерела можна спрогнозувати, і вжити адекватних заходів;

- стихійні джерела – дана група об'єднує обставини, що становлять непереборну силу (стихійні лиха або інші обставини, які неможливо передбачити або запобігти або можливо передбачити, але неможливо запобігти), такі обставини, які носять об'єктивний і абсолютний характер, що поширюється на всіх. Такі джерела загроз абсолютно не піддаються прогнозуванню і, тому заходи проти них повинні застосовуватися завжди. Стихійні джерела, як правило, є зовнішніми відносно об’єкта, що захищається, і під ними, як правило, розуміються природні катаклізми;

- обумовлені технічними засобами (техногенні джерела) – ці джерела загроз менш прогнозовані, безпосередньо залежать від властивостей техніки і тому вимагають особливої уваги. До них,

як до джерел дестабілізуючого впливу на інформацію, слід віднести: технічні засоби відображення (фіксації), збереження, обробки, відтворення, передачі інформації і засоби зв'язку; системи забезпечення функціонування технічних засобів відображення, зберігання, обробки, відтворення і передачі інформації; технологічні процеси окремих категорій промислових об'єктів; природні явища і людський фактор.

Серед перерахованих найпоширенішим, різноманітним і небезпечним ***джерелом дестабілізуючого впливу*** на інформацію, яка захищається, є ***люди***, яких можна віднести до таких ***категорій:***

1) до співробітників даного підприємства; до осіб, які не працюють на підприємстві, але мають доступ до інформації підприємства, що захищається, в силу службового становища (з вищих, суміжних (в тому числі посередницьких) підприємств, контролюючих органів державної і муніципальної влади та ін.);

2) до співробітників державних органів розвідки інших країн і розвідувальних служб конкуруючих вітчизняних та зарубіжних підприємств;

3) до осіб з кримінальних структур.

У частині співвідношення з видами і способами дестабілізуючого впливу на інформацію ці категорії людей поділяються на **дві групи:** ті, що мають доступ до носіїв даної інформації, що захищається, технічних засобів її відображення, зберігання, обробки, відтворення, передачі і системам забезпечення їх функціонування і ті, що не мають такого.

Людський фактор є найрізноманітнішим, тому що в порівнянні з іншими джерелами, йому притаманна значно більша кількість видів і способів дестабілізуючого впливу на інформацію. Він же є і найнебезпечнішим, тому що він наймасовіший, його вплив з боку носить не епізодичний, а постійний характер і його вплив може бути не тільки ненавмисним, як з боку інших джерел, а навпаки свідомо навмисним, в результаті чого спричинений ним вплив може призвести до всіх форм прояву уразливості інформації (з боку ж інших джерел, – тільки до окремих форм).

Технічні засоби відображення, зберігання, обробки, відтворення, передачі інформації та засоби зв'язку є другим за

значенням ***джерелом дестабілізуючого впливу*** на інформацію, яка вимагає захисту, в силу їхнього різноманіття, а також існуючих з їх боку способів дестабілізуючого впливу. До цього джерела прийнято відносити: електронно-обчислювальну техніку; електричні та автоматичні друкарські машинки і копіювально-розмножувальну техніку; засоби відео- та звукозаписувальної та відтворювальної апаратури; засоби телефонної, телеграфної, факсимільної, гучномовної передачі інформації; засоби телекомунікацій, радіомовлення і телебачення.

До наступного джерела дестабілізуючого впливу на інформацію слід віднести системи електропостачання, водопостачання, теплопостачання, кондиціонування. На особливу увагу заслуговують технологічні процеси об'єктів ядерної енергетики, хімічної промисловості, радіоелектроніки, а також об'єктів з виготовлення деяких видів озброєння і військової техніки, які змінюють природну структуру оточуючого об'єкт середовища. Нарешті, самі природні явища у вигляді стихійних лих і атмосферних проявів найчастіше є дестабілізуючими діями на інформацію.

4.3. Інформаційна зброя як загроза безпеці інформації в умовах дестабілізуючого впливу на неї

Очевидно, що сучасному соціуму притаманне використання інформаційних і комунікаційних технологій на тлі стрімкого вдосконалення обчислювальних систем і систем зв'язку з близькою перспективою освоєння навіть рівня квантової реалізації. Однак, на жаль, збільшуються й негативні впливи на світову спільноту в багатьох галузях їхньої життєдіяльності, включно з інформаційною сферою буття. Зокрема, завершуючи виклад питань уразливості інформації, нижче висвітлимо широко обговорювану на різних рівнях проблему інформаційної зброї [10].

Почнемо з тези про те, що інформаційна залежність усіх сфер сучасної життєдіяльності суспільства і держави є надзвичайно високою. Так за оцінками американських експертів

порушення роботи комп'ютерних мереж, що використовуються у системах управління державними і банківськими структурами США, шляхом виведення з ладу обчислювальних і телекомунікаційних засобів або знищення інформації, яка зберігається в мережах, здатне завдати економіці країни настільки серйозної шкоди, що його можна порівнювати зі збитком від застосування проти США ядерної зброї.

Спочатку термін ***«інформаційна війна»*** з'явився і використовувався в американських військових колах. **Інформаційна війна – це перш за все психологічний тиск на все суспільство або його частину.** Вміла подача необхідної інформації допомагає створити певні настрої і викликати потрібну реакцію.

Інформаційна війна може вестися як усередині держави, так і між різними країнами і є частиною складного процесу протиборства. Наявність інформаційного тиску на суспільство є показником закулісних політичних дій або підготовкою до будь-яких змін. Вона не вимагає великих фінансових вкладень і зусиль. Ефективність інформаційної війни залежить від правильно складеної агітації, що спирається на почуття і бажання членів соціума [11].

Суть інформаційної війни полягає у впливі на суспільство за допомогою інформації. До ***<u>ознак інформаційної війни</u>*** належать:

- обмеження доступу до певної інформації: закриття веб-ресурсів, телевізійних програм, друкованих видань;
- поява різних інформаційних джерел з однаковою інформацією;
- створення негативного психологічного фону з конкретних питань;
- поява в суспільстві емоційної напруженості;
- проникнення насаджуваної інформації в різні сфери суспільства: політику, культуру, бізнес, освіту.

Інформаційні війни між країнами стали звичайним явищем. Хоча про використання у військових конфліктах інформаційної пропаганди відомо ще з 19 століття, особливу силу цей вид війни набув в кінці 20-го століття. Це пов'язано зі збільшенням кількості інформаційних ресурсів: газет, журналів, телепередач, веб-ресурсів. ***Чим більше інформації має суспільство у***

вільному доступі, тим легше проводити інформаційну пропаганду.

Для ведення інформаційної війни немає необхідності переконувати людей або нав'язувати їм свою точку зору. Треба просто зробити так, щоб навіювана інформація потрапляла на очі якомога частіше і не викликала відторгнення. При цьому людина може і не підозрювати, що стала учасником інформаційного впливу. Для ведення інформаційної війни наймають фахівців, що мають глибокі знання з маркетингу, соціальної психології, політики та історії.

Ведення інформаційної війни є однією зі складових політики багатьох держав. Бій за людські уми не є самоціллю, а відноситься до комплексу заходів щодо збереження безпеки своєї держави або щодо впливу на громадян іншої держави. Виходячи з цього, **інформаційна війна** має такі **цілі:**

- забезпечення безпеки своєї держави;
- підтримка патріотичних настроїв;
- вплив на громадян іншої держави з метою дезінформації і досягнення певних цілей.

При цьому, інформаційна війна може застосовуватися і серед військових, і серед мирного населення. Для цього може використовуватися один з видів інформаційної війни або комплекс заходів. До ***видів інформаційного протистояння*** відносяться:

- *інформаційна війна в інтернеті* – пропонується різна і часто суперечлива інформація, що застосовується для заплутування супротивника;
- *психологічні операції* – підбір і подача такої інформації, яка звучить як контраргумент на настрої, що існують в суспільстві;
- *дезінформація* – просування неправдивої інформації з метою спрямування ворожої сторони по неправильному сліду;
- *руйнування* – фізичне знищення або блокування електронних систем, важливих для противника;
- *заходи безпеки* – посилення охорони своїх ресурсів з метою збереження планів і намірів;
- *прямі інформаційні атаки* – змішування помилкової та правдивої інформації.

- *інформаційна війна в ЗМІ.*

Інформаційну війну називають холодною, тому що вона призводить до бажаних результатів без застосування класичного зброї. Існують ***напрямки ведення інформаційної війни*** серед мирного населення у вигляді реалізації:

- методу «участь авторитетів», суть якого полягає в підтримці необхідних дій або гасел відомими авторитетними людьми;

- методу «точні твердження», у якому бажані гасла подаються як стовідсотково вірні і такі, що не потребують доказів;

- методу «переможна сторона», де суспільству пропонують вибрати рішення, яке подається як найкраще і є виграшним;

- методу «примусу», який часто застосовується у гаслах і звучить як точна вказівка до дії;

- методу «підміни джерела інформації», коли не виходить зупинити проникнення небажаної інформації, її автором називають джерело, який не користується довірою у суспільства.

Як правило, інформаційна війна ефективно застосовується в політичній сфері. З її допомогою претенденти на посаду борються за голоси виборців. З огляду на той факт, що більшість виборців не має доступу до правдивої інформації, для впливу на них застосовуються техніки психологічного впливу. Інформаційна війна в ЗМІ є популярним способом впливу на суспільство. У цьому випадку в політичній пропаганді може використовуватися метод підміни інформації, спотворення дійсності, примусу, участі авторитетів.

Очевидно, що інформаційна війна використовується у різних сферах. Завдяки сучасним технологіям інформаційні війни нашого часу можуть вестися по всьому світу. При цьому з'явилася можливість створювати реальність, яка не відповідає дійсності. Сучасні світові інформаційні війни ведуться як між державами, так і всередині держави, між політиками, компаніями, організаціями, релігійними деномінаціями. Такі війни в політиці мають на меті дискредитувати опонента в очах громадськості і сформувати у членів суспільства необхідну

думку. Для вирішення цих завдань наймають фахівців з інформаційних диверсій – айворщиків, які виробляють атаку на опонента за допомогою різних інформаційних джерел.

Основними методами інформаційних атак є: монтаж, чутки, міфи, погроза, блеф, перекручування інформації. При цьому основною зброєю в інформаційній війні виступають засоби масової інформації (ЗМІ). Повний контроль над ними дозволяє подати суспільству лише ту інформацію, яка сформує необхідний погляд на проблему. Наприклад, всі бойові дії у сучасному світі висвітлюються в ЗМІ таким чином, щоб показати необхідність ведення війни і сформувати негатив у протиборчих сторін. Так військові конфлікти в Сирії та Україні є яскравими прикладами цього. Інформаційна війна і тероризм також безпосередньо пов'язані між собою.

Таким чином, з появою нових інформаційних форм боротьби, які використовують інформаційну зброю і названих як інформаційна війна, відбувається якісна зміна сучасного світопорядку. Розібратися в тому, що ж насправді відбувається між протиборчими сторонами, звичайній людині дуже складно, тому що насамперед необхідно чітко виявляти в цьому процесі пізнання, що є інформаційною зброєю, які цілі переслідуються і які методи ведення інформаційних війн реалізуються.

Під ***інформаційною зброєю***, у найзагальнішому вигляді, можуть розумітися *засоби і методи ведення інформаційних війн, здійснення інформаційного тероризму і здійснення інформаційних злочинів.* Термін «зброя» у понятті інформаційна зброя дещо відрізняється від звичного нам поняття, яке зазвичай застосовується до традиційних видів озброєнь.

Деякі дослідники порівнюють інформаційну зброю зі зброєю масового знищення (перший аспект). Деякі вважають, що інформаційна зброя на відміну від зброї масового знищення є зброєю масового спотворення (другий аспект). На відміну від зброї масового знищення, основною ціллю і ефектом зброї масового спотворення є не спричинення масових руйнувань, а скоріше спотворення інформації таким чином, щоб противник міг бути пригнічений з мінімальним використанням фізичних сил.

Ще раз акцентуємо, що зазначене вище розходження в розумінні суті інформаційної зброї відображає і представляє саме два зазначених аспекти інформаційної безпеки. Розгляд інформаційної зброї як зброї масового знищення в більшій мірі пов'язане з другим аспектом. Дійсно, наслідки застосування негативних засобів і методів впливу на інформаційну та комунікаційну структуру держави, особливо в разі якщо багато критичних структур сильно залежать від їх функціонування, може призвести до воістину драматичних наслідків, які можна порівняти з наслідками застосування зброї масового знищення. Наприклад, в результаті впливу шкідливих програм перестане функціонувати кредитно-фінансова система, що безумовно призведе до порушення нормального функціонування економіки. Розуміння інформаційної зброї, як зброї масового спотворення відображає перший аспект інформаційної безпеки і пов'язаний з поширенням інформації, що завдає шкоди інтересам особистості, суспільства і держави в інформаційному просторі, тобто з психологічним або ідеологічним впливом.

Таким чином, *інформаційна зброя – це засоби і методи, що застосовуються з метою впливу і нанесення збитку інформаційним і комунікаційним структурам, у тому числі критичним структурам держави і суспільства, а також з метою надання психологічного та ідеологічного впливу.*

Інформаційна зброя буває різних видів. Відразу слід обмовитися, що на нашу думку основним критерієм віднесення певних засобів до інформаційної зброї є використовуваний метод, а саме інформаційний метод, а не об'єкт впливу зброї. Якщо використовувати критерій об'єкта впливу, то до інформаційної зброї можна віднести будь-яку зброю, яка використовується, наприклад, для руйнування інформаційної інфраструктури (комп'ютерів, мереж і т. д.). Тобто, якщо використовувати критерій об'єкта впливу, до інформаційної зброї можна віднести звичайний пістолет, так як він може бути використаний для знищення комп'ютера або, наприклад, вибухівку і т. д. Інформаційний метод впливу поняття досить умовне і використовується в цьому дослідженні для того, щоб акцентувати увагу на те, що інформаційна зброя, по-перше, є результатом розвитку інформаційних і комунікаційних

технологій і функціонує в інформаційному просторі так само як і інші інформаційні і комунікаційні засоби (наприклад комп'ютерні програми), але тільки з негативним знаком, з негативним ефектом. По-друге, інформаційна зброя є власне інформація скомпонована таким чином, щоб чинити сильний психологічний або ідеологічний вплив на свідомість людини.

Виходячи з аспектів інформаційної безпеки можна виділити ***два види інформаційної зброї.*** Перший – це особливим чином сформульована або оформлена інформація, яка спеціально призначена для психологічної або ідеологічної обробки населення, для підриву моральних і етичних засад суспільства, а також спеціальні інформаційні або комунікаційні засоби, призначені для негативного впливу на інформаційну або комунікаційну інфраструктуру. Другий вид інформаційної зброї включає в себе комп'ютерні віруси у вигляді: логічна бомба, сніфери, троянський кінь, комп'ютерні хробаки, тимчасова бомба і електронно-поштові бомби, задні двері або люки тощо.

Інформаційну зброю також можна розділити на наступальну зброю, яка використовується для нападів або для заподіяння шкоди, захисну зброю, яка використовується для захисту від нападів і зброю подвійного призначення.

Наступальна зброя включає в себе перераховані вище засоби і, перш за все, комп'ютерні віруси.

Захисна зброя включає в себе шифрування, автентифікацію, системи контролю доступу, мережеві екрани, антивірусне програмне забезпечення, пристрої перевірки функціонування системи, програми відстеження проникнень в систему.

Зброя подвійного призначення може бути використана як для полегшення нападу, так і для захисту від нападу. Прикладами цього виду зброї можуть бути програми для зламування паролів, ключів, програми сніфери, сканери для виявлення недоліків системи і т. д.

Міжнародно-правові питання, що виникають у зв'язку з інформаційною зброєю, є дуже складними. Наприклад, яким чином можна встановити режим контролю за зазначеною зброєю, якщо вона тісно пов'язана з поширенням інформаційних технологій, обмежувати які, значить позбавити багато держав можливості розвиватися і стати повноправними членами

сучасного суспільства. Якими способами здійснювати контроль за використанням та поширенням зазначеної зброї, і взагалі чи можливо це технічно і т. д.

Як бачимо, розвиток інформаційних технологій і поява нових методів і засобів впливу на державу через його інформаційні і комунікаційних структури, в тому числі з використанням інформаційної зброї, спонукає появу значно більшої кількості питань, перш за все міжнародного характеру, ніж відповіді, які ще тільки формулюються.

Швидше за все термін інформаційна зброя використовується для позначення негативного впливу засобів і методів на інтереси особистості, суспільства і держави в інформаційному просторі, а також для позначення руйнівної спрямованості зазначених засобів і методів по відношенню до інформаційної та комунікаційної структури держави. В цьому випадку в залежності від джерела інформації досить актуальним стає сам процес виявлення способів впливу на поточну інформацію, який може бути безпосереднім, або опосередкованим, через інше джерело впливу. При цьому з боку людей можливі наступні **види впливу:** 1) *безпосередній вплив* на носії інформації, що захищається; 2) *несанкціоноване поширення* конфіденційної інформації; 3) *виведення з ладу* технічних засобів відображення, зберігання, обробки, відтворення, передачі інформації і засобів зв'язку; 4) *порушення режиму роботи* перерахованих засобів та технології обробки інформації; 5) *виведення з ладу і порушення режиму* роботи систем забезпечення функціонування названих засобів.

Способами безпосереднього впливу на носії інформації, що захищається, можуть бути: 1) фізичне руйнування носія (поломка, руйнування і ін.); 2) створення аварійних ситуацій для носіїв (підпал, штучне затоплення, вибух і т. д.); 3) видалення інформації з носіїв; 4) створення штучних магнітних полів для розмагнічування носіїв; 5) внесення фальсифікованої інформації у носії.

Цей вид дестабілізуючого впливу призводить до реалізації **трьох форм прояву уразливості інформації:** *знищення, спотворення і блокування*.

До безпосереднього впливу на носії інформації, що захищається, можна з застереженням віднести і ненавмисне залишення їх в неохоронюваній зоні, найчастіше у громадському транспорті, магазині, на ринку, що призводить до втрати носіїв.

Несанкціоноване розповсюдження конфіденційної інформації може здійснюватися шляхом: 1) словесної передачі (повідомлення) інформації;

2) передачі копій (знімків) носіїв інформації; 3) показу носіїв інформації;

4) введення інформації в обчислювальні мережі; 5) опублікування інформації в пресі; 6) використання інформації у відкритих публічних виступах, у тому числі на радіо, телебаченні.

До несанкціонованого розповсюдження може призвести і втрата носіїв інформації. Цей вид дестабілізуючого впливу призводить до розголошення конфіденційної інформації.

До способів виведення з ладу технічних засобів відображення, зберігання, обробки, відтворення, передачі інформації і засобів зв'язку можна віднести: 1) неправильний монтаж засобів; 2) поломку (руйнування) засобів, у тому числі розрив (пошкодження) кабельних ліній зв'язку; 3) створення аварійних ситуацій для засобів (підпал, штучне затоплення, вибух та ін.);

4) відключення засобів від систем; 5) виведення з ладу або порушення режиму роботи систем забезпечення функціонування засобів; 6) умонтування в ЕОМ руйнівних радіо- і програмних закладок.

Цей вид дестабілізуючого впливу призводить до реалізації трьох форм прояву уразливості інформації: знищення, спотворення і блокування.

Способами порушення режиму роботи технічних засобів відображення, зберігання, обробки, відтворення, передачі інформації, засобів зв'язку і технології обробки інформації можуть бути:

- пошкодження окремих елементів засобів;
- порушення правил експлуатації засобів;
- внесення змін до порядку обробки інформації;

- зараження програм обробки інформації шкідливими програмами;
- видача неправильних програмних команд;
- перевищення розрахункового числа запитів;
- створення перешкод у радіоефірі за допомогою додаткового звукового або шумового фону,
- зміни (накладення) частот передачі інформації;
- передача хибних сигналів;
- підключення пригнічуючих фільтрів у інформаційні ланцюги, ланцюги живлення і заземлення;

порушення (зміна) режиму роботи систем забезпечення функціонування засобів.

Даний вид дестабілізуючого впливу також призводить до знищення, спотворення і блокування інформації.

До способів виведення з ладу і порушення режиму роботи систем забезпечення, функціонування технічних засобів відображення, зберігання, обробки, відтворення і передачі інформації слід віднести:

- неправильний монтаж систем;
- поломку (руйнування) систем або їх елементів;
- створення аварійних ситуацій для систем (підпал, штучне затоплення, вибух і т. д.);
- відключення систем від джерел живлення;
- порушення правил експлуатації систем.

Цей вид дестабілізуючого впливу призводить до тих же результатів, що і два попередні види.

До **видів дестабілізуючого впливу на інформацію, яка захищається, з боку другого джерела впливу** (тобто технічних засобів відображення, зберігання, обробки, відтворення, передачі інформації) і засобів зв'язку відносяться:

- ✓ виведення засобів з ладу;
- ✓ збої в роботі засобів;
- ✓ створення електромагнітних випромінювань.

Вихід засобів з ладу, що призводить до неможливості виконання операцій, може відбуватися шляхом:

- технічної поломки, аварії (без втручання людей);

– загоряння, затоплення (без втручання людей);
– виходу з ладу систем забезпечення функціонування засобів;
– впливу природних явищ;
– впливу зміненої структури навколишнього магнітного поля;
– зараження програм обробки інформації шкідливими програмами (шляхом розмноження останніх або із заражених носіїв);
– руйнування або пошкодження носія інформації, в тому числі розмагнічування магнітного шару диска (стрічки) через осипання магнітного порошку.

Цей вид дестабілізуючого впливу призводить до реалізації трьох форм прояву уразливості інформації: знищення, спотворення, блокування.

Збої в роботі засобів, що призводять до неправильного виконання операцій (помилок), можуть здійснюватися за допомогою:

– виникнення технічних несправностей елементів засобів;
– зараження програм обробки інформації шкідливими програмами (шляхом розмноження останніх або з заражених носіїв);
– впливу природних явищ;
– впливу навколишнього магнітного поля;
– часткового розмагнічування магнітного шару диска (стрічки) через осипання магнітного порошку;
– порушення режиму функціонування засобів.

Даний вид дестабілізуючого впливу призводить до реалізації **чотирьох форм прояву уразливості інформації: *знищення, спотворення, блокування, розголошення.***

Як приклад, це – з'єднання з номерів телефону, не того абонента, який набирався або чутність розмови інших осіб через несправність в ланцюгах комунікації телефонної станції.

Електромагнітні випромінювання, у тому числі побічні, що утворюються в процесі експлуатації засобів, призводять до розкрадання інформації.

Третє джерело дестабілізуючого впливу на інформацію – системи забезпечення функціонування технічних засобів відображення, зберігання, обробки, відтворення і передачі інформації – включає **два види впливу**: вихід систем з ладу і збої в роботі систем.

Вихід систем з ладу може відбуватися шляхом:

- ✓ поломки, аварії (без втручання людей);
- ✓ загоряння, затоплення (без втручання людей);
- ✓ виходу з ладу джерел живлення;
- ✓ впливу природних явищ.

Цей вид дестабілізуючого впливу призводить до реалізації трьох форм прояву уразливості інформації: знищення, блокування, спотворення.

Збої в роботі систем можуть здійснюватися за допомогою:

- ✓ появи технічних несправностей елементів систем;
- ✓ впливу природних явищ;
- ✓ порушення режиму роботи джерел живлення.

Результатом дестабілізуючого впливу також є знищення, блокування, спотворення інформації.

Видом дестабілізуючого впливу на інформацію з боку технологічних процесів окремих промислових об'єктів (як четверте джерело) є ***зміна структури навколишнього середовища.*** Цей вплив здійснюється шляхом:

- – зміни природного радіаційного фону навколишнього середовища, що відбувається при функціонуванні об'єктів ядерної енергетики;
- – зміни хімічного складу навколишнього середовища, що відбувається при функціонуванні об'єктів хімічної промисловості;
- – зміни локальної структури магнітного поля, що відбувається внаслідок діяльності об'єктів радіоелектроніки і по виготовленню деяких видів озброєння і військової техніки.

Цей вид дестабілізуючого впливу в кінцевому підсумку призводить до розкрадання конфіденційної інформації.

П'яте джерело дестабілізуючого впливу на інформацію – **природні явища,** як уже зазначалося, включає стихійні лиха і атмосферні явища (коливання).

До ***стихійних лих*** і одночасно видів впливу слід віднести:

землетрус, повінь, ураган (смерч), шторм, зсуви, лавини, виверження вулканів.

До ***атмосферних явищ*** (видів впливу) слід віднести:

грозу, дощ, сніг, перепади температури і вологості повітря, магнітні бурі.

Способами впливу з боку і стихійних лих, і атмосферних явищ можуть бути руйнування (поломка), землетрус, спалення носіїв інформації засобів відображення, зберігання, обробки, відтворення, передачі інформації і засобів зв'язку, систем забезпечення функціонування цих засобів, порушення режиму роботи засобів і систем, а також технології обробки інформації, створення паразитних наведень (грозові розряди).

Ці види впливу призводять до п'яти форм прояву уразливості інформації: втрати, знищення, спотворення, блокування і розкрадання.

При розгляді ознак і складових загрози інформації, яка захищається, було сказано, що в основі будь-якого дестабілізуючого впливу лежать певні причини, спонукальні мотиви, які зумовлюють появу того чи іншого виду і способу впливу. Разом з тим і причини мають під собою підстави – обставини або передумови, які викликають ці чинники, що сприяють їхній появі. Однак наявність джерел, видів, способів, причин і обставин (передумов) дестабілізуючого впливу на інформацію являє потенційно існуючу небезпеку, яка може бути реалізована тільки при наявності певних умов для цього.

Оскільки види і способи дестабілізуючого впливу залежать від джерел впливу, то і причини, обставини (передумови) і умови повинні бути прив'язані до джерел впливу.

Стосовно до людей причини, обставини і умови в більшості випадків пов'язані ще і з **характером впливу – навмисним або ненавмисним.**

До ***причин***, що викликають ***навмисний дестабілізуючий вплив***, слід віднести:

- ✓ прагнення отримати матеріальну вигоду (підзаробити);
- ✓ прагнення завдати шкоди (помститися) керівництву або колезі по роботі, а іноді і державі;
- ✓ прагнення надати безкорисливу послугу приятелю з конкуруючої фірми;
- ✓ прагнення просунутися по службі;
- ✓ прагнення убезпечити себе, рідних і близьких від погроз, шантажу, насильства;
- ✓ прагнення показати свою значимість.

Обставинами (передумовами), що сприяють появі цих причин, можуть бути:

- ✓ важке матеріальне становище, фінансові труднощі;
- ✓ користолюбство, жадібність; схильність до розваг, пияцтва, наркотиків;
- ✓ заздрість, образа;
- ✓ невдоволення державним устроєм, політичне або наукове інакомислення;
- ✓ особисті зв'язки з представниками конкурента;
- ✓ невдоволення службовим становищем, кар'єризм;
- ✓ боягузтво, страх;
- ✓ марнославство, зарозумілість, завищена самооцінка, хвастощі.

До ***умов, що створює можливість для дестабілізуючого впливу*** на інформацію, можна віднести:

- – недостатність заходів, що вживаються для захисту інформації, в тому числі через нестачу ресурсів;
- – недостатня увага і контроль з боку адміністрації щодо питань захисту інформації;
- – прийняття рішень з виробничих питань без урахування вимог щодо захисту інформації;
- – погані відносини між співробітниками і співробітників з адміністрацією.

Причинами ненавмисного дестабілізуючого впливу на інформацію з боку людей можуть бути:

- ✓ некваліфіковане виконання операцій;

- ✓ недбалість, безвідповідальність, недисциплінованість, несумлінне ставлення до виконуваної роботи;
- ✓ недбалість, необережність, неакуратність;
- ✓ фізичне нездужання (хвороби, перевтома, стрес, апатія).

До обставин (передумов) появи цих причин можна віднести:

- ✓ низький рівень професійної підготовки;
- ✓ зайву балакучість, звичку ділитися досвідом, давати поради;
- ✓ незацікавленість в роботі (вид роботи, її тимчасовий характер, зарплата), відсутність стимулів для її вдосконалення;
- ✓ розчарованість в своїх можливостях і здібностях;
- ✓ перевантаженість роботою, терміновість її виконання, порушення режиму роботи;
- ✓ погане ставлення з боку адміністрації.

Умовами для реалізації ненавмисного дестабілізуючого впливу на інформацію можуть бути:

- – відсутність або низька якість правил роботи з інформацією , яка захищається;
- – незнання або порушення правил роботи з інформацією виконавцями;
- – недостатній контроль з боку адміністрації за дотриманням режиму конфіденційності;
- ✓ недостатня увага з боку адміністрації щодо умов роботи, профілактики захворювань, підвищення кваліфікації.

Причинами дестабілізуючого впливу на інформацію ***з боку технічних засобів*** відображення, зберігання, обробки, відтворення, передачі інформації і засобів зв'язку можуть бути:

- ✓ нестача або погана якість засобів;
- ✓ низька якість режиму функціонування засобів;
- ✓ перезавантаженість засобів;
- ✓ низька якість технології виконання робіт; дестабілізуючий вплив на засоби з боку інших джерел впливу.

До обставин (передумов), що викликає ці причини, слід віднести:

- ✓ недостатність фінансових ресурсів, що виділяються на придбання і експлуатацію засобів;
- ✓ поганий вибір засобів;
- ✓ старіння (знос) засобів;
- ✓ конструктивні недоробки або помилки при монтажі засобів;
- ✓ помилки при розробці технології виконання робіт, у тому числі програмного забезпечення;
- ✓ дефекти використовуваних матеріалів;
- ✓ надмірний обсяг оброблюваної інформації;
- ✓ причини, що лежать у основі дестабілізуючого впливу на засоби з боку інших джерел впливу.

Умовами, що забезпечують реалізацію дестабілізуючого впливу на інформацію з боку технічних засобів, можуть бути:

- недостатня увага до складу і якості засобів з боку адміністрації, нерідко через недорозуміння їх значення;
- нерегулярний профілактичний огляд засобів; низька якість обслуговування засобів.

Причини, обставини (передумови) і умови дестабілізуючого впливу на інформацію з боку систем забезпечення функціонування засобів відображення, зберігання, обробки, відтворення, передачі інформації і засобів зв'язку «вписуються» в причини і обставини впливу з боку самих засобів.

Причиною дестабілізуючого впливу на інформацію з боку технологічних процесів окремих промислових об'єктів є специфіка технології, ***обставиною*** – необхідність такої технології, а ***умовою*** – відсутність можливостей протидії зміні структури навколишнього середовища.

В основі **дестабілізуючого впливу на інформацію з боку природних явищ** закладені ***внутрішні причини і обставини***, непідконтрольні людям, а отже, вони не піддаються нейтралізації або усуненню.

Таким чином, загрози інформаційним ресурсам необхідно розглядати не тільки як потенційно можливі випадки антропогенного, техногенного або природного (стихійного) характеру, що здатні чинити небажаний вплив на інформаційно-

телекомунікаційні системи, а й як загрози зі сфери соціальної інженерії. Через такі загрози, за вдалого використання інформаційної зброї на адресу службової інформації підприємства, можливі серйозні перебої як у роботі інформаційних систем з його управління, так і в зниженні рівня реалізації адекватної діяльності самого підприємства. І ті (у вигляді інформаційних систем), і інші (у вигляді об'єктів підприємницької діяльності) можуть, за своєю значущістю на життєдіяльність соціуму, бути віднесеними до об'єктів критичної інфраструктури.

Таки системи та об'єкти критичної інфроструктури здатні виступати як ключовими елементами національної або регіональної безпеки, так і стратегічними умовами для забезпечення сталого розвитку суспільства в умовах глобалізації та зростаючої технологічної залежності. При цьому необхідна не тільки успішна адаптація задіяних систем управління підприємств різної сфери діяльності до сучасних викликів безпеці (що вимагає глобального підходу, який охоплює і технологічні, і організаційні, і правові, і навчальні аспекти та ініціативи), а й адекватно-оптимальна взаємодія між учасниками процесу управління (менеджменту), задіяних у сфері виробництва, науково-освітніх, суспільно-господарських, урядових та інших структур соціуму.

4.4. Основи менеджменту інформаційної безпеки та його правові аспекти

У контексті викладеного вище, сучасні інформаційні системи (ІС) підприємства пов'язані з його технологічними процесами і безпосередньо з багатопрофільною службовою інформацією, яка підлягає різноплановим формам приймання, аналізу та трансформації конкретної інформації з наступним її перетворенням у рамках реалізації достовірного безпечного передавання та адекватного зберігання для потреб споживача (підприємства).

Очевидно, що залежно від різного ступеня секретності службової інформації виникає питання про захищеність не тільки

ІС підприємства від потенційних загроз, а й питання забезпечення безпечної працездатності підприємства та обслуговуючого персоналу [12]. Перш за все, це пов'язано з особливою уразливістю інфраструктури та високої професійної відповідальністю співробітників критично важливих об'єктів (КВО), від роботи яких залежить не тільки штатне функціонування цих об'єктів, але і ступінь захисту від будь-яких загроз та їх передумов, здатних викликати техногенну, екологічну або фінансову катастрофу [13]. При цьому, розвиток управління підприємств різної сфери діяльності дозволяє розглядати нові самостійні галузі управління, пов’язані з управлінням інформаційними ресурсами, впровадженням і використанням інформаційних технологій в діяльності підприємств і організацій, управлінням процесами опрацювання інформації в організаціях [14, с. 9]. Проте прогрес в інформаційно-технічній сфері створив і потенційні загрози у вигляді розроблення нових та удосконалення вже відомих методів пошукового шпигунства. Наприклад, згідно з [15], найбільш поширені види потенційних загроз та небезпек для сучасного комерційного підприємства у сфері інформаційної діяльності прийнято вважати відсутність: захисного мережевого екрану від Інтернет атак; копіювання бухгалтерських та організаційно розпорядчих документів на матеріальних носіях даних; ведення протоколів змін у програмному забезпеченні; регулювання доступу користувачів до різних типів інформації та баз даних; схем інформаційного забезпечення рівнів управління. Крім того, − це можливість несанкціонованого втручання в програмне забезпечення та базу даних; крадіжка засобів зберігання інформації; промислове шпигунство; хакерські атаки, шкідливе програмне забезпечення та комп’ютерні віруси; піратське програмне забезпечення та не ліцензовані антивірусні програми, а також наявність непідзвітних посадових осіб у системі управління підприємством та недобросовісне використання інформації працівниками підприємства.

Отже, інформаційні системи виконують багато важливих функцій, де об’єднувальною є управлінська система, яка потребує сучасного менеджменту інформаційної безпеки (див. Додаток «Євроатлантична правова інтеграція у сфері

кібербезпеки ОКІ у межах ISO/SEC згідно захисту суверенітету держави та розвитку суспільства»), якому має бути притаманна відповідність із міжнародним стандартам типу ISO/IEC 27001:2015 Information technology – Security techniques – Information security management systems – Requirements (Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги) та подальші серії ISO [16 -20].

Зокрема, стандарт ISO/IEC 27001:2015 створений для визначення вимог для розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та постійного вдосконалення системи управління інформаційною безпекою (СУІБ). Крім того, доцільно зазначити, що в [23, табл. 2.1., с.25] детально наведено «Звід основної сучасної національної та міжнародної нормативної бази в галузі інформаційної безпеки».

Цілком очевидно, що прийняття системи управління інформаційною безпекою є стратегічним рішенням для будь-якої організації (підприємства), де на проектування та впровадження системи управління інформаційною безпекою організації впливають потреби та цілі організації, вимоги щодо безпеки, застосовувані організаційні процеси, розмір і структура організації [21,22]. При цьому система управління інформаційною безпекою забезпечує збереження конфіденційності, цілісності й доступності інформації за допомогою запровадження процесу управління ризиками, що і буде викладено в розділі 6.

Таким чином, сфера інформаційного менеджменту – це сукупність необхідних для управління рішень на всіх етапах життєвого циклу підприємства, що включає дії та операції, які пов'язані з інформацією у різних формах і станах, та з підприємством у цілому. Крім того, між системою інформації і структурою управління в підприємстві існує органічний взаємозв'язок і взаємозалежність, де непосредственно система управління інформаційною безпекою підприємства должна быть побудована на основі вимог міжнародних стандартів ISO, що дозволить організувати ефективну систему для створення, управління, контролю і захисту важливої інформації та документів. При цьому, вирішуються завдання визначення

цінності й ефективності використання інформації і знань, а також цінності та інших ресурсів підприємства, що входять у контакт із інформацією: технологічних, кадрових та фінансових

Контрольні запитання до Розділу 4

1. Що таке технологія інформаційного забезпечення менеджменту?
2. Викладіть режими інформування менеджерів під час реалізації технології інформаційного забезпечення менеджменту в сучасній інформаційній системі організації.
3. Поясніть, будь ласка, терміни «відмовостійкість» (fault tolerance) та «живучість» (survivability).
4. Що зазвичай входить до переліку основних відомостей конфіденційного характеру?
5. Які використовуються основни підходи до розуміння таємниці.
6. Інформація з обмеженим доступом і «конфіденційна» інформація - це синоніми чи як?
7. Які є критерії віднесення інформації до відкритої інформації чи до конфіденційної?
8. Що таке комерційна таємниця?
9. Що може виступати носієм інформації?
10. Обґрунтовано перелічіть носії конфіденційної інформації, яким потрібен захист.
11. Що означає безпека інформації?
12. Що відносять до сутнісних проявів загрози?
13. Опишіть основні джерела загроз інформаційній безпеці.
14. Що означає термін «інформаційна війна», які існують її ознаки та напрямки ведення?
15. Що відносять до видів інформаційного протистояння?
16. Що розуміти під інформаційною зброєю?

17. Які є форми прояву уразливості інформації та джерела дестабілізуючого впливу на неї?
18. Які є умови для реалізації ненавмисного дестабілізуючого впливу на ІС?
19. Які є причини дестабілізуючого впливу на інформацію з боку технічних засобів ІС?
20. Які є причини дестабілізуючого впливу на інформацію з боку природних явищ?

Список використаних джерел під час підготовки тексту розділу 4

1. Р.В. Мещеряков, О.І. Жуковський, П.В. Сенченко, Ю.Б. Гриценко, М.М. Міліхін Особливості архітектури єдиного інформаційного простору під час управління складними технологічними процесами Доповіді ТУСУРу, том 20, № 4, 2017, с.75-81.
2. Замрій І.В., Вишнівський В.В. Структура єдиного інформаційного простору підприємства з критичною інфраструктурою // Телекомунікаційні та інформаційні технології, 2021, №3 (72). С. 12-24
3. ДСТУ 2860-94* Надійність техніки. Терміни та визначення. (Чинний від 1996—01—01) Додаток В (довідковий), Перелік рекомендованих термінів та визначень.
4. Алексенцев А. І. Визначення складу конфіденційної інформації. Довідник секретаря офіс-менеджера. – 2003. – № 2,3
5. Конвенція про заборону розробки, виробництва, накопичення, застосування хімічної зброї та про її знищення: (джерело документа: https://zakon.rada.gov.ua). – К.: Паливода А. В.. – 132 с.
6. Забара І.М. Міжнародно-правове регулювання обміну інформацією // Інформація і право. – 2013. – № 2 (8). – С. 56-64.
7. Про інформацію. Закон України від 02.10.1992 № 2657-XII. Відомості Верховної Ради України (ВВР). 1992. № 48, ст. 650. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text

8. Галицький О. В., Рябко С. Д., Шаньгін В. Ф. Захист інформації у мережі. - М.: ДМК Прес, 2014. – 616 с.

9. Петренко С. А., Курбатов В. А. Політики інформаційної безпеки. - М.: Компанія АйТі, 2014. – 400 с

10. Л. В. Воронцова, Д. Б. Фролов «Історія та сучасність інформаційного протистояння» Видавництво: "Гаряча Лінія – Телеком " (2006) С.192.

11. Інформаційна війна в сучасному світі. [Электронный ресурс] – URL: http://kak-bog.ru/informacionnaya-voyna-v-sovremennom-mire.

12. Апріорна вразливість сучасного захисту персоналу та вдосконалення анонімності їх роботи /Тарасенко Ю.С., Луценко В.В., Філіпов М.С. // Міжнародна наукова інтернет-конференція «Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення (випуск 44)» / Збірник тез доповідей: випуск 44 (м. Тернопіль, 12 грудня 2019 р.). – Частина 1. – Тернопіль. 2019. -120 с. С. 85-86.

13. Іванченко О.В. Концепція управління готовністю критичних інфраструктур на основі застосування інформаційних технологій/О.В. Іванченко, К.В. Смоктій, О.Д. Смоктій, В.С. Харченко // Системи та технології. –2016. – Вып.1 (55). С.5-23.

14. Спрінсян В. Г., Бірюкова Т. Л. Ресурси та технології інформаційного менеджменту : навчальний посібник. Одеса : ОНПУ, 2012. 248 с.

15. Панченко В.А. Менеджмент інформаційної безпеки комерційного підприємства / В.А. Панченко // Центральноукраїнський науковий вісник. Економічні науки, 2019, вип. 3(36). С.219-228.

16. ISO/IEC 27001:2015 Information technology – Security techniques – Information security management systems – Requirements (Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги) та подальші серії ISO, такі як:

17. ISO/IEC 27002-2012 (це Інструкція з менеджменту інформаційної безпеки для телекомунікаційних організацій);

18. ISO/IEC 27003-2012 (це Інструкція з реалізації системи менеджменту ІБ); - ISO/IEC 27004-2011 (це Менеджмент інформаційної безпеки вимірювання);

19. ISO/IEC 27005-2010 (це Менеджмент ризику інформаційної безпеки який конкретизує поняття інформаційного ризику);

20. ISO/IEC TR 13335-2: 1997 (це Настанови з керування безпекою інформаційних технологій (IT)).

21. Матвієнко О. В., Цивін М. Н. Основи менеджменту інформаційних систем: навчальний посібник. Київ : Центр навчальної літератури, 2005. 176 с.

22. Низенко Е. І., Каленяк В. П. Забезпечення інформаційної безпеки підприємництва : навч. посіб. Київ : МАУП, 2006. 134 с.

23. Якименко І.З.. Конспект лекцій з дисципліни Менеджмент інформаційної безпеки. Тернопіль – 2019. С.136.

5. АНАЛІЗ ДЖЕРЕЛ І КАНАЛІВ НЕСАНКЦІОНОВАНОГО ДОСТУПУ. ДІЛОВА РОЗВІДКА ЯК ІНТЕЛЕКТУАЛЬНИЙ ІНСТРУМЕНТАРІЙ ЗАБЕЗПЕЧЕННЯ СТРАТЕГІЧНОГО МЕНЕДЖМЕНТУ ПІДПРИЄМСТВА

5.1. Несанкціонований доступ до інформації, канали впливу та їх реалізації

На підставі раніше викладеного можна стверджувати, що несанкціонований доступ до інформації, – це навмисне, не маючи на те дозволу, оволодіння (придбання) конфіденційною інформацією, з метою, як правило, здійснити свідомий дестабілізуючий вплив на її конфіденційність.

До **каналів несанкціонованого доступу до конфіденційної інформації** відносяться:

1. Встановлення контакту з особами, що мають або мали доступ до конфіденційної інформації. Даний канал є найпоширенішим, різноманітним за методами несанкціонованого доступу, а тому і найнебезпечнішим. Сюди входять особи, які працюють на даному підприємстві, а також непрацюючі на ньому, але мають доступ до конфіденційної

інформації підприємства в силу службового становища. До числа таких осіб слід також віднести звільнених або відсторонених від даної конфіденційної інформації співробітників. Контакт з цими людьми може бути встановлений різними шляхами, наприклад на семінарах, виставках, конференціях та інших публічних заходах. Також з ними можливий опосередкований контакт. Широко використовуються методи: отримання конфіденційної інформації у вигляді вивідування інформації підслушним приводом; переманювання співробітників конкуруючих підприємств з тим, щоб крім використання їх знань і умінь, отримати необхідну конфіденційну інформацію, що відноситься до колишнього місця їх роботи; покупки конфіденційної інформації, коли активно шукають незадоволених заробітком, керівництвом або просуванням по службі; примусу до видачі конфіденційної інформації шантажем, погрозами, застосуванням фізичного насильства як до особи, яка володіє інформацією, так і до його родичів і близьких. Очевидна можливість отримання конфіденційної інформації шляхом переконання, лестощів, обману, в тому числі з використанням національних, політичних, релігійних факторів, осіб, які володіють такою інформацією.

2. Вербування та впровадження агентів. За допомогою агентів розвідувальні служби зазвичай прагнуть отримати доступ до конфіденційної інформації, яку не можна добути через інший, менш небезпечний канал. Агенти можуть отримувати не тільки конфіденційну інформацію, що відноситься до їх службової діяльності, а й іншу, використовуючи різні методи несанкціонованого доступу до неї, а також здійснювати інший дестабілізуючий вплив на інформацію.

3. Організація фізичного проникнення до носіїв конфіденційної інформації співробітників розвідувальних служб. Використовується порівняно рідко, оскільки він (цей канал) пов'язаний з великим ризиком і вимагає знань про місце зберігання носіїв і систему захисту інформації. Зазвичай фізичне проникнення осіб, які не працюють на об'єкті, включає два етапи: проникнення на територію, що охороняється, і проникнення до носіїв конфіденційної інформації.

При проникненні на територію об'єкта можливе застосування таких методів:

- використання підробленого, викраденого або купленого пропуску;
- маскування під іншу особу;
- прохід під виглядом зовнішнього обслуговуючого персоналу;
- відволікання уваги охорони для проходу непоміченим;

- ізоляція або знищення охорони (як правило, в рідкісних, надзвичайних обставинах) та ін.

Проникнення до носіїв конфіденційної інформації може здійснюватися шляхом злому дверей сховищ і сейфів або їх замків, з відключенням сигналізації, телевізійних засобів спостереження, або, шляхом проходу в кімнати виконавців, які працюють з конфіденційними документами, у виробничі і складські приміщення для огляду технологічних процесів і продукції, а також у приміщення, в яких проводиться обробка інформації.

Проникнення до носіїв конфіденційної інформації може здійснюватися і під час їх транспортувань з використанням, у залежності від виду, умов і маршруту транспортування, відповідних методів.

4. Підключення до засобів відображення, зберігання, обробки, відтворення і передачі інформації, засоби зв'язку. Може здійснюватися особами, які перебувають на території об'єкта і поза нею. Несанкціоноване підключення, а отже, і несанкціонований доступ до конфіденційної інформації може здійснюватися:

- з персонального комп'ютера з використанням телефонного набору або з несанкціонованого терміналу зі зломом парольно-ключових систем захисту або без злому за допомогою маскування під зареєстрованого користувача;

- за допомогою програмних і радіоелектронних західних пристроїв;

- за допомогою прямого приєднання до кабельних ліній зв'язку, зокрема з використанням паралельних телефонних апаратів;

- за рахунок електромагнітних наведень на паралельно прокладені дроти або методів високочастотного нав'язування.

5. Прослуховування мовної конфіденційної інформації, яка широко використовується і найчастіше здійснюється за двома напрямками у вигляді:

- підслуховування безпосередніх розмов осіб, допущених до даної інформації;
- прослуховування мовної інформації, зафіксованої на носії, за допомогою підключення до засобів її звуковідтворення.

6. Візуальне знімання конфіденційної інформації, яке як правило, здійснюється наступними методами:

- читанням документів на робочих місцях користувачів;
- переглядом інформації, що відтворюється засобами відео відтворювальної техніки і телебачення;
- спостереженням за технологічними процесами виготовлення, обробки продукції;
- зчитуванням інформації в масивах інших користувачів, у тому числі читанням залишкової інформації та ін.

7. Перехоплення електромагнітних випромінювань. Методами перехоплення є виявлення сигналів і їх фільтрація з метою знімання конфіденційної інформації, її подальшої обробки та аналізу. Даний канал несанкціонованого доступу, у порівнянні з іншими каналами, має суттєві переваги: великий обсяг і висока достовірність одержуваної інформації, оперативність її отримання, можливість знімання у будь-який час, скритність отримання, можливість оприлюднення без загрози перекриття каналу.

8. Дослідження продукції, що випускається, виробничих відходів і відходів процесів обробки інформації. Методи отримання конфіденційної інформації:

- придбання і розробка виробів, що випускаються, зворотний інжиніринг;
- збір і вивчення поламаних виробів, макетів виробів, бракованих вузлів, блоків, пристроїв, деталей, створених на стадії дослідно-конструкторських розробок, а також руди і шлаків, що дозволяють визначити склад матеріалів, а нерідко і технологію виготовлення продукції;

- збір і прочитання чернеток і проектів конфіденційних документів, копіювального паперу, фарбувальної стрічки друкуючих пристроїв, зіпсованих магнітних дискет.

9. Вивчення доступних джерел інформації, з яких можна отримати конфіденційні відомості, використовуючи методи:

- вивчення наукових публікацій, що містяться у спеціалізованих журналах;
- перегляду або прослуховування засобів масової інформації;
- вивчення каталогів виставок;
- прослуховування публічних виступів на семінарах, конференціях та інших публічних заходах;
- вивчення формованих спеціалізованими комерційними структурами банків даних про підприємства.

Метою вивчення є не тільки отримання прямої конфіденційної інформації, а й накопичення, узагальнення, зіставлення відкритої інформації, зібраної з різних джерел і за певний проміжок часу, що дозволяє «вивести» конфіденційну інформацію. До таких, наприклад, можна віднести виміри і взяття проб оточуючого об'єкт середовища, аналіз архітектурних особливостей деяких категорій об'єктів і т. д. Незважаючи на уявний парадокс, такий аналіз дає можливість отримати значну кількість конфіденційної інформації.

Несанкціонований доступ, навіть навмисний, не завжди є протиправним. Найчастіше він, звичайно, буває незаконним, але нерідко не носить кримінального характеру.

Очевидно, що використання того чи іншого каналу має здійснюватися за допомогою певних, властивих конкретному каналу методів і технологій несанкціонованого доступу. Найпоширенішим, різноманітним за методами несанкціонованого доступу, а тому і найнебезпечнішим каналом є встановлення контакту з особами, що мають або мали доступ до конфіденційної інформації.

Перш за все сюди входять особи, які працюють на даному підприємстві, а також не працюючі на ньому, але такі, шо мають доступ до конфіденційної інформації підприємства в силу службового становища (з органів влади, вищих, суміжних

підприємств і ін.). Не слід виключати з цього списку і осіб звільнених або відсторонених від даної конфіденційної інформації, але тих, що продовжують працювати на підприємстві, а також емігрантів і «перебіжчиків». Ця група найнебезпечніша, оскільки нерідко має додаткові причини для розголошення інформації (образа за звільнення, невдоволення державним устроєм і ін.).

Несанкціоноване підключення, а, отже, і несанкціонований доступ до конфіденційної інформації може здійснюватися:

- з персонального комп'ютера з використанням телефонного набору або з несанкціонованого терміналу зі зломом парольно-ключових систем захисту або без злому за допомогою маскування під зареєстрованого користувача;
- за допомогою програмних і радіоелектронних пристроїв;
- за допомогою прямого приєднання до кабельних ліній зв'язку, в тому числі з використанням паралельних телефонних апаратів;
- за рахунок електромагнітних наведень на паралельно прокладені дроти або методів високочастотного нав'язування;
- за допомогою високочастотного знімання, фільтрації і розпізнавання електромагнітних наведень в телекомунікаційних системах.

Як бачимо, несанкціонований доступ здійснюється через існуючі або спеціально створювані канали доступу, тобто гіпотетично дозволяє визначити шлях, використовуючи який, можна отримати недозволений доступ до конфіденційної інформації.

Склад реальних для конкретного підприємства каналів несанкціонованого доступу до конфіденційної інформації та ступінь їх небезпеки залежать від: виду діяльності підприємства, категорій носіїв, способів обробки інформації, системи її захисту, а також від прагнень і можливостей конкурентів. При цьому, якщо навіть конкуренти відомі, визначити їх наміри і можливості практично не вдається.

Отже, як розробка, так і безпосередньо створені засоби захисту інформації у своїй експлуатаційній сфері зобов'язані забезпечувати умови, при яких реалізується, з апріорі заданим

рівнем надійності, перекриття всіх потенційно існуючих для конкретного підприємства каналів уразливості і витоку інформації

5.2. Ділова розвідка як інтелектуальний інструментарій забезпечення стратегічного менеджменту фірми

Цілком виправдана думка, що об'єкти інформатизації являють собою певну сукупність інформаційних ресурсів, засобів і систем обробки інформації, які використовуються відповідно до заданої інформаційної технології, зокрема, й засоби забезпечення цих об'єктів інформатизації у вигляді будівель і споруд, у яких вони встановлені, включно з приміщеннями, призначеними для ведення конфіденційних переговорів. Як правило, у реальному житті всі ці окремі «об'єкти інформатизації» розташовані в межах одного підприємства та є сукупністю інформаційних ресурсів і систем обробки інформації. При цьому сучасне підприємство – це велика кількість різнорідних компонентів, об'єднаних у складну систему для виконання поставлених цілей, які в процесі свого функціонування можуть трансформуватися (модифікуватися), набуваючи нових якостей, зазвичай не властивих складовим її компонентам. Причому характерною особливістю подібних систем насамперед слід вважати як наявність людини в кожній з її складових, так і можливість потенційної і віддаленості, і просторової (on-line) відокремленості людини від об'єкта її діяльності. Переважно це пов'язано з тим, що множина компонентів, які становлять об'єкт інформатизації, інтегрально реалізується за допомогою сукупності трьох підсистем: 1) люди (біосоціальна підсистема); 2) техніка (технічні підсистеми і приміщення, в яких вони розташовані); 3) програмне забезпечення, що є інтелектуальним посередником між людиною і технікою (інтелектуальна підсистема).

Сукупність цих трьох підсистем (груп) і утворює соціотехнічну систему, де аспекти кадрово-інтелектуальної безпеки під час реалізації засобів захисту підприємства та супутньої штатної інформації буде розглянуто в розділі 7. У

цьому параграфі обмежимося лише викладом безпеки підприємства у сфері його конкурентоспроможності з позицій здійснення або ж протидії діловій розвідці як інтелектуального інструментарію забезпечення стратегічного менеджменту підприємництва.

Як відомо, основне завдання ділової (комерційної) розвідки - це забезпечення стабільного зростання стратегічного менеджменту підприємства (фірми), зокрема й у сфері його генеральної маркетингової стратегії (чи стратегій) [1]. Така розвідка зазвичай пов'язана з отриманням, передусім, сучасної штатної інформації прогресивного характеру, що й надає конкурентні переваги, які дають змогу ухвалювати грамотні рішення (стратегічного чи тактичного напряму діяльності), адекватні оперативній ситуації, що складається в умовах конкурентоспроможності, як одній з ключових характеристик економічної діяльності та її результатів.

Прийнято виділяти, принаймні, чотири її рівня: конкурентоспроможність товару (послуги), конкурентоспроможність фірми, регіональна та національна конкурентоспроможність. У наш час – це нагальна потреба будь-якої корпорації, яка хоче жити і розвиватися. Керівники підприємств не можуть дозволити собі опинитися на хиткому ґрунті неповної або, що ще гірше, неточної інформації про те, куди планують рухатися їхні конкуренти, або про те, як ті, хто ще не є конкурентами, швидко і таємно завойовують свою частку ринку. Вони розуміють, що перемога сьогодні всього лише дає можливість бути конкурентоспроможними завтра. Така діяльність отримала благозвучну назву – ***ділова розвідка***, яка має на увазі етично витримані і законодавчо не обмежені збір, систематизацію та аналіз відкритої інформації.

Слід розрізняти поняття ділової та конкурентної розвідок. Предметом ділової розвідки є зовнішнє оточення підприємства – ділова і політична кон'юнктура, законодавство, розподіл сфер впливу, в тому числі конкуренти. Мета ділової розвідки – отримання конкурентних переваг за рахунок отриманої інформації при прийнятті управлінських рішень. Ділова розвідка має два напрямки: стратегічна (або макроекономічна) і оперативна (або мікроекономічна) розвідка.

Стратегічна ділова розвідка – збір і аналіз інформації про процеси в економіці, політиці, технологіях. Оперативна ділова розвідка – збір інформації для прийняття управлінських рішень з поточних проблем підприємства. Роботу служби ділової розвідки можна умовно розділити на дві складові:

- систематичний збір інформації, наприклад, про кон'юнктуру ринку, макро- і мікроекономічні тенденції, нові товари та ін.;
- виконання спеціальних разових запитів в інтересах окремих служб: аналітичні огляди, пошук інформації в ЗМІ, фінансові оцінки інших підприємств, економічні показники та ін.

Відзначимо, що згідно з чинним законодавством протиправним є збір інформації про приватну особу. Збір інформації про приватну особу можливий тільки з його згоди, збір інформації про фірму не заборонений.

Предметом конкурентної розвідки є реальні і потенційні конкуренти, включаючи збір і аналіз інформації як про них, так і про ділове конкурентне середовище з метою формування і досягнення конкурентних переваг шляхом використання знання, отриманого в результаті, для прийняття ефективних та якісних стратегічних і важливих тактичних рішень.

Конкурентна розвідка (англ. Competitive Intelligence, скор. CI) – це збирання та опрацювання даних із різних джерел, для вироблення управлінських рішень з метою підвищення конкурентоспроможності комерційної організації, що проводяться в межах закону та з дотриманням етичних норм (на відміну від промислового шпигунства); а також структурний підрозділ підприємства, що виконує ці функції [2, с. 53-60].

Поняття «конкурентна розвідка», за визначенням Міжнародного товариства професіоналів конкурентної розвідки (англ. Society of Competitive Intelligence – SCIP, створено у 1986 році), – це законний спосіб збору та аналізу інформації з дотриманням етичних норм, що дозволяє судити про можливості, наміри, уразливості бізнес-конкурентів.

Отже, конкурентна розвідка – це цілеспрямована, постійна система збору, обробки, аналізу конкурентних відомостей і використання отриманої об'єктивної інформації про ділове середовище, а також про ресурси, уразливі елементи, наміри

конкурентів. Вона діє в рамках існуючого законодавства та етичних норм, спрямована на мінімізацію можливих ризиків, отримання переваг в організації бізнесу і додаткового прибутку. Конкурентна розвідка займається законним збором інформації про конкурентів і відрізняється від промислового шпигунства, оскільки джерела інформації для конкурентної розвідки завжди «відкриті» і загальнодоступні, хоча і не всі вони опубліковані або виставлені на загальний огляд.

Серед знакових відмінностей української конкурентної розвідки (КР) від загальноприйнятих у світі є так званий «інтелектуальний» фактор [3, с. 3-11]. За словами експертів, керівники та власники українських компаній часто недооцінюють або не розуміють значення КР. Вважається, що в цій діяльності є щось заборонене, таке, що не збігається з національними моральними цінностями. Водночас самі аналітики, які працюють у зазначеній сфері, свідчать: конкурентна розвідка - це спеціальна аналітична діяльність, спрямована на те, щоб її результати стали ефективним інструментом у справі стратегічного і тактичного планування. У КР не застосовується економічне шпигунство, а шляхом вивчення та аналізу відкритих інформаційних джерел робляться висновки з необхідного питання. Звісно, це складний вид діяльності, але, як показує практика, без КР у сучасному світі не обійтися [4].

Тут під **промисловим шпигунством** розуміють якусь форму недобросовісної конкуренції, при якій здійснюється незаконне отримання, використання, розголошення інформації, що становить комерційну, службову або іншу таємницю, яка охороняється законом, з метою отримання переваг при здійсненні підприємницької діяльності, а так само отримання матеріальної вигоди. Тобто в основі промислового шпигунства, як виду діяльності, лежить здобування і подальше використання комерційної або службової таємниці. Фактично в цьому і полягає відмінність конкурентної розвідки від промислового шпигунства: конкурентна розвідка – це діяльність в рамках правового поля, а промислові шпигуни «працюють» за рамками цього поля.

Традиційно процес формування конкурентоспроможності підприємства представлявся у вигляді формування унікального ланцюжка цінностей: постачальник-підприємство-споживач, що володіє тими чи іншими перевагами (якість, терміни виконання замовлень, рівень цін та ін.) порівняно з іншими аналогічними ланцюжками. Перехід до інформаційного суспільства супроводжується змінами у функціонуванні ринкових механізмів: зростає роль інформації у конкурентних відносинах, скорочуються видатки на прийняття рішень, на вибір конкурентної стратегії, що, безумовно, змінює поведінку підприємства. Бурхливий розвиток передових інформаційних і комунікаційних технологій фундаментально змінив природу ринкових і конкурентних взаємин, сприяв появі нових можливостей для конкуренції, економічного і соціального розвитку. Такі нові інформаційно-технічні системи, як Інтернет, персональні комп'ютери і мобільний зв'язок перетворили інформацію в основний ресурс розвитку суспільства, створивши передумови для домінуючого положення інформаційного сектора в сучасній світобудові.

Розвиток конкуренції вимагав докорінної перебудови внутрішньо фірмових систем управління, а також зміни основних поглядів на цілі, принципи та інструментарій управління підприємницькими структурами. У сучасних умовах підприємства стають все більш залежними від подій, що відбуваються у зовнішньому середовищі, а його нестабільність стає одним з основних джерел ризиків існування. Отже, особливої актуальності набуває розробка внутрішніх механізмів сканування ділового середовища, з метою раннього виявлення в ній ознак значущих змін, розпізнавання характеру і прогнозування їх наслідків для нормальної життєдіяльності з метою запобігаючого опрацювання та прийняття превентивних рішень, спрямованих на забезпечення конкурентоспроможності підприємства [5].

Принципове значення для забезпечення конкурентоспроможності сучасних підприємств набувають регулярний збір, оновлення, коректна систематизація і формалізація всієї сукупності інформації про сферу її діяльності. Розглянуті зміни в управлінні інформаційними ресурсами

підприємства з метою забезпечення його конкурентоспроможності мають своїм наслідком трансформацію традиційної системи функцій, що, природно, відбивається на організаційній структурі підприємства. Через збільшення організаційної та технічної складності задач формування, актуалізації та використання інформаційних ресурсів підприємства, інформаційно-аналітичні структури підприємства трансформуються в організаційно відокремлювану підсистему ділової розвідки.

Таким чином, *основне завдання ділової (комерційної) розвідки***,** – це вироблення стратегічного менеджменту (сукупності методів управління підприємством) підприємства, його генеральної, у тому числі маркетингової (комплекс організаційних, рекламних та інших заходів, що забезпечує стійкий збут продукції) стратегії (або стратегій), на основі володіння:

- ✓ інформацією попереджувального характеру;
- ✓ інформацією, що надає конкурентні переваги (тактичного або стратегічного характеру);
- ✓ інформацією, що дозволяє приймати грамотні рішення,

адекватні оперативній обстановці, яка складається, і умов оточуючого конкурентного, агресивного середовища.

При цьому, в умовах інтеграції інформаційних потоків і надмірної завантаженості комунікацій необхідне комплексування діяльності їхнього менеджменту з ведення розвідки. Тільки так можна запобігти загрозам зовнішнього середовища, що носять різнобічний, комплексний характер, своєчасно виявивши «слабкі сигнали» про початок деструктивних процесів і прийнявши превентивні заходи з нейтралізації ризиків. З іншого боку, більш повна та оперативна інформованість дозволяє створити передумови для використання шансів своєчасного і безболісного «вбудовування» фірми в сприятливі тенденції розвитку ринків, модернізації господарських інститутів, зміни в державному регулюванні та ін. Отже, в сучасних умовах доцільно використовувати більш «ємний», «широкий» термін у вигляді, – «ділова розвідка».

Тут складова терміну «ділова» означає, що мова йде про господарську діяльність і впливаючі на неї фактори. А слово

«розвідка» слід сприймати як комплекс специфічних інформаційних процесів. У найбільш загальному розумінні ділова розвідка позначає особливу форму діяльності менеджменту фірми, що включає цілеспрямований пошук, у тому числі з використанням сучасних технічних засобів, інформації про стан і тенденції зміни ділового середовища фірми, комплексне вивчення отриманих матеріалів, а також аналіз повідомлень, публікацій та виступів у засобах масової інформації, статистичних даних, відомостей із загальнодоступних (публічних) банків даних з метою виявлення чинників, що впливають на конкурентоспроможність фірми, виявлення механізмів цього впливу і розробки пропозицій, спрямованих на підвищення ефективності управління конкурентоспроможністю з урахуванням факторів зовнішнього середовища.

Розгляд поняття «ділова розвідка» пов'язане не тільки з термінологічними новаціями в управлінні. Йдеться про більш глибокі зміни. Відмінність інформаційно-аналітичної роботи традиційних служб (маркетингової, фінансової, кадрової та ін.) від діяльності підрозділів ділової розвідки можна порівняти з відмінностями інформації та комунікації. Якщо інформацією прийнято позначати деякі відомості, одержувані разово, то комунікація носить більш регулярний характер і крім власне інформації, включає в себе ряд суб'єктів, що беруть участь в її генеруванні, кодуванні, передачі та обробці. І якщо інформаційно-аналітична діяльність найчастіше закінчується передачею інформації кінцевому користувачу (або її накопиченням у форматі, зручному для інтерактивного використання), то ділова розвідка своїм результатом має дію. Тому її ефективність, з позицій вирішення задач забезпечення конкурентоспроможності, набагато вище.

Цілями створення підрозділів ділової розвідки можна вважати не тільки виявлення на можливо більш ранній стадії загроз конкурентних переваг підприємства і сприяння в управлінні ризиками бізнесу, але також розкриття і оцінку сприятливих можливостей, що впливають на успіх бізнесу, забезпечення конкурентних переваг за рахунок своєчасного (превентивного – на основі аналізу «слабких» сигналів)

прийняття управлінських рішень. Тобто ведення ділової розвідки тісно пов'язане зі стратегічним менеджментом і забезпеченням конкурентоспроможності.

В якості основних задач ділової розвідки можна виділити як традиційні, що розглядаються як типові задачі інформаційного забезпечення діяльності менеджменту:

1) збір важливої для формування і забезпечення реалізації конкурентних переваг фірми інформації на регулярній основі;

2) автоматизований аналіз зібраних відомостей;

3) своєчасне інформування штабних фахівців, функціональних і лінійних керівників про критично важливі події;

4) забезпечення підготовки можливих варіантів рішень;

5) оцінка сценаріїв розвитку подій та ін.,

так і нові, пов'язані з розвитком інформаційних технологій і формуванням основ інформаційно-мережевої економіки, а саме:

1) аналіз неструктурованої і структурованої інформації з метою отримання нових знань (закономірностей, причинно-наслідкових зв'язків та ін.);

2) синтез нових знань, що впливають на ефективність менеджменту.

Таким чином, якісна відмінність ділової розвідки від інших інструментів управління полягає в тому, що даний інструмент забезпечення конкурентоспроможності є більш інтелектуальноємним. Він вимагає для свого ефективного застосування адекватних ресурсів:

- ***інформаційно-технологічних*** (програмне забезпечення, мережі передачі даних, обчислювальні пристрої, корпоративні сховища інформації та ін.),

- ***кадрових*** (спеціально підготовлених фахівців, що володіють навичками і знаннями як в області інформаційно-аналітичних технологій, так управлінськими і економічними),

- ***науково-методичних*** у вигляді алгоритмів і систем продукування нових знань, різних механізмів інтелектуального виведення, експертних систем і т. д.

Фактично дана діяльність ділової (комерційної) розвідки здійснюється *пасивними методами***,** (тобто роботою з вторинними джерелами, що в більшості випадків має на увазі

методи конкурентної розвідки) і ***активними методами*****,** тобто роботою з першоджерелами (агентурні можливості), підключаючи різнопланові методи здобування достовірної розвідувальної інформації у вигляді спостереження або проведенням активних заходів.

Активні методи розвідувальної діяльності дуже часто, і небезпідставно, відносять до методів промислового шпигунства, проте саме вони можуть надати конкурентні переваги фірмі (її розвідувальному органу), яка здійснює розвідку. При цьому зовсім необов'язково, що методи ділової (комерційної) розвідки є злочинними (протизаконними), інша справа, що в більшості випадків вони здійснюються негласно, тобто таємно. Аналогічно можна стверджувати, що контррозвідувальна діяльність (контррозвідка), призначена в нашому випадку для захисту і забезпечення безпеки суб'єкта підприємницької діяльності, здійснюється також негласно, тобто таємно. Як об'єкти контррозвідки можуть виступати різні фактори групи ризику, які здійснюють, у тій чи іншій мірі негативний вплив на суб'єкт захисту, основними з яких є:

- протиправна діяльність конкурентів, кримінальних структур,
- прояв фактів промислового (комерційного) шпигунства, шахрайства та інших діючих ризиків.

Основне завдання контррозвідки, – забезпечення безпеки і захист суб'єкта підприємницької діяльності, тобто несе оборонний характер перш за все проти промислового шпигунства.

Чітку межу між промисловим шпигунством і діловою розвідкою провести важко. І все ж головна відмінність ділової розвідки полягає в тому, що вся інформація здобувається законними способами.

Якщо в промисловому шпигунстві використовують методи, які мають на увазі пряме порушення закону: шантаж, підкуп, злодійство, насильство, фізичне усунення, – то в діловій розвідці неможливе звернення до таких прийомів. Інший аспект – це дотримання норм моралі. Адже в даному випадку при їх порушенні не буде ніяких каральних акцій. Тому багато компаній декларують кодекс поведінки, піклуючись про ім'я та репутацію

фірми і страхуючи себе від безлічі негативних наслідків (наприклад, судових розглядів).

Як етичні принципи ведення ділової розвідки виділяють, перш за все, відмову від отримання інформації шляхом обману, шантажу і відмову від протиправних дій.

В принципі, всі виділені аспекти зайвий раз нагадують про те, що при проведенні ділової розвідки необхідно використовувати законні методи, недотримання цих норм тягне за собою дисциплінарну, цивільно-правову, адміністративну або кримінальну відповідальність.

Як правило, більшу частину всієї інформації розвідка отримує з відкритих джерел. Наприклад, через Інтернет відкривається доступ до ЗМІ, сайтів компаній, професійних баз даних і т. п. Інтернет-мережа надає можливість отримати відомості про будь-яку людину, товар, підприємство. Головна проблема такого пошуку в тому, що дані не структуровані і часто їх неможливо знайти за допомогою пошукових систем. Друга група джерел – всілякі паперові документи: підшивки газет і журналів, реклама, прес-релізи, легальні бази даних держустанов. Особливо часто використовуються державні бази даних і недержавні бази даних, наприклад, складені на основі публікацій провідних видань, за допомогою яких можна отримати велику інформацію про конкретні персоналії і компанії. Широко використовують *метод візуального моніторингу (спостереження),* – у сферу огляду і аналізу може увійти буквально все, що дає матеріал про товарний асортимент, роботу персоналу, послуги, цінову політику, портрети покупця і т. п. аж до неформального спілкування з колегами і партнерами. Часто крихти інформації можна виявити в необережному інтерв'ю або необдуманому коментарі. Навіть реклама або список опублікованих вакансій здатні навести на роздуми про плановані заходи. Очевидно, що без застосування сучасних комп'ютерних технологій і вміння працювати з інформацією позитивних результатів не буде. При цьому мова йде про роботу не стільки із засобами масової інформації, скільки зі спеціальними, складними інформаційними системами, що забезпечують доступ до всіх відкритих джерел. Практичне використання програмних продуктів мережевої розвідки дає, зокрема, можливість:

- постійно відстежувати і аналізувати інформацію, що має відношення до ділової діяльності клієнта;

- вибирати специфічну інформацію, яку зазвичай не надають інформаційно-пошукові системи загального користування;

-налагодити постійний потік інформації про дії конкурента (таких як цінова політика, злиття і поглинання, рекламні оголошення і анонси);

-розкривати плани конкурента ще до їх реалізації;

-проводити вивчення потенційного попиту на продукцію і послуги.

Основний принцип інформаційної розвідувальної діяльності є чіткий поділ понять виду: дані (відомості), інформація і знання.

При цьому найчастіше змішують понятійні терміни «дані» та «інформація», – часто буває багато даних, а інформації – недостатньо. Слід розуміти, що дані засновані на фактах (перш за все це можуть бути статистичні дані, або уривчаста інформація про об'єкти або суб'єкти спостереження і т. д.), тобто про все те, що являє оперативний інтерес. Інформація, навпаки, являє собою певну сукупність даних, які були відібрані, оброблені і проаналізовані, після чого їх можна використовувати для подальших дій для винесення синтезованих рішень або рекомендацій, що представляє собою кінцевий інформаційний продукт у вигляді знання.

Очевидно, що тому, хто приймає рішення, потрібні не просто дані, а саме така інформація, яка в процесі самого отримання, подальшої фільтрації і розпізнавання, скрупульозного аналізу і оцінки, дозволили б йому перетворити вихідну інформацію в знання. Тому при вирішенні будь-якої інформаційної задачі необхідно сформулювати її мету, терміни виконання, обсяг роботи, форму викладу і методику рішення, підхід до роботи. Останній повинен залежати від того, в яких напрямах будуть використані отримані результати. Зазвичай починають з уточнення використовуваних понять, оскільки питання термінології завжди вважався найскладнішим у будь-якій сфері діяльності. Чіткі визначення змушують чітко мислити і зосередитися на досягненні дійсно бажаної цілі та захищають від помилок. Далі деталізують наявні джерела отримання інформації

із зазначенням граничних меж використання кожного джерела і області їх достовірності. Чим більше джерел, тим легше зробити повторну перевірку. При використанні багатьох джерел розвідувальна інформація отримує більш широку основу, питання, що розглядаються, висвітлюються глибше і зменшується можливість допуститися серйозної помилки.

Фактично інформаційне забезпечення ділової розвідки складається з етапів ознайомлення з об'єктом розвідки, визначення використовуваних термінів і понять, збору фактів і їх тлумачення, побудови робочих гіпотез і їх апробація на достовірність і, заключного рішення з формулюванням отриманих результати у вигляді висновків із зазначенням ступеня достовірності кожного твердження

5.3. Аспекти менеджменту ризику інформаційної безпеки та модель потенційного порушника

У попередніх розділах були розглянуті аспекти уразливості інформації з точки зору визначення складу інформації, що потребує захисту, та її класифікації за видами таємниці і ступенями конфіденційності, а також види і джерела дестабілізуючого впливу на інформацію і її підтримуючої інфраструктури. Тому, процес їх штатної та безпечної реалізації завжди потребує адекватного захисту від сучасних інформаційних атак на адресу не лише держави, а й у напрямку підприємства та особистості (див. рис. 5.1). Раніше були використані такі терміни як загроза, вразливість, ризики у сфері інформаційної безпеки, однак без акцентування на небезпеку їхньої підміни та використання як синонімів у сфері передавання та захисту інформації. Хоча і, (орієнтуючись на міжнародні стандарти серії ISO/IEC 27000, ухвалених Міжнародним союзом електрозв'язку та відповідні вітчизняні ДСТУ, наприклад [6 - 8]), існують їх різні визначення.

Наприклад, у термін (поняття) ризику, особливо під час представлення інформаційної безпеки підприємства з її супутньою системою циклічності ухвалення рішень щодо вибору засобів адекватного захисту та управління інформацією (які

зазвичай розглядаються як єдиний об'єкт критичної інфраструктури - ОКІ) [9] часто вкладають різний, (див. мал. 5.2 та 5.3), смисловий зміст [10]:

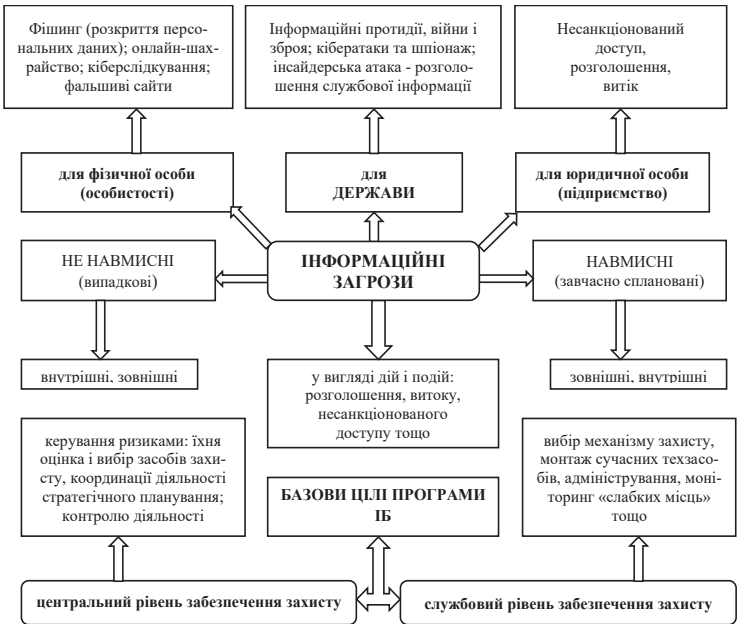

Рисунок 5.1. Види сучасних інформаційних загроз та базові цілі програми інформаційної безпеки

- або як поєднання ймовірності події та її наслідків;
- або як імовірність заподіяння шкоди внаслідок того, що певну загрозу (об'єкту дослідження) реалізують унаслідок наявності певної вразливості (цього об'єкта);
- або як поєднання ймовірності події та її наслідків у вигляді потенційної небезпеки заподіяння шкоди організації внаслідок реалізації певної загрози з використанням вразливостей активу або групи активів;

- або як поєднання ймовірності заподіяння шкоди й тяжкості її завдання що стосується події, її наслідків або ймовірності, розуміння або знання про неї

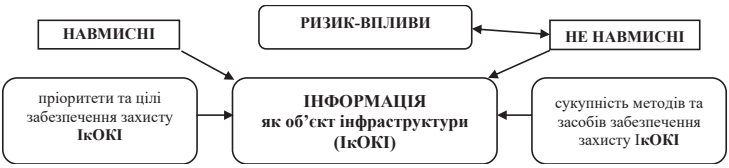

Рисунок 5.2. Представлення інформації як ОКІ із супутніми ризик-впливами

Дуже часто ризик характеризується посиланням на потенційні «події» та «наслідки» або їхню комбінацію чи виражається у вигляді комбінації наслідків події (включно зі змінами обставин) і пов'язаної з ними «ймовірності» настання.

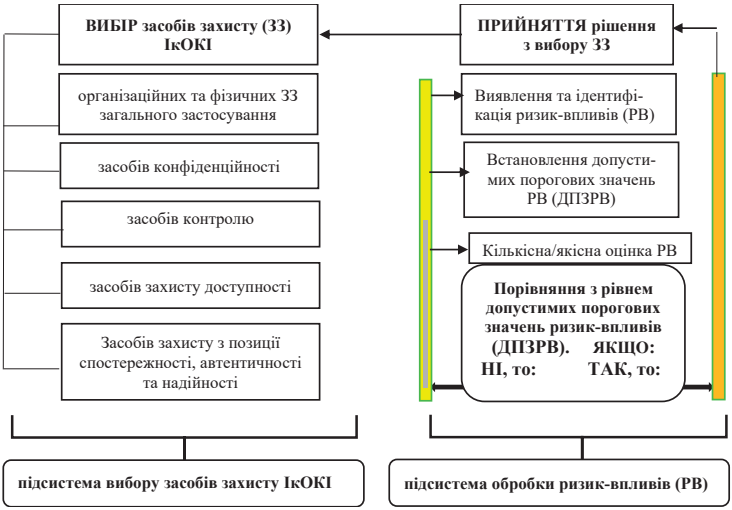

Рисунок 5.3. Представлення циклічності прийняття рішень з вибору засобів захисту (ЗЗ)

Трохи конкретніше йдуть справи з поняттями загроза і вразливість. Так загроза (див. мал. 5.4 та 5.5, згідно [12 та 13]), - це:

- або потенційна причина небажаного інциденту, результатом якого може бути нанесення шкоди системі або організації;
- або сукупність умов і чинників, що створюють потенційну або реально існуючу небезпеку порушення безпеки інформації;
- або сукупність умов і чинників, що створюють небезпеку несанкціонованого, у тому числі випадкового, доступу до службових даних, результатом якого може стати їх знищення, зміна, блокування, копіювання, поширення, а також інших несанкціонованих дій під час їх оброблення в іншій інформаційній системі;
- або потенційне джерело небезпеки, шкоди тощо.

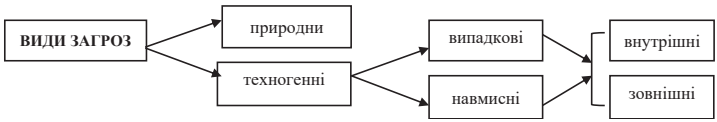

Рисунок 5.4. Загальна класифікація загроз для інформації в інформаційно-телекомунікаційних систем (ІТС) згідно [11]

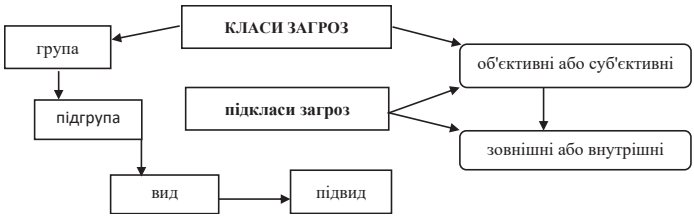

Рисунок 5.5. Класифікація загроз безпеці згідно [13, с.11. Рекомендації MCE-T X.ncns-1, Архітектура і структура безпеки: National IP-based Public Networks Security Center for Developing Countries. Женева, квітень 2011]

Щодо терміна уразливості (vulnerability) можна констатувати (див. рис. 5.6, адаптованому з [14]), що це:

- або слабкість одного або декількох активів, яка може бути використана однією або декількома загрозами;

- або пролом, через який з'являється можливість реалізації в інформаційній системі загроз для її безпеки та для інформації, яка в ній обробляється;

- або це вада (слабкість) програмного (програмно-технічного) засобу або системи та мережі загалом, який(а) може бути використаний(а) для реалізації загроз безпеці інформації.

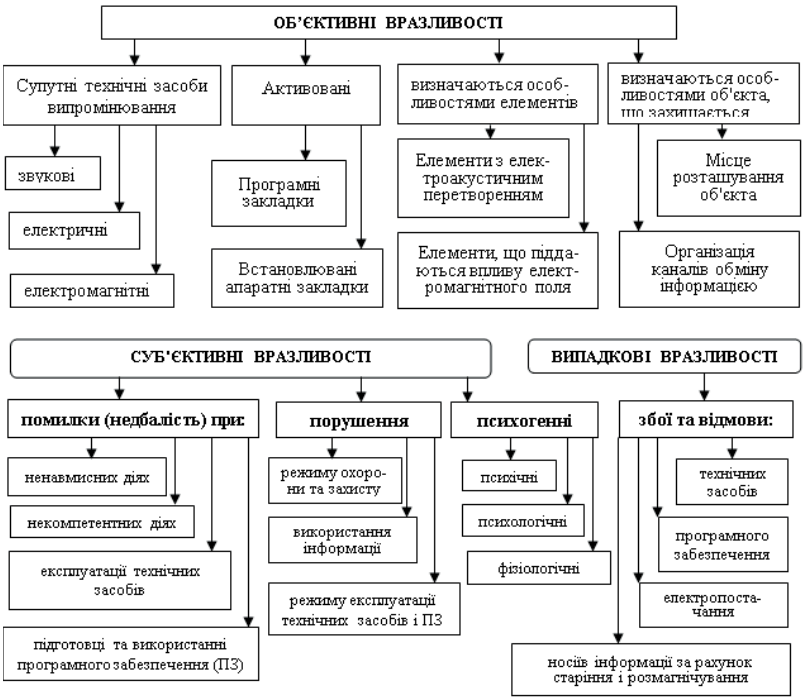

Рисунок 5.6. Уразливості безпеки інформації в ІТС: об'єктивні *(залежать від устаткування);* ***суб'єктивні*** *(залежать від дій співробітників);* ***випадкові*** *(залежать від довкілля тощо)*

Таким чином, незважаючи на те, що немає єдиного загальноприйнятого визначення для таких ключових у галузі інформаційної безпеки понять, як ризик і загроза, можна їх узагальнити у вигляді лінгвістичного твердження, що:

Ризик = Загроза + Вразливість + Актив,

де Загроза - це щось погане, Вразливість - це особливість активу, а Актив може бути будь-яким об'єктом нашого розгляду (дослідження). При цьому алгоритм процесу оцінки ризику може відповідати його структурно-функціональній схемі, наведеній на рис.5.7, адаптованому з [13, с. 10].

Рисунок 5.7. Структурно-функциональная схема процесса оценки риска

Отже, у контексті наведеного вище розгляду систем менеджменту інформаційної безпеки ризики інформаційної безпеки можна оцінити з позицій впливу невизначеності на цілі інформаційної безпеки, де їхнє нівелювання насамперед пов'язане з усуненням потенційних вразливостей виробничої діяльності підприємства і його негативного впливу на штатну роботу інформаційних активів з метою підвищення конкурентоспроможності організації. Причому, під час реалізації систем інформаційної безпеки центральне місце в системі її управління належить інформаційно-телекомунікаційним системам (ІТС), кількісно-імовірнісна оцінка яких, безсумнівно, є актуальною задачею.

У великому різноманітті підходів і методик оцінки ризиків працездатності таких систем віддамо перевагу методиці оцінки ризиків для активів інформаційно-телекомунікаційних систем,

що задовольняє вимогам міжнародних стандартів і рекомендацій і вимог національного законодавства та регламентує цю сферу діяльності, виходячи з посилу, що ризик порушення безпеки - це можливість реалізації загрози, яка завдає шкоди (збитків) її власнику. Існує кількісна та якісна оцінка ризиків. Суть кількісної оцінки ризиків зводиться до пошуку єдиного оптимального рішення з організації захисту інформації з безлічі наявних. До кількісних методик управління ризиками належать такі методики, як: CRAMM (CCTA Risk Analysis and Management Method) і їй подібні. Суть якісного оцінювання ризиків зводиться до проведення загальних і приватних оцінок, що дають змогу виробити обґрунтоване рішення про необхідність захисту інформації з оцінкою майбутніх витрат на цей захист. До якісних методик управління ризиками належать такі методики та відповідні програмні продукти, як: MSAT (Microsoft Security Assessment Tool) тощо. [14].

Очевидно, що **розробка ефективних моделей і методів управління безпекою ІТС з метою протидії кібернетичній злочинності,** є актуальною і складною задачею, що зумовлена такими ***факторами,*** як [15]:

- необхідністю виконання сукупності технічних вимог для спільної роботи програмних продуктів і обладнання різних виробників;
- необхідністю ефективного використання каналів зв'язку та дотримання вимог електромагнітної сумісності;
- наявності потенційних загроз для безпеки ІТС і оброблюваної в ній інформації;
- необхідності здійснення не передбачуваних або запланованих модернізацій;
- надмірний рівень собівартості та інше.

При цьому, з огляду на широкий спектр юридичних і фізичних осіб, що надають послуги, обладнання і програмне забезпечення для інформаційно-телекомунікаційних систем Міжнародним союзом електрозв'язку в рекомендації МСЕ-Т Х.805 запропонована архітектура захисту для систем, що забезпечують зв'язок між кінцевими пристроями [16]. Вона забезпечує комплексну, від верху до низу наскрізну область мережевого захисту і може застосовуватися до елементів мережі,

послуг і додатків, з тим, щоб виявляти, прогнозувати і виправляти вразливість захисту.

Прийнята архітектура захисту систем, що забезпечують зв'язок між кінцевими пристроями, дозволяє більш якісно провести оцінку ризику безпеки ІТС. З цією метою, виходячи з рекомендацій міжнародного стандарту ISO / IEC 27005 «Менеджмент ризику інформаційної безпеки», у початковій стадії прийняття рішення проводиться облік активів, вразливість яких може вплинути на ступінь захищеності ІТС. У зв'язку з чим необхідно виділяти такі площини захисту ІТС у вигляді: *управління, контролю і кінцевого користувача*.

Дотримуючись рекомендацій МСЕ-Т Х.805 [16], для кожної площини відповідно до призначення, виявляються активи, які відносяться до рівня інфраструктури, послуг, що надаються, застосовуваних програм. Безумовно, до цього процесу повинен бути задіяний персонал, що має високу кваліфікацію, досвід роботи і навички ділової та управлінської взаємодії.

На наступному етапі визначаються загрози для ідентифікованих активів. Загрози для ІТС за своєю природою поділяються на природні та техногенні, останні в свою чергу діляться на випадкові і навмисні. На даному етапі також визначається джерело загроз і «область» дії загрози, тобто, на які складові частини ІТС може впливати дана загроза.

Вимірювання захисту (тобто його оцінка) за своєю суттю представляють у вигляді комплексу реалізованих заходів щодо захисту ІТС. Прийнято виділяти вісім основних вимірів захисту [16] у вигляді:

1) управління доступом;
2) автентифікації;
3) збереження інформації;
4) конфіденційності даних;
5) безпеки зв'язку;
6) цілісності даних;
7) доступності;
8) секретності.

Цілком очевидно, що у разі успішної реалізації загрози активам може бути завдано шкоду, яка може привести до втрати властивостей інформації або керованості ІТС, тобто її: цілісності

(i); доступності (a); конфіденційності (c); спостережності наблюдаемості (s). Тоді результати оцінки вразливості активів на прикладі апріорних загроз, які потенційно можуть бути реалізовані з урахуванням вразливості протоколів міжмережевої взаємодії, доцільно представляти, наприклад, у вигляді таблиці 5.1. Використовуючи ці дані, можна отримати кількісну оцінку вразливості конкретного активу від ймовірних загроз за такою формулою:

$$T_k = \frac{\{c_k + i_k + a_k + s_k\}}{4} \cdot p_k$$

Таблиця 5.1 Загрози для інформаційної безпеки ІТС

№	Загрози	Конфіденційність	Цілісність	Доступність	Спостережність	Ваговий коефіцієнт
1	Аналіз протоколів	c_1	i_1	a_1	s_1	p_1
2	Сканування мереж	c_2	i_2	a_2	s_2	p_2
3	Автоматичний підбір паролів	c_3	i_3	a_3	s_3	p_3
4	Spoofing	c_4	i_4	a_4	s_4	p_4
5	Захват мережевих підключень	c_5	i_5	a_5	s_5	p_5
6	Підміна мережевих об’єктів	c_6	i_6	a_6	s_6	p_6
7	Рознесена відмова в обслуговуванні	c_7	i_7	a_7	s_7	p_7
8	Віддалене вторгнення	c_8	i_8	a_8	s_8	p_8

Ваговий коефіцієнт p_k визначає частоту появи даної загрози щодо сукупності можливих загроз і обчислюється на основі аналізу статистичних даних або з використанням відомих методик [15]. Надалі питання прийняття ризику в спрощеній

формі зводиться до алгоритму, представленого на рисунку 5.8, реалізація закінчення якого не здійснюється до тих пір, поки $N \neq N_{max}$.

Таким чином, оцінка ризиків – це процес, який охоплює ідентифікацію ризику, його аналіз і порівняльну (в тому числі кількісно-ймовірнісну) оцінку

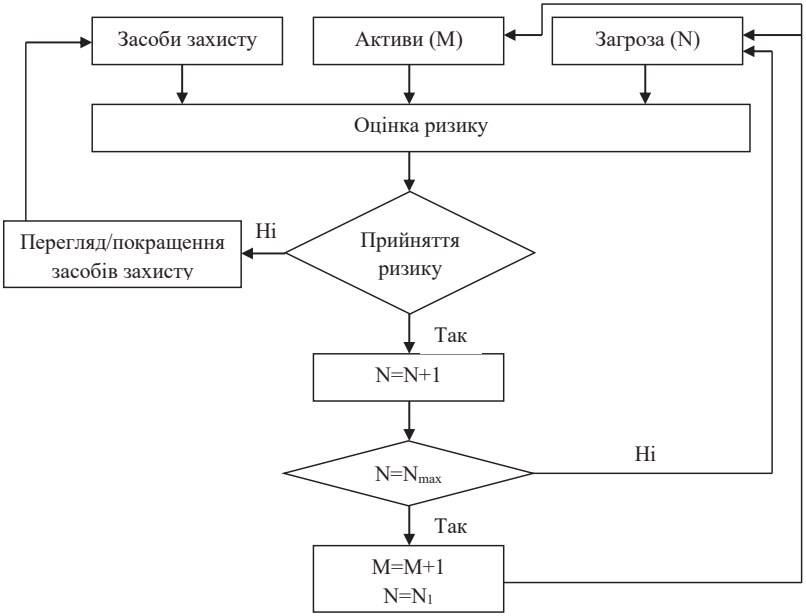

Рисунок 5.8 – Блок-схема алгоритму оцінювання ризику ІБ

Типовий проект з оцінки ризиків інформаційної безпеки зазвичай включає наступні стадії:

1. Підготовка проекту, тобто визначення меж проведення оцінки ризиків, узгодження термінів проведення, визначення залучених фахівців з боку Замовника;

2. Початок проекту, – це отримання вихідних даних від Замовника, вивчення бізнес-цілей компанії (підприємства) і галузевих особливостей, складання карти активів;

3. Проведення обстеження, що включає збір інформації про організаційні заходи (це вивчення політик, положень, інструкцій, програм і результатів навчання співробітників, проведення інтерв'ювання відповідальних співробітників Замовника, спостереження за роботою співробітників Замовника) і про технічні засоби (у вигляді інструментального аналізу інформаційної інфраструктури, вивчення документів, що описують роботу технічних засобів, та існуючих налаштувань технічних засобів), а також про фізичну безпеку підприємства у вигляді огляду приміщень, аналізу існуючих процедур і застосовуваних засобів забезпечення фізичної безпеки;

4. Побудова моделі загроз, пам'ятаючи, що актуальність та повнота складеної моделі загроз безпеки інформації є визначальною умовою успішної і достовірної оцінки ризиків. При цьому, модель загроз безпеки інформації є унікальною для кожної компанії. Як правило, при побудові моделі загроз безпеки інформації використовуються каталоги загроз, наприклад, описані в методичних документах регулюючих органів і галузевих регуляторів країни Складений перелік загроз, як правило, доповнюється загрозами, виявленими під час проведення обстеження Замовника.

5. Аналіз ризиків, який реалізує:

- оцінку активів на основі інформації, отриманої на етапах початку проекту і проведення обстеження. Оцінка активів може бути як кількісна, так і якісна;
- оцінку вразливостей, виявлених у ході проведення обстеження. Оцінка вразливостей може проводитися з використанням різних методик;
- оцінку загроз у вигляді обчислення ймовірності її виникнення;
- розрахунок ризиків по якісній або кількісній методиці;
- ранжування ризиків з метою визначення черговості обробки ризиків.

6. Розробку плану обробки ризиків, тобто вибір оптимальних захисних заходів, оцінка їх вартості та ефективності, розробка пропозицій щодо вжиття, уникнення або передачі частини ризиків.

По закінченню виконання типового проекту з оцінки ризиків інформаційної безпеки зазвичай відбувається презентація результатів оцінки ризиків керівництву компанії і технічному персоналу.

Очевидно, що у зв'язку з широким спектром загрозливих факторів, безпеку об'єкта, що захищається, повинна бути комплексною для вирішення задач підтримки безпечного стану об'єкта, попередження загроз, їх виявлення, протидії загрозам, ліквідації наслідків максимальної кількості з повного набору можливих загроз для даного об'єкта.

Особливе місце відведено людському фактору, пов'язаному з виявленням і припиненням дій людей, що намагаються таємно або відкрито (але несанкціоновано) проникнути на територію об'єкта, що охороняється. В сучасних умовах несанкціоновані дії фізичних осіб (диверсантів, терористів, злочинців, екстремістів) становлять особливу небезпеку, так як можуть привести до виникнення більшості прогнозованих загроз. Тому на етапі аналізу загроз формується модель імовірних виконавців погроз (порушників) у вигляді моделі порушника, тобто виробляються типові як кількісні, так і якісні їх характеристики (оснащеність, тактика дій і т. п.). **Фактично модель порушника – це сукупність параметрів і характеристик, властивих потенційному порушнику, що визначають його ймовірні дії.**

Існує наступна ***класифікація порушників*** (виконавців загроз) у залежності від їх підготовленості [17]:

1) *Випадковий порушник* – той, який не знає, що об'єкт охороняється і не має спеціальної цілі проникнення на об'єкт.

2) *Непідготовлений порушник* – здатний проникнути на об'єкт зі спеціальною ціллю і такий, що передбачає можливість охорони об'єкта, але не має уявлення про систему охорони і принципи її функціонування. Напрямок вторгнення такого порушника переважно визначається прилеглою до об'єкта топологією місцевості (дороги, стежки і т. д.), наявністю міської забудови.

3) *Підготовлений порушник* – має інформацію про можливі методи обходу діючих засобів охорони, який пройшов відповідну підготовку приховано долати зони виявлення засобів зі складу комплексної системи безпеки. Як правило, він має уявлення про

фізичні принципи функціонування засобів виявлення, але не має відомостей про організацію системи охорони. Напрямок вторгнення визначається порушником після попереднього вивчення об'єкта з метою гарантованого подолання зони виявлення. Топологія місцевості і міська забудова прилеглої території також відіграють роль.

4) *Обізнаний порушник* – володіє спеціальною підготовкою, який має відомості про організацію системи охорони на об'єкті. Як правило, він знає фізичні принципи функціонування засобів виявлення і має навички подолання зон виявлення.

5) *Співробітник підприємства або охоронець* – володіє спеціальною підготовкою, часто діє в змові з обізнаним порушником (характерно для великого підприємства).

В основі ефективної протидії загрозам проникнення порушника у приміщення, що охороняються (сейфові кімнати, переговорні приміщення, архіви конструкторсько-технологічної документації, сховища інформаційних баз даних і т. п.) лежить проведення наступних апріорних оцінок:

- пріоритетів у системі захисту (тобто слід визначити, що може становити великий інтерес для порушника і має захищатися в першу чергу);
- шляхів можливого проникнення порушників;
- інформації, якою може володіти порушник про організацію системи захисту підприємства;
- технічних можливостей порушника (його технічної озброєності).

Розглянута вище сукупність оцінок дозволяє деталізувати поняття «моделі» порушника і уточнює кількісні та якісні характеристики ймовірного порушника. Така модель, поряд з категорією об'єкта, служить основою для вибору методів організації охорони об'єкта, визначає складність і скритність застосовуваних технічних засобів охоронної сигналізації та відеоспостереження, варіанти інженерно-технічного захисту, кадровий склад служби охорони і т. д.

Спроба реалізувати несанкціонований доступ до інформаційних мереж з метою що-небудь зробити з даними в мережі є **комп'ютерне піратство,** а особи, схильні до цих дій в залежності від цілей або мотивів, підрозділяють на ідейних

хакерів, шукачів пригод, хакерів-професіоналів, ненадійних співробітників.

Шукач пригод, – зазвичай молодий студент або школяр, без продуманого плану реалізації атак. Він вибирає випадкову ціль. Ідейний хакер – вибирає конкретну ціль. Свої досягнення розповідає широкій аудиторії або розміщує дані на веб-ресурсах. Хакер-професіонал – це людина з чітким планом дій. Його атаки (збір інформації та безпосередній злом) продумані. Зазвичай такі люди фінансуються для цілей, які йому не властиві, але йому платять. Ненадійний співробітник небезпечний, його дії можуть мати великі наслідки, так як він довірена особа системи. Йому не потрібно вигадувати складні атаки для реалізації своєї мети. Існує думка, що близько 70% всіх порушень, пов'язаних з безпекою інформації, відбуваються саме співробітниками підприємства. Людина, крім усього іншого, є першим за значимістю носієм інформації. Вона забезпечує функціонування системи, її охорону і захист. У той же час вона, за певних обставин, може стати головним джерелом загрози інформації, що захищається.

Для досягнення своїх цілей порушник повинен докласти певних зусиль, витратити певні ресурси. Дослідивши причини порушень, можна вплинути на самі ці причини (звичайно, якщо це можливо), або точніше визначити вимоги до системи захисту від даного виду порушень чи злочинів.

У кожному конкретному випадку, виходячи з конкретної технології обробки інформації, може бути визначена своя модель порушника, яка повинна бути адекватна реальному порушнику для даної системи.

При конкретизації моделі порушника визначаються [17]:

- припущення про категорії осіб, до яких може належати порушник;

- припущення про мотиви дій порушника (цілях, що переслідує порушник);
- припущення про кваліфікацію порушника і його технічної оснащеності (про використовувані для вчинення порушення методах і засобах);

- обмеження і припущення про характер можливих дій порушників.

Очевидно, що відносно охоронюваної системі **порушники** можуть бути як ***внутрішніми*** (з числа персоналу системи), так і ***зовнішніми*** (сторонніми особами), а їх злочинні дії можуть бути викликані:

- безвідповідальністю, тобто коли співробітник цілеспрямовано або випадково без злого умислу здійснює будь-які дії по компрометації інформації;

- егоїзмом і/або кар'єризмом, тобто коли співробітник підприємства заради самоствердження «зондує систему» на надійність експлуатації, щиро вважаючи при цьому, що такі його наміри абсолютно нешкідливі;

- проявом користі, тобто співробітник цілеспрямовано намагається подолати систему захисту для доступу до інформації, що зберігається, передається і обробляється на підприємстві, з метою отримання винагороди, – і не обов'язково грошового;

- бажанням знайти більш перспективну роботу за допомогою акцентування на свій, ніким гідно не оцінений, професіоналізм. Добре відома практика переманювання фахівців, так як це дозволяє послабити конкурента і додатково отримати інформацію про підприємство. Таким чином, не забезпечивши закріплення талановитих фахівців і осіб, обізнаних в секретах, неможливо в повній мірі зберегти секрети підприємства. Питанням попередження плинності кадрів необхідно приділяти особливу увагу. Якщо розглядати компанію як сукупність різних ресурсів, то люди повинні стояти на першому місці, тому що саме вони втілюють технологію і в них, в першу чергу, полягає конкурентоспроможна сила фірми;

- негативним психологічним впливом конфіденційної інформації на свою життєдіяльність, тому що будь-який процес збереження чого-небудь у таємниці звужує сферу людського спілкування: співробітник постійно знаходиться під страхом можливої втрати документів, що містять секрети. Виконуючи вимоги режиму секретності, він змушений діяти в рамках обмеження своєї свободи, що може привести до стресів,

психологічних зривів і, як наслідок до порушення статусу інформації.

Усіх **порушників** можна **класифікувати** наступним чином [17]:

1. За рівнем знань про систему:

- знає функціональні особливості, основні закономірності формування у ній масивів даних, вміє користуватися штатними засобами;

- володіє високим рівнем знань і досвідом роботи з технічними засобами системи та їх обслуговування;

- має високий рівень знань в області програмування та обчислювальної техніки, проектування і експлуатації автоматизованих інформаційних систем;

- знає структуру, функції і механізм дії засобів захисту, їх сильні і слабкі сторони.

2. За рівнем можливостей (використовуваним методам і засобам):

- «Експерт» – індивід, чиї професійні знання і контакти (як робота, так і хобі) забезпечують першокласну орієнтацію у питанні, що розробляється. Він може допомогти по-новому поглянути на існуючу проблему, видати базові матеріали, вивести на невідомі джерела інформації. Загальна надійність одержуваних при цьому даних найчастіше вища.

- «Внутрішній інформатор (інформатор)» – людина з угруповання противника (конкурента), завербований і той, що поставляє інформацію з матеріальних, моральних та інших причин. Цінність даних, що надаються нею, істотно залежить від її можливостей і мотивів видавати потрібні відомості, достовірність яких при відповідному контролі може бути досить високою.

- «Гарячий інформатор» – будь-яка знаюча особа з прихильників противника або його контактерів, що проговорює інформацію під впливом активних методів впливу в стилі жорсткого форсованого допиту, тортури, гіпнозу, шантажу і т. д. Так як істинність повідомлення у даному випадку не гарантована, така імпровізація прийнятна лише в період гострої необхідності, коли немає часу, бажання або можливостей «няньчитися» з

іншими джерелами. На відміну від завербованого інформатора особистісний контакт тут головним чином одномоментний.

- «Впроваджене джерело» – своя людина, яка тим чи іншим манером просочилася в оточення об'єкта (людини, групи, організації). Цінність наданих нею даних залежить від її індивідуальних якостей і досягнутого рівня впровадження.

- «Легковажний інформатор (базіка)» – людина противника, контактер або будь-яка інформована особа, яка проговорює цікаві факти у діловій, дружній, компанійський або інтимній бесіді. Випадково згадане повідомлення може бути надзвичайно цінним, хоча не виключені як безтурботна брехня, так і навмисна дезінформація.

- «Контактери» – люди, які коли-небудь контактували з досліджуваною особою (групою, організацією). Це можуть бути стабільні або випадкові ділові партнери родичі і друзі, службовці сервісу і т. д. Поряд з повідомленням певних фактів, вони можуть сприяти в підході до досліджуваної людині або ж брати участь в прямому вилученні у неї інформації, яка цікавить зловмисника.

- «Союзник» – людина або громадська, державна або кримінальна структура, яка виступає як противник або «наглядач» об'єкта. Рівень і надійність матеріалів, які віддаються, залежать від насущних інтересів, особистих взаємин і знань джерела. Крім абсолютно нової, він здатний передати і підтверджуючу інформацію.

- «Випадкове джерело» – людина, що абсолютно не розглядається як потенційний інформатор, раптом опиняється носієм унікальної інформації. З огляду на явну непередбачуваність на таку людину не дуже розраховують, але, випадково виявивши, розробляють до кінця.

3. За часом дії:

- в процесі функціонування системи (під час роботи компонентів системи);

- в період неактивності компонентів системи (в неробочий час, під час планових перерв у її роботі, перерві для обслуговування і ремонту і т. п.);

- як в процесі функціонування, так і в період неактивності компонентів системи.

4. За місцем дії:

- без доступу на контрольовану територію організації;
- з контрольованої території без доступу в будівлі і споруди;
- всередині приміщень, але без доступу до технічних засобів;
- з робочих місць кінцевих користувачів (операторів);
- з доступом в зону даних (баз даних, архівів і т. п.);
- з доступом в зону управління засобами забезпечення безпеки.

Таким чином, розглянувши модель потенційного порушника, можна зробити висновок, що людина є важливою ланкою системи і головним джерелом інформації.

5.4. Нівелювання електромагнітної вразливості інформації з обмеженим доступом[*,32]

Як відомо, загрози інформаційним ресурсам необхідно розглядати як потенційно можливі випадки антропогенного, техногенного або природного (стихійного) характеру, що можуть спричинити небажаний вплив на інформаційно-телекомунікаційну систему (ІТС), а також на інформацію, яка зберігається в ній. Виникнення загрози, тобто віднаходження джерела актуалізації певних подій у загрози, характеризується таким елементом, як вразливість. Вразливість зазвичай розуміється як слабкий момент інформаційной системи (ІС), на основі якої можлива успішна реалізація загрози. Зі свого боку, загроза – це потенційно можлива подія, дія, явище чи процес які можуть завдати шкоди системному ресурсу [19]. Саме за наявносності вразливості, як певної характеристики системи, відбувається активізація базових (найбільш поширених) загроз безпеці інформації: доступності (розкриття інформаційних ресурсів та несанкціонованого доступу до них); цілісності (умисний антропогенний вплив); конфіденційності (викрадення, утрата інформації та засобів її обробки). Загрози доступності і цілісності інформації пов’язані з неправомірним впливом на неї

*[32] Тарасенко Ю.С. Нівелювання електромагнітної вразливості інформації з обмеженим доступом. // Системи та технології, 2023, 65 (1). С. 56-65.

у вигляді факторів (явищ, дій або процесу), результатом яких можуть бути несанкціоноване знищення, модифікація (спотворення або підміна) або блокування доступу до інформації. Загрози конфіденційності інформації реалізуються за допомогою витоку інформації у вигляді неконтрольованого поширення підзахисної інформації, у результаті чого можливим є несанкціонований до неї доступ і її розголошення зацікавленим суб'єктам, у тому числі державам, іноземним розвідкам, юридичним і фізичним особам. Реалізація таких загроз забезпечується технічними (апаратними) засобами виявлення, прийому (перехвату), регістрації та обробки інформативних сигналів і є найбільш відмінною рисою будь-якої технічної розвідки (ТР) об'єктів інформатизації (ОІ). Під ОІ прийнято розуміти сукупність інформаційних ресурсів, засобів і систем обробки інформації у відповідності до заданої інформаційної технології, включаючи будівлі, споруди, приміщення і технічні засоби, у яких ці засоби та системи встановлені. При цьому об'єкти інформатизації, на яких обробка інформації здійснюється з використанням засобів обчислювальної техніки (ЗОТ), називають об'єктами ЗОТ.

Нажаль, будь-яка, навіть гіпотетично наднадійна, система захисту інформації від навмисних або випадкових впливів природного або штучного походження не здатна повністю забезпечити режим безпечного функціонування як суб'єктів генерування інформації, так і її підтримуючої інфраструктури. Очевидно, що доцільно попереджувати, ніж отримувати наслідки інформаційного протиборства в сфері досягнення односторонніх переваг зловмисником при отриманні, зборі, обробці та використанні інформації обмеженого доступу. Тому, серед більшого різноманіття демаскуючих ознак вразливості інформації, насамперед доцільно розглядати можливості нівелювання різноманітних електричних і електромагнітних витоків, які можна вважати особливо шкідливими. Їх реалізація можлива на будь-якому підприємстві, що використовує комп'ютери, сервісні стійки, мережі. При цьому основними причинами виникнення електричних каналів витоку інформації є наведення інформативних сигналів, під якими розуміють струми і напруги в струмопровідних елементах, що викликають

інформативні та не інформативні побічні (паразитні) електромагнітні випромінювання (ПЕМІ), що призводять до додаткових ємнісних і індукцій. паразитних електромагнітних випромінювань та наведень (ПЕМІН).

Як правило, базовим джерелом інформаційного сигналу є засоби обчислювальної техніки, яким властива побічна генерація паразитних електричних і електромагнітних випромінювань і наведень у вигляді ПЕМІ та ПЕМІН. Використовуючи ці супутні фізичні явища, можна засобами ТР вилучати будь-яку інформацію обмеженого доступу, яка оброблюється ЗОТ. Даний процес прийнято називати витоком інформації. Для такої інформації найбільш значимими (актуальними) є наступні форми витоків:

1) розголошення інформації, тобто передача носія інформації сторонній особі (навмисне) або обробка інформації на ЗОТ у присутності сторонньої особи (ненавмисне);

2) несанкціонований доступ (НСД) до інформації, наприклад шляхом: розкриття системного блоку ЗОТ і вилучення HDD диску для копіювання (фізичний); скиду встановлених параметрів BIOS та зміною пріоритету послідовності завантаження носія з наступним завантаженням альтернативної операційної системи і копіюванням цікавої інформації на flash-накопичувач (програмно-апаратний); впровадження в ЗОТ шкідливих програм для здійснення НСД до інформації або її копіювання (програмний);

3) викрадення носіїв інформації;

4) розповсюдження (витік) інформації по технічним каналам приміщень або об'єктів (будівель, споруд, технічних засобів), в яких ці засоби і системи обчислювальної техніки встановлені.

Під технічним каналом витоку інформації (ТКВІ) розуміють сукупність об'єкту розвідки, технічного засобу розвідки (ТЗР), за допомогою якого добувається інформація про цей об'єкт, і фізичного середовища, у якій розповсюджується інформаційний сигнал. По суті, під ТКВІ розуміють спосіб отримання з допомогою ТЗР розвідувальної інформації про об'єкт. Причому під розвідувальною інформацією зазвичай розуміють дані чи сукупність даних про об'єкти розвідки незалежно від форму їх представлення.

У залежності від природи виникнення інформативного сигналу технічні канали витоку інформації можна розділити на натуральні та спеціально створювані.

Натуральні канали витоку інформації створюються:

1) за рахунок побічних електромагнітних випромінювань, що виникають при обробці інформації ЗОТ (що і прийнято називати електромагнітними каналами витоку інформації – ЕМКВІ). Основними причинами їх виникнення є:

– побічні електромагнітні випромінювання, що виникають внаслідок протікання інформативних сигналів по елементам технічних засобів і систем, які безпосередньо оброблюють інформацію обмеженого доступу (ТСОІ);

– модуляція інформативним сигналом побічних електромагнітних випромінювань високочастотних генераторів ТСОІ;

– модуляція інформативним сигналом паразитного електромагнітного випромінення ТСОІ (наприклад, яке виникає внаслідок самозбудження підсилювачів низької частоти);

2) внаслідок наведень інформативних сигналів у лініях електроживлення і заземлення ЗОТ, з'єднувальних лініях допоміжних технічних засобів і систем (ДТСС) і сторонніх провідниках у вигляді металічних труб систем опалення, водопостачання, будь-яких металоконструкцій і т.д., що і прийнято називати електричними каналами витоку інформації (ЕКВІ).

До спеціально створюваним каналам витоку інформації відносять канали, реалізовані шляхом впровадження в ЗОТ електронних закладних пристроїв перехоплення інформації або шляхом високочастотного опромінення засобів обчислювальної техніки.

З позицій кібербезпеки ІТ-інфраструктури прийнято аналізувати інформаційну безпеку з використанням двох способів: аудиту системи або проведення тестів на проникнення (penetration test, pentest) [20, 21]. Ці тести на проникнення або пентести реалізують метод оцінки безпеки комп'ютерних систем або мереж засобами моделювання атаки зловмисника. З позицій кібербезпеки об'єктів критичної інфраструктури (ОКІ) нівелювання таких загроз за своєю сутністю мають багатогранну

сферу діяльності, включаючи и багатоликий арсенал технічних засобів розвідок. Основна їх відмінність від легальної розвідки, яка добуває інформацію при різноманітних офіційних зв'язках і контактах із засобів масової інформації, пов'язана з використовуваною спецапаратурою і способами ведення розвідки. Зазвичай к ТСР відносять такі види розвідок: радіоелектронні, гідроакустичні, акустичні, оптико-електронні, візуально-оптичні, хімічні, радіаційні, сейсмічні, магнітометричні, комп'ютерні, фотографічні та їх різновиди. Зокрема, радіоелектронна розвідка (РЕР) дозволяє отримувати інформацію шляхом прийому та аналізу електромагнітного випромінення (ЕМВ) радіодіапазону, створюваного різноманітними радіоелектронними засобами.

Безперечно всі ці ТСР направлені також и на об'єкти інформаційної безпеки, що об'єднують інформаційні ресурси, канали інформаційного обміну та телекомунікації, механізми забезпечення функціонування телекомунікаційних систем і мереж та інші елементи інформаційної інфраструктури [22].

Для протидії загрозам інформаційній безпеці (ІБ), зниження ризиків ІБ, результативної обробки інцидентів ІБ і ефективної боротьби з методами будь-яких розвідок необхідно забезпечувати, і протягом тривалого часу, зберігати штатний рівень ІБ у вигляді стабільного стану захищеності інформації у відповідності з позиціями законодавчої реалізації сукупності її властивостей: доступності, цілісності, достовірності, конфіденційності, автентичності і т.д.

Інформативні ПЕМІ, як небажані електромагнітні випромінювання, призводять до витоку інформації, що обробляється. Неінформативні ПЕМІ дозволяють одержати лише уявлення про режим роботи ЗОТ, але не розкривають характер інформації, оброблюваної на ціх ЗОТ. Тому з погляду захисту інформації небезпеку створюють лише інформативні ПЕМІ, що представляє є високочастотну несучу, модульовану інформацією оброблюваної засобами обчислювальної техніки. Вони виникають за різних режимах обробки інформації засобами обчислювальної техніки. Зокрема, при: виведенні інформації на монітор; введення даних із клавіатури; запису/читанні інформації на/з накопичувачів; передачі даних в канали зв'язку та на

друковані пристрої тощо. Залежно від режиму роботи і типу ЗОТ виникають свої ознаки, що демаскують, включаючи і характерні амплітудно-частотні особливості ПЕМІ, частотний діапазон яких може становити від сотень Гц до десятків ГГц. При цьому навколишній простір, в межах якого можливий перехоплення побічних електромагнітних випромінювань і подальше відновлення інформації, що міститься в них, залежить від інтенсивності ПЕМІ і чутливості приймальної апаратури ТСР.

Відносно ПЕМІН необхідно акцентувати увагу на тому, що вони проявляються як результат електромагнітного наведення інформативних сигналів від ЗОТ, що викликані побічними електромагнітними випромінюваннями у вигляді індукованих струмів і напруг в струмопровідних елементах з ємкісними та індуктивними зв'язками. Такі електромагнітні наведення можуть призводити до витоку інформації по струмопровідним комунікаціям, що мають вихід за межі безпечної (контрольованої) зони. При цьому виявлення інформативних сигналів з інженерних комунікацій ТСР ПЕМІН залежить від відстані між джерелом випромінювання, типу електроживлення, якості заземлення ЗОТ, характеристик антени, що приймає (зондує), рівня супутніх пасивних шумів і активних перешкод, а також і інших факторів.

Залежно від фізичних причин виникнення ПЕМІ та ПЕМІН за рахунок ЗОТ використовують різні методи (принципи) їх реалізації або нівелювання. До активних способів такого впливу (наприклад, перехоплення) інформації, що обробляється ЗОТ, відносять технічні канали витоку інформації (ТКВІ) з високочастотним опроміненням ЗОТ та встановленням у ЗОТ спеціальних закладних пристроїв.

У першому випадку, наприклад, для їх нівелювання, на ЗОТ впливають потужним високочастотним сигналом, бажано реалізованому в режимі співпування, завдяки чому перекривається (активно зашумлюється) вторинне випромінювання у вигляді ПЕМІ та ПЕМІН, апріорі промодульовані інформативним сигналом. Таким чином, порушується можливий несанкціонований відбір інформації.

У другому випадку для перехоплення інформації, що обробляється ЗОТ, встановлюють у них спеціальні заставні

пристрої, що забезпечують або витік інформації, або блокування, або порушення цілісності інформації. Класифікацію таких закладних пристроїв можна проводити за багатьма ознаками, у тому числі:

– за способом передачі інформації (по радіо або оптичному каналу, по мережі електроживлення, використання цифрових накопичувачів типу flash-пам'яті і т.д.);

– за засобом передачі інформації (типу ІЧ-порту або пристроїв типу Wi-Fi, Bluetooth, WiMAX і т.д.);

– за місцем установки (у корпусі системного блоку, або монітора, або клавіатури, або принтера тощо);

– за видом перехоплюваної інформації (з клавіатури, з принтера, з відеозображення монітора можуть використовувати або апаратні кейлоггер[33] (keylogger hardware) по каналами зв'язку при запису як на жорсткий диск комп'ютера (HDD) або на зовнішні накопичувачі типу flash-пам'яті, CD, DVD, USB, або апаратні кейлогери* з передачею інформації з радіоканалу);

– за типом джерела живлення, способами накопичення та кодування, за видом виконання та способом управління передавачем.

Закладні пристрої складаються з електроних блоків перехоплення/передачі інформації (або модуля запису інформації), радиотехничного блоку дистанційного управління і електричного блоку живлення. Очевидно, що виявлення таких блоків та захист від їх шкідливих впливів потребують серйозних, і не лише технічних засобів інформаційної безпеки. До найперспективніших захисних заходів щодо нівелювання таких впливів слід вважати методи з використанням безеховості, екранування та технологію нелінійної радіолокації [23, 24], в основі якої використовують нелінійні властивості напівпровідників, наявні у складі будь-яких радіоелектронних закладок.

---

* Кейло́гер, кейло́ггер – програмне забезпечення або апаратний пристрій, що реєструє різні дії користувача - натискання клавіш на клавіатурі комп'ютера, рухи і натискання клавіш миші тощо.

У першому випадку режим безеховості реалізують, наприклад, за допомогою безехових камер (БЕК), які, крім того, здатні конструктивно забезпечувати будь-який заданий рівень екранування [24]. В основі створення режиму безеховості лежить принцип поглинання електромагнітного сигналу від будь-якої перешкоди на шляху розповсюдження акустичної або електромагнітної хвилі. Під перешкодою прийнято розуміти будь-яку неоднорідність параметрів середовища, в якій поширюється хвиля. Для електромагнітних хвиль – це будь-яка зміна діелектричної та/або магнітної комплексних проникностей середовища, яка оцінюється як неоднорідність. Основними факторами, що визначають якість БЕК, є їх розміри й форма, а також якість застосованого радіопоглинаючого матеріалу. Очевидно, що чим менше значення паразитних розсіяних полів, тем менший коефіцієнт безеховості (КБЕ) й тим краща якість БЕК. При цьому робочий об'єм БЕК, як область простору БЕК з апріорі заданим КБЕ, (який прийнято також називати безеховою зоною), варто використовувати для ЗОТ. В такому випадку забезпечується додаткова екранування джерел паразитних електромагнітних випромінень и наведень від ЗОТ у вигляді потенційно можливих ПЕМІ та ПЕМІН, що не виходять за кордони контрольованої зони об'єкту інформатизації. Крім того реалізується можливість оцінки рівня достовірності контрольних (експертних) вимірювань через апостеріорне їх підтвердження або оптротестування, так необхідних при аналізі штатної працездатності ЗОТ. Хоча залишковий вибір рішення по використанню задіяної контрольно-вимірювальної апаратури може бути оцінений тільки після її експериментальної апробації.

З появою ближньої, а в подальшому й нелінійної радіолокації з'явилася можливість вирішувати, крім радіолокаційних, цілий ряд інших прикладних задач, наприклад, задач діагностичного й дефектоскопічного характеру, криміналістики та боротьби з тероризмом [25, 26]. З огляду на це виявлення прихованих закладних пристроїв в ЗОТ, як об'єктів штучного походження, які перебувають в умовах взаємодії з контрольна–вимірювальною радіоапаратурою які використовують ефекти нелінійного розсіювання електромагнітних хвиль (ЕМХ), випромінюваних

радіолокаційної станцією ближній взаємодії, також не є проблематичним. При цьому у якості мобільного технічного засобу, що реалізує вивчення за витоком ПЕМІН в ІТС за межі кордону контрольованої зони об'єкта дослідження, доцільно використовувати дрони з відповідною контрольно-вимірювальною апаратурою (КВА), що забезпечує режими виявлення, вимірювання, розпізнавання і дозволу ТКВІ.

Як правило, у прихованні роботи безпілотних літальних апаратів (БЛА, дронів або безпілотних авіаційних систем – БПЛС) зацікавлені усі сторони, особливо в період їхньої конфронтації. Тому дрони, залежно від позицій конфліктуючих сторін, прийнято ділити на ворожі та свої. Причому за відсутності конкретної нормативно-правової основи на рівні ISO, незважаючи на серію стандартів на кшталт ISO 21384 та ISO 23629 щодо БЛА, не існує чіткої класифікації дронів. Проте очевидно, що дуже ефективним, під час виконання завдань забезпечення безпеки підвідомчих об'єктів (і не тільки від ворожого моніторингу), є використання дронів, здатних реалізовувати як відеоспостереження з урахуванням комп'ютерного зору [27], так й виявлення ПЕМІН від ЗОТ. В обох випадках використання радіодіапазону, як і раніше, є актуальне. Таким чином, фактично методи радіолокації виявлення, дозволу, вимірювання та розпізнавання стають основними при створенні систем контролю та управління доступу, перш за все, до об'єктів критичної інфраструктури [28], до яких слід відносити і ЗОТ.

Зазвичай у дронах використовують різні рівні автономності: від керованих дистанційно до автоматичного рівня. У випадку дистанційно пілотованого дрона успішність виконання польотного завдання багато в чому визначатиметься властивостями інформаційно-вимірювальної системи дронів, яка має володіти як елементами інтелекту, так і відповідною системою захисту від несанкціонованих до неї вторгнень з метою порушення штатної працездатності дрону. Такі дрони вертолітного типу у найнижчіх ешелонах (тобто притискаючись до землі) могут входить у зони дії ближньої, а також і нелінійної радіолокації. У таких реальних умовах відповідна КВА з визначенням паразитних випромінювань за межами

контрольованої зони об'єкта ЗОТ реализує вимірювання у зовнішньому ефірі витоків ПЕМІН с високою достовірністю і надійністю.

При цьому використовуючи оптимальну фільтрацію, наприклад, кореляційним приймачем, граничний пристрій якого налаштований відповідно до критерію Неймана-Пірсона або за критерієм ідеального спостерігача, можна навіть забезпечити автоматичну індикацію (в аналоговій, в цифровий, в звуковий або у візуальній формі) сигналу тривоги про перевищення допустимого рівня витоку. Очевидно, що рівень достовірності тривоги доцільно виставляти (вибирати) за апріорі заданою величиною ймовірності правильного виявлення або ймовірності хибної тривоги. Вибір останніх регламентують не тільки в процесі метрологічного калібрування чутливості КВА, а й її потенційної роздільної здатності за вторинним електромагнітним перевипромінюванням у вигляді каліброваних цілей на кшталт сфери, кутових відбивачів, металевих поверхонь різної геометрії і т.д. Отже, підключаючи методи радіолокаційної роздільної здатності, з'являється можливість розпізнавання джерела паразитного витоку, використовуючи арсенал апріорних значень ефективних поверхонь розсіювання об'єкта інформатизації. Якщо контрольовані зони об'єктів ІБ мають вигляд закритих приміщень, то бажано всі виявлені під час пуско-налагоджувальних робіт так звані «блискучі точки» нівелювати шляхом використання радіопоглинаючих матеріалів.

Таким чином, у частині, що стосується витоку інформації по технічних каналах об'єкта інформатизації, можна значно нівелювати електромагнітні вразливості службової інформації, що виникають при роботі засобів обчислювальної техніки, реалізуючи відповідні (наведені вище) заходи протидії щодо недостатнього екранування, побічних електромагнітних випромінювань, ворожого впливу потужним високочастотним сигналом та електромагнітних наведень

Контрольні запитання до Розділу 5

1. Що таке несанкціонований доступ до інформації?
2. Поясніть, чому вразливість інформаційної системи зумовлює успішну реалізацію загрози для ІС.
3. Перелічіть основні канали несанкціонованого доступу до конфіденційної інформації.
4. Які основні методи використовують під час організації фізичного проникнення до носіїв конфіденційної інформації?
5. Що таке комп'ютерне піратство?
6. Як можна здійснювати несанкціоноване підключення, а також і несанкціонований доступ до конфіденційної інформації?
7. Викладіть основні способи несанкціонованого підключення до засобів відображення та зберігання службової інформації в ІС.
8. Модель потенційного порушника, - що це?
9. Викладіть основні способи несанкціонованого підключення до засобів опрацювання, оброблення, відтворення та передавання службової інформації в ІС.
10. Якими методами забезпечують візуальне знімання конфіденційної інформації?
11. Що таке ділова розвідка?
12. У чому відмінність ділової від конкурентної розвідки?
13. Що таке промислове шпигунство та його відмінність від ділової та конкурентної розвідки?
14. У чому полягає процес оцінювання ризику?
15. Що прийнято називати натуральним каналом витоку інформації?
16. Що прийнято називати технічним каналом витоку інформації?
17. Що прийнято називати електричними каналами витоку інформації?

18. Поясніть суть кількісного та якісного оцінювання ризиків із позицій пошуку оптимального рішення з організації захисту інформації з безлічі апріорі наявних.
19. Що таке паразитне електромагнітне випромінювання в телекомунікаційних системах та їхній згубний вплив у сфері безпеки ОКІ?
20. Що таке режим безеховості и як він створюється?

Список використаних джерел під час підготовки тексту розділу 5

1. Інформаційна безпека підприємства: Навчальний посібник/Н.В. Гришин. - 2-е вид., Дод. - М.: Форум: НІЦ ІНФРА-М, 2015. - 240 с.

2. Н. І. Горбаль, Л. В. Смерека, О. З. Микитин. Конкурентна розвідка: сутність, значення, перспективи розвитку / Менеджмент та підприємництво в Україні: етапи становлення та проблеми розвитку. Т. 1, № 2, 2019. С. 53-60.

3. Сєдєлкін К.Ю. Ділова розвідка як інтелектуальний інструмент забезпечення конкурентоспроможності фірми нової економіки // Креативна економіка. – 2009. – Том 3. – № 1. – С. 3-11

4. Биткін С.В. Конкурентна розвідка у зовнішньоекономічній діяльності: інженерно-економічні методи/С.В. Биткін, В.М. Литвин. – Х., 2015. – 240 с

5. Інформаційна війна в сучасному світі. [Электронный ресурс] – URL: http://kak-bog.ru/informacionnaya-voyna-v-sovremennom-mire.

6. ДСТУ ISO/IEC 27000:2019 (ISO/IEC 27000:2018, IDT) Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Огляд і словник термінів. Київ ДП «УкрНДНЦ». Наказ від 16.10.2019 № 312.

7. ISO/IEC 27001:2013 Інформаційні технології - Методи забезпечення безпеки - Системи менеджменту інформаційної безпеки - Вимоги /Information technology — Security techniques —

Information security management systems —Requirements/ Вторая редакція. 2013-10-01.

8. ДСТУ ISO/IEC 27005:2019 Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки (ISO/IEC 27005:2018, IDT) Дата початку дії 01.11.2019. (ДП «УкрНДНЦ») International standard ISO/IEC 27005:2019 Information technology – Security techniques – Information secure risk management. https://www.google.com/url

9 Tarasenko Yurii, Maksymchuk Nikita. Mitigating Threats to Information Security, Starting with Education. Pp. 238-242. Scientific Collection «InterConf», (№162): with the Proceedings of the 14th International Scientific and Practical Conference «Scientific Research in XXI Century». Date of the Conference: July 16-18, 2023. Number of pages: 296. Published: 18.07.2023. Venue: Ottawa, Canada.

10. Nic_Kazantsev. Ризики VS Загрози. Інформаційна безпека. 7 листопада 2021. Адаптовано з: Habr https://habr.com.

11. В.Я. Воропаєва, І.Л. Щербов. Адаптування інформаційно-телекому-нікаційних систем до зовнішніх впливів / Наукові праці ДонНацТехн ун-ту. Серія: Обчислювальна техніка та автоматизація. — 2012. — Вип. 23. — С. 83–89

12. Захист інформації у телекомунікаційних системах / https://www.bsut.by /

13. Рекомендации МСЭ-Т X.NCNS-1, Архітектура та структура безпеки National IP-based Public Networks Security Center for Developing Countries. Женева, квітень 2011

14. Загрози, уразливості та ризики інформаційної безпеки телекомунікаційних систем. Біл. держ. університет транспорту https://www.bsut.by

15. Воропаєва В. Я., Щербов І.Л. Хаустова Е.Д. Управління інформаційною безпе-кою інформаційно-телекомунікаційних систем на основі моделі «plan-do-check-act» // Наукові праці Донецького національного технічного університету. Серія: Обчислювальна техніка та автоматизація. Випуск 25. – Донецьк, ДонНТУ, 2013. С. 104-110

16. Архітектура безпеки для систем, що забезпечують зв'язок між кінцевими пристроями (ITU-T X.805«Security architecture for systems providing end-to-end communications»).

17. Інформаційна безпека підприємства: Навчальний посібник/Н.В. Гришин. - 2-е вид., Форум: НІЦ ІНФРА, 2015. – 240 с.

18. Тарасенко Ю.С. Нівелювання електромагнітної вразливості інформації з обмеженим доступом. // Системи та технології, 2023, 65 (1). С. 56-65.

19. Юдін О.К., Бучик С.С. Державні інформаційні ресурси. Методологія побудови класифікатора загроз: монографія. Київ: НАУ, 2015. 214 с

20. Frank Swiderski and Window Snyder. Threat Modeling. Microsoft Press, 2004. 288 pages.

21. Стеценко І. В., Савчук В. В. Метод автоматизації тестування на проникнення вебатак. Технічні науки та технології. 2021. № 1 (19). С. 98–103.

22. Ліпкан В. А., Максименко Ю. Є., Желіховський В. М. Інформаційна безпека України в умовах євроінтеграції: навчальний посібник. Київ: КНТ, 2006. 280 с. (Серія: Національна і міжнародна безпека)

23. Тарасенко Ю.С. Фізичні основи радіолокації. Дніпро: Пороги, 2011. 487 с.

24. Тарасенко Ю.С., Смірнов В.В. та ін. Режим безеховості в інформаційно-вимірю-вальної системі митного контролю. Системи та технології. 2019. № 2 (58) С. 170–182.

25. Тарасенко Ю.С., Смірнов В.В., Прокопович-Ткаченко Д.І. Особливості виявлення прихованих об’єктів штучного походження в умовах митного контролю. Системи та технології. 2019. № 2 (58) С. 161–169.

26. Юсупов В. В., Приходько Ю. П., Фурман Я. В. та ін. Пошук та знешкодження саморобних вибухових пристроїв: метод. рек. Київ : Нац. акад. внутр. справ, 2017. 31 с.

27. Вовк С.М., Гнатушенко В.В., Бондаренко М.В. Методи обробки зображень та компютерний зір : навчальний посібник. Д. : ЛІРА, 2016. 148 с.

28. Tarasenko Yu.S., Klym V.Yu. Safety of critical infrastructure objects from the positions of risk effectiveness reduction. System technologies. 2022. Vol. 4. No. 141. Pp. 158–168.

6. СУЧАСНИЙ СТАН МОДЕЛЮВАННЯ ІНФОРМАЦІЙНИХ СИСТЕМ ЗАХИСТУ ТА ЇХ ТЕХНОЛОГІЧНА ПОБУДОВА. МЕНЕДЖМЕНТ БЕЗПЕКИ ОКІ

6.1. Моделювання, принципи побудови та класифікаційні ознаки моделей

У загальному випадку під моделлю прийнято розуміти або образ (умовний або уявний у вигляді зображення, опису, схем, креслень, графіків, карт і т. п.), або прообраз (зразок) будь-якого об'єкта («оригіналу» даної моделі), що використовується в якості «заступника» або «представника». Дослівно **модель** (від франц. modèle, від лат. modulus) – міра, мірило, зразок, норма. Фактично модель відображає ідею або «імітації» (описи) чогось «сущого» (якоїсь дійсності, що є первинною по відношенню до моделі), або, навпаки, реалізує принцип «реального втілення» деякої умоглядної концепції, в якій первинним поняттям виступає вже сама модель. Поняття моделі в конкретних науках так чи інакше пов'язують із застосуванням моделювання, тобто зі з'ясуванням (або відтворенням) властивостей будь-якого об'єкта, процесу або

явища за допомогою іншого об'єкта, процесу або явища – його «моделі». У даний час сучасну науку неможливо уявити без широкого застосування фізичного та математичного моделювання.

Фізичне моделювання полягає в заміні конкретного об'єкта або явища експериментальним дослідження його моделі, що має ту ж фізична природу. Суть математичного моделювання полягає в заміні вихідного об'єкта його образом – математичною моделлю і подальшому вивченні моделі за допомогою реалізованих на комп'ютерах обчислювально-логічних алгоритмів. Цей метод поєднує в собі переваги, як теорії, так і експерименту, оскільки робота відбувається не з самим об'єктом (явищем, процесом), а з його моделлю, що дозволяє відносно швидко і без істотних витрат досліджувати його властивості і поведінку в різних ситуаціях. У той же час обчислювальні експерименти з моделями об'єктів забезпечують, спираючись на потужність сучасних обчислювальних методів і технічних засобів інформатики, всебічне вивчення об'єктів, часто недоступне чисто теоретичними підходами. Особливо це є актуальним в умовах постійного зростання вимог до ефективності пристроїв, застосовуваних у системах передачі та обробки інформації, до скорочення термінів їх дослідження і розробки нових телекомунікаційних систем і мереж.

Таким чином, під моделлю розуміють фізичний або абстрактний об'єкт, властивості якого в певному сенсі схожі з властивостями досліджуваного об'єкта. При цьому вимоги до моделі визначаються розв'язуваною задачею і наявними засобами. Існує ряд **загальних вимог до моделей** у вигляді:

- ✓ ***адекватності,*** що реалізує досить точне відображення властивостей об'єкта;
- ✓ ***повноти,*** що дає об'єктивне надання отримувачу всієї необхідної інформації про об'єкт;
- ✓ ***гнучкості,*** що забезпечує можливість відтворення різних ситуацій у всьому діапазоні зміни умов і параметрів;
- ✓ ***трудомісткості,*** оскільки розробка повинна бути прийнятною для наявного часу і програмних засобів.

Процес побудови моделі об'єкта і подальшого її (моделі) дослідження включає два основних етапи: перший – це

безпосередня розробка моделі, а другий – подальше дослідження моделі з метою отримання конкретних висновків, протокольно оформлених у вигляді підсумкових результатів. При цьому на кожному з етапів вирішуються різні задачі та використовуються методи і засоби, які відрізняються по суті, використовуючи найчастіше напівнатурне моделювання і макетування, тобто включення до складу моделі реальної апаратури. Поряд з реальною апаратурою в замкнуту модель зазвичай входять імітатори впливів і перешкод, математичні моделі зовнішнього середовища і процесів, для яких невідомо досить точний математичний опис. Включення реальної апаратури або реальних систем в контур моделювання складних процесів дозволяє зменшити апріорну невизначеність і досліджувати процеси, для яких немає точного математичного опису. За допомогою напівнатурного моделювання дослідження виконуються з урахуванням малих постійних часу і нелінійностей, властивих реальній апаратурі. При дослідженні моделей з включенням реальної апаратури використовується поняття динамічного моделювання, при дослідженні складних систем і явищ – еволюційного, імітаційного і кібернетичного моделювання.

Рішення практичних задач математичними методами послідовно здійснюється шляхом формулювання задачі (розробки математичної моделі), вибору методу дослідження отриманої математичної моделі, аналізу отриманого математичного результату. Математичне формулювання задачі зазвичай представляється у вигляді геометричних образів, функцій, систем рівнянь і т. п. Опис об'єкта (явища) може бути представлено за допомогою безперервної або дискретної, детермінованої або стохастичної та іншими математичними формами. Теорія математичного моделювання забезпечує виявлення закономірностей протікання різних явищ навколишнього світу або роботи систем і пристроїв шляхом їх математичного опису та моделювання без проведення натурних випробувань. При цьому використовуються положення і закони математики, що описують моделюються явища, системи або пристрої на деякому рівні їх ідеалізації.

Математична модель являє собою формалізований опис системи (або операції) деякою абстрактною мовою, наприклад, у

вигляді сукупності математичних співвідношень або схеми алгоритму, тобто такий математичний опис, який забезпечує імітацію роботи систем або пристроїв на рівні, досить близькому до їх реальної поведінки, що отримується при натурних випробуваннях систем або пристроїв. Будь-яка математична модель описує реальний об'єкт, явище чи процес з деяким ступенем наближення до дійсності. Вид математичної моделі залежить як від природи реального об'єкта, так і від задач дослідження.

Метою математичного моделювання є аналіз реальних процесів (в природі або техніці) математичними методами. У свою чергу, це вимагає формалізації такого процесу. Модель може являти собою математичний вираз, що містить змінні, поведінка яких аналогічно поведінці реальної системи. Модель може включати елементи випадковості, або може представляти реальні змінні параметри взаємопов'язаних частин діючої системи.

Математичне моделювання для дослідження характеристик систем можна розділити на **аналітичне, імітаційне і комбіноване.** У свою чергу, математичні моделі діляться на імітаційні та аналітичні.

Для аналітичного моделювання характерно, що процеси функціонування системи записуються у вигляді деяких функціональних співвідношень (алгебраїчних, диференціальних, інтегральних рівнянь). Аналітична модель може бути досліджена такими методами:

1) аналітичним, коли прагнуть отримати у загальному вигляді явні залежності для характеристик систем;

2) чисельним, коли не вдається знайти рішення рівнянь у загальному вигляді та їх вирішують для конкретних початкових даних;

3) якісним, коли при відсутності рішення знаходять деякі його властивості.

Аналітичні моделі вдається отримати тільки для порівняно простих систем. Для складних систем часто виникають великі математичні проблеми. Для застосування аналітичного методу йдуть на суттєве спрощення початкової моделі. Однак дослідження на спрощеній моделі допомагає отримати лише

орієнтовні результати. Аналітичні моделі математично вірно відображають зв'язок між вхідними і вихідними змінними і параметрами. Але їх структура не відображає внутрішню структуру об'єкта.

Безумовно, знаходження аналітичних рішень при аналітичному моделюванні виявляється виключно цінним для виявлення загальних теоретичних закономірностей простих лінійних ланцюгів, систем і пристроїв. Однак його складність різко зростає в міру ускладнення впливів на модель і збільшення порядку і числа рівнянь стану, що описують модельований об'єкт. Можна отримати більш-менш доступні для огляду результати при моделюванні об'єктів другого або третього порядку, але вже при більшому порядку аналітичні вирази стають надмірно громіздкими, складними і такими, що важко осмислюються.

Одним із різновидів аналітичного моделювання є чисельне моделювання, яке полягає в отриманні необхідних кількісних даних про поведінку систем або пристроїв будь-яким відповідним чисельним методом.

При імітаційному моделюванні алгоритм, який реалізує модель, відтворює процес функціонування системи в часі. Імітуються елементарні явища, що становлять процес, зі збереженням їх логічної структури і послідовності протікання в часі.

Основною перевагою імітаційних моделей у порівнянні з аналітичними є можливість вирішення більш складних задач. Імітаційні моделі дозволяють легко враховувати наявність дискретних або безперервних елементів, нелінійні характеристики, випадкові впливи та ін. Тому цей метод широко застосовується на етапі проектування складних систем. Основним засобом реалізації імітаційного моделювання служить ЕОМ, що дозволяє здійснювати цифрове моделювання систем і сигналів. У зв'язку з цим уточнимо словосполучення «комп'ютерне моделювання», яке регулярно використовується в літературі.

Будемо вважати, що комп'ютерне моделювання – це математичне моделювання з використанням засобів обчислювальної техніки. Відповідно, **технологія комп'ютерного моделювання** передбачає виконання таких дій:

- ✓ визначення мети моделювання;
- ✓ розробки концептуальної моделі;
- ✓ формалізації моделі;
- ✓ програмної реалізації моделі;
- ✓ планування модельних експериментів;
- ✓ реалізації плану експерименту;
- ✓ аналізу та інтерпретації результатів моделювання.

Зміст перших двох етапів практично не залежить від математичного методу, покладеного в основу моделювання (і навіть навпаки – їх результат визначає вибір методу). А от реалізація решти п'яти етапів істотно розрізняється для аналітичного і імітаційного моделювання.

При імітаційному моделюванні використовувана математична модель відтворює алгоритм («логіку») функціонування досліджуваної системи в часі при різних поєднаннях значень параметрів системи і зовнішнього середовища. Прикладом найпростішої аналітичної моделі може служити рівняння прямолінійного рівномірного руху. При дослідженні такого процесу за допомогою імітаційної моделі має бути реалізовано спостереження за зміною пройденого шляху з плином часу.

Очевидно, в одних випадках більш доцільним є аналітичне моделювання, а в інших – імітаційне (або поєднання того й іншого). Щоб вибір був удалим, необхідно відповісти на два питання. З якою метою проводиться моделювання? До якого класу може бути віднесено явище, що моделюється? Відповіді на обидва ці питання можуть бути отримані в ході виконання двох перших етапів моделювання.

Імітаційні моделі не тільки за властивостями, але і за структурою відповідають об'єкту, що моделюється. При цьому є однозначна і явна відповідність між процесами, які отримуються на моделі, і процесами, що протікають на об'єкті. Недоліком імітаційного моделювання є великий час вирішення задачі для отримання хорошої точності. Результати імітаційного моделювання роботи стохастичної системи є реалізаціями випадкових величин або процесів. Тому для знаходження характеристик системи потрібно багаторазове повторення і подальша обробка даних. Найчастіше в цьому випадку

застосовується різновид імітаційного моделювання – статистичне моделювання (або метод Монте-Карло), тобто відтворення в моделях випадкових факторів, подій, величин, процесів, полів. За результатами статистичного моделювання визначають оцінки імовірнісних критеріїв якості, загальних і приватних, що характеризують функціонування і ефективність керованої системи. Статистичне моделювання широко застосовується для вирішення наукових і прикладних задач у різних областях науки і техніки. Методи статистичного моделювання широко застосовуються при дослідженні складних динамічних систем, оцінці їх функціонування і ефективності. Заключний етап статистичного моделювання заснований на математичній обробці отриманих результатів. Тут використовують методи математичної статистики (параметричне і непараметричне оцінювання, перевірку гіпотез). Прикладом параметричної оцінки є вибіркове середнє показника ефективності. Серед непараметричних методів велике поширення отримав метод гістограм.

Розглянута схема заснована на багаторазових статистичних випробуваннях системи і методах статистики незалежних випадкових величин. Ця схема є далеко не завжди природною на практиці і оптимальною за витратами. Скорочення часу випробування систем може бути досягнуто за рахунок використання більш точних методів оцінювання. Як відомо з математичної статистики, найбільшу точність при заданому обсязі вибірки мають ефективні оцінки. Оптимальна фільтрація і метод максимальної правдоподібності дають загальний метод отримання таких оцінок.

У задачах статистичного моделювання обробка реалізацій випадкових процесів необхідна не тільки для аналізу вихідних процесів. Дуже важливий також і контроль характеристик вхідних випадкових впливів. Контроль полягає в перевірці відповідності розподілів процесів, що генеруються, заданим розподілам. Ця задача часто формулюється як задача перевірки гіпотез.

Загальною тенденцією моделювання з використанням ЕОМ у складних керованих систем є прагнення до зменшення часу моделювання, а також проведення досліджень у реальному

масштабі часу. Обчислювальні алгоритми зручно представляти в рекурентній формі, що допускає їх реалізацію в темпі надходження поточної інформації.

Накопичений до теперішнього часу досвід в області розробки і використання математичних моделей дозволяє сформулювати наступні принципи побудови:

1. Принцип інформаційної достатності. За повної відсутності інформації про досліджувану систему побудова її моделі неможлива. За наявності повної інформації про систему її моделювання позбавлене сенсу. Існує певний критичний рівень апріорних відомостей про систему (рівень інформаційної достатності), при досягненні якого може бути побудована її адекватна модель.

2. Принцип здійсненності. Створювана модель повинна забезпечувати досягнення поставленої мети дослідження з ймовірністю, що істотно відрізняється від нуля, і за скінченний час.

3. Принцип множинності моделей. Даний принцип є ключовим. Йдеться про те, що створювана модель повинна відображати в першу чергу ті властивості реальної системи (або явища), які впливають на обраний показник ефективності. Відповідно при використанні будь-якої конкретної моделі пізнаються лише деякі сторони реальності. Для більш повного її дослідження необхідний ряд моделей, що дозволяють з різних сторін і з різним ступенем детальності відбивати розглянутий процес.

4. Принцип агрегування. У більшості випадків складну систему можна подати такою, що складається з агрегатів (підсистем), для адекватного математичного опису яких виявляються придатними деякі стандартні математичні схеми. Принцип агрегування дозволяє, крім того, досить гнучко перебудовувати модель залежно від задач дослідження.

5. Принцип параметризації. У ряді випадків система, що моделюється, має в своєму складі деякі відносно ізольовані підсистеми, що характеризуються певним параметром, у тому числі векторним. Такі підсистеми можна замінювати у моделі відповідними числовими величинами, а не описувати процес їх функціонування. За необхідності залежність значень цих величин

від ситуації може задаватися у вигляді таблиці, графіка або аналітичного виразу (формули). Принцип параметризації дозволяє скоротити обсяг і тривалість моделювання. Однак треба мати на увазі, що параметризація знижує адекватність моделі.

Очевидно, що ступінь реалізації перерахованих принципів і кожної конкретної моделі може бути різною, причому це залежить не тільки від бажання розробника, але і від дотримання ним технології моделювання. А будь-яка технологія передбачає наявність певної послідовності дій. При цьому, загальна ціль моделювання може бути сформульована таким чином: це визначення (розрахунок) значень обраного показника ефективності для різних стратегій проведення операції (або варіантів реалізації проектованої системи). При розробці конкретної моделі ціль моделювання повинна уточнюватися з урахуванням використовуваного критерію ефективності. Для критерію придатності модель, як правило, повинна забезпечувати розрахунок значень показника ефективності для усієї множини допустимих стратегій. При використанні критерію оптимальності модель повинна дозволяти безпосередньо визначати параметри досліджуваного об'єкта, що дають екстремальне значення показника ефективності.

Таким чином, мета моделювання визначається як ціллю досліджуваної операції, так і планованим способом використання результатів дослідження. Наприклад, проблемна ситуація, що вимагає ухвалення рішення, формулюється так: знайти варіант побудови обчислювальної мережі, який володів би мінімальною вартістю при дотриманні вимог щодо продуктивності і щодо надійності. У цьому випадку ціллю моделювання є відшукання параметрів мережі, що забезпечують мінімальне значення показника ефективності, в ролі якого постає вартість.

Задача може бути сформульована інакше: з кількох варіантів конфігурації обчислювальної мережі вибрати найбільш надійний. Тут в якості показника ефективності вибирається один з показників надійності (середнє напрацювання на відмову, імовірність безвідмовної роботи і т. п.), а ціллю моделювання є порівняльна оцінка варіантів мережі за цим показником.

Наведені приклади свідчать про те, що сам по собі вибір показника ефективності ще не визначає «архітектуру» майбутньої моделі, оскільки на цьому етапі не визначена концептуальна модель досліджуваної системи.

Загалом при вирішенні будь-якої задачі побудови моделі основну роль відіграють такі чотири елементи: 1) експеримент; 2) модель; 3) показники ефективності; 4) критерії прийняття рішень. Необхідно належним чином визначити перераховані елементи і зрозуміти їх взаємозв'язок, оскільки вони мають великий вплив на **проектування системи** і на планування її роботи в цілому. Критерії прийняття рішень дозволяють вибрати найбільш ефективні параметри системи. Зазвичай цей процес називається **оптимізацією**.

Прийнято в процесі побудови моделі розрізняти три види або стадії побудови: ***уявна модель, концептуальна модель і формальна модель***.

При спостереженні за об'єктом в голові дослідника формується уявний образ об'єкта, його ідеальна модель. Формуючи таку модель, розробник, як правило, прагне відповісти на конкретні питання. Від реального дуже складного влаштування об'єкта відсікається все непотрібне з метою отримання його більш компактного і лаконічного опису. Подання уявної моделі на природній мові називається **змістовною моделлю**. За **функціональною ознакою** і цілями змістовні моделі діляться на *описові, пояснювальні і прогностичні*. *Описовою моделлю* називається будь-який опис об'єкта. *Пояснювальна модель* дозволяє відповісти на питання: чому це відбувається? *Прогностична модель* описує майбутню поведінку об'єкта.

Концептуальна (змістовна) модель – це абстрактна модель, яка визначає структуру модельованої системи, властивості її елементів і причинно-наслідкові зв'язки, властиві системі і суттєві для досягнення цілі моделювання. Іншими словами, це змістовна модель, при формулюванні якої використовуються поняття і уявлення предметних областей, пов'язаних з моделлю. Наприклад, математична модель формулюється мовою математики – за допомогою математичних структур: формул, просторових форм і т. п.

Виділяють три види концептуальних моделей: логіко-семантичні, структурно-функціональні та причинно-наслідкові.

Логіко-семантична модель – опис об'єкта термінами відповідних предметних областей знань. Аналіз таких моделей здійснюється засобами логіки із залученням спеціальних знань. При побудові **структурно-функціональної моделі** об'єкт розглядається як цілісна система, яку розчленовують на окремі підсистеми або елементи. Частини системи пов'язують структурними відношеннями, що описують підпорядкованість, логічну і тимчасову послідовність вирішення задач. **Причинно-наслідкова модель** служить для пояснення і прогнозування поведінки об'єкта. Такі моделі орієнтовані на наступні моменти: 1) виявлення головних взаємозв'язків між підсистемами; 2) виявлення певного впливу різних чинників на стан об'єкта; 3) опис динаміки параметрів, що цікавлять розробника.

Концептуальна модель представлена за допомогою формальних мов (до таких відносять алгоритмічні мови, мови моделювання, математичний апарат) прийнято називати ***формальною моделлю***.

Побудова концептуальної моделі включає етапи: 1) визначення типу системи; 2) опис зовнішніх впливів; 3) декомпозиція системи.

На першому етапі здійснюється збір фактичних даних (на основі роботи з літературою і технічною документацією, проведення натурних експериментів, збору експертної інформації і т. д.), а також висунення гіпотез щодо значень параметрів і змінних, для яких відсутня можливість отримання фактичних даних. Якщо отримані результати відповідають принципам інформаційної достатності і здійсненності, то вони можуть служити основою для віднесення модельованої системи до одного з відомих типів (класів).

Одним з класифікаційних ознак модельованої системи є потужність множини і станів системи, що моделюється. За цією ознакою системи ділять на статичні і динамічні. Система називається статичною, якщо множина її станів містить один елемент. Якщо станів більше одного, або вони можуть змінюватися у часі, система називається динамічною. Процес зміни станів називається рухом системи. Розрізняють **два**

основних типи динамічних систем: з дискретними станами (множина станів скінченна або зліченна) та з безперервною множиною станів.

Системи з дискретними станами характеризуються тим, що в будь-який момент часу можна однозначно визначити, в якому саме стані знаходиться система. Для такої ідентифікації обов'язково потрібно знати ту ознаку, яка відрізняє один стан системи від іншого. Наприклад, при дослідженні систем масового обслуговування в якості такої ознаки зазвичай використовують число заявок в системі. Відповідно, зміна числа заявок в системі інтерпретується як перехід системи в новий стан. Якщо ж не вдається підібрати таку ознаку, або його поточне значення неможливо зафіксувати, то систему відносять до класу систем з безперервною множиною станів. Зміна станів може відбуватися або в фіксовані моменти часу, множина яких дискретна (наприклад, надходження нових заявок на обслуговування), або безперервна (зміна температури тіла при нагріванні). Відповідно до цього розрізняють системи з дискретним часом переходів (зміни станів) і системи з безперервним часом переходів (точніше, «живуть» в безперервному часу). За умовами переходу з одного стану в інший розрізняють детерміновані системи і стохастичні.

У детермінованих системах новий стан залежить тільки від часу і поточного стану системи. Іншими словами, якщо є умови, що визначають перехід системи в новий стан, то для детермінованої системи можна однозначно вказати, в який саме стан вона перейде.

Для стохастичної системи можна вказати лише множину можливих станів переходу і, в деяких випадках, – імовірнісні характеристики переходу в кожний з цих станів.

Розглянута схема класифікації систем важлива не сама по собі. На етапі розробки концептуальної моделі вона, по-перше, дозволяє уточнити цілі і задачі моделювання і, по-друге, полегшує перехід до етапу формалізації моделі. Крім того, значно пізніше, на етапі оцінки якості розробленої моделі, знання класифікаційних ознак дає можливість оцінити ступінь її відповідності початковому задуму розробника.

Необхідно відзначити, що розглянуті класифікаційні ознаки застосовні і для визначення типу моделі, що розробляється. При цьому досліджувана система і її модель можуть відноситися як до одного, так і до різних класів. Наприклад, реальна система може бути піддана впливу випадкових чинників і, відповідно, буде відноситися до класу стохастичних систем. Якщо розробник моделі вважає, що впливом цих факторів можна знехтувати, то створювана модель буде являти собою детерміновану систему. Аналогічним чином можуть бути відображені системи з безперервним часом зміни станів у модель з дискретними переходами і т. д.

З наведеного матеріалу випливає, що існує досить велика кількість методів моделювання, причому вище була озвучена тільки частина з них. Слід зазначити, що множина параметрів системи і їх значень відображає її внутрішній зміст – структуру і принципи функціонування або існування. Набір же і значення параметрів виділяють систему серед інших систем. Отже, перелік класифікаційних ознак, при бажанні, може бути завжди розширено. При цьому, як правило, характеристики системи – це в основному її зовнішні ознаки, які важливі при взаємодії з іншими системами. Значення характеристик відображають ступінь взаємозв'язку між системами. У свою чергу характеристики системи знаходяться у функціональній залежності від її параметрів. Кожна характеристика системи визначається в основному або повністю обмеженою підмножиною конкретних параметрів. Інші параметри не впливають або мало впливають на значення даної характеристики системи. Оскільки в кінцевому підсумку дослідника цікавлять тільки деякі характеристики досліджуваної системи при конкретних зовнішніх впливах на систему, то модель – це завжди більш спрощена система зі своїми множинами параметрів і характеристик. Очевидно, що оригінал і модель подібні за одним параметрам і різні за іншим, а заміщення одного об'єкта іншим правомірно, якщо характеристики, які цікавлять дослідника, оригіналу і моделі визначаються однотипними підмножинами параметрів і пов'язані однаковими залежностями з цими параметрами. При цьому, незалежно від класифікаційних ознак моделей усі моделі можна об'єднати в

чотири великі групи у порядку збільшення їх абстрактності і зменшення їх зовнішньої схожості з модельованим об'єктом [1], - тобто у вигляді моделі фізичної подібності (матеріальні); аналогові; символічні (математичні) та інфологічні (вербально-описові, тобто словесно-описові). Очевидно, що іноді можлива і їх трансформація у змішані моделі. Проте спільним для них є реалізація обов'язкових вимог у вигляді того, що модель має бути адекватною об'єкту дослідження і повною. Останнє означає, що вона має давати принципову можливість за допомогою відповідних способів і методів вивчення моделі дослідити і сам об'єкт, тобто отримати деякі твердження щодо його властивостей, принципів роботи, поведінки в заданих умовах.

Таким чином, основним завданням моделювання є забезпечення дослідників технологією створення таких моделей, які б з достатньою повнотою і точністю відображали властивості об'єктів моделювання, що цікавлять, піддавалися дослідженню більш простими й ефективними методами, а також допускали перенесення результатів такого дослідження на реальні об'єкти.

6.2. Аспекти побудови архітектурних моделей захисту інформаційних ресурсів підприємства

В контексті даного навчального посібника нижче доцільно розглянути архітектурну побудову комплексної системи захисту інформаційних ресурсів підприємства з позиції оптимізації її системних заходів із зберігання, шифрування, моніторингу отримання, доставки, обробки, обміну та зберігання інформації, в кожній з яких, окрім людського фактору, використовуються засоби телекомунікації і зв'язку. Така КСЗІ повинна забезпечувати заданий рівень безпеки і надійний захист інформації від різного роду вірусних і хакерських загроз; збереження даних при фізичній втраті та поломці інформаційних носіїв; безпеку доступу до збережених ресурсів; якісне відновлення інформаційної системи у разі пошкоджень.

У цьому випадку роль методу моделювання у сфері захисту інформації дуже важлива, оскільки в даній області часом модель

(або сукупність моделей, яка найчастіше називається архітектурою) є єдиним інструментом аналізу внаслідок неможливості (або обмеженої можливості) проведення експериментів з реальними об'єктами і системами.

Питання моделювання систем і процесів захисту інформації широко досліджуються і обговорюються фахівцями в даній області. З цією метою робляться спроби систематизації і класифікації існуючих моделей, у базис побудови яких зазвичай закладають наявні як сукупність методів і засобів захисту інформації (див. рис. 6.1), так і їхню класифікацію (рис. 6.2).

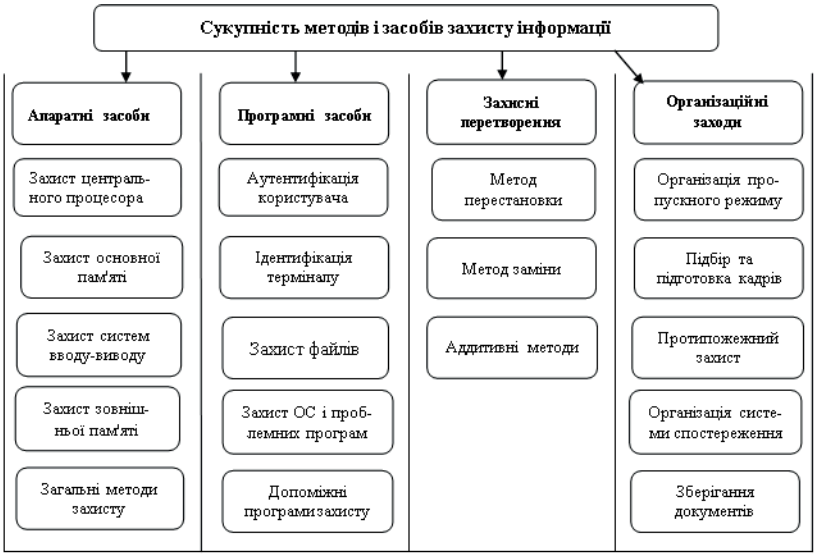

Рисунок 6.1. Сукупність методів і засобів захисту інформації згідно з [2, с.4]

За проблемною орієнтацією зазвичай прийнято оцінювати **чотири групи архітектурних моделей захисту:** *концептуальні моделі; моделі управління безпекою; моделі відношень доступу і дій та потокові моделі.*

У першій групі (концептуальні моделі) об'єднуються моделі за загальносистемною класифікаційною ознакою, що дозволяють

виділити системний об'єкт і визначити його властивості. Проблема захисту інформації вирішується безпосередньо в середовищі системного об'єкта і щодо самого системного об'єкта. У цьому випадку системний підхід вимагає концептуального вирішення поставленої задачі, в зв'язку з чим проблему захисту інформації оцінюють на моделях концептуального рівня. У таких концептуальних моделях аналізується потенційні загрози для системи, канали доступу до інформації, області вразливих місць. Цілі моделювання у цьому випадку – визначення загальної стратегії захисту і можливих нештатних каналів доступу до інформації, прийняття рішення про розміщення додаткових засобів захисту в них, поліпшення складу і модернізація структури системи захисту, оцінка уразливості оброблюваної інформації, вартісних витрат на проектування і експлуатацію системи захисту. Як об'єкти аналізу, елементи предметної області, можуть бути фізичні компоненти системи, а також структурні, інформаційні та керуючі зв'язки між ними.

При проектуванні складних систем захисту інформації може використовуватися певний набір моделей концептуального характеру, сукупність яких дозволяє в достатній мірі визначити властивості системи і прийняти проектні рішення.

Другу групу моделей (моделі управління безпекою) доцільно виділити відповідно до класифікаційної ознаки, що відображає основне функціональне призначення засобів і систем захисту інформації – управління безпекою. За цільової класифікації система захисту інформації відноситься до систем управління. Для дослідження властивостей і закономірностей побудови систем управління використовуються різні кібернетичні моделі, які дозволяють проектувати механізми управління, визначати оптимальні алгоритми перетворення інформації для прийняття рішень і вироблення керуючих впливів на об'єкти управління.

У третій групі моделей (моделі відношень доступу і дій) предметом аналізу є відносини доступу між елементами системи і дій певного елемента по відношенню до інших елементів. Як відношення виступають права доступу і дій суб'єкта до об'єкта. Суб'єктом може бути будь-який активний елемент системи, здатний маніпулювати іншими елементами (пасивними об'єктами). Права доступу і дій користувачів по відношенню до

ресурсів та інформації системи і породжені ними права доступу між елементами системи визначають множину відносин доступу і дій. Ціллю моделювання є виявлення множини цих відношень, їх допустимість і певні можливості несанкціонованих дій по відношенню до інформації за допомогою допустимих (дозволених) перетворень первинних прав. У рамках моделей цієї групи також можуть вирішуватися задачі оптимальної структурної побудови та розміщення інформаційного забезпечення з прав доступу і дій.

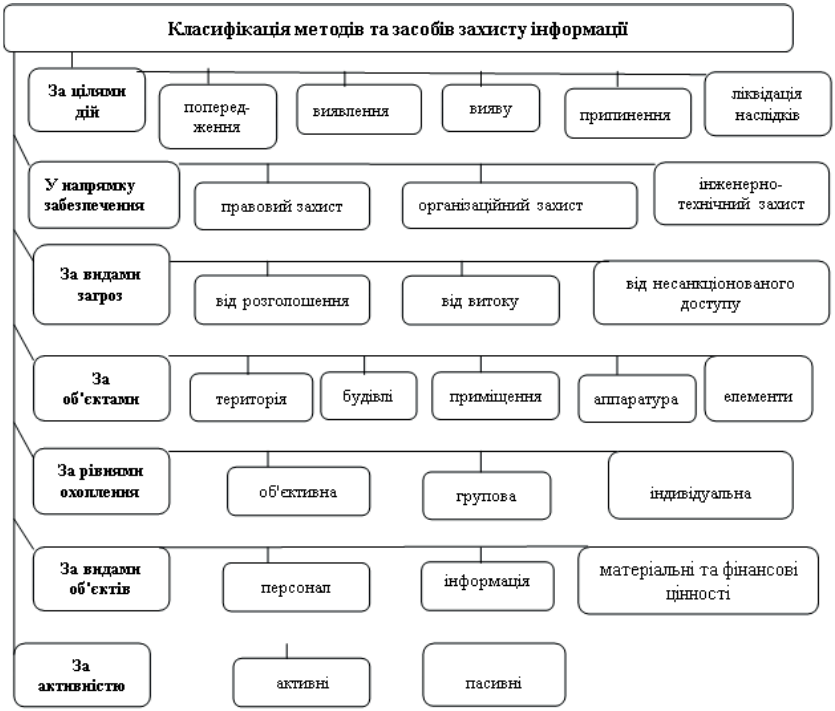

Рисунок 6.2. Сукупність класифікації методів і засобів захисту інформації згідно з [2, с.9]

До четвертої групи (потокові моделі) відносяться моделі, пов'язані з технологією проходження інформації через структурні компоненти системи, які визначаються в предметної

області моделювання як об'єкти системи. У потокових моделях з кожним об'єктом (суб'єкти є окремим випадком об'єктів) зв'язується свій клас захисту, який може змінюватися в процесі роботи системи за суворо визначеними правилами, а інформаційний потік від об'єкта до об'єкта дозволяється, якщо класи захисту знаходяться в установленому відношенні. На моделях перевіряється, чи може в будь-який об'єкт потрапити неприпустима інформація. Об'єкти системи розглядаються спільно із засобами захисту як ланки технологічного процесу обробки даних. Засоби захисту контролюють інформаційні потоки між об'єктами. У деяких моделях засоби захисту вводяться як самостійні об'єкти системи з контролюючими функціями. Зі змісту потокових моделей можна зробити висновок про те, що вони виділяються в самостійну групу за класифікаційною ознакою визначення динаміки інформаційних процесів в умовах безпеки.

Зазначені вище види моделей орієнтуються на певні фази проектування. На ранніх стадіях проектування (проектне обстеження, технічний проект) аналізуються канали доступу до інформації, формується концепція захисту. В цьому випадку концептуальні моделі використовують для визначення цілей захисту: яку інформацію і ресурси і від кого необхідно захищати. Тобто формується задум системи захисту і стратегія захисту. Якщо переважним задумом системи захисту є реалізація цільової функції управління безпекою, то для розробки можуть бути застосовані моделі управління безпекою.

Застосовуючи моделі відношень доступу і дій, моделюються права доступу до інформації, що захищається, виявляються породжувані цими правами відношення доступу між елементами системи. Вирішується питання про структуру і виду подання службової інформації з прав доступу, в тому числі для її використання при прийнятті рішень з управління безпекою. На наступній фазі проектування можливе використання моделей інформаційних потоків. Типовою задачею, шо розв'язується на цих моделях, є ухвалення рішення про розміщення засобів захисту.

Таким чином, модель, спрощуючи образ реального об'єкту або процесу, відображає найсуттєвіші властивості цього об'єкта і

заміщає його в ході вивчення. Очевидно, що для складного об'єкта може створюватися не одна, а кілька моделей різних типів. Сукупність моделей, що відображають загальну організацію, склад компонентів КСЗІ і топологію їх взаємодії, як уже вище було зазначено, прийнято називати архітектурою комплексної системи захисту інформації [1]. Вона охоплює формування наступних моделей: кібернетичної, функціональної, інформаційної, організаційної та структурної.

Розглянемо структуру та зміст цих моделей.

Кібернетична модель. Для того щоб сформувати і потім керувати складною системою, необхідна інформація про структуру, параметри та інші важливі характеристики і властивості суб'єкта та об'єкта управління, що утворюють систему. В даному випадку таку інформацію міститиме в собі кібернетична модель КСЗІ. Саме вона дозволить приступити до вирішення задачі управління системою захисту на об'єкті.

Виходячи з отриманої на етапі формування архітектури КСЗІ інформації, в цю описову за своїм типом модель будуть включені відомості, що відображають роль і місце КСЗІ в більш великій і складній системі. Наприклад, місце КСЗІ конкретного підприємства в загальній державній системі захисту інформації. Ця модель демонструє різні види зв'язків даної системи захисту підприємства з іншими системами.

Функціональна модель відображає склад, зміст і взаємозв'язки тих функцій, здійснення яких досягається ціллю діяльності модельованих систем. ***Основними складовими*** функціональної моделі є:

– перелік функцій, призначених для безпосереднього забезпечення захисту інформації;

– перелік функцій для управління механізмами безпосереднього захисту;

– загальний вміст функцій, тобто перелік їх взаємозв'язків, основних процедур КСЗІ;

– класифікація функцій, тобто розподіл їх по функціональним підрозділам КСЗІ.

Функціональна модель включає у себе два **види функцій**:

I. Для безпосереднього забезпечення захисту інформації призначена функція:

- ✓ попередження умови, що породжує дестабілізуючі чинники;
- ✓ попередження появи дестабілізуючих чинників;
- ✓ виявлення прояви дестабілізуючих чинників;
- ✓ попередження впливу дестабілізуючих чинників;
- ✓ виявлення впливу дестабілізуючих чинників;
- ✓ локалізації впливу дестабілізуючих чинників;
- ✓ ліквідації наслідків впливу дестабілізуючих чинників;

II. Для управління механізмом безпосереднього захисту призначена функція:

- ✓ планування;
- ✓ оперативно-диспетчерського управління;
- ✓ календарно-планового керівництва;
- ✓ забезпечення повсякденної діяльності.

Інформаційна модель відображає структуру, зміст, обсяг і напрям циркуляції тих інформаційних потоків, які необхідні для вирішення всіх задач підприємства і КСЗІ. Особливість інформаційної моделі КСЗІ в тому, що систему захисту інформації підприємства організовують з метою захисту інформації в тих потоках, які циркулюють як в процесі функціонування всього підприємства, так і в процесі функціонування КСЗІ.

Складовими компонентами інформаційної моделі є:

- тип інформаційного потоку за функціональним призначенням;
- вид інформації, що циркулює в потоці;
- етапи циркуляції потоку;
- схема циркуляції інформації кожного виду;
- кількісні характеристики потоків кожного виду.

В інформаційній моделі **циркулює кілька видів інформації:**

- ✓ кореспонденція;
- ✓ технічна документація;
- ✓ періодика (журнали та ін.);
- ✓ книги;

✓ фактографічна швидко змінна інформація інформація;

✓ фактографічна повільно змінна інформація (вихідна і регламентна);

✓ фактографічна постійна інформація.

При цьому інформація циркулює в інформаційній моделі в кілька етапів:

✓ генерування інформації;

✓ введення в систему обробки;

✓ передача інформації;

✓ прийом,

✓ зберігання, накопичення інформації;

✓ пошук інформації;

✓ етап функціональної переробки інформації

✓ і етап видачі інформації для використання.

Організаційна модель КСЗІ показує склад, взаємозв'язок і підпорядкованість в управлінській ієрархії підрозділів, що входять до складу комплексної системи захисту інформації. На побудову даної моделі впливає безліч факторів різної природи:

– специфіка задач, що вирішуються функціональними підрозділами;

– принципи і методи, обрані в даній системі управління;

– технологія реалізації основних функцій;

– кадровий склад співробітників, та інші.

Дана модель формується з урахуванням структури системи управління підприємства, де створюється або функціонує КСЗІ, а також з урахуванням складу основних функцій, що здійснюються в системі захисту.

Структурна модель відображає зміст таких компонентів КСЗІ, як кадровий, організаційно-правовий та ресурсний. При цьому ресурсний компонент включає технічне, математичне, програмне, інформаційне та лінгвістичне забезпечення. Фактично, організаційно-правовий компонент являє собою комплекс організаційно-технічних заходів і правових актів, які є основою, що регулює функціонування основних підсистем КСЗІ. У той же час КСЗІ — це взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів і методів

захисту інформації, головна мета якої полягає в забезпеченні конфіденційності, цілісності та доступності інформації, що обробляється в дата-центрі або хмарному середовищі. Доступ до цієї сукупності (інформації), що забезпечує також зберігання конфіденційної інформації на спеціальному секретному і віддаленому сервері, визначає і контролює керівництво підприємства, тобто є обмеженим і може бути дозволений тільки певним співробітникам за списком. При цьому, архітектурна модель КСЗІ (без опису телекомунікаційної системи зв'язку) передбачає наявність інтегрованих модулів виду *термінального модуля, модуля резервного копіювання, модуля шифрування і модуля реагування*.

Термінальний модуль являє собою централізовану, керовану IT інфраструктуру підприємства з ізольованим сервером для зберігання інформації. З його допомогою забезпечують збір даних в безпечному місці (на одному або декількох секретних серверах) і їх захист від несанкціонованого доступу.

Модуль резервного копіювання служить для створення копій усіх інформаційних даних на основному і резервному секретному сервері. Якщо виникає якась позаштатна ситуація (наприклад, відключення або збій основного секретного сервера), системи модуля перенаправляють інформацію на резервний сервер. Вся інформація, що збирається і зберігається таким чином, шифрується модулем шифрування.

Модуль шифрування здійснює кодування літерних і цифрових даних крипостійкими алгоритмами. Ключі кодування і шифрування інформації передаються користувачеві (керівнику) підприємства і не відомі обслуговуючому систему захисту персоналу. Даний модуль забезпечує захист баз даних, архівів, додатків, електронної пошти. Завдяки йому, можна приховати сам факт наявності будь-якої конфіденційної інформації. У разі виникнення будь-якої загрози інформаційні дані блокуються модулем реагування.

Модуль реагування – це модуль віддаленої дії. Він дозволяє за допомогою так званої «тривожної кнопки» включати, вимикати і перезавантажувати секретний сервер. Кнопкою може бути радіо-брелок або кодове SMS-повідомлення. Сигнал, поданий «тривожною кнопкою», автоматично відключає усі

системи віддаленого сервера. Інформація, що зберігається, при цьому шифрується на жорстких дисках. Відновити інформацію можна буде тільки за допомогою спеціального ключа, який зберігається у першої особи підприємства. Розшифрувати інформацію секретного сервера практично неможливо. Навіть якщо «тривожна кнопка» з якоїсь причини не спрацювала і сигнал на відключення секретного сервера поданий не був, то перед вилученням і транспортуванням службової інформації живлення сервера буде відключено. В цьому випадку в момент відключення живлення паролі і ключі доступу з оперативної пам'яті сервера автоматично видаляються і знищуються. Після відновлення електропостачання (тобто його повторного включення) увійти в систему і розшифрувати диски буде не можливо. Це можна зробити тільки при наявності апаратного ключа, що зберігається у першої особи підприємства. У найгіршому випадку (коли секретний сервер вилучений або знищений), а для нормального функціонування підприємства необхідна інформація, яка на ньому зберігалася, то її можна буде отримати з резервного сервера, використовуючи модуль резервного копіювання.

При додатковій оцінці інформаційної безпеки з урахуванням телекомунікаційних систем зв'язку необхідно також проводити оцінку на відповідність офіційним критеріям захищеності інформації в ІТС. Зокрема, при аналізі інформаційної безпеки критично важливих об'єктів зі штатними ІТС слід визначати допустимі межі використовуваних систем за критеріями захищеності інформації хоча б для області апріорного несанкціонованого доступу (НСД). Такі критерії захищеності інформації в ІТС, прийняті в Україні, і основні моделі, що прийнято вивчати в процесі науково-дослідних робіт (НДР) по КСЗІ, наведені на рис. 6.3, адаптованому з [3, с.45, 220]. При цьому наведені послуги є більш-менш незалежними. Якщо ж така залежність виникає, тобто реалізація будь-якої послуги неможлива без реалізації іншої, наприклад, при моделюванні КСЗІ в процесі її НДР, то цей факт відображається як необхідні умови для даної послуги (або її рівня).

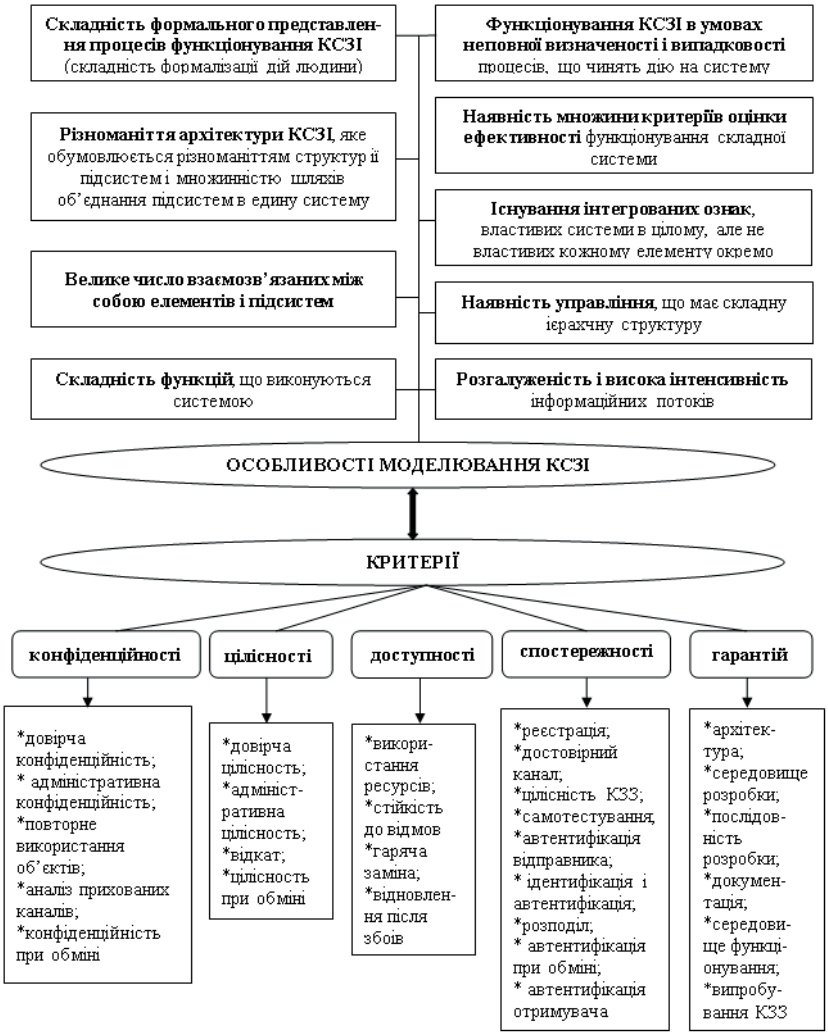

Рисунок 6.3. Особливості моделювання КСЗІ та система офіційних критеріїв захищеності інформації в ІТС від НСД

Таким чином, описана комплектація архітектурної моделі комплексного захисту інформації з точки зору проблемної

орієнтації охоплює всі чотири групи архітектурних моделей захисту (концептуальні моделі; моделі управління безпекою; моделі відношень доступу і дій; потокові моделі), що в сукупності дозволяє самостійно контролювати стан інформаційної системи підприємства, вчасно і надійно блокувати доступ до важливої і конфіденційної інформації підприємства, а також, у разі надзвичайної ситуації (пожежі або інших стихійних лих) надалі відновити втрачені після блокування і поломок дані.

6.3. Методологічні та технологічні основи побудови систем автоматизованого проектування захисту службової інформації

Система захисту інформації характеризується великим числом взаємодіючих між собою засобів і багатофункціональним характером розв'язуваних з її допомогою задач. Перш за все для ефективного забезпечення безпеки інформації потрібне створення розвиненого методологічного базису, що дозволяє вирішити наступні **комплексні завдання:**

− створення системи органів, відповідальних за безпеку інформації;

−розробки теоретико-методологічних основ забезпечення безпеки інформації;

−вирішення проблем з управління захистом інформації та її автоматизації;

− створення нормативно-правової бази, яка регламентує виконання задач забезпечення безпеки інформації;

− налагодження виробництва засобів захисту інформації;

− організації підготовки фахівців із захисту інформації;

− підготовки нормативно-методичної бази для проведення робіт щодо забезпеченню безпеки інформації.

У зв'язку з чим доцільно нижче, не дивлячись на раніше введені понятійні визначення, уточнити і деталізувати деякі основні терміни, що використовуються в області захисту інформації, а саме:

- захист інформації – діяльність, спрямована на запобігання витоку інформації, що захищається,

несанкціонованих і навмисних впливів на інформацію, що захищається;

- інформація, що захищається, – інформація, яка є предметом власності і підлягає захисту відповідно до вимог правових документів або вимогами, встановленими власником (держава, юридична особа, група фізичних осіб або окрема фізична особа) інформації;

- захист інформації від витоку – діяльність, спрямована на запобігання неконтрольованого розповсюдження інформації, що захищається в результаті її розголошення, несанкціонованого доступу до інформації та отримання інформації, що захищається розвідками;

- захист інформації від несанкціонованого впливу – діяльність, спрямована на запобігання впливу на інформацію, що захищається, з порушенням встановлених прав і (або) правил на зміну інформації, що призводить до її спотворення, знищення, блокування доступу до інформації, а також до втрати, знищення або збою функціонування носія інформації;

- захист інформації від ненавмисного впливу – діяльність, спрямована на запобігання впливу на інформацію, що захищається, помилок її користувача, збою технічних і програмних засобів інформаційних систем, природних явищ чи інших не цілеспрямованих на зміну інформації заходів, що призводять до спотворення, знищення, копіювання, блокування доступу до інформації, а також втрати, знищення або збою функціонування носія інформації;

- захист інформації від розголошення – діяльність, спрямована на запобігання несанкціонованого доведення інформації, що захищається, до споживачів, які не мають права доступу до цієї інформації;

- захист інформації від несанкціонованого доступу – діяльність, спрямована на запобігання отримання інформації, що захищається, зацікавленим суб'єктом (держава, юридична особа, група фізичних осіб, у тому числі громадська організація, окрема фізична особа) з порушенням встановлених правовими документами чи власником, власником інформації прав або правил доступу до інформації, що захищається.

- захист інформації від розвідки – діяльність, спрямована на запобігання отримання інформації, що захищається, розвідкою, як іноземною, так і вітчизняною;

- система захисту інформації – сукупність органів і (або) виконавців, техніки захисту інформації, що використовується ними, а також об'єктів захисту, яка організована і функціонує за правилами, встановленими відповідними правовими, організаційно-розпорядчими та нормативними документами у галузі захисту інформації;

- захід щодо захисту інформації – сукупність дій, спрямованих на розробку і (або) практичне застосування способів і засобів захисту інформації;

- техніка захисту інформації – засоби захисту інформації, засоби контролю ефективності захисту інформації, засоби і системи управління, призначені для забезпечення захисту інформації;

- об'єкт захисту інформації – інформація, або носій інформації, або інформаційний процес, які необхідно захищати відповідно до поставленої мети захисту інформації;

- спосіб захисту інформації – порядок і правила застосування певних принципів і засобів захисту інформації;

- контроль стану захисту інформації – перевірка відповідності організації та ефективності захисту інформації встановленим вимогам і (або) нормам захисту інформації;

- засіб захисту інформації – технічний, програмний засіб, речовина і (або) матеріал, призначені або використані для захисту інформації;

- контроль організації захисту інформації – перевірка відповідності організації, наявності та змісту документів вимогам правових, організаційно-розпорядчих та нормативних документів у галузі захисту інформації.

Очевидно, що державна політика у сфері формування інформаційних ресурсів та інформатизації обов'язково повинна бути спрямована на створення умов для ефективного і якісного інформаційного забезпечення вирішення стратегічних і оперативних задач соціального та економічного розвитку країни. При цьому, вирішуючи проблему забезпечення безпеки підприємницької діяльності, недостатньо обмежитися

побудовою системи безпеки, необхідна розробка *концепції безпеки підприємницької діяльності*.

Концепція безпеки є комплексом технічних і організаційних заходів, спрямованих на попередження, припинення і ліквідацію наслідків максимальної кількості загроз з повного набору можливих загроз для цієї підприємницької діяльності. Концепція безпеки дає змогу захистити як один, так і групи різнорідних об'єктів, забезпечуючи при цьому централізований контроль, автоматизовану реєстрацію всіх подій і централізоване управління.

Використовуючи системний підхід, модель формування і реалізації концепції безпеки підприємницької діяльності можна подати у вигляді рис. 6.4, адаптованому з [4]. Цей малюнок (у вигляді моделі формування та реалізації концепції безпеки підприємницької діяльності) досить детально відображає можливий алгоритм створення інтегральної системи безпеки (ІСБ) організації, починаючи з обстеження підприємства, вивчення його видів діяльності, аналізу загроз і ступеня ризиків та виявлення об'єктів захисту.

Далі потрібно визначити, як впливає кожен елемент системи безпеки на реалізацію конкретної загрози (сприяння, незалежність, конфлікт) для одержання значень коефіцієнтів ефективності кожної підсистеми, що входить до складу ІСБ.

Як бачимо, щоб така складна система захисту інформації ефективно функціонувала, необхідно розглянути цілий комплекс питань ще на стадії її створення. Для вирішення таких проблем потрібно організована діяльність багатьох осіб, що реалізована в рамках штучних (тобто створених людиною) формувань. У цьому випадку такі формування називають організаційними системами.

Основним елементом будь-якої організаційної системи (ОС) є люди, що умовно розбиваються на організаторів і виконавців. Множина виконавців з їх знаряддями праці утворює об'єкт управління (ОУ), множина організаторів (керівників) разом з інформацією, технікою, фахівцями і обслуговуючим персоналом – суб'єкт управління (СУ). Чітку межу між ОУ та СУ провести неможливо, оскільки виконавча діяльність нероздільна з

управлінською, а остання без виконавчої безглузда, проте для цілей побудови ОС такий поділ є корисним.

Рисунок 6.4. Модель формування і реалізації концепції безпеки підприємницької діяльності

З поняттям ОС тісно пов'язане поняття «діяльність», так як основна задача ОС полягає в тому, щоб координувати і здійснювати діяльність людей, спрямовану на вирішення проблеми. У зв'язку з цим діяльність можна визначити як усвідомлене і спрямоване на вирішення проблеми поводження людей. Поняття «діяльність» будемо відносити не тільки до

окремої людини або групи людей; але і до ОС в цілому. Остання може включати також і забезпечуючі підсистеми, які виконують допоміжну діяльність, наприклад постачання, ремонт, інформаційне обслуговування, енергозабезпечення та ін.

Кожна ОС побудована за ієрархічним принципом. Найбільшого поширення набули структури, реалізовані за:

- лінійним принципом, де кожен виконавець (В) підпорядковується тільки одному керівнику (К) з усіх питань своєї діяльності. Основний недолік лінійних структур – сильна залежність результатів роботи всієї ОС від якості рішень першого керівника;

- ***функціональним принципом,*** де кожен виконавець підпорядковується кільком функціональним керівникам (ФК) одночасно, причому кожному зі строго визначених питань. При цій структурі керівні вказівки більш кваліфіковані, але порушується принцип єдиноначальності;

- ***лінійно-штабним принципом,*** коли система управління побудована таким чином, щоб у кожній ланці управління були створені штаби (ради, відділи, лабораторії), в яких є фахівці з окремих важливих питань. Призначення штабу – підготувати кваліфіковане рішення, яке затверджує і передає їх на нижні рівні лінійний керівник;

- ***програмно-цільовим (матричним) принципом,*** що поєднує у собі особливості всіх розглянутих вище структур.

Як правило, для вирішення найскладнішого виду проблем (так званих непрограмованих проблем) шляхом організаційної системи реалізують такі технологічні етапи:

1. Постановка проблеми, яку потрібно вирішити.

2. Дослідження проблеми: збір і аналіз усіх доступних об'єктивних даних і знань про проблему та фактори, що впливають на її рішення, формування банку проблемних знань, побудова та дослідження моделі проблеми (якщо проблема допускає модельне уявлення).

3. Визначення меж (складу) проблемного об'єкта, тобто усіх потенційних учасників вирішення проблеми (організацій, колективів і осіб, від діяльності яких залежить її рішення).

4. Обстеження проблемного об'єкта. Проводиться обстеження ОС, що входять до складу проблемного об'єкта, і

вибирається комплекс заходів щодо вирішення проблеми. На цьому етапі формується план заходів (або цільова комплексна програма) щодо вирішення проблеми і вирішується питання про доцільність створення ОС.

5. Вибір критерію ефективності ОС. На цьому етапі розпочинається власне розробка майбутньої ОС. Вибір критерію ефективності системи дає можливість надалі об'єктивно оцінювати альтернативні проекти ОС.

6. Вибір меж (складу) ОУ. З усіх потенційних учасників вирішення проблеми відбираються ті, хто увійде до складу ОУ проектованої ОС.

7. Обстеження ОУ. Проводиться поглиблене обстеження організацій, що входять до складу ОУ, з метою отримання даних, необхідних для формування альтернативних варіантів побудови СУ і ОС в цілому.

8. Розробка технічного завдання на створення ОС. Виробляються вибір найефективнішого варіанту побудови ОС і розробка технічного завдання.

9. Технічне і робоче проектування ОС.

10. Впровадження ОС.

Перераховані вище етапи не обов'язково повинні бути строго послідовними. На кожному з них допускається повернення до одного з попередніх. Залежно від особливостей проблеми і умов її вирішення можливе об'єднання кількох етапів у один або пропуск окремих етапів. При цьому пропонована технологічна схема має рекомендаційний, а не обов'язковий, характер і вимагає в кожному конкретному випадку деталізації та уточнення в залежності від специфіки розв'язуваної проблеми.

Поряд з органами, що здійснюють управління по вертикалі, створюються додаткові органи, покликані забезпечувати управління по горизонталі. При проектуванні КСЗІ, тобто в процесі розробки і впровадження проекту організаційної та функціональної структури системи (систем) захисту, слід використовувати можливості існуючих методів і засобів захисту з метою забезпечення надійного функціонування об'єкта (підприємства) в сучасних умовах, використовуючи сучасні автоматизовані системи проєктування (САПР). Причому для кожної системи повинна бути сформульована мета, до якої вона

прагне. Ця мета може бути описана як призначення системи, як її функція. Чим точніше і конкретніше вказано призначення або перераховані функції системи, тим швидше і правильніше можна вибрати кращий варіант її побудови. Залежно від повноти переліку питань, що підлягають дослідженню, проектні роботи представляють у вигляді розробок комплексного або локального проекту. Перелік напрямів комплексного проектування визначають залежно від потреб конкретного підприємства і поставлених перед проектом завдань і умов. Відповідно, при локальному проектуванні коло завдань звужується і проект може бути обмежений розробками за одним із напрямків. Але локальні проекти повинні здійснювати як частини комплексного проекту, послідовно реалізовані в ході роботи. Інакше впровадження проекту може привести до негативних результатів. Можна виділити також індивідуальне і типове проектування. Індивідуальне являє собою розробку проекту для якого-небудь конкретного підприємства, з урахуванням його специфічних особливостей, умов і вимог. Типові проекти мають на меті уніфікацію та стандартизацію процесів захисту на різних підприємствах.

Найкращих результатів досягають, як правило, тоді, коли целі чітко розділяється на окремі етапи, результати яких фіксуються, обговорюються і офіційно затверджуються. Рекомендується процес реалізації систем будь-якого рівня складності розділяти на передпроектну стадію, на стадію проектування і на стадію введення в експлуатацію:

Передпроектна стадія складається з наступних етапів:

1. Етапу розробки техніко-економічного обґрунтування, на якому аналізується діяльність об'єкта, готуються для техніко-економічного обґрунтування (ТЕО) вихідні дані. Головне на цьому етапі обґрунтування доцільності і необхідності створення системи захисту, орієнтовний вибір каналів, що захищаються, визначення обсягів і складу робіт зі створення системи захисту, кошторису і терміни їх виконання. Техніко-економічне обґрунтування має узгоджуватися з усіма організаціями та службами, відповідальними за забезпечення безпеки, і затверджуватися особою, що приймає рішення.

2. Етапу розробки технічного завдання, що включає розробку і обґрунтування вимог до структури системи захисту з урахуванням забезпечення сумісності і взаємодії усіх засобів. Головне на цьому етапі – збір і підготовка вихідних даних, визначення складу системи, плану її створення і оцінка витрат. Розробка технічного завдання починається після затвердження техніко-економічного обґрунтування.

На стадії проектування реалізується:

1. Етап розробки технічного проекту, тобто обґрунтовують усі проектні рішення, вибирають найкращий, уточнюють переліки технічних засобів, порядок і терміни їх поставки. У технічному проекті можуть розглядати 2-3 варіанти вирішення поставленого завдання зі створення системи захисту. Усі варіанти повинні супроводжуватися розрахунком ефективності, на основі якого можуть бути зроблені висновки про оптимальний варіант. При створенні системи захисту невеликого або простого об'єкта етап технічного проектування може бути виключений.

Етап розробки робочого проекту призначений для деталізації проектних рішень, прийнятих на попередньому етапі. Зокрема:

- визначають і фіксують регламент взаємодії окремих служб і складових системи забезпечення безпеки;
- складають технологічні та посадові інструкції персоналу;

розробляють робочу документацію. До складу робочої документації входять: специфікація обладнання і матеріалів, схеми розміщення технічних засобів системи захисту (охоронно-пожежної сигналізації, охоронного телебачення, охоронного освітлення тощо), схеми прокладки кабельного зв'язку системи захисту, схеми прокладки електроживлення системи захисту.

Як правило, кожна система захисту унікальна, тому документація строго індивідуальна і залежить не тільки від типу і розміру об'єкта захисту, а й від можливостей і досвіду замовника, який буде її експлуатувати. Оскільки документація містить конфіденційні відомості, коло осіб, допущених до ознайомлення і роботи з нею, повинно бути обмеженим.

На стадії введення в експлуатацію систем захисту забезпечують виконання робіт, що включають:

− комплектацію технічного забезпечення системи;

− монтажні або будівельно-монтажні роботи та пусконалагоджувальні роботи;

− навчання персоналу (попередньо повинні бути укомплектовані усі служби системи забезпечення безпеки з урахуванням необхідної кваліфікації);

− дослідну експлуатацію компонентів і системи в цілому;

− приймальні випробування і приймання системи в експлуатацію.

Усі ці роботи починаються тільки після затвердження всіх документів і виділення фінансових коштів. При цьому слід мати на увазі, що, як правило, інформаційну базу структурно-функціональної схеми у вигляді моделі САПР-захисту інформації (яка для прикладу наведена на рис. 6.5 і адаптована з [1]) зазвичай використовують як проблемно-орієнтований банк даних, до якого входять: файл вихідних даних; файл стандартних засобів захисту; файл штатних засобів захисту; каталог стратегій нападу Y; каталог заходів захисту X і норми ефективності захисту. Згідно з цим розробник системи захисту проводить технічне і комерційне порівняння всіх пропозицій від конкуруючих фірм-виробників захисного обладнання, після чого вибирає постачальника, укладає договір на поставку обладнання та оплачує його. При отриманні обладнання бажано відразу проводити його перевірку на відповідність супровідним документам і технічним умовам, а також (якщо це можливо) перевірку працездатності в умовах експлуатації. Усі роботи з монтажу і налагодженні системи захисту повинні виконувати фахівці.

Силами замовника можна виконувати тільки специфічні і невеликі за трудовитратами роботи такі, як, наприклад, установка прихованого телеспостереження, перенесення датчиків охоронної сигналізації, ремонт системи радіозв'язку тощо. Очевидно щоб у монтажі і налаштуванні захисних систем брали участь ті співробітники служби охорони об'єкта, які будуть їх експлуатувати.

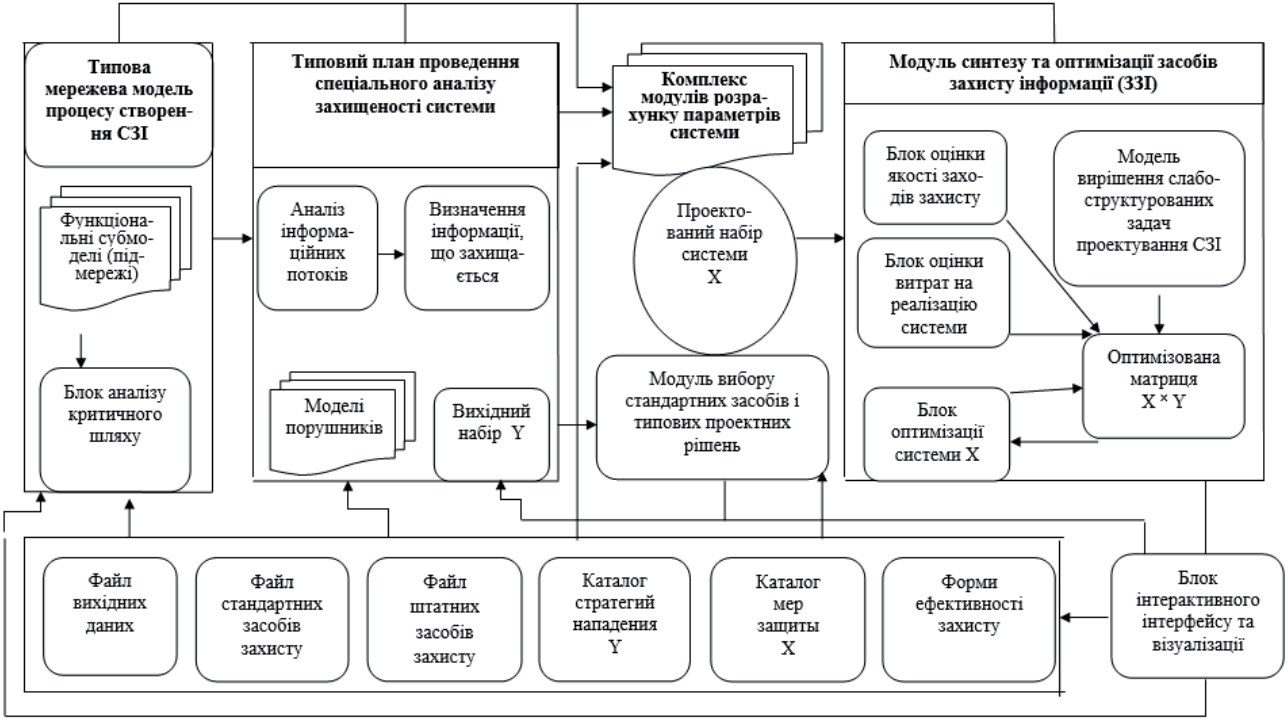

Рисунок 6.5. Модель системи автоматизованого проектування захисту інформації

Зрозуміло, що після закінчення робіт і випробувань прийнято уточнювати (порівнювати) відповідність тактико-технічних характеристик реалізованої системи з даними апріорної моделі прототипу з метою подальшого більш достовірного забезпечення гарантійного та післягарантійного обслуговування реалізованої системи захисту.

Зазвичай (див. рис. 6.5):

− каталог потенційних стратегій нападу, спрямованих на несанкціоновані дії, є результатом спеціального інженерного аналізу;

− каталог заходів захисту - перелік заходів, що забезпечують захист від стратегій нападу;

− каталог норм ефективності захисту містить апріорі задані межі норм ефективності захисту інформації в АСЗД від витоку інформації під впливом конкретної стратегії нападу, що називається допустима ймовірність несанкціонованого доступу до інформації під час реалізації даної стратегії нападу в умовах протидії з боку захисту.

Однак для цілої низки прикладних завдань із захисту інформації ці норми відсутні. У таких випадках як орієнтири використовують вимоги замовника, узгоджені з розробником системи.

Таким чином, критерієм оптимального впровадження СЗЗІ може слугувати мінімізація витрат на їхню реалізацію та подальшу експлуатацію за умови забезпечення заданих рівнів захищеності інформації від несанкціонованих дій з боку всіх імовірних стратегій нападу на життєдіяльність підприємства.

6.4. Менеджмент безпеки об’єктів критичної інфраструктури з позицій зниження результативності ризиків

В основі штатної працездатності об'єктів критичної інфраструктури (ОКІ), відповідно до методології побудови пізнавальної моделі їх захисту та безпеки [5], лежала процедура перевірки справжності доступу до них – аутентифікації. Реалізація останньої була розглянута з позицій стандартів

України, які мають аналоги у межах ISO щодо оцінювання супутніх ризиків згідно фізичної та інформаційної безпеки. Саме з цих позицій ***менеджмента ризику*** (risk management) [6] – «скоординованих дій з керівництва та управління організацією в області ризику» – продовжено аналіз запропонованої Системи оцінювання ризику безпеки сукупності об'єктів критичної інфраструктури (СОКІ) та доступу до неї з позицій зниження результативності ризиків. При цьому, із врахуванням вибору критеріїв ризику та «ступеню реалізації запланованих робіт і досягнення запланованих результатів» (тобто результативності [7, п.3.7.11]) доцільно розглянути наступні підсистеми: стандартів України [8 -11] загального оцінювання ризику, які є аналоги у межах ISO; методів загального оцінювання ризику згідно IEC/ISO 31010 2013 (Додаток В) [12]; оцінювання втрат безпеки згідно ДСТУ ISO/IEC 27000:2019 (конфіденційності, цілісності, доступності, спостережності, автентичності, надійності [13] та стійкості рубежів захисту [14]); фільтрації даних ризиків, згідно ДСТУ ISO/IEC 27001:2013 та підтримки прийняття рішень (ПсППР) доступа до СОКІ [15, Ст.1, п.1, поз.9].

Слід звернути увагу, що в цих стандартах аспекти безпеки мають інформативний характер, де від провадження загального оцінювання ризику маємо деякі основні вигоди [12, с.2], а саме: розуміння ризику та його потенційного впливу на досягнення цілей; надання інформації особам, які приймають рішення; поліпшення розуміння ризиків з тим, щоб допомогти у вибиранні варіантів їх обробляння; ідентифікування важливих чинників, що сприяють ризикам, і слабких ланок у системах та організаціях; порівняння з ризиками в альтернативних системах, технологіях або підходах; обмінювання інформацією про ризики та невизначеності; допомога в установленні пріоритетів; запобігання інцидентам на основі розслідування їхніх причин та наслідків; вибирання різних форм обробляння ризику; задоволення регуляторних вимог; забезпечування інформацією, яка дає змогу оцінити, наскільки ризик потрібно прийняти, якщо брати до уваги попередньо визначені критерії; загальне оцінювання ризиків, пов'язаних з утилізацією продукції після закінчення строку її служби.

З наданих в стандарті [11, с.4,5] формулювань випливає, що загальне оцінювання ризику – це спільний процес: *ідентифікування ризику*, *аналізування ризику та оцінювання ризику.* Причому загальне оцінювання ризику повинно відповідати його (ризику) критеріям, які встановлюють на початку процесу оцінки ризику, а у разі потреби обов'язково переглядають та коригують. Більш того, необхідно враховувати умови для вибору критеріїв ризику, виходячи з оцінки їх значущості за підтримки процесів прийняття рішень, які мають бути узгоджені зі структурою управління ризиками та адаптовані до конкретних цілей та обсягів аналізованої діяльності згідно ДСТУ ISO 31000:2018 [9, п.6.3.4] (табл. 1).

Таблиця 1 Умови для вибору критеріїв ризику (їх залежність)

Позначення	**Зміст залежності умов від наступних чинників:**
ВК.1	характеру та типу невизначеностей, які можуть вплинути на результати та досягнення цілей (як матеріальні, так і нематеріальні)
ВК.2	способу визначення та оцінки наслідків (як позитивних, так і негативних) та їх ймовірність
ВК.3	факторів, пов'язаних з часом
ВК.4	коректності та узгодженості застосовуваних методів вимірювань
ВК.5	порядку визначення рівня ризику
ВК.6	способу обліку комбінації та послідовності множинних ризиків
ВК.7	масштабу організації, підприємства, офісу та ін.

Отже, оцінка ризику (див. табл. 2) – це фактично процес, спрямований на досягнення цілей як за змістом (у різних галузях життєдіяльності соціуму), так і за призначенням (наприклад, як розробки проектів, технологій, продукції тощо), який, забезпечуючи ідентифікацію ризику, аналіз ризику та порівняльну оцінку ризику

[9, п.6.4.1], має використовувати сучасну методологію побудови, у даному випадку СОКІ, з оптимізацією відомих та

створенням нових систем контролю та управління доступу (СКУД) до них.

Таблиця 2 Методи загального оцінювання ризику

Позначення	Зміст методів
B.1	Мозкова атака
B.2	Структуроване чи напівструктуроване опитування
B.3	Метод Дельфі
B.4	Переліки контрольних запитань
B.5	Попереднє аналізування небезпечних чинників (PHA)
B.6	Метод HAZOP (HAZard and Operability study) – дослідження небезпечних чинників і працездатності
B.7	Аналізування небезпечних чинників і критичні точки контролю
B.8	Загальне оцінювання екологічного ризику
B.9	Структурований метод «Що – якщо» (SWIFT)
B.10	Аналізування сценарію
B.11	Аналізування впливу на діяльність (BIA)
B.12	Аналізування першопричин (RCA)
B.13	Аналізування видів і наслідків відмов (FMEA) і аналізування видів, наслідків і критичності відмов (FMECA)
B.14	Аналізування дерева відмов (FTA)
B.15	Аналізування дерева подій (ETA)
B.16	Аналізування причин і наслідків
B.17	Аналізування причинно-наслідкових зв’язків
B.18	Аналізування рівнів захисту (LOPA)
B.19	Аналізування дерева рішень

Позначення	Зміст методів
B.20	Загальне оцінювання надійності людини (HRA)
B.21	Аналізування діаграми «краватка-метелик»
B.22	Технічне обслуговування, зорієнтоване на забезпечення безвідмовності
B.23	Аналізування паразитних впливів (SA) і аналізування паразитних схем (SCA)
B.24	Марковське аналізування
B.25	Імітаційне моделювання методом Монте-Карло
B.26	Байєсівська статистика та мережі Байєса
B.27	Криві FN
B.28	Індекси ризику
B.29	Матриця наслідків/імовірностей
B.30	Аналізування витрат і вигод (CBA)
B.31	Багатокритерійне аналізування рішень (MCDA)

З метою запобігання несанкціонованому фізичному доступу, будь-яким пошкодженням та втручанню зі втратою (частковою або повною) конфіденційності, цілісності, доступності, спостережності, автентичності та надійності як службової інформації організації, так і цілісності виробничої системи організації з її засобами отримання, обробки та зберігання інформації необхідно виконати вибір методу оцінювання ризику та реалізації відповідного захисту, які суттєво залежать від наступних чинників:

- внутрішнього та зовнішнього середовища організації [9, п.5.4.1];
- стійкості рубежів захисту зон безпеки і безпеки обладнання [14, п.А.11];
- професіоналізму співробітників [9, п.5.4.2,3] у процесі прийняття рішень

та змісту методів згідно [12, Додаток В (довідковий) с. 18-71] та ДСТУ IEC/ISO 31010:2013 у межах (IEC/ISO 31010:2009, IDT).

Мета подальшого викладу полягає в обґрунтуванні та аналізі запропонованої пізнавальної структурно-лінгвістичної схеми (СЛС) методології побудови Системи захисту та безпеки об’єктів критичної інфраструктури (ОКІ) (див. рис.6.6) з позицій зниження результативності ризиків, згідно рекомендацій ДСТУ ISO 9000:2015 (ISO 9000:2015,IDT) відносно п.3.12.4 [7].

Очевидно, що підвищення рівня захисту СОКІ, оцінювання втрат безпеки (згідно з гіпотетичним кіберінцидентам, які мають ймовірнісний характер), – це динамічний процес залучення ресурсів (методів, способів та алгоритмів) мультисервісної мережі зв'язку (криптографічних, канальних та інших) з її кореляційними пристроями, що фільтрують, реалізованими під конкретні вимоги (завдання) користувачів для передачі інформації, що захищається. Отже, вибір рівнів спрацьовування кінцевих порогових блоків має багатопрофільний характер і залежить від задекларованих ймовірностей правильного виявлення чи пропуску кібератак чи кіберзагроз [5].

Підсистема фільтрації даних ризиків виконує вирішальну роль щодо наступних об'єктів та процесів: управління доступом; зон фізичної безпеки та захисту від навколишнього середовища; безпеки під час обробки інформації; безпеки зв'язку; придбання, розробка та підтримка систем та управління інцидентами інформаційної безпеки. Причому детальний опис змісту аспектів, згідно вимог менеджменту інформаційної безпеки, наведено у [14], а найбільш важливі для процесів оцінки та обробки ризиків безпеки СОКІ висвітлені в табл. 3. Хоча очевидно, що жодна підсистема фільтрації (обробки) даних ризиків не здатна забезпечувати 100% ефективність.

Наведені дані в таблиці 3 дозволяють оптимізувати доступ до СОКІ завдяки підсистемі підтримки прийняття рішень (ПсППРД) доступу до СОКІ. Ця підсистема завжди функціонуватиме в умовах «невизначеності», у тому числі залежної від зміни кліматичних умов навколишнього середовища. Причому, в ДСТУ ISO 31000:2018 [п.3.1, Примітка 5], акцентують увагу на тому, що «невизначеність – це стан повної або часткової відсутності інформації, необхідної для розуміння події (3.5), її наслідків (3.6) та їх ймовірностей», де мають місце наступні формулювання: «подія (event):

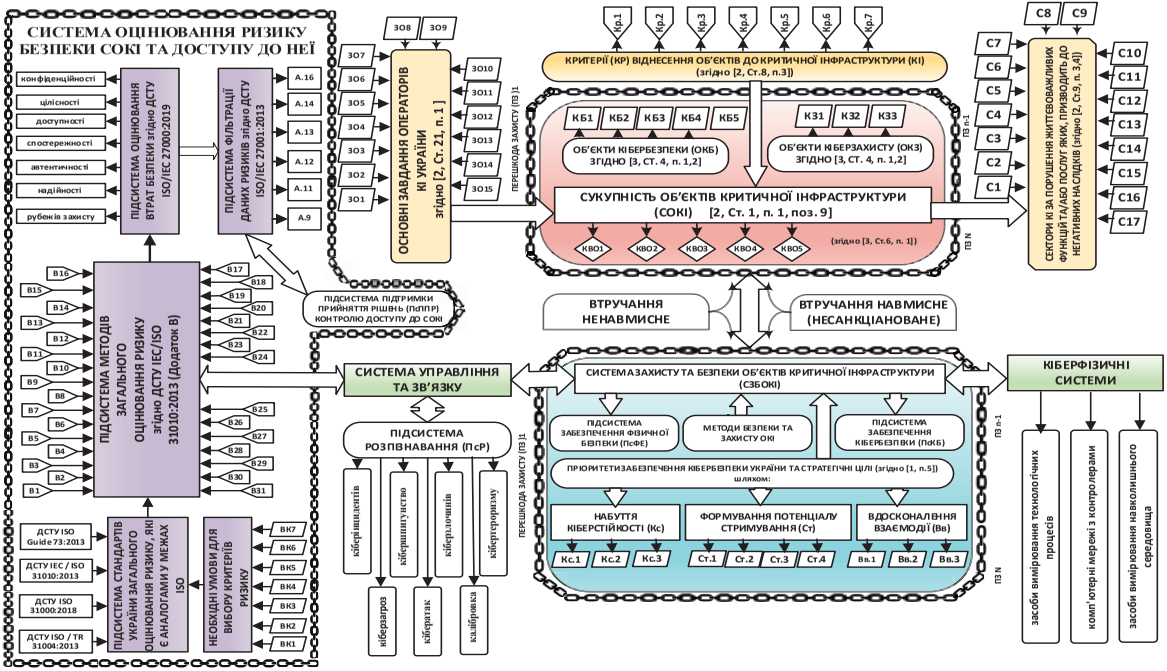

Рисунок 6.6. Структурно-лінгвістична схема методології побудови (з підсистемою фільтрації даних ризик та вибору критеріїв ризику) Системи захисту та безпеки об'єктів критичної інфраструктури (ОКІ) з позицій зниження результативності ризиків

- виникнення або зміна специфічного набору умов»; «наслідки (consequence): - результат впливу події (3.5) на об'єкт».

Однак, слід зауважити, що відповідно до документів ISO/IEC будь-які вимірювання засобами вимірювання (ЗВ), у тому числі пов'язані з контролем навколишнього середовища або параметрів технологічних процесів, також піддаються принципу невизначеності. Тому доцільно виставляти підвищені зобов`язання до надійності і безпеки ЗВ з метою виконання жорстких вимог з оцінки ризиків кібербезпеки в умовах реалізації принципу невизначеності [16] при забезпеченні метрологічної достовірності вимірювань за допомогою будь-яких ЗВ [17].

Отже, ПсППР доступу до СОКІ зобов'язана забезпечувати розв'язання задач як щодо фізичного захисту від наслідків впливу навколишнього середовища, так і при реалізації безпеки безпосереднього процесу отримання та обробки супутньої інформації, що гіпотетично підпадає під можливі кіберінциденти.

Як відомо, добре організована з використанням сучасних технічних засобів системи контролю та управління доступом (СКУД) дозволяють вирішувати цілу низку завдань, до яких (як найважливішим) можна віднести такі [18]: протидія промисловому шпигунству; протидія крадіжкам; протидія саботажу; протидія умішленному пошкодженню матеріальних цінностей; облік робочого часу; контроль своєчасності приходу і відходу співробітників; захист конфіденційності інформації; регулювання потоку відвідувачів; контроль в'їзду і виїзду транспорту. Крім цього, СКУД є бар'єром для цікавих.

Останнім часом, при реалізації конкретних СКУД, також використовують різні способи та реалізують пристрої для ідентифікації та аутентифікації особистості. Отже, правильно побудована (адекватна реальності) модель СОКІ з його Системою захисту та безпеки, а також модель порушника, в якій відображаються його практичні та теоретичні можливості, апріорні знання, час і місце дії та інші характеристики, є важливою складовою успішного проведення аналізу ризику та визначення вимог до складу та характеристик інтегральної системи захисту. Однак слід нагадати, що навіть в умовах багаторівневої системи перешкод жодна пізнавальна модель не може одночасно виконувати необхідно безліч завдань "захисного

напрямку" [19, с.93]. Саме цьому доцільно оцінювати ефективність моделі в конкретному (обраному) аспекті її реалізації. Причому в області СКУД не приділено достатньо серйозної уваги щодо контролю за подоланням повітряних рубежів захисту до підриву конкретної захисної (охоронюваної) оболонки об'єкта. Тому для прикладу з виявленням несанкціонованих повітряних атак зловмисників, які використовують дрони, підходить демонстрація (задача) можливості забезпечення штатного рівня захисту ОКІ шляхом реалізації кореляційних радіолокаційних пристроїв ближньої взаємодії [20, с. 403] із супутніми пороговими блоками. При цьому завдання загальної та параметричної ідентифікації розпізнавання потенційних атак за допомогою дослідження гіпотетичної сигнальної аналогової дії слід також зводити до кореляційного аналізу зондувальних та відбитих сигналів, наприклад від дронів, які вторглись у повітряну область КВО, що охороняється.

Таким чином, сенс інформаційної безпеки полягає в неможливості нанесення шкоди штатному функціонуванню та властивостей ОКІ або їх структурним складовим. Отже на державному (і не тільки) рівні вимушені створювати системи кібербезпеки, цілеспрямовані дії яких пов'язані з кіберзахистом, - сукупністю «організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем» [21, Стаття 1, п.7.]. При цьому необхідно створити сучасні інтегровані засоби захисту як безпосередньо підприємства, так і супутньої інформаційної сфери в процесі їх реалізації та життєдіяльності при постійному моніторингу як за змістом (у різних галузях соціуму), так і за призначенням (наприклад, у вигляді розроблення проектів, технологій, продукції тощо), де одним із значущих з області менеджменту безпеки є забезпечення ідентифікації ризику, аналіз ризику та порівняльної його (ризику) оцінки [9. п.6.4].

У зв'язку з викладеним продовжимо методологічну побудову структурно-лінгвістичної схеми (СЛС) підтримки ухвалення

рішень з позицій ризик-інформаційної безпеки сукупності об'єктів критичної інфраструктури (СОКІ). Як оціночний позитивний приклад нижче доказово викладено конкретний метод реалізації фізичної безпеки СОКІ.

Отже, згідно з [5, 22], системи захисту та безпеки ОКІ завжди функціонують у царині ймовірнісних подій, що піддаються принципу невизначеності щодо ризику [7,п.3.7.9-11,]: впливу невизначеності ефективності, результативності, процесу вимірювання та інших. Отже, будь-який вплив з позиції зниження ризику [23, поз.3.7]) вимагає чіткого уявлення про предмет дослідження та сферу його подальшого застосування. Фактично такий ризик-орієнтований вплив (РОВ) - це процес циклічних вимірювань з уточнення заключної оцінки впливу конкретної реалізації ризику на об'єкт його (ризику) впливу. При цьому, в умовах підвищених зобов'язань до надійності і безпеки засобів вимірювання (ЗВ), в умовах невизначеності вимірювань [16], вимоги забезпечення метрологічної достовірності вимірювань, також є актуальними в галузі будь-яких засобів вимірювання. У підсумку отримуємо, що такий багатопрофільний процес впливів необхідно розглядати з позицій невизначеностей і мінливості як самих результатів, так і їхніх імовірностей, де поняття "погрішності результату вимірювань" зобов'язане корелювати з поняттям істинного значення, чого принципово неможливо досягти.

Це дає змогу використовувати "ризик-орієнтоване мислення" (РОМ) [24, п.0.3.3], що, підтримуючи концепцію управління ризиками, здатне забезпечувати планування і впровадження будь-якої діяльності з управління та контролю ризиків, що впливають на штатну працездатність ОКІ з позиції ризик-інформаційної безпеки. При цьому, залежно від внутрішніх і зовнішніх чинників ризику та відповідно до поставлених цілей слід обирати як відповідну політику менеджменту ризику, так і конкретні принципи, необхідні для ефективного впровадження його менеджменту з позиції ризик-орієнтованих процесів забезпечення безпеки ОКІ.

Саме з цих позицій планування та впровадження заходів і методів, що використовуються для управління та контролю супутніх ризиків, які впливають на досягнення запланованих

цілей безпеки [24], запропоновано до реалізації підсистема підтримки прийняття рішень з позицій ризик-інформаційної безпеки сукупності об’єктів критичної інфраструктури (СОКІ) у межах ISO/IEC TR 13335-4:2000, IDT. Структурно логічну схему (СЛС) зазначеної Підсистеми модернизовано та наведено на рис. 6.7 у рамках загальної Схеми методології побудови розширеної системи захисту та безпеки ОКІ [5, 22], де її (підсистеми) працездатність забезпечується за рахунок "Радіофізичних та/або кіберфізичних систем", використовуючи "Систему управління та зв'язку". З їхньою допомогою, спираючись на РОМ, можна реалізовувати безпосередню оцінку вибору як за методами забезпечення власної безпеки, так і за способами здійснення конфіденційності, цілісності, повноти та доступності одержуваної інформації. забезпечення власної безпеки, так і за способами здійснення конфіденційності, цілісності, повноти та доступності одержуваної інформації.

Методологію такої побудови виконано відповідно до законодавства країни щодо менеджменту ризику, що використовує зворотні зв'язки під час реалізації коригувальних впливів, адекватних вище озвученим аспектам. Саме з цих позицій аналізу безпеки СОКІ в табл. 4 наведено впорядковані дані щодо вибору апріорних засобів захисту в межах ISO/IEC TR 13335-4:2000, IDT, включно з безпекою супутніх інформаційних технологій.

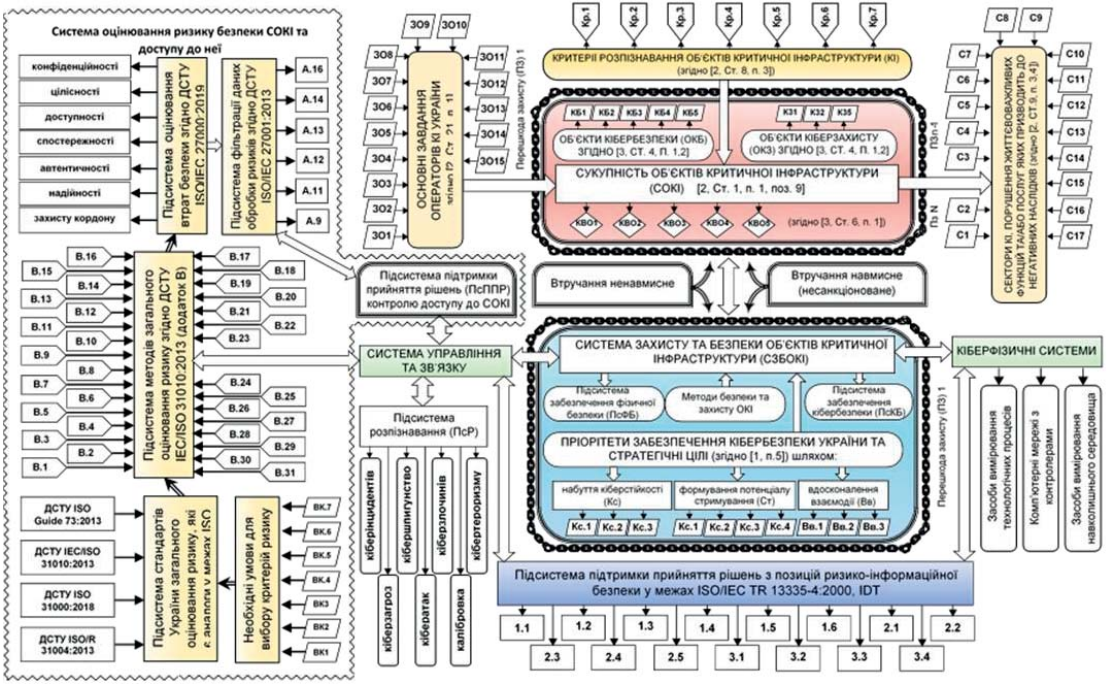

Рисунок 6.7. Схема методології побудови розширеної (з підсистемою підтримки прийняття рішень з позицій ризико- інформаційної безпеки) системи захисту та безпеки об'єктів критичної інфраструктури

Таблиця 4.

Зміст вибору засобів захисту, з позицій риск-інформаційної безпеки у межах ISO/IEC TR 13335-4:2000, IDT
1. Організаційні та фізичні засоби захисту загального застосування:
Керування інформаційною безпекою та політика безпеки
Перевіряння узгодженості безпеки
Реагування на порушення
Персонал та питання експлуатації
Планування неперервності бізнесу
Фізична безпека
2. Специфічні засоби захисту інформаційної системи:
Ідентифікація та автентифікація (I&A)
Контролювання логічного доступу та аудит
Захист від зловмисного коду
Керування мережею
Криптографія
3. Засоби захисту відповідно до утрат конфіденційності, цілісності, доступності, спостережності, автентичності, надійності та загроз у межах забезпечення безпеки ОКІ
3.1 Засоби конфіденційності з позиції:
3.1.1. Підслуховування 3.1.2. Електромагнітне випромінення 3.1.3. Зловмисний код 3.1.4. Приховування ідентичності користувача 3.1.5. Неправильне направлення/перенаправлення повідомлень 3.1.6. Збої програмного забезпечення 3.1.7. Крадіжки 3.1.8. Несанкціонований доступ до комп'ютерів, даних, служб та програм 3.1.9. Несанкціонований доступ до носіїв даних

Зміст вибору засобів захисту, з позицій риск-інформаційної безпеки у межах ISO/IEC TR 13335-4:2000, IDT
3.2 Засоби контролю цілісності з позиції:
3.2.1. Псування носіїв даних
3.2.2. Помилки обслуговування
3.2.3. Зловмисний код
3.2.4. Приховування ідентичності користувача
3.2.5. Неправильне направлення/перенаправлення повідомлень
3.2.6. Неспростовність
3.2.7. Збої програмного забезпечення
3.2.8. Збої постачання (живлення, кондиціонування повітря)
3.2.9. Технічні пошкодження
3.2.10. Помилки передавання
3.2.11. Несанкціонований доступ до комп'ютерів, даних, служб та програм
3.2.12. Використання несанкціонованих програм та даних
3.2.13. Несанкціонований доступ до носіїв даних
3.2.14. Помилки користувача

У зазначеній таблиці відображено: організаційні та фізичні засоби захисту загального застосування; специфічні засоби захисту інформаційної системи; засоби захисту відповідно до проблем (від втрат конфіденційності; цілісності; доступності; спостережності; автентичності та надійності) і загроз у межах забезпечення безпеки ОКІ. Причому, в контексті загального організаційного управління зазначимо, що концепціям безпеки (інформаційної, виробничої, технологічної тощо аж до захисту приватного життя) притаманна тенденція досконалості, а отже безперервний процес захисту та безпеки в усіх сферах життєдіяльності соціуму завжди супроводжуватиме модернізаційні тенденції на міжнародному і вітчизняному законодавчому рівні стосовно удосконалення стандартів щодо їхньої безпеки.

Отже, підвищення рівня захисту СОКІ, оцінювання втрат безпеки (згідно з гіпотетичними кіберінцидентами, що мають імовірнісний характер), - це динамічний процес залучення ресурсів (методів, способів та алгоритмів) мультисервісної мережі зв'язку (криптографічних, канальних та інших) з її фільтруючими (у вигляді, наприклад, авто- та взаємокореляційних блоків) пристроями, реалізованими під конкретні вимоги (завдання) користувачів. Звідси, - вибір рівнів спрацьовування кінцевих порогових блоків носитиме багатопрофільний характер і залежатиме від задекларованих імовірностей правильного виявлення або пропуску кібератак чи кіберзагроз.

Відтак, успішно реалізовані ризик-орієнтовані плани та процеси забезпечення безпеки СОКІ (або її моделі) за умови адекватної оцінки апріорних впливів (наприклад, у вигляді певної моделі порушника, в якій відображаються його практичні та теоретичні можливості, апріорні знання, час і місце дії та інші характеристики) є важливою складовою успішного проведення як політики ризик-менеджменту, так і супутнього зниження ризик невизначеності в процесі аналізу ризиків та визначення вимог до складу та характеристик необхідної інтегральної системи захисту.

На жаль, в умовах багаторівневої системи перешкод, жодна пізнавальна модель не може одночасно виконувати необхідно безліч завдань захисного напрямку. Саме цьому доцільно оцінювати ефективність безпеки у конкретній (обраній) області її реалізації та задіяних технологій процесу отримання, опрацювання та зберігання службової інформації щодо як потенційних (можливих) атак, так і щодо наступних відомостей (у вигляді практичного матеріалу) з їхнього відбиття. Так, сучасній захист від зовнішніх впливів на інформаційну сферу підприємства как на об'єкт критичній інфраструктури (ОКІ) з його апаратно-програмним забезпеченням та інформаційно-телекомунікаційної системою доцільно здійснювати з радіолокаційними системами виявлення, розрішення, вимірювання та розпізнавання цілей [20]. Наприклад, система виявлення комп'ютерних атак (СОА) "Форпост" (версії 2.0 ЗАТ "РНТ") здатна забезпечувати [25, с. 349]:

• захист від можливих порушніків та источников загроз, тобто від потенційного нанесення атак на ОКІ;

• виявлення комп'ютерних атак, спрямованих на сервери телематичних служб (WEB, FTP, електронна пошта, СУБД тощо) і робочі станції;

• запобігання розвитку мережевих комп'ютерних атак шляхом блокування джерел атак за допомогою відправки мережевому обладнанню (міжмережевому екрану, комутатору, маршрутизатору), за протоколами RS-232, telnet, відповідної послідовності команд на основі шаблонів;

• оповіщення адміністратора безпеки про виявлені атаки та контроль цілісності власних ресурсів СОА і ресурсів АІС;

• контроль цілісності власних ресурсів СОА і ресурсів АІС, а також, за рахунок цього механізму, можливість відстеження дій порушників по відношенню до контрольованих ресурсів в скомпрометованій системі;

• ведення журналу системних повідомлень, що містить службову інформацію, яка формується компонентами СОА;

• інтеграцію із зовнішніми системами шляхом передачі повідомлень про зафіксовані комп'ютерні атаки з журналу СОА за протоколом syslog;

• генерацію звітів на основі вмісту журналів СОА;

• відстеження появи нових повідомлень системних журналів.

При цьому підсистема власної безпеки дозволяє шифрувати інформацію, що передається між компонентами, з використанням вітчизняних СКЗІ, здійснювати контроль цілісності власних ресурсів і ресурсів захищаємої АІС.

Таким чином, інформаційна безпека (ІБ) мережі зв'язку загального користування (ССОП) досягається комплексним використанням організаційних, технічних, апаратно-програмних і криптографічних засобів захисту інформаційної сфери ССОП, а також здійсненням безперервного контролю за ефективністю реалізованих заходів щодо забезпечення ІБ ССОП, яка передбачає створення перешкод для можливого несанкціонованого втручання в процес її функціонування. При цьому, як правило, орієнтуються на моделі інформаційної безпеки у вигляді або тріади конфіденційності, доступності, цілісності (КДЦ) 1975 року появи, або одну з найвідоміших її

альтернатив у вигляді Гексади Паркера, - 1998 рік появи (див. рис. 6.8).

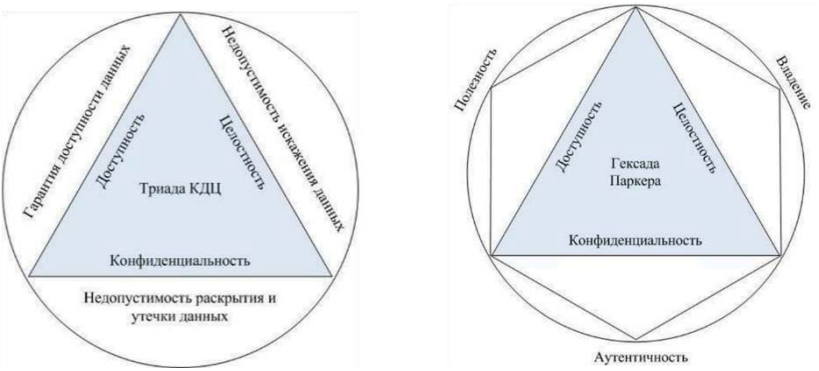

Рис. 6.8. Моделі інформаційної безпеки, згідно [2, Защита информации в телекоммуникационных системах. Тема 3»]. (https://www.bsut.by).

Очевидно, що такі зовнішні впливи (з їхньою нестаціонарністю, нестабільністю, складністю в прогнозуванні та високою мінливістю сфери життєдіяльності соціуму та зовнішнього середовища проживання) можуть загалом серйозно нашкодити процесу прийняття рішення і для їхнього нівелювання, наприклад, можуть бути використані відповідні алгоритми адаптації ІТС до зовнішніх впливів.

Наприклад, алгоритм адаптації, запропонований [26] та наведений на рис. 6.9, включає етапи визначення мети створення ІТС, аналіз умов функціонування системи, класифікацію зовнішніх впливів, вібір оптимального варіанту адаптації системи, аудит та затвердження обраного рішення. Його реалізація, насамперед, необхідна для ухвалення рішення як класифікувати загрози ІТС, виходячи із властивостей інформації, що циркулює, а саме її цілісності, доступності, конфіденційності. При цьому завдання багатокритеріальної оптимізації слід трансформувати в однокритеріальну шляхом введення скалярної функції корисності, нормованих показників якості та призначення вагових коефіцієнтів їх

важливості. Для цього необхідно використовувати сучасні системи проектування та експертні системи підтримки прийняття рішень, включно зі штатними операторами зв'язку з системи управління NCNS [27], яка також потребує забезпечення власної безпеки.

Рисунок 6.9. Алгоритм адаптації інформаційно-телекомунікаційних систем (ІТС) до зовнішніх впливів

Зауважимо, що абревіатура NCNS виникла у зв'язку з появою Рекомендації ITU-T X.ncns-1 «Національний центр безпеки мережі зв'язку загального користування», що базується на протоколі IP для країн, що розвиваються, яка розроблена для створення безпечної, стабільної та стійкої національної мережевої інфраструктури на базі протоколу IP і описує архітектуру Національного центру (далі - NCNS).

Отже, з погляду забезпечення безпеки функціонування системи управління NCNS і з урахуванням можливого впливу порушника безпеки на її інфраструктуру (включно з локацією засобів системи управління), заведено розміщення обладнання умовно розділяти на 4 зони: безпечну зону; безпечну, але вразливу зону; небезпечну, але контрольовану оператором зв'язку зону; небезпечну зону (див. рис. 6.10, який адаптований з [27, с.15]).

Безпечна (зелена) зона. Елементи, в якій вони ніколи безпосередньо не пов'язані з обладнанням, не призначеним для управління системою супроводу операційної підтримки (ССОП). Загальні особливості елементів мережі в цій зоні - те, що вони розташовані в приміщеннях, які забезпечують функціонування системи управління, і перебувають під повним контролем оператора цієї системи (забезпечується їхня фізична безпека), і

що вони пов'язані тільки з елементами в «безпечній» зоні та з елементами в «безпечній, але вразливій» зоні.

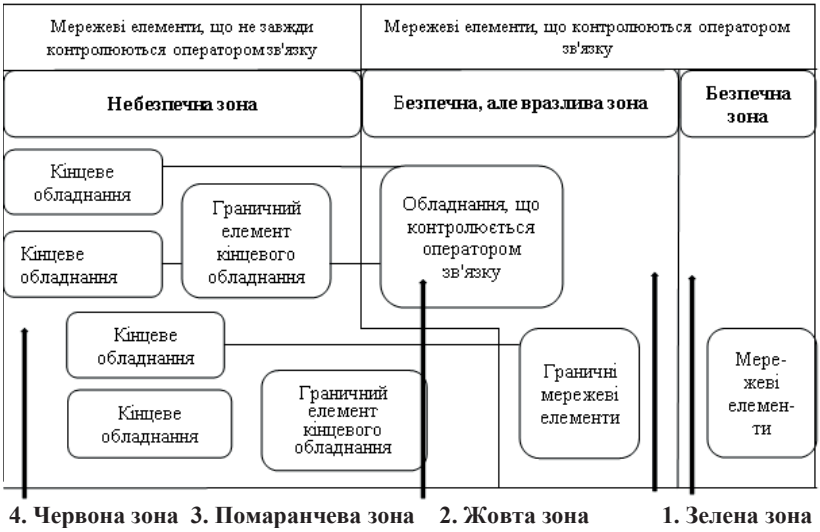

Рисунок 6.10. Зони адаптації ІТС до зовнішніх впливів

Безпечна, але вразлива (жовта) зона. Обладнання розташоване в межах зони оператора системи управління, але може перебувати під його контролем або під контролем оператора мережі передачі даних. Воно пов'язане з елементами і в зоні, що «безпечна», і з елементами в «небезпечній» зоні, яка визначає те, чому вони «вразливі». Їхня головна функція безпеки полягає в тому, що вони мають захистити (убезпечити) мережеві елементи в «безпечній» зоні від атак на безпеку, породжених у «не безпечній» зоні.

Не безпечна, але контрольована оператором зв'язку (помаранчева) зона. Обладнання розташоване поза зоною оператора системи управління і може перебувати під його контролем або під контролем оператора мережі передачі даних. Воно пов'язане тільки з елементами в зоні, яка «безпечна, але вразлива», і з елементами в «не безпечній» зоні.

Не безпечна (червона) зона. З погляду оператора системи управління зона, яка включає всі елементи оператора мережі передавання даних або можливо рівнозначні мережі чи зони інших операторів зв'язку за межами своєї власної «безпечної» зони.

Залежно від розміщення обладнання в тій чи іншій зоні ймовірність реалізації загроз відрізняється. Якщо обладнання знаходиться поза контрольованою зоною, це значно збільшує можливості зловмисників щодо реалізації загроз. У разі неможливості розміщення обладнання в контрольованій зоні необхідно вживати заходів щодо забезпечення ІБ у рамках системи забезпечення інформаційної безпеки.

Технічні засоби зв'язку є вразливими за багатьма параметрами, проте тільки деякі з них можуть використовуватися порушником, через обмеженість його можливостей або через перевищення його зусиль і ризику виявлення над досягнутими результатами.

Причому описуються два різних архітектурних рішення для проектування і формування NCNS, внутрішня структура функціонування якого представлена на рис. 6.11, який адаптований згідно [27, с.18].

В основі першого рішення лежить архітектура і методика організації та супроводу системи підтримки операційної діяльності NCNS у взаємодії з центрами управління мереж зв'язку, включно з технологічними та виділеними мережами зв'язку, що мають приєднання до ССОП (системи супроводу операційної підтримки).

Основу другого рішення становить концепція збору даних стану мереж зв'язку, одержуваних у режимі реального часу від інженерних систем моніторингу та управління мережевими елементами, з подальшим *ситуаційним аналізом та інтерпретацією зібраних даних* для регламентованого ухвалення рішень уповноваженими особами в умовах кризи та катастрофи.

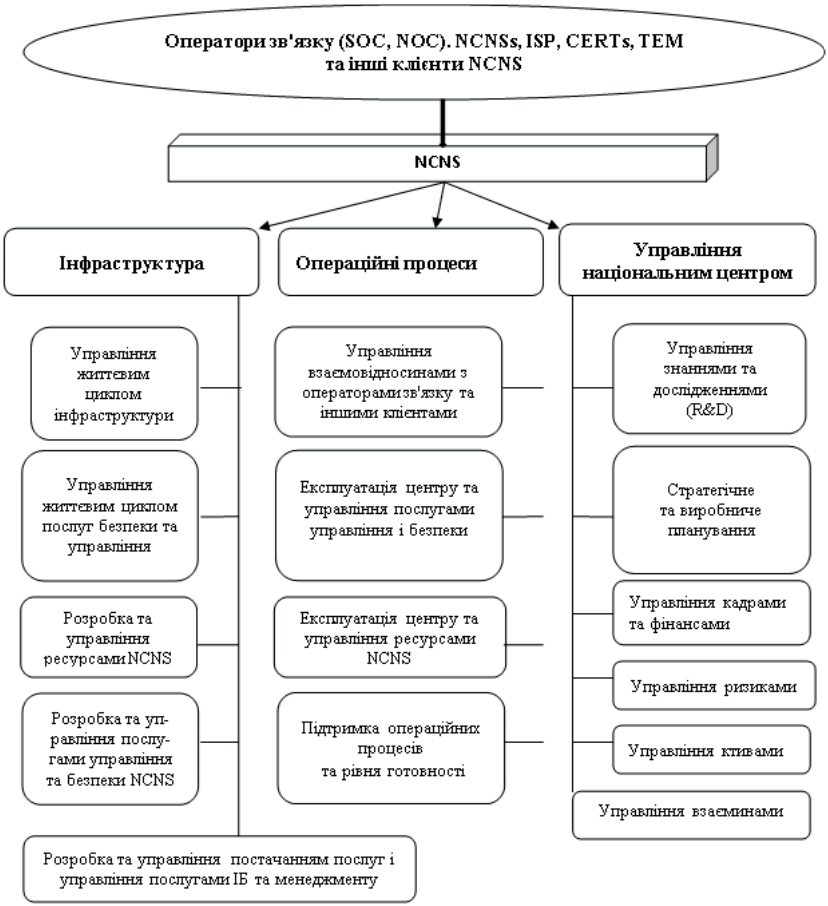

Рисунок 6.11. Внутрішня структура функціонування NCNS – Національного центру безпеки мережі зв'язку загального користування

Очевидно, что оба решения для организационно-технической схемы NCNS только способствуют улучшению взаимодействия аппаратно-программных комплексов на платформе интеграции услуг, реализуя таким образом эффект синергетики з метою вихіду підприємства на більш якісний та ефективний рівень господарювання, що дасть змогу покращити і

економічну, і екологічну, і соціальну компоненту підприємництва. При цьому операторами зв'язку процес отримання, оброблення та зберігання інформації про апріорні і апостеріорні інциденти та здійснені атаки, методи використовуваного захисту та кінцеві (підсумкові від них) результати можуть бути забезпечені: відповідно до структурної схеми рис. 6.12 (незалежно від зон підвідомчого контролю зі сфери життєдіяльності певного підприємства [27, с.22]) або згідно зі структурно-функціональною схемою рис. 6.7, опублікованій в [5, 22].

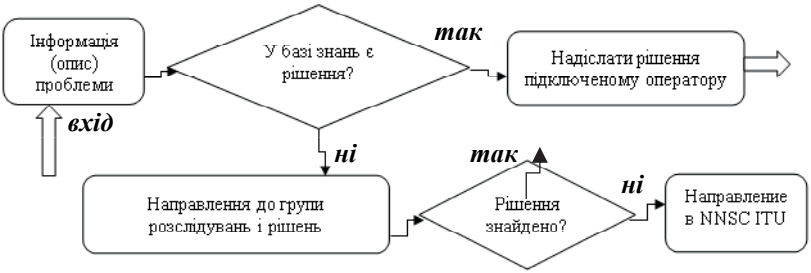

Рисунок 6.12. Структурна схема опрацювання повторних інцидентів і атак

Контрольні запитання до Розділу 6

1. Що таке фізичне моделювання та яка його мета?
2. Перелічіть загальні вимоги до моделей.
3. Що являє собою математичне моделювання?
4. Поясніть суть аналітичного та імітаційного моделювання.
5. Які дії передбачає технологія комп'ютерного моделювання?
6. Сформулюйте, будь ласка, принципи побудови математичних моделей.
7. Поясніть види або стадії побудови моделей: уявна модель, концептуальна модель та формальна модель.
8. Що таке інформаційна модель та її складові компоненти?

9. За якім принципом побудована організаційна система моделі формування і реалізації концепції безпеки підприємницької діяльності та її суть
10. Що таке менеджмент ризику (risk management) та оцінка ризику?
11. Що таке ідентифікація та автентифікація?
12. Сформулюйте та поясніть, з позицій риск-інформаційної безпеки, організаційні, фізичні та специфічні засоби захисту інформаційної системи.
13. Чому доцільно здійснювати резервне копіювання?
14. Які, у межах забезпечення безпеки ОКІ, є засоби захисту відповідно до їх інформаційних утрат конфіденційності, цілісності, доступності, спостережності, автентичності та надійності?
15. Як слід розуміти управління технічними уразливістю?
16. Поясніть, будь ласка, що таке: псування носіїв даних, зловмисний код, збої програмного забезпечення та постачання (живлення, кондиціонування повітря).
17.
18. До чого може привести використання несанкціонованих програм та даних?
19. Що таке триада КДЦ та Гексада Паркера?
20. Поясніть суть чотирьох зон забезпечення безпеки функціонування системи управління NCNS з урахуванням можливого впливу порушника безпеки на її інфраструктуру.

Список використаних джерел під час підготовки тексту розділу 6

1. Інформаційна безпека підприємства: Навчальний посібник/Н.В. Гришин. - 2-е вид., Дод. - М.: Форум: НІЦ ІНФРА-М, 2015. – 240 с.

2. Захист інформації у телекомунікаційних системах. Тема 3 // https://www.bsut.by

3. * Васильєв, М. Н. Служивий. Математичне моделювання систем зв'язку. Навчальний посібник / – Ул.: УлДТУ, 2010. – 170 с.

4. Менеджмент безпеки: навч. посіб. / М. О. Левченко. — К. : ДП «Вид. дім «Персонал», 2013. — 406 с.

5. * Тарасенко Ю.С., Клим В.Ю. Методологія побудови пізнавальної моделі безпеки критичної інфраструктури. стор 38-50. Monographic series «European Science». / Prospective global scientific trends' 2022": sge11-01, Chapter 15. ScientificWorld-NetAkhatAV Karlsruhe Germany 2022 (DOI, ISBN, IndexCopernicus, Карлсруэ, Германия). Тарасенко Ю.С. The methodology of building the cognitive model of critical infrastructure's security/ Ю.С.Тарасенко, В.Ю. Клим // Materials of International scientific symposium: "Prospektive globale wissenschaftliche Trends '2022 / Prospective global scientific trends' 2022", Karlsruhe, Germany, May, 2022. – 10 с.

6. ДСТУ ISO Guide 73:2013. Керування ризиком. Словник термінів (ISO Guide 73:2009, IDT).

7. ДСТУ ISO 9000:2015 (ISO 9000:2015,IDT) Системи управління якістю. Основні положення та словник термінів. Київ ДП «УкрНДНЦ», 2016. 51 с.

8.**** 1. ДСТУ IEC/ISO 31010:2013 Керування ризиком. Методи загального оцінювання ризику (IEC/ISO 31010:2009, IDT). [Чинний від 2014–07–01]. Вид. офіц. Київ: Мінекономрозвитку України, 2015. 80 с.

9.. ДСТУ ISO 31000:2018 Менеджмент ризиків. Принципи та настанови (ISO 31000:2018 Risk Management – Principles and guidelines on implementation, IDT). ДСТУ ISO 31000:2018 Менеджмент ризиків. Принципи та настанови (ISO 31000:2018 Risk Management – Principles and guidelines on implementation, IDT). [Чинний від 2019–01–01]. [Електронний ресурс]. – Режим доступа: https://www.iso.org/obp/ui/#iso:std:iso:31000:ed– 2:v1:en

10.. ДСТУ ISO/TR 31004:2013 Управління ризиками – Керівництво з впровадження ISO 31000 (Risk management – Guidance for the implementation of ISO 31000, IDT).

11. ДСТУ ISO Guide 73:2013. Керування ризиком. Словник термінів (ISO Guide 73:2009, IDT). * ДСТУ ISO Guide

73:2013. Керування ризиком. Словник термінів (ISO Guide 73:2009, IDT). [Чинний від 2014–07–01]. Київ: Мінекономрозвитку України, 2014. 17 с.

12.* ДСТУ IEC/ISO 31010:2013 Керування ризиком. Методи загального оцінювання ризику (IEC/ISO 31010:2009, IDT). Київ: Мінекономрозвитку України, 2015. 80 с.

13** ДСТУ ISO/IEC 27000:2019 (ISO/IEC 27000:2018, IDT) Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Огляд і словник термінів. Київ ДП «УкрНДНЦ».

14.*** ISO/IEC 27001:2013 Інформаційні технології - Методи забезпечення безпеки - Системи менеджменту інформаційної безпеки - Вимоги /Information technology — Security techniques — Information security management systems — Requirements/ Вторая редакція. 2013-10-01.

15.**** Закон України Про критичну інфраструктуру № 1882 - IX від 16.11.2021р. // Голос України. . – № 236 (14.12.2021).

16. * ISO/IEC Guide 98– 1:2009, Uncertainty of measurement – Part 1: Introduction to the expression of uncertainty in measurement, IDT. Невизначеність виміру. Частина 1. Введення в посібники з виразу невизначеності виміру. М. Стандартінформ. 2017.

17.** Тарасенко Ю.С. Інформаційні системи з позицій забезпечення надійності та невизначеності вимірювань / Ю.С.Тарасенко, В.Г. Соляніков // Збірник матеріалів міжнародної науково-практичної інтернет-конференції «Інноваційні технології, моделі управління кібербезпекою – «ІТМК– 2021», Дніпро, 14 – 16 квітня 2021 р. – С.29 – 30.

18.*** Ворона В. А. Системи контролю та управління доступом / В. А. Ворона, В. А. Тихонов. - М.: Гаряча лінія - Телеком, 2010. – 272 с

19.* Вострецова Є. В. Основи інформаційної безпеки: навчальний посібник для студентів вузів / Є. В. Вострецова – Є.: вид-во Ур. ун-ту, 2019. – 204 с.

20.Тарасенко Ю.С. Фізичні основи радіолокації [Текст]: навч. посіб. Т 19 / Ю.С. Тарасенко. – Д.: «Пороги», 2011.– 487с

21.* Закон України Про основні засади забезпечення кібербезпеки України (Відомості Верховної Ради (ВВР), 2017, №

45, ст.403) {Із змінами від 21.06.2018, від 17.06.2020, від 17.09.2020}

22.Yu.S. Tarasenko, V.Iu. Klym. Safety of critical infrastructure objects from the positions of risk effectiveness reduction. Vol. 4 No. 141 (2022): System technologies. Pp. 158-168. Published: 2023-03-04. Дніпро, 2022. – 205с.

23*** ДСТУ ISO/IEC 27005:2019 Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки (ISO/IEC 27005:2018, IDT). Мова документа Англійська. International standard ISO/IEC 27005:2019 Information technology – Security techniques – Information secure risk management. https://www.google.com/url

24.* ISO 9001-2015. Міжнародний стандарт. Системи управління якістю – Вимоги. Quality management systems - Requirements. П'ята редакція 2015-09-15.

25. Левченко М.О. Менеджмент безпеки: Навчальний посібник. К.: ДП «Вид. дім «Персонал», 2013. 406 с.

26. В.Я. Воропаєва, І.Л. Щербов. Адаптування інформаційно-телекомунікаційних систем до зовнішніх впливів. / Наукові праці Донецького національного технічного університету. Серія: Обчислювальна техніка та автоматизація. №23 (201), 2012. С. 83 – 89

27.* Рекомендації МСЕ-Т X.ncns-1, Національний центр безпеки мережі зв'язку загального користування, що базується на протоколі IP, для країн, що розвиваються.

7. ОСНОВИ СИТУАЦІЙНОГО МЕНЕДЖМЕНТУ, СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ ТА КАДРОВО-ІНТЕЛЕКТУАЛЬНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

7.1. Ситуаційний підхід до розроблення управлінського рішення

У сфері будь-якої практичної діяльності з високим рівнем невизначеності динамічного розвитку подій як у зовнішньому середовищі, так і у виробничій царині необхідна адекватна реакція на апріорні негативні атаки у сфері життєдіяльності сучасного соціуму. При цьому, в основі реалізації такої адекватної реакції доцільно використовувати, перш за все, спеціальний вид управління - ситуаційний менеджмент, який деякі дослідники ще називають адаптивним, а інші альтернативним менеджментом [1].

Зазвичай завдання, що виникають у практиці управління, за своєю суттю, є або функціональними, або ситуаційними. До функціональних (стабільних) завдань відносять завдання процесу розподілу (поділу) праці у виробництві та в його управлінні.

Ситуаційні завдання - є наслідком порушень взаємодії спеціалізованих підсистем і елементів організації під впливом дестабілізуючих чинників виробництва.

У загальному випадку із ситуацією не завжди пов'язаний тільки негативний вплив і наслідки її реалізації на життєдіяльність підприємства, тому що вона (ситуація) характеризує тільки стан справ в організації, що склався, на цей момент, і залежно від рівня своєї достовірності може бути як задовільним, так і незадовільним із погляду суб'єкта управління - особи, що ухвалює (приймає) рішення (ОУПР). В останньому випадку така ситуація стає проблемою, оскільки вона характеризує реальну розбіжність бажаного (апріорного) і дійсного (апостеріорного) рівнів задоволення потреб керівника. Причому в більшості випадків конкретна проблемна ситуація може бути сформульована у вигляді сукупності різних проблем, кожна з яких може мати свою методологію рішення. Зокрема, дії ОУПР щодо ухвалення рішення і безпосередньо процес функціонального його проходження, представлений на рис. 7.1, який адаптований згідно [1, с. 68] і реалізований, як один із трьох можливих варіантів вирішення проблемних ситуацій, на рис. 7.2 згідно [1, с.69].

Рисунок 7.1. Структурна схема процесу функціонального управління

Отже, у загальному випадку розвиток проблемної ситуації може відбуватися за трьома варіантами:

перший - це коли власними силами розвиток негативної ситуації призупинено, відновлено виробничо-економічний механізм системи та її подальше управління триває за функціональною схемою управління (див. рис. 7.1);

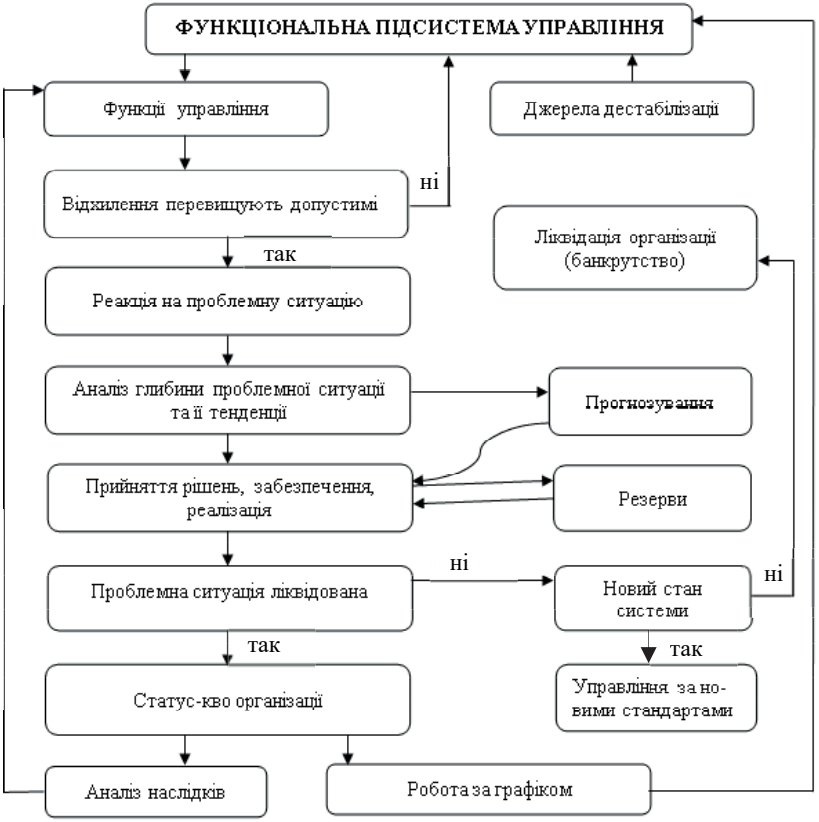

Рисунок 7.2 Укрупнена технологічна схема управління за ситуацією

другий - це коли розвиток ситуації набув кризового характеру, тому що не вдалося реалізувати перший, і первісна система функціонування підприємства не зруйнована, але вже має небезпечний, надзвичайний (або на межі цього), характер. Тому необхідне рішення про доцільність переходу виробництва

на більш сучасний рівень його реалізації з метою досягнення високої конкурентоспроможності;

третій, - це, коли всі зусилля антикризового характеру не спрацювали і надзвичайні заходи з порятунку підприємства не приносять бажаних результатів, приводячи підприємство на межу банкрутства.

Отже, у разі перевищення допустимих відхилень функціонування системи від апріорі заданого рівня порогового пристрою блоку «Функції управління» (рис. 7.1), штатне управління може відбуватися за ситуаційною схемою (рис. 7.2), як одного з трьох можливих шляхів (варіантів) розв'язання проблемних ситуацій.

У контексті викладеного слід звернути увагу на те, що виробничій діяльності підприємства в період назрівання, прояву, ліквідації та після кризового управління зазвичай притаманне три види ситуацій [1]: звичайній виробничій ситуації та двом проблемним - кризовій і надзвичайній. Перша (***звичайна виробнича ситуація***) - це коли показники діяльності підприємства або його підрозділу, включно з кліматом у колективі, перебувають на штатному рівні, встановленим стандартами цього підприємства на будь-який момент часу роботи в зоні допустимого ризику. Друга (***кризова ситуація***) - як одна з форм проблемної, характеризується можливістю втрат через відхилення, що перевищують межі обмежень, що властиво зоні критичного ризику. Третя (***надзвичайна ситуація***) - це та сама проблемна ситуація, але вже в зоні катастрофічного ризику, успішна реалізація якого може призвести до банкрутства підприємства.

Наведена класифікація, на думку авторів Василенка В.О. і Шостка В.І. [1], є більш вдалою, тому що сумісна з ризиками, які за допомогою імовірнісних величин і теорії надійності можна кількісно виразити, наприклад, у відсотках і перевести в грошовий еквівалент. Причому, якщо у звичайних ситуаціях управління здійснюється звичайними прийомами і при цьому використовується функціональна схема управління, то в проблемних ситуаціях її недостатньо. Необхідні спеціальні прийоми і підходи, які повинні використовуватися при управлінні за ситуацією, як на стратегічному, так і на тактичному

рівнях відповідно до концептуальної моделі ситуаційного менеджменту (рис. 7.3 згідно [1, с. 92]).

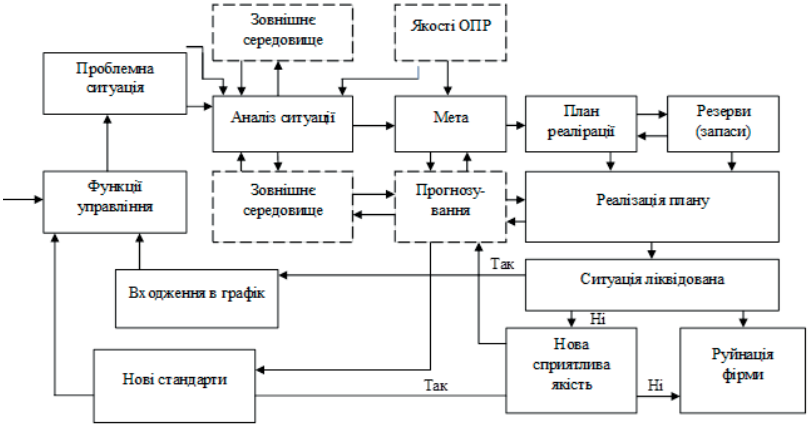

Рисунок 7.3. Підсистема ситуаційного менеджменту на об'єкті підприємства

Особливе місце в ситуаційному менеджменті, природно, посідають питання вивчення проблемних ситуацій та їх вирішення. Загальний порядок дій цілком узгоджується із загальною теорією ухвалення рішень, але має більш стрімкий характер, стислий у часі, а ціна ухвалюваних управлінських рішень різко зростає. Крім того, в ситуаційному менеджменті сильно розвинений блок прогнозування, без якого неможливе застосування цього виду управління.

Періодичність і ступінь деталізації розв'язуваних завдань за ситуаційною схемою різна. Усе залежить від виду виробництва, ступеня його ризику, ієрархії, частоти виникнення проблемних ситуацій, особливо наголошуючи на тому, що в сучасних умовах практично неможливо домогтися гарних результатів без сприятливого творчого соціально-психологічного клімату в колективі.

Очевидно, що саме соціально-психологічні аспекти формування добротного (сприятливого) психологічного клімату

в колективі стають особливо важливими в кризових ситуаціях. Причому компетенція керівника, а також складові компетенції штатних працівників є цінним багажем будь-якої організації, а вміння грамотно ним (багажем) розпоряджатися, розвивати і збагачувати його - запорука успішної діяльності підприємства. При цьому, концепція людських відносин, в яких

підкреслюється величезна роль у процесі виробництва соціально-психологічних чинників, стверджує, що на поведінку працівників впливають не тільки економічні стимули, а й соціально-психологічні потреби людей, які беруть участь у всіх складових цього процесу. Відносини ж між учасниками процесу розроблення управлінських рішень базуються на людській поведінці, її психологічній сутності, індивідуальності, її базових і програмувальних властивостях. Як приклад, на рис. 7.4 (який адаптований згідно [1, с. 241]) наведено деякі (далеко не всі) чинники соціально-психологічної властивості, які зумовлюють можливу (адекватну або неадекватну) реакцію співробітника підприємства (аж до ОПР) на ті чи інші ситуації.

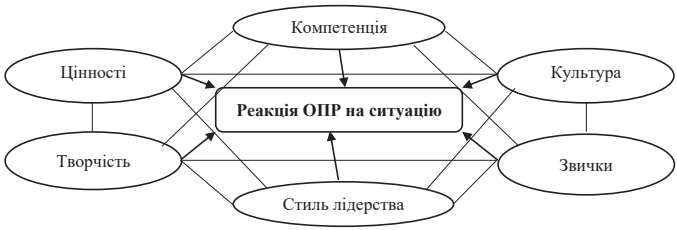

Рисунок 7.4. Частина чинників, що формують реакцію особи, яка приймає рішення (ОПР) на ситуацію

Очевидно, що успішне здійснення ситуаційного антикризового управління підприємством (а також реалізація його безпосередньої конкурентоспроможності) можливе тільки в команді соціально згуртованих і професійно підготовлених працівників, виокремлюючи, насамперед, їхній талант, енергію, виняткову працьовитість, багаторічний досвід і готовність до взаєморозуміння та своєчасного колективного співробітництва.

Таким чином, ситуаційний менеджмент з його динамічними реаліями і супутніми труднощами існуватиме завжди, причому в безпосередньому контакті зі сферою невизначеності сучасного соціуму і його соціальної інженерії.

7.2. Тіньові сторони соціальної інженерії, хакінгу та зниження стороннього деструктивного кібернетичного впливу з їхньою допомогою

Історично склалося так, що в поняття соціальної інженерії (СІ) сучасної інфраструктури здебільшого закладають сенс хакерства з використанням людського чинника (соціального хакерства), що саме по собі властиво феномену соціального невігластва. Останнє пов'язане з інерційністю нашої поведінки: в адекватній оцінці конкретної ситуації: нам часто заважає присутність (або думка) інших людей (особливо так званих авторитетів - «фундаторів» програм соціального наслідування), реакція яких є зумовлювальною до того, як ми ухвалюємо конкретне рішення, підспутно зберігаючи при цьому (принаймні не погіршуючи) свою особисту самооцінку.

Однак слід звернути увагу на те, що в основі поняття СІ покладень термин інжене́рія (від лат. ingenium — здібність, винахідливість), який відображає людську інтелектуальну діяльность по застосуванню досягнень науки до вирішення конкретних проблем людства, де вона (інженерна діяльність) являє собою зрілу форму трудової діяльності безпосередньо спрямованої на вирішення технічних завдань і створення техніки. У функції же СІ входить забезпечення нормального функціонування цієї техніці в суспільстві з достойной організації соціальних умов впровадження та реалізації необхідних псіхологічних основ соціального програмування (СП), які пов’язані функціонувати з максимальними зручностями і користю для людини [2, 3].

Аналіз СП, реалізований, наприклад у рамках програм «поступливості», «взаємодопомоги», «соціального наслідування», «поклоніння авторитетові» та їм аналогічним [4], дає змогу констатувати, що більшість людей практично й не

підозрюють, що їм притаманна автоматична модель (інерційність) поведінки, яка начебто знімає з них особисту соціальну відповідальність у процесі їхньої життєдіяльності при розв'язанні різноманітних завдань соціального характеру. Понад те, зростаючій тенденції інерційності поведінки соціуму сприяє і їхнє надмірне перебування у віртуальній реальності, де електронно-опосередковані комунікації дають змогу недобросовісним авторам інформації (як правило, залишаючись при цьому «невидимими») впливати не лише на буття, а й на механізми управління соціальними процесами через соціальну інженерію. Саме тому терміну СІ, що характерно для розвитку відносно молодих наук, притаманні багатозначні поняття: від методології управління діями людини без використання технічних засобів до соціології, - сукупності підходів прикладних соціальних наук. Причому парадигми соціальної інженерії, з одного боку, виражають історичну послідовність у розвитку теоретичних уявлень про соціальну інженерію, а з другого, - співіснують і взаємодіють в рамках сучасної епохи як спеціалізовані способи соціоінженерних розробок залежно від характеру досліджуваних конкретних соціальних систем.

У контексті вивчення інформаційної безпеки суспільства соціальна інженерія спрямована на забезпечення надійності технологій інформаційного впливу як виду діяльності, що здійснюється під час соціальних комунікацій. А оскільки знання та інформація, а також можливість маніпуляції ними, стають значними в управлінні сучасним суспільством, то й не обійшлося без соціального хакерства (СХ), що використовує, за рідкісним винятком, людські вади та слабкості.

Під час реалізації хакерських атак з метою досягнення необхідного інформаційного впливу використовують ті самі психологічні аспекти СІ, що орієнтовані на цілеспрямовану зміну організаційних структур, які визначають людську поведінку та забезпечують контроль за такою трансформованою поведінкою. Механізми впливу зловмисників з арсеналу СІ різноманітні, а оптимальність їхнього вибору залежить від царини застосування, специфіки та рівня соціально-психологічної жертви, тобто від індивідуальності людини (зокрема, від її психотипу та життєвого досвіду), а також ранґу в упорядкованості домінування та

підпорядкування, тобто місцеположення на драбині чинів або на ієрархічних сходах буття. Саме тому, щоб зрозуміти методи та передбачити кроки зловмисника, доцільно принаймні знати та вміти реалізовувати захист від конкретних технологій інформаційного впливу (ТІВ).

З позиції СП та ТІВ соціальний хакер, оволодівши навичками трансакційного (трансактного) аналізу [5], в основу якого покладено твердження, що будь-яка людина у будь-якій ситуації спілкування проявляється в одній із трьох позицій: батько, дорослий або дитина, - здатен спрогнозувати розвиток багатьох ситуацій соціального характеру. Фактично за допомогою соціальних хакерів можливе здійснення деструктивних впливів на потенційно значущі інформаційні ресурси організацій, як на державному, з погляду, так званого, «промислового шпигунства», так і на рівні терористичних і кримінальних структур. Насамперед, це пов'язано з особливою вразливістю інфраструктури та високою професійною відповідальністю працівників критично важливих об'єктів (КВО), від роботи яких залежить не тільки штатне функціонування цих об'єктів, а й ступінь захисту від будь-яких загроз та їхніх передумов, здатних спричинити техногенну, екологічну або фінансову катастрофу [6]. Тому при ранжируванні можливих загроз інформаційній безпеці більшості ключових систем інформаційної інфраструктури (КСІІ) найслабшою її ланкою є людський фактор. Саме від якості (морально-професійного рівня) задіяного кадрового складу, що забезпечує специфічні заходи, зокрема й щодо прогнозування, виявлення, стримування, запобігання, відбиття інформаційних загроз і ліквідації наслідків їхнього прояву, а найчастіше й від анонімності їхньої роботи [7], залежить безпечне функціонування КВО та КСІІ.

Саме тому соціальні інженери в пошуках захисту своїх об’єктів від кібернетичного тероризму (КбТ), здійснюваного на першому етапі з допомогою кібернетичної розвідки (КР) з послідующій реалізацій кібернетичних атак (КбА), беруть до уваги психологічний стан колективу. Як правило, у сучасних організаціях (установах, компаніях) потенційними жертвами КР та КбА можуть бути адміністратори, начальники, користувачі та

навіть більш чи менш знайомі будь-кого зі згаданих категорій осіб [8]. Акцентував серйозно увагу моніторингу соціальних мереж з соціально-технічної системи, належить з особою пильністю віднестись насамперед і к підбору персоналу власної соціальної служби аж до аналізу умов роботи медперсоналу, зачастую применяя и технологию полиграфа.

На думку авторів, оскільки соціальна інженерія має багатий арсенал методики технологій захисту від КР та КбА, серед основних загроз інформаційній та кібербезпеці за типу реалізації є комбінації технічних та психологічних факторів прямого впливу на людину. Супутні уразливості зростають, коли сама людина надає можливість, за допомогою цифрових пристроїв та систем, в яких так чи інакше циркулює, зберігається та обробляється інформація. В наслідок чого зловмиснику, методами психології з арсеналу СІ, відкривається вплив на людину і, як результат, полегшується отримувати необхідний доступ до службової таємниці. Комбінуючи апаратно-програмні комплекси і методи та звичайну психологію, цей метод

включає в себе базовий метод виду як прямий вплив. У даному випадку соціальний інженер у ролі зловмисника має можливість напряму застосовувати на людину. А саме, спочатку він шукає інформацію про цю людину, включаючи його інтереси та образ мислення. Якщо є можливість він проводить первинну оцінку, спостерігає як людина себе поводить, що вона каже. На основі цих даних визначає для себе як поставити діалог, як поводитись з ним, як говорити з людиною, як вести розмову з цією людиною, що можна сказати, в яких моментах потрібна делікатність з цією людиною. Соціальний інженер, зможе вміло імпровізувати, навіть без спостерігання за людиною. Це все для того, щоб отримати потрібну інформацію в звичайному діалозі ненав'язливо, поступово. Це може буде неробоча та навіть не домашня обстановка. Зловмисник вибере місце де людина зможе розслабитись, спокійно говорити, тобто такий соціальний інженер зробить все таким чином, що ціль впливу буде цілком довіряти, а при повній довірі до зловмисника людина сам того не розуміючи видає необхідну інформацію. Цей ефект досягається саме розумінням інтересів, урахуванням поведінки людини його потреб наприклад, потреба висказатися. Людина прагне

виговоритися і саме в цей момент можна дізнатись різного роду інформацію. Тому і в цьому аспекті легше діяти випередження КбА, чим виправити наслідок ей успішної роботи.

Зокрема, на цей час розроблено системи комп'ютерного зору [9], які, безперечно, володіють широким позитивним спектром застосування (зокрема, й у сфері забезпечення безпеки), та досягли рівня розв'язання завдань не лише виявлення, а й розпізнавання постатей людей у пішохідних потоках, що з позицій соціального хакера вже слід розглядати як потенційну можливість відстежування професіонала з КСІІ. Тому має право на існування та подальшу реалізацію можливих контрзаходів (тобто методів і способів захисту від конкретних технологій інформаційного впливу), включно з їхнім парічнем і забезпеченням особистої безпеки персоналу через створення режиму анонімності їхньої роботи. Як такі (контрзаходи) пропонується використовувати активні та пасивні радіолокаційні методи захисту [10], спрямовані на нівелювання, а найчастіше й на повну нейтралізацію так званих у радіолокації «блискучих точок» об'єктів спостереження. Ця пропозиція ґрунтується на тому факті, що наявні методи розпізнавання образів, викладені, наприклад, у [11], базуються на алгоритмі формування HOG дескрипторів, завдяки чому «об'єкт на ділянці зображення може бути описаний напрямком країв або розподілом градієнтів яскравості. Реалізація таких дескрипторів здійснюється поділом зображення на зв'язні області (комірки), і підрахунком напрямків градієтів для кожної комірки або напрямків країв пікселів усередині. Комбінація гістограм і називається дескриптором. Щоб збільшити точність - проводять нормалізацію за контрастом для локальних гістограм. Фактично алгоритм отримання кінцевого результату «нормалізації за контрастом локальних гістограм» аналогічний до радіолокаційного розпізнавання об'єктів, сформованого за високої роздільної здатності у вигляді певного образу з конфігурацій блискучих крапок, які в цьому разі є аналогом градієнтів яскравості (країв пікселів).

Акцентувавши серйозну увагу моніторинґу соціальних мереж інформаційно-технічної системи, слід з особливою пильністю поставитися і до проявів хакінґу [12,13] у вигляді використання методів як соціальної інженерії, коли «споживач-

жертва» зазнає безпосереднього впливу на її особисту і службову інформацію з боку хакера, так і у вигляді опосередкованого його ворожого впливу на організуючу інформаційну ситуацію у сфері комунікації та її дискурс-аналізу [14] , добиваючись таким чином потрібного для суб'єкта впливу синергетичного ефекту, який може бути досягнуто в процесі реалізації процесу просування дискурсу і експлуатації сучасної інформаційної комунікації. При цьому механізми (інструменти) такого інформаційного впливу (хакінгу) являють собою складноорганізовану діяльність із реалізації процесу як у просуванні дискурсу, так і під час експлуатації сучасної інформаційної комунікації. Тому часто стверджують, що хакінг за своєю сукупністю, крім соціальної інженерії та malvertising (тобто реклам зі шкідливим ПЗ), є узагальнюючим терміном більшості шкідливих кібератак на комп'ютери та їхні мережі. Так як комп'ютерні системи або мережі требуют адекватного виявлення та виправлення уразливостей їхньої системи безпеки, що сприяє підвищенню кібербезпеки і захисту від потенційних кіберзагроз, то для їх тестування використовують ***етичний хакінг***, також відомий як тестування на проникнення або "білошапочний" хакінг, у вигляді людини[*,34], яка навмисно проникає в комп'ютерні системи або мережі з дозволу власників. При цьому, етичні хакери використовують різні техніки та інструменти для моделювання реальних атак і виявлення потенційних вразливостей. Їх підхід включає такі етапи:

- ***збір інформації*** відносно системи, мереж та додатків, щоб зрозуміти їх структуру, компоненти та потенційні слабкі місця;

- ***сканування*** для виявлення відкритих портів, служб, що працюють на цих портах, потенційних вразливостей, пов'язаних з цими службами ***та перелічення*** для збору детальної інформації про цілі, такі як облікові записи користувачів та конфігурації систем;

---

*[34] Ця людина - етичний хакер або білий хакер (на відміну від хакерів іншого кольору) використовує свої технічні знання для розв'язання складних завдань тестування комп'ютерів та їхніх систем з метою подальшої їхньої безпечної експлуатації, тоді як **крекери або чорні хакери** (хакери-зломщики) прагнуть отримати доступ до цих систем, до їхньої конфіденційної інформації та завдати їм шкоди, отримуючи особисту вигоду.

- ***аналіз вразливостей,*** які можуть бути використані для несанкціонованого доступу або порушення роботи цільових систем;

- ***експлуатації,*** де етичні хакери демонструють власникам виявлені вразливості для оцінки їхнього потенційного негативного впливу на рівень безпеки системи або мережі;

- ***після експлуатації,*** де етичні хакери намагаються зберегти доступ до

скомпрометованих систем для проведення додаткових тестів і збору додаткової інформації;

- ***звітування та рекомендації,*** де після завершення фази тестування

описують виявлені вразливості, їх потенційний вплив, надають рекомендації щодо усунення цих вразливостей, підвищення заходів безпеки та мінімізації ризику майбутніх атак, - тобто готують детальні звіти.

Таким чином, етичний хакінг - це бажана практика тестування комп'ютерної системи, мережі, а також їхнього різного роду застосунків, включно із заходами та сучасними системами їхнього захисту щодо виявлення поточних і потенційних вразливостей, якими можуть скористатися зловмисники. При цьому слід зазначити, що в царині використання хакінгу, крім наявності білих хакерів, можна зустріти і чорних, і сірих хакерів. Усі вони здатні реалізовувати не тільки етичний, а й неетичний злом або щось середнє між ними. У зв'язку з цим і незважаючи на те, що злом не завжди може бути шкідливою дією, озвучений термін міцно асоціюють із кіберзлочинністю з огляду на те, що будь-який злом означає проникнення в комп'ютерну систему, пристрій або мережу з метою отримання доступу до інформації або даних.

7.3. Ключові моменти при підборі персоналу

З раніше викладеного випливає, що відомі загрози інформаційній безпеці підприємства і сучасні засоби їх захисту не можуть існувати без впливу на них так званого людського фактору. Сьогоднішня проблема інформаційної безпеки в

діяльності будь-якої організації **з урахуванням людського фактору** стає наріжним каменем, що вимагає своєчасного (бажано заздалегідь прогнозованого і вчасно реалізованого) реагування на ***реальні види загроз***, до актуальних видів яких відносять:

1. Неуважність і недбалість лояльних співробітників, які навіть не думаючи, наприклад, про псування, спотворення, втрати і т. д. аж до крадіжки важливих даних, дозволяють найчастіше скопіювати файл з конфіденційною інформацією на планшет або флешку для продовження своєї роботи в домашніх умовах або у відрядженні. Перелік таких недбалих дій співробітників різноманітний, – а кінцевий результат такої ненавмисної шкоди конфіденційних відомостей очевидний – в таких ситуаціях службова інформація може бути втрачена або використана у ворожих цілях.

2. Використання піратського програмного забезпечення в результаті непродуманих дій керівництва, яке не до кінця усвідомлює, що неліцензійні програми не забезпечують належного захисту від зловмисників, зацікавлених у крадіжці службової інформації за допомогою вірусів. Не отримуючи технічної підтримки, своєчасних оновлень, що надаються компаніями-розробниками, неліцензійний продукт здатний завдати шкоди системі комп'ютерної безпеки (в тому числі і КСЗІ) аж до крадіжки службової інформації.

3. Загрози з боку співвласників бізнесу, оскільки саме легальні користувачі – одна з основних причин витоків службової інформації. Такі витоки фахівці називають інсайдерськими, а всіх інсайдерів умовно ділять на кілька груп:

«Порушники», – у процесі ненавмисних (а по суті шкідливих) дій у вигляді онлайн-покупок з робочих комп'ютерів, використовуючи особисту пошту, у вигляді комп'ютерних ігор і т. д., зручно успішно реалізовувати зовнішні кібератаки.

«Злочинці» в особі топ-менеджера, який має доступ до важливої інформації і зловживає своїми привілеями, самостійно встановлюючи різні додатки аж до розсилки конфіденційної інформації зловмисникам.

«Кроти» – це, як правило, досить досвідчені співробітники, вміло знищують всі сліди своїх злочинів, які навмисне крадуть важливу інформацію за матеріальну винагороду від конкурента.

4. Загрози з боку конкурентів, часто реалізовані за допомогою використання звільнених і ображених на попередню роботу співробітників, які зазвичай забирають з собою всю інформацію, до якої вони мали доступ.

На жаль, кількість і витонченість успішно реалізованих загроз інформаційної безпеки щорічно зростає, незважаючи на те, що індустрія послуг із захисту інформації стрімко розвивається. Зловмисникам часто все ж вдається бути на крок попереду. Щоб забезпечити максимальну конфіденційність інформації, доводиться створювати багаторівневу систему її захисту, приділяючи належну увагу людському фактору, починаючи з підбору персоналу, тобто з вирішення завдань «кадрової та інтелектуальної» безпеки.

Під **кадрово-інтелектуальною безпекою** розуміють деякий комплекс заходів, спрямований на запобігання та усунення загроз і ризиків, а також негативних для економічного стану підприємства наслідків, пов'язаних з роботою і поведінкою персоналу, його інтелектуальним потенціалом, трудовими відносинами в цілому. Все це зайвий раз підтверджує вищесказане і додатково акцентує увагу на те, що кадрова безпека займає чільне місце серед інших елементів системи безпеки, так як персонал задіяний у всіх процесах КСЗІ.

Прийнято вважати, що ефективна організація роботи служб з управління персоналом у забезпеченні кадрової безпеки може майже на 60% знизити прямі і запобігти побічним збиткам підприємства, що пов'язані з людським фактором. Серед загроз кадрової безпеки компанії слід розрізняти внутрішні (велика частина з них вже викладена вище) і зовнішні. До зовнішніх загроз відносять негативні впливи зовнішнього середовища, які впливають як на процеси всередині компанії в цілому, так і на її кадрову безпеку, а саме:

− інфляційні процеси (їх неможливо не враховувати при розрахунку заробітної плати та інших виплат);

− ситуація на ринку праці (дефіцит певних фахівців викликає труднощі в підборі якісного персоналу);

− наявність у конкурентів більш привабливих умов праці аж до переманювання співробітників конкурентами;

− здійснення зовнішнього тиску на співробітників (підкуп, шантаж) або потрапляння співробітників в різні види залежності (алкогольна, наркотична та ін.).

Ключовими моментами, що визначають кадрову безпеку, є:

1) вжиття заходів безпеки при прийомі на роботу, включаючи прогноз благонадійності, де безпосередньо процес «безпечного» найму починають з розгляду питань безпеки підприємства на етапах пошуку кандидатів, їх відбору, документального та юридичного забезпечення прийому на роботу, закінчуючи встановленням для кандидата випробувального терміну;

2) формування лояльності персоналу, оскільки безпека будь-якого підприємства безпосередньо залежить від позитивного настрою і відносин співробітників в колективі;

3) контроль за дотриманням правил, норм, зафіксованих документально у вигляді регламентів, обмежень, режимів, технологічних процесів, оціночних операцій, процедур безпеки і т. д.

Отже, кадрову безпеку в організації слід розглядати з різних позицій.

З одного боку – це процес забезпечення поточної і потенційної захищеності персоналу організації від різноманітних загроз, у процесах відбору та адаптації персоналу, розвитку та кар'єрного зростання співробітників, оцінки його ділових і особистісних характеристик і оплати праці, а також при переміщенні і вивільненні з організації. Для персоналу в цьому випадку основним джерелом загроз виступає роботодавець, який грубо порушує права та гарантії працівників.

З іншого боку, кадрову безпеку можна вибудовувати з точки зору активного захисту, в якій має потребу сама організація. Йдеться про економічну безпеку, імідж і сталий розвиток внутрішніх бізнес-процесів, про загрози, що створюються несанкціонованими свідомими чи несвідомими діями персоналу даної організації, які можуть вступати в сумнівні з точки зору закону трудові відносини. Це може бути корупційна діяльність чиновників і осіб, що приймають рішення, які зловживають своїм

становищем. Працівники організації можуть вступати в змову, передавати секретну інформацію третім особам або використовувати її не за прямим призначенням. Окремі співробітники можуть здійснювати вербування дефіцитних фахівців, переманювати їх у конкуруючі організації.

Таким чином, необхідно створювати гнучку систему кадрової безпеки, здатну вчасно діагностувати насування загрози і своєчасно їй запобігти.

7.4. Основні аспекти діяльності служби (відділу) кадрів підприємства та методи його відбору з точки зору забезпечення кадрової безпеки

Головним інструментом роботи служби кадрової безпеки є тотальний контроль на всіх ділянках роботи персоналу [15]. Це відеоспостереження, прослуховування телефонних розмов, контроль доступу і роботи комп'ютера, контроль використання робочого і вільного часу співробітників, переміщень, тобто контроль в процесі трудової діяльності і якийсь час після звільнення співробітника. Звісно, що плідність вирішення такого завдання ускладнюється законністю використовуваних методів добування необхідної інформації.

В даний час активно застосовують найрізноманітніші методи відбору персоналу, законні і, найчастіше, – не зовсім. Звідси і така їх різноманітність: від традиційного хедхантингу («headhunting»), «переманювання» осіб, котрі приймають рішення («executive search»), кадрового браконьєрства («talent poaching»), кадрових нальотів («talent raiding»), до «агресивного» або «партизанського» рекрутингу [16-23].

Підбір персоналу (рекрутинг) – це процес виявлення найбільш придатних і підготовлених працівників із числа кандидатів на вакансію. Професійний («правильний») процес рекрутингу складається з декількох етапів. Починаючи з планування потреби в персоналі, збору і узгодження заявок на підбір, бюджетування процесу, розміщення вакансії у відкритому доступі при пошуку кандидатів, проведення співбесіди з кандидатом і лінійним керівником, а також отримання висновку

за підсумками перевірки нашого кандидата службою безпеки, і закінчуючи підписанням трудового договору. У великих компаніях вже давно вдаються до складання операграм [15], які допомагають координувати виконання необхідних функцій для здійснення бізнес-процесу і значно спрощують роботу. За допомогою операграми [15, 24] легко простежити, на якому етапі здійснюється процес, хто є ініціатором і виконавцем підбору, в якій послідовності і кому передаються повноваження, а також хто є джерелом порушення запланованого ходу заходів. Фактично служби персоналу розбивають на дві служби: службу підбору і службу кадрової безпеки. В цілому, вона (служба персоналу) носить універсальний характер і може незначно коригуватися у зв'язку з особливостями конкретної компанії.

Для ефективної організації праці служб підбору і кадрової безпеки, їх спільної ефективної взаємодії в рамках одного і того ж процесу підбору кадрів, необхідно чітко розмежувати сфери їх діяльності, закріпивши за кожною зі сторін свій специфічний функціонал.

До служби безпеки слід віднести функції:

- ✓ організації службового розслідування;
- ✓ планування заходів з діагностики та викриття виявлених загроз;
- ✓ спеціальне навчання власних співробітників і працівників інших підрозділів з виконання ними відповідних дій для збереження правопорядку;
- ✓ виконання цільових запитів в організації (податкові, міграційні служби, психоневрологічний диспансер, вивчення кредитних історій і т. п.);
- ✓ перевірка достовірності документів (паспорта, трудової книжки);
- ✓ збір характеристик з попередніх місць роботи для перевірки трудових історій (конфліктності), фінансової стабільності (благонадійності), можливо, дані про родичів, якщо є в цьому гостра необхідність (дивлячись на яку посаду претендує людина).

Якщо аналізувати сучасні методи впливу на персонал, то в службах безпеки вони розподілені за наступними напрямками: методи діагностики загроз кадрової безпеки, як з боку зовнішніх,

так і внутрішніх факторів впливу, і методи, що протистоять потенційній та/або реальній кадровій загрозі для організації [27].

Служба роботи з персоналом організації (служба підбору) реалізує функції з підбору, забезпечення розвитку та мотивації, формуванню лояльності співробітників, високого рівня відповідальності за ефективну і ініціативну роботу на місцях; функціональну і професійну мобільність, професійну грамотність [25, 26].

На додаток до викладеного розглянемо класифікацію методів діагностики кадрової безпеки у вигляді [15]:

- ✓ групи методів цілеспрямованого впливу;
- ✓ групи методів таємного примусу; впливу;
- ✓ групи методів інформаційно-психологічного впиву.

До методів цілеспрямованого впливу відносять припинення шахрайства, рейдерського захоплення, запобігання корупційній діяльності в організації, та ін.

Методи таємного примусу включають конкурентну розвідку, вербування працівників, різного роду маніпуляції, в тому числі використання нейролінгвістичного програмування, промислове шпигунство та ін.

До методів інформаційно-психологічного впливу відносять: порушення прав працівників на робочому місці, дискримінації (за статево-віковою ознакою, стосовно людей з обмеженими фізичними можливостями, хворих СНІДом, людей, що ведуть нездоровий спосіб життя); психічне насильство: мобінг, буллінг, харасмент. До цих же методів віднесемо поширення чуток, пліток, провокацій; витік/викрадення інформації; несанкціонований збір, зберігання, обробка, використання персональних даних співробітників, передача їх третім особам, та ін.

Методи, що протистоять потенційній та/або реальній кадровій загрозі, класифікуємо як профілактичні, припиняючі або відбиваючі і караючі; це можуть бути методи легітимного і нелегітимного характеру, відверто кримінального характеру (вербування, шантаж, хабарі).

Перераховані методи впливу на персонал дозволяють діагностувати або протистояти загрозам кадрової безпеки. Вони абсолютно відрізняються від методів роботи фахівців кадрових

служб. Фахівці цих структур працюють паралельно в досягненні єдиної мети, у нашому випадку – це заповнення вакантних позицій гідними кандидатами. Однак слід розуміти, що змішувати, і, тим більше, підміняти або дублювати дії цих двох служб абсолютно неправомірно. Через застосування різних форм і методів роботи, розділяючи сфери діяльності служб, можливий більш повний і якісний збір необхідної інформації про претендента, що дозволяє гарантовано охороняти організацію від можливих кадрових упущень в роботі та загроз кадрової безпеки організації.

Хочеться особливо відзначити той факт, що сучасна діяльність служби персоналу з точки зору забезпечення кадрової безпеки серйозно видозмінена. У даний час це не колишній відділ кадрів радянських часів, не механізм по документуванню прийому на роботу і звільнення, а один із найважливіших ресурсів щодо забезпечення стійкості підприємства на ринку. Ключові співробітники служби персоналу наділяються відповідними повноваженнями, які повинні бути не тільки надані, але публічно делеговані і зафіксовані документально. У цих питаннях є дуже важливою підтримка керівництва компанії, проведення узгодженої та послідовної політики забезпечення безпеки на всіх рівнях управління. Фахівці служби персоналу повинні мати безпосередній доступ до **необхідних корпоративних ресурсів**: планів стратегічного розвитку компанії, інформаційних масивів і баз даних (в тому числі і конфіденційного характеру), до аналітичних матеріалів. **Фінансування** служби персоналу повинно здійснюватися як з урахуванням витрат на реалізацію програм роботи з персоналом (залучення кваліфікованих кадрів, навчання, оцінка, розвиток, кадрові переміщення, управління лояльністю і т. д.), так і на заходи щодо забезпечення кадрової безпеки підприємства. Служба персоналу повинна приймати безпосередню участь в **розробці документаційного забезпечення безпеки**. Керівник служби відповідає за наявність необхідних регламентів і процедур, їх функціональність і відповідність чинним нормативно-правовим актам. Існує ряд обов'язкових документів, безпосередньо пов'язаних з безпекою компанії: трудовий договір, правила внутрішнього трудового розпорядку, договори про

повну індивідуальну та колективну матеріальну відповідальність, документація з охорони праці та т. п. І, звичайно, до складу «паперового» забезпечення безпеки, що знаходиться в прямій компетенції служби персоналу, входить документування дисциплінарної практики на підприємстві і в підрозділах. Крім того, служба персоналу повинна мати право на участь – пряму або опосередковану, ініціативну або експертну – в роботі по створенню іншої документації, пов'язаної з безпекою, наприклад, пакета документів, що регламентують безпеку конфіденційної інформації або Положення про внутрішню «гарячу лінію» (нею будь-який співробітник компанії може анонімно вказати на проблеми або порушення в галузі безпеки, що ведуть до втрат і збитків).

Очевидно, що результативність в системі кадрової безпеки немислима без чіткої та ефективної взаємодії всіх підрозділів. У компанії повинен бути регламентований і описаний розподіл прав і обов'язків між співробітниками служби персоналу і їх колегами зі служби безпеки та інших відділів. Документально це може бути закріплено у вигляді деякого, автономно створеного для даного підприємства, Положення про взаємодію у галузі забезпечення безпеки. У ньому викладають: порядок взаємодії служб на різних етапах роботи по забезпеченню безпеки, розподіл фінансування, порядок узгодження при прийнятті рішень, ступінь доступності для окремих категорій співробітників внутрішньої інформації і рівень її конфіденційності, відповідальність конкретних посадових осіб і т. п. При цьому взаємодія служби персоналу і служби безпеки має бути тісною, постійною і взаємодоповнюючою, таким, що гідно забезпечить поширені перевірочні заходи, а саме:

- перевірка за «поліцейським» обліками – судимості, суттєві адміністративні стягнення, загублені паспорти, наявність розшукових справ;
- перевірка рекомендацій з місць попередньої роботи через служби безпеки компаній або легендовано (в цьому випадку при запиті інформації не вказують назву організації, посаду перевіряючого і причини перевірки);

- перевірка реєстрації за місцем проживання (перебування);
- перевірка кредитної історії через служби безпеки або кредитні відділи банків;
- перевірка на наявність зв'язків в кримінальному середовищі (в тому числі зв'язків через родичів і членів сім'ї);
- перевірка наявності нерухомого та рухомого майна (в тому числі на відповідність заявленому);
- перевірка участі в капіталі (заснування, акціонування і т. д.) організацій – юридичних осіб;
- перевірка участі (заснування, опікування) в некомерційних організаціях - фондах, товариствах, асоціаціях, громадських організаціях;
- перевірка документів, що надаються (диплом, паспорт) на справжність і т. д.

Результати таких перевірок, проведених службою безпеки, в документованій формі представляють співробітникам служби персоналу і враховуються при ухваленні рішення про прийом кандидата на роботу.

Серед інших напрямків співробітництва цих двох служб: оцінка благонадійності як кандидатів, так і співробітників, розробка програм фізичного захисту персоналу, участь служби безпеки в процедурах звільнення працівників, спільна робота в комісіях з матеріальної відповідальності при розгляді випадків нанесення шкоди компанії і т. д. Не слід забувати також про необхідність оперативного зв'язку керівника служби персоналу з керівником служби безпеки.

Крім перерахованих вище напрямків щодо забезпечення КСЗІ та їх реалізації не слід забувати також і про правильну організацію моніторингу всіх доступних каналів інформації, як однієї з найважливіших функцій служби персоналу при забезпеченні кадрової безпеки компанії. Зокрема, під час **моніторингу каналів неофіційної (кулуарної) інформації** контроль неформальних інформаційних потоків здійснюється різними способами, а за його результатами можуть бути визначені загальний стан мотивації персоналу і рівень

популярності керівництва, виявлені неформальні лідери груп і конкретні винуватці внутрішніх порушень, випадків розкрадання і прояви недбалості. Контроль «чуток» – важливе завдання в контексті забезпечення кадрової безпеки компанії. При **моніторингу ринку праці дуже важливо** вивчати стан ринку праці, рівень безробіття в регіоні, динаміку зміни рівнів середніх зарплат за ключовими позиціями і т. д. Важливо постійно відстежувати, що пропонують ваші безпосередні конкуренти: умови праці, рівень оплати і т. д. Важливу роль у забезпеченні кадрової безпеки відіграє і **моніторинг змін у законодавстві**, що проводиться спільно з юридичним відділом. Упущення тут призводять до прямих втрат і коштують дуже дорого. З точки зору кадрової безпеки, обов'язковим є **моніторинг рівнів лояльності** як кандидатів на вакансії, так і працівників компанії. Для служби персоналу дуже корисно визначати ступінь задоволеності співробітників роботою та психологічним кліматом у колективі, а також з'ясовувати їхнє ставлення до керівництва і до компанії. Щоб контролювати питання кадрової безпеки, потрібно не тільки аналізувати отримані результати, але і обов'язково відстежувати динаміку змін. В результаті формується уявлення про психологічне благополуччя співробітників, а також і про можливість появи конфліктних ситуацій на підприємстві, які мають пряме відношення до кадрової безпеки.

Очевидно, що конфлікти слід розглядати як загрозу кадрової безпеки компанії. ***Конфлікти*** традиційно поділяють на ***організаційні та міжособистісні***. І ті й інші неминучі і можуть приводити або до розвитку (конструктивні), або до руйнування (деструктивні) людських відносин і організації в цілому. Часто виникають конфлікти з приводу невиконання правил внутрішнього трудового розпорядку, вимог посадових інструкцій, зобов'язань про нерозголошення конфіденційної інформації. Постійно призводить до напруженості і проблем конфлікт інтересів – використання співробітниками ресурсів компанії у своїх особистих цілях, встановлення ними приватних відносин з конкурентами, постачальниками або споживачами. У взаємовідносинах служби персоналу і працівників компанії також безліч потенційно конфліктних моментів: незадоволеність

умовами праці, рівнем оплати, результатами атестації, можливостями для кар'єрного зростання і т. п. В окремий ряд прийнято виділяти конфлікти персоналу з співробітниками служби безпеки і охороною. Частина таких конфліктів, що мають пряме відношення до безпеки компанії, породжуються відмінністю в статусі конфліктуючих сторін: наприклад, начальник змушений у деяких питаннях підкорятися простому охоронцеві. Невирішені конфлікти небезпечні не тільки самі по собі (люди відволікаються від роботи, через стреси частіше хворіють, через негативні емоції падає продуктивність праці), а й тим ефектом, який вони здійснюють на інших працівників (погіршується морально-психологічний клімат в колективі , знижуються трудова мотивації і лояльність до роботодавця). Важкі конфліктні ситуації можуть привести до зміни ставлення співробітника до колег і компанії в цілому, що загрожує можливими порушеннями, проявом недбалості, а іноді і цілеспрямованого шкідництва (наприклад, з почуття помсти). Тому своєчасне і грамотне вирішення конфліктів – дуже важливий і складний момент в організації кадрової безпеки.

Очевидно, що вирішення конфліктів багато в чому залежить від психологічних особливостей людини, його особистих якостей, а, отже, способи запобігання перерахованих вище порушень випливають з аналізу спонукальних мотивів: ретельний підбір персоналу, підготовка персоналу, підтримання здорового робочого клімату, мотивація і стимулювання діяльності співробітників. У будь-якій професійній діяльності є стабільні складові і змінні, пов'язані з конкретними умовами, в яких ця діяльність здійснюється. При підборі кадрів важливо брати до уваги обидві складові, тобто оцінюються психологічні характеристики, дотримання яких необхідно для виконання певних професійних обов'язків. У психограму включають вимоги, що пред'являються до професійної діяльності, (щодо пам'яті, уяви, сприйняття), до психічного стану (втоми, апатії, стресу), до уваги для оцінки стану свідомості, до емоційних (стриманість, індиферентність) і вольових (наполегливість, імпульсивність) характеристик. Деякі з цих психологічних вимог є основними, головними, без них узагалі неможлива якісна діяльність. Психологічна невідповідність вимогам професії

особливо сильно проявляється в складних ситуаціях, коли потрібна мобілізація всіх особистісних ресурсів для вирішення складних завдань. Тому це особливо важливо в рамках комплексної системи захисту інформації.

Однак, опису психологічних вимог недостатньо, щоб, орієнтуючись тільки на них, підбирати людину для роботи. При підборі кадрів необхідно орієнтуватися не тільки на окремі характеристики психіки, а на риси особистості як її системні властивості. Прийнято виділяти найбільш результативні методи вивчення особистості, а саме:

- ✓ вивчення життєвого шляху особистості, думки колективу, в якому працює особа, і найближчого оточення особистості;
- ✓ створення ситуації, найбільш підходящої для прояву професійно важливих якостей і властивостей;
- ✓ вивчення висловлювання особистості про власну роль в справах колективу.

Відтак, розуміючи провідну роль особистості у збереженні секретів, важливо пам'ятати, які характерні якості людини не сприяють збереженню довіреної їй таємниці. Фактично основи успішної безпеки інформації пов'язані з якостями, до яких відносять: чесність, сумлінність, принциповість (суворе дотримання основних правил), старанність, пунктуальність, дисциплінованість, емоційна стійкість (самоконтроль), прагнення до успіху і порядку в роботі, самоконтроль у вчинках і діях, правильна самооцінка власних здібностей і можливостей, обережність, вміння зберігати секрети, тренована увагу і непогана пам'ять. До якостей, які не сприяють збереженню довіреної таємниці слід віднести: – емоційний розлад, неврівноваженість поведінки, розчарування в собі, відчуженість від колег по роботі, невдоволення своїм службовим становищем, ображене самолюбство, егоїстичні інтереси, нечесність, вживання наркотиків і алкоголю, які поступово руйнують особистість.

Крім перерахованих вище напрямків щодо забезпечення КСЗІ та їх реалізації не слід забувати також і про рівень підготовки (перепідготовки) персоналу, від якого залежить розвиток компанії, зміцнення її конкурентоспроможності,

безпеки, стійкості на ринку. Очевидно, що в результаті навчання підвищується кваліфікація працівників, скорочується плинність кадрів, забезпечуються гідні умови щодо формування лояльності персоналу, тобто в кінцевому підсумку підвищується кадрова безпека підприємства.

Таким чином, будь-яке серйозне підприємство крім згаданого вище Положення про взаємодію у галузі забезпечення безпеки, в якому регламентовано розподіл прав і обов'язків між співробітниками служби персоналу і їх колегами зі служби безпеки та інших відділів, має розробити якусь політику індивідуальної поведінки для кожного співробітника підприємства, затверджену у вигляді єдиного документа. Зокрема, за кордоном в якості такого документа, заснованого на рекомендаціях Організації економічного співробітництва і розвитку (ОЕСР), запропонований **Кодекс корпоративної поведінки** [28]. Здебільшого кодекси корпоративної поведінки включають дві частини: ідеологічну (цінності, цілі, місія) і нормативну (стандарти робочої поведінки) [29]. Однак деякі корпорації (підприємства) обмежують кодекс корпоративної поведінки описом лише моральних цінностей, називаючи такий кодекс етичним. Існують кодекси, які містять заяви тільки про цінності, або кодекси, в які не включена частина, що стосується ідеології. Фактично, в залежності від рангу підприємства конкретизація Кодексу специфічно індивідуальна, але з точки зору побудови власного інформаційного захисту – майже ідентична.

7.5. Розробка кодексу корпоративної поведінки

Відповідно до викладеного вище впровадження кодексу корпоративної поведінки є найефективнішим у діяльності будь-якого поважного підприємства. В такому кодексі мають бути максимально чітко позначені пріоритетні цілі і задачі організації, її місія, а також розставлені акценти у внутрішніх і зовнішніх відносинах, включаючи співробітників, клієнтів і керівництво. Це елемент традиційної корпоративної культури, що поліпшує і зміцнює психологічну атмосферу колективу. Кодекс

корпоративної поведінки може виконувати три **основні функції** [30]: ***репутаційну, управлінську та функцію розвитку корпоративної культури.***

Репутаційна функція кодексу полягає в формуванні довіри до організації з боку референтних зовнішніх груп (держави, замовників, клієнтів, конкурентів і т. д.). Наявність у компанії кодексу корпоративної поведінки стає загальносвітовим діловим стандартом.

Управлінська функція кодексу полягає в регламентації поведінки в складних етичних ситуаціях. Підвищення ефективності діяльності співробітників здійснюється шляхом регламентації пріоритетів у взаємодії зі значущими зовнішніми групами, шляхом визначення порядку прийняття рішень в складних етичних ситуаціях і шляхом вказівки на неприйнятні форми поведінки.

Корпоративна етика (культура) є складовою частиною організаційної політики. Кодекс покликаний виявляти пріоритетні для організації цінності і доводити їх до кожного співробітника, як новачка, так і досвідченого професіонала. В ідеалі персонал буде орієнтований на єдині цілі, тим самим підвищуючи корпоративну ідентичність і прихильність загальній справі.

Зміст кодексу компанії визначають, перш за все, її особливостями, структурою, задачами розвитку, установками її керівників. Раніше відзначали, що, як правило, кодекси містять дві частини: ідеологічну (місія, цілі, цінності) і нормативну (стандарти робочої поведінки). При цьому ідеологічна частина може не включатися до змісту кодексу.

У професійно однорідних організаціях (банки, дослідні центри, консультаційні компанії) часто використовуються кодекси, що описують в першу чергу вузькоспеціальні дилеми. Ці кодекси є похідними від кодексів професійних співтовариств. Відповідно, зміст таких кодексів, в першу чергу, регламентує поведінку співробітників в складних професійних етичних ситуаціях. У банківській діяльності, наприклад, це доступ до конфіденційної інформації про клієнта і відомостей про стійкість банку. В цьому випадку кодекс описує правила поводження з такою інформацією, забороняє використовувати відомості з

метою особистого збагачення. В першу чергу тут вирішуються управлінські задачі. Доповнення такого кодексу главами про місію та цінності компанії сприяє розвитку корпоративної культури. При цьому кодекс може мати значний обсяг і складний специфічний зміст і адресуватися усім співробітникам компанії.

У великих неоднорідних корпораціях поєднання всіх трьох функцій стає складним. З одного боку, існує ряд переваг (рекомендацій) і ситуацій, традиційно закріплених етичними кодексами в міжнародній практиці. Це політика переваг по відношенню до клієнтів, постачальників, підрядників. Опис ситуацій, пов'язаних з можливими зловживаннями, наприклад хабарі, підкуп, розкрадання, обман, дискримінація. Виходячи з управлінської функції, кодекс описує стандарти зразкової поведінки в таких ситуаціях. Такий кодекс має значний обсяг і досить складний зміст. Адресація його всім групам співробітників в умовах значної різниці в освітньому рівні і соціальному статусі працівників утруднена. У той же час розвиток корпоративної культури компанії вимагає єдиного кодексу для всіх співробітників – він повинен задавати єдине розуміння місії та цінностей компанії для кожного співробітника.

По суті, декларативний варіант кодексу – це тільки його ідеологічна частина без регламентації поведінки співробітників. Причому в конкретних ситуаціях співробітники самі повинні орієнтуватися, як їм себе вести, виходячи з базових етичних норм, позначених в кодексі. Проте в ряді випадків співробітникам важко оцінити етичну правомірність конкретного вчинку виходячи із загальних принципів. У розгорнутих варіантах кодексу з докладною регламентацією етики поведінки співробітників фіксуються конкретні вчинки персоналу в окремих областях, де ризик порушень найвищий або виникають складні етичні ситуації. Ці регламенти описуються як політики (рекомендації) щодо замовників, держави, клієнтів, політичної діяльності, конфлікту інтересів, безпеки праці. При цьому великий обсяг і складність змісту таких кодексів визначають їх вибіркову адресацію за характеристикою організації (професійно однорідні або великі, тобто професійно неоднорідні), за рівнем охоплення основних функцій (частково, повністю або в сукупності двох або трьох видів функцій: – репутаційної,

керуючої і корпоративної), за формою викладу (діловою, понятійною або спеціалізовано-професійною мовою) і т. д. У більшості компаній такі кодекси розробляються для вищої та середньої ланки (менеджменту) і не є загальним документом, об'єднуючим всіх співробітників.

Як видно, кожна компанія вирішує свої власні задачі, використовуючи такий інструмент, як Кодекс корпоративної поведінки. Але створення кодексу, природно, не обмежується тільки написанням тексту документа. Існує специфіка виконання подібних документів: змусити виконувати етичний кодекс не можна. Тому для того, щоб він дійсно працював, ще на етапі його створення необхідно передбачити процедури, які включають в процес розробки проекту кодексу за можливості всіх співробітників компанії. В якості таких процедур використовують заходи щодо залучення кожного співробітника підприємства до процесу безпосереднього обговорення базових цінностей організації і повноважень вищих керівників шляхом внесення своїх пропозицій і подальшого детального обговорення положень проекту Кодексу. При цьому, загальний план розробки проекту Кодексу як документа складається з трьох етапів: ***етапу проектування, етапу обговорення і етапу інтеграції***.

Етап проектування полягає в розробці проекту кодексу, де основним акцентом при формуванні цілей і цінностей підприємства важливе місце відведено контролю безпеки і збереженню конфіденційної інформації. Тут же зазвичай зазначено ставлення перших осіб і вищого керівництва до існуючої в організації проблематики етичного характеру. Для цього проводиться аналіз існуючих кодексів інших компаній у контексті їх застосування. Визначаються базові цінності і цілі даного підприємства, а також найактуальніші сфери застосування кодексу. В результаті формулюється концепція кодексу, його ідеологія, формат, сфери застосування і видається попередній проект тексту.

Етап обговорення проекту кодексу безпосередньо реалізується в трудових колективах, у всіх підрозділах підприємства з метою збору пропозицій з доопрацювання тексту кодексу і обраного алгоритму його виконання шляхом залучення рядових співробітників до процесу безпосереднього створення

Кодексу. На цьому етапі зазвичай пояснюють співробітникам сенс, значення і сфери застосування кодексу з метою створення позитивної громадської думки щодо кодексу серед персоналу, а також підготовки менеджменту і кваліфікованих співробітників як ресурсу по впровадженню кодексу в практику щоденної діяльності. Під час обговорення проекту Кодексу використовують:

- очну і заочну форми обговорення, які дозволяють співробітникам стати співавторами кодексу;
- сучасні методики групової роботи по обговоренню проекту кодексу, як з керівниками, так і з неформальними лідерами громадської думки, які б ініціювали подальше обговорення документа в трудових колективах;
- оперативну обробку і передачу даних очного обговорення для негайного використання у заочному обговоренні, яке здійснюється паралельно, в корпоративних засобах масової інформації;
- інтерактивну модульну схему інформаційної кампанії, що дозволяє вести в діалоговому режимі ключові роз'яснення сенсу кодексу і його деталей.

Як видно, очне обговорення орієнтоване на включення в діалог працівників, зацікавлених в майбутньому своєї організації, у яких є що висловити і запропонувати заради підвищення загального морального клімату. Заочне обговорення (із залученням державних і корпоративних засобів масової інформації, включаючи і корпоративні віртуальні мережі) теоретично здатне охопити більш високий відсоток співробітників, ніж фізично можна здійснити при очному обліку масштабів корпорації. У період обговорення проекту Кодексу необхідно задіяти всі доступні засоби (друковані видання, стінгазети, корпоративні сайти організації).

При цьому треба добре налагодити так званий зворотній зв'язок, оскільки саме обговорення кодексу вже є початком його впровадження. Процес обговорення служить основою для пошуку спільних інтересів співробітників і керівництва, побудови єдиної ціннісно-цільової картини і розвитку діалогу між співробітниками і керівництвом.

Етап інтеграції включає: аналіз всіх пропозицій, що надійшли, внесення змін в зміст проекту, вироблення механізмів виконання і впровадження документа. Крім того доцільно вивчення досвіду інших компаній. Як правило, підсумком третього етапу проекту стає створення остаточного варіанту тексту кодексу, його поліграфічне виконання та поширення серед персоналу.

Очевидно, що через деякий час можливо потрібно коригування тексту прийнятого кодексу корпоративної поведінки з т. з. втрати актуальності, морального старіння і т. д. У такому випадку вищому керівництву доцільно скликати комісію з оптимізації тексту Кодексу, і в разі рішення про неминучість внесення змін, розробити новий проект кодексу, з обов'язковим урахуванням минулого досвіду.

Таким чином, формування позитивної корпоративної культури з урахуванням специфіки безпеки зачіпає зміну таких істотних представлень, як внутрішній психологічний клімат колективу, фундаментальні цінності, сукупність формальних і неформальних вимог до персоналу у вигляді норм поведінки, і, нарешті, загальні уявлення представників колективу про навколишнє середовище, організації та індивідуальності кожного із співробітників. Усі ці поняття є складовими організаційної культури і обумовлюють діяльність, здійснювану свідомо чи непідконтрольно окремими нормами субкультур організації, які повинні бути скореговані таким чином, щоб не протистояти первинним цінностям безпеки, встановленим основною домінуючою культурою, не перебувати в опозиції до них. При цьому, щоб дії, що переслідують цілі зміцнення механізмів безпеки, були адекватно сприйняті і прийняті колективом, вони повинні бути не тільки розумні, а й відповідати базовим уявленням співробітників про справедливість, чому сприяє вивчення і розуміння корпоративної культури. Підсвідомого неприйняття або навіть відкритої протидії політиці безпеки можна уникнути, якщо вчасно провести ретельне спостереження, в ході якого повинен бути виявлений переважаючий тип корпоративної культури кожного структурного підрозділу, який може варіюватися в залежності від функціональних, вікових, професійних, географічних чи інших особливостей. Також вкрай

важливо визначити неформальних лідерів, виявити найбільш авторитетні субкультури, які впливають на внутрішню життєдіяльність підприємства. Важливо вибрати найбільш ефективну субкультуру і використовувати її в якості вихідної позиції для введення інновацій. У світлі викладеного, можна сподіватися, що Кодекс корпоративної поведінки стимулює вдосконалення корпоративного законодавства оскільки він охоплює і деталізує такі поняття як: принципи корпоративної поведінки; загальні збори акціонерів; рада директорів товариства; виконавчі органи суспільства; корпоративний секретар товариства; істотні корпоративні дії; розкриття інформації про суспільство; контроль над фінансово-господарською діяльністю; дивіденди; врегулювання корпоративних конфліктів, аж до вирішення питань інформаційної безпеки.

Отже, викладена методика створення Кодексу формально є базовою, а сам кодекс стимулює нормальне функціонування і життєдіяльність будь-якого підприємства, що затвердив його цінності.

Нижче, як підтверджуючий приклад викладеного раніше, наведені деякі (частково скорочені) положення Кодексу ділової поведінки та етики [28] Приватного акціонерного товариства «МТС УКРАЇНА» (далі – ПрАТ «МТС УКРАЇНА»).

Отже з Вступу (стиль подальшого викладу і змісту повністю збігається з оригіналом вихідного документа) випливає, що «Кодекс ділової поведінки та етики (далі – Кодекс) містить основні принципи ведення бізнесу. Тому Кодекс ділової поведінки та етики слід розглядати як документ, що містить мінімальний набір стандартів і вимог, прийнятих в Компанії, з метою сприяння чесного і етичного ведення бізнесу і запобігання зловживань. У Кодексі визначено правила і стандарти, якими співробітникам необхідно керуватися в повсякденній роботі».

Під терміном «Співробітники» розуміються всі особи, на яких поширюється дія Кодексу і які повинні бути ознайомлені з Кодексом та дотримуватися викладених у ньому принципів і процедур.

Робочі умови в ПрАТ «МТС УКРАЇНА» викладені в п. 1.1., зокрема:

«У Компанії формується доброзичлива корпоративна культура, атмосфера подяки, турботи і визнання для тих, хто допомагає розвивати бізнес, – наших колег! Компанія зобов'язується дотримуватися всіх чинних законів і правил, які стосуються трудового права, забезпечувати соціальну захищеність співробітників, а також дотримуватися принципу рівних можливостей по відношенню до всіх співробітників, виходячи з їх професіоналізму. Це відноситься до всіх аспектів трудової діяльності, включаючи прийом на роботу, навчання, підвищення по службі, компенсації, дисципліну і звільнення.

Запорука професійного росту співробітників нашої Компанії – якісне і сучасне навчання... ».

В п.1.3 звернута увагу на можливість загроз діяльності підприємства згідно конфлікту інтересів, а саме: «Компанія очікує від кожного співробітника сумлінного виконання своїх обов'язків і не допускає отримання особистих вигод за рахунок займаної посади». Акцентується, що конфлікт інтересів виникає, коли у співробітника є будь-які особисті відносини, фінансові чи інші інтереси, які могли б перешкодити йому діяти в інтересах Компанії, в тому числі неупереджено і ефективно виконувати свою роботу, а також привести до додаткових фінансових збитків для Компанії. Усі співробітники повинні уникати дій або відносин, які суперечать або можуть суперечити інтересам Компанії. Зазначається, що законодавство України поділяє два види конфлікту інтересів – потенційний і реальний:

Потенційний конфлікт інтересів – наявність у особи особистого інтересу в сфері, в якій вона виконує свої службові або представницькі повноваження, що може вплинути на об'єктивність або неупередженість прийняття ним рішень, або на вчинення чи не вчинення дій під час виконання зазначених повноважень.

Реальний конфлікт інтересів – суперечність між приватним інтересом особи та її службовими або представницькими повноваженнями, що впливає на об'єктивність або неупередженість прийняття рішень, або на вчинення чи не вчинення дій під час виконання зазначених повноважень.

Особистий інтерес – будь-який майновий або немайновий інтерес особи, в тому числі обумовлений особистими, сімейними, дружніми або іншими позаслужбовими відносинами з фізичними та юридичними особами, включаючи ті, які виникають у зв'язку з членством або діяльністю в громадських, політичних, релігійних або інших організаціях...

«З метою недопущення можливих ситуацій конфліктів інтересів проводиться щорічна сертифікація керівництва. Також при прийомі на роботу в Компанію Співробітники знайомляться з Політикою «Управління конфліктом інтересів в ПрАТ «МТС УКРАЇНА», заповнюють і підписують форму «Розкриття відомостей про конфлікт інтересів»...».

Тактовно розібрані ситуації, пов'язані з даруванням і отриманням подарунків, а також відвідуванням ділових і розважальних заходів (див. п. 1.4). Прийнято вважати, що «в певних ситуаціях така практика може нести серйозний ризик для бізнесу Компанії. Тому в Компанії діє ряд обмежень, які визначають можливі обставини дарування та прийняття подарунків і запрошень на заходи, а також встановлюють критерії допустимих подарунків і їх одержувачів. У рамках антикорупційної політики в Компанії прийнято окреме Положення «Про подарунки і розважальні заходи », яке повинні знати всі Співробітники Компанії. У Компанії допустимо дарування та прийняття символічних подарунків, властивих звичайній діловій практиці, що відповідають вимогам місцевого законодавства. Українське антикорупційне законодавство забороняє особам, уповноваженим на виконання функцій держави або місцевого самоврядування, отримувати у зв'язку з виконанням службових (посадових) обов'язків не передбачені законодавством України винагороди (позики, грошову та іншу винагороду, послуги, оплату розваг, відпочинку, транспортних витрат) і подарунки від фізичних та юридичних осіб. Використовувати подарунки (так само як і інші види гостинності) будь-якій особі з метою отримання комерційної вигоди і просування бізнесу неприйнятно для ПрАТ «МТС УКРАЇНА». Подарунки та участь у розважальних заходах не повинні ніяким чином впливати на здатність співробітника приймати неупереджені і справедливі ділові рішення. Іншими словами,

подарунки та участь у розважальних заходах ніколи не повинні надаватися в обмін на інформацію, сприятливе ставлення або можливості для бізнесу, які в іншому разі не були б надані.

Подарунки в грошовій формі, а також їх еквівалент (подарункові карти, ваучери, сертифікати) заборонені.

При цьому всі витрати на подарунки та розважальні заходи повинні бути враховані в звітах про витрати....

Дуже детально виписаний п. 1.5. «Конфіденційна, або інформація, що є власністю компанії», у такій редакції: «У процесі роботи в Компанії співробітник стикається з інформацією і матеріалами, що мають конфіденційний характер. Перелік інформаційних матеріалів, що розглядаються як комерційна таємниця, наведено в Політиці «Забезпечення режиму безпеки (конфіденційності) інформації в ПрАТ «МТС УКРАЇНА». Їх захист від несанкціонованого доступу життєво важливий для успіху діяльності Компанії та може мати суттєве значення для збереження робочих місць всіх Працівників.

При прийнятті на роботу в Компанію новий співробітник бере на себе етичне і правове зобов'язання не розголошувати конфіденційну або інформацію, що представляє комерційну таємницю, навіть якщо в подальшому він прийме рішення піти з Компанії.

Рекомендується завжди блокувати робочий комп'ютер, коли ви залишаєте робоче місце. Уважно ставтеся до документів, що містять конфіденційну інформацію, не залишайте їх на робочому місці. Користуйтеся шредером для знищення непотрібної документації, що містить конфіденційну інформацію. Усі Співробітники Компанії повинні добре знати і дотримуватися правил безпеки для захисту конфіденційної інформації від розголошення. Це найдієвіший спосіб уникнути випадкового розкриття конфіденційної інформації».

Серйозну увагу приділено в п. 2.3. боротьбі з фродом[*,35], [31, 32] як поширеним видом шахрайства в області інформаційних

[*35] У контексті того, що викладається, фрод (англ. fraud - «шахрайство») - це вид шахрайства у сфері інформаційних технологій, що реалізується в процесі видалення або модифікації інформації при несанкціонованому втручанні в

технологій, зокрема, у вигляді несанкціонованих дій і неправомірним користуванням ресурсами і послугами у мережах зв'язку і з іншими загрозами у відомстві (див. п. 2.4.).

Зокрема: «Фрод на мережах зв'язку – навмисна діяльність осіб у мережах зв'язку, в тому числі шахрайська, щодо неправомірного отримання послуг і використання ресурсів клієнта і/або оператора зв'язку, без належної їх оплати, неправомірного доступу до службової інформації клієнта і/або оператора, в тому числі з метою отримання прибутку, а також інші дії, спрямовані на заподіяння збитків чи іншої шкоди клієнту та/або оператору. До таких дій, наприклад, відноситься клонування SIM-карт, злом обладнання та генерація трафіку на міжнародні PRS-напрямки, несанкціонований доступ до особистих даних абонентів з метою виведення грошових коштів, несанкціонована термінація міжнародного трафіку. Компанія вживає заходів для боротьби з фродом на мережах зв'язку.

Фрод, пов'язаний з SMS-послугами, фрод контент-провайдерів – це один з найпоширеніших видів фрода на мережах зв'язку, фінансові втрати від яких несуть абоненти. ПрАТ «МТС УКРАЇНА» активно бореться з такими видами фрода. Впроваджено систему, що дозволяє виявляти і фільтрувати шахрайські SMS-повідомлення і SMS-спам, що надходить абонентам ПрАТ «МТС УКРАЇНА» з мереж інших операторів зв'язку, в тому числі і від зарубіжних операторів зв'язку. Проводиться регулярний аналіз скарг абонентів на дії контент-провайдерів. У разі якщо дії контент-провайдера були визнані недобросовісними, до нього застосовуються штрафні санкції.

Фрод з використанням GSM- та ISUP-шлюзів на мережах зв'язку. Компанія проводить постійний контроль з метою виявлення нелегально встановлених на мережі ПрАТ «МТС УКРАЇНА» шлюзів.

Фрод при використанні послуг передачі даних. У Компанії встановлено контроль за підвищеним споживанням послуг передачі даних, у тому числі абонентами, що знаходяться в міжнародному роумінгу.

роботу засобів обробки або передачі даних в інформаційно-телекомунікаційних мережах.

Фрод у роумінгу. Здійснюється контроль за підвищеним споживанням голосових послуг і послуг передачі даних у міжнародному та національному роумінгу, а також контроль підключення абонентам послуг «Міжнародний роумінг», «Міжнародна лінія».

У п.2.4. «Захист персональних даних» відзначено, що «Будучи одним з провідних операторів зв'язку в Україні, ПрАТ «МТС УКРАЇНА» також є великим оператором персональних даних, який одним з перших почав приводити свою систему захисту персональних даних у відповідність до Закону України «Про захист персональних даних», так як конфіденційність абонентської інформації є таким же обов'язком оператора, як і безперервність надання послуги зв'язку.

Співробітники, що працюють з персональними даними, повинні дотримуватися таких правил:

• обробка персональних даних працівника повинна здійснюватися в суворо визначених цілях;

• підставами для обробки персональних даних в роботі ПрАТ «МТС УКРАЇНА» є укладений з абонентом договір, у якому абонент є стороною в договорі, згода абонента на обробку його персональних даних, трудовий договір з працівником;

• передача персональних даних повинна здійснюватися з обов'язковим забезпеченням конфіденційності таких даних і їх захисту від несанкціонованого доступу;

• обробка спеціальних категорій персональних даних не допускається, за винятком деяких випадків, передбачених законом.

ПрАТ «МТС УКРАЇНА» прагне забезпечити своїм абонентам впевненість в надійності Компанії та гарантувати захист їх персональних даних. Політика «Обробка персональних даних в ПрАТ «МТС УКРАЇНА»» визначає принципи, порядок та умови обробки персональних даних абонентів, працівників ПрАТ «МТС УКРАЇНА» та інших осіб, чиї персональні дані обробляються ПрАТ «МТС УКРАЇНА», а також третіми особами за дорученням ПрАТ «МТС УКРАЇНА».

Корпоративна соціальна відповідальність викладена в п. 3.1 цитованого Кодексу, а саме: «Корпоративна соціальна відповідальність в ПрАТ «МТС УКРАЇНА», як важлива складова

стратегії розвитку Компанії, інтегрована в усі рівні Компанії, включаючи продукти, послуги та процеси. Ми будуємо свою стратегію розвитку відповідно до запитів суспільства і споживачів, головною метою, якої є підвищення якості життя людини. Ми розглядаємо корпоративну соціальну відповідальність, як відповідальність за вплив прийнятих рішень і діяльності на суспільство і навколишнє середовище через прозоре та етичне ведення бізнесу, яке:

- сприяє сталому розвитку суспільства, зміцненню здоров'я та підвищенню добробуту людей; - враховує очікування зацікавлених сторін; - інтегровано в діяльність Компанії і реалізується нею на практиці; - відповідає законодавству і узгоджується з міжнародними нормами поведінки; - сприяє підвищенню прозорості Компанії та вдосконаленню системи управління.

ПрАТ «МТС УКРАЇНА» бере активну участь у житті країни, на практиці впроваджуючи принципи корпоративної соціальної відповідальності, реалізує важливі соціальні проекти в галузі медицини, освіти, екології та спорту....».

З позицій захисту і безпеки інформації викладено п. 3.3. «Публічні виступи, заяви і взаємини зі ЗМІ та соціальними мережами», а саме:

«Відділ зв'язків з громадськістю є єдиним підрозділом Компанії, яке має право робити офіційні заяви, прес-релізи, коментарі, а також погоджує всі комунікації представників Компанії, уповноважених взаємодіяти зі ЗМІ.

Співробітникам ПрАТ «МТС УКРАЇНА» категорично заборонено надавати коментарі самостійно. Співробітники повинні бути уважні і дотримуватись певних правил при розміщенні інформації.

У популярних соціальних мережах, таких, як Facebook, «В контакте», Twitter ПрАТ «МТС УКРАЇНА» представлена у вигляді офіційних сторінок. Сторінки адмініструються, модеруються та заповнюються контентом співробітниками Відділу зв'язків з громадськістю. Будь-який коментар від імені Компанії на сторінках може вважатися офіційним і публічним для представників ЗМІ. У разі якщо зі сторінок ПрАТ «МТС УКРАЇНА» в соціальних мережах необхідно донести про запуск

проекту або ініціативи Компанії, така інформація повинна бути передана співробітникам Відділу зв'язків з громадськістю.

Співробітники не повинні розголошувати в соціальних мережах приватну або конфіденційну інформацію про Компанію, співробітників, клієнтів, постачальників або покупців. Необхідно розмежовувати особисте спілкування і спілкування в якості офіційного представника Компанії. Якщо повідомлення є особистим, але відноситься до роботи, варто уточнити, що воно не є офіційною думкою Компанії. У разі звернень до співробітників ПрАТ «МТС УКРАЇНА» користувачів соціальних мереж з претензіями або питаннями необхідно повідомити про це на pr@mts.com.ua. У разі якщо співробітник звернув увагу на скаргу або негативний відгук про ПрАТ «МТС УКРАЇНА» в мережі, він може направити його за тією ж адресою. Співробітники ПрАТ «МТС УКРАЇНА» можуть брати участь в дискусії про продукти ПрАТ «МТС УКРАЇНА» самостійно, але перед цим необхідно повідомити блог-секретаря Компанії (на pr@mts.com.ua, в темі необхідно вказати «Для блог-секретаря») про таку дискусію і узгодити свою участь. Наполегливо не рекомендується брати участь в дискусіях на теми, коментування яких у публічному полі заборонено, як таке, що завдає шкоди репутації Компанії та її капіталізації при появі в ЗМІ. Дане обмеження поширюється на наступні теми:

• технічні несправності мережі, білінгу, послуг і сервісів ПрАТ «МТС УКРАЇНА»;

• публічні вибачення;

• відносини з держорганами і органами місцевого самоврядування, а також дії органів влади, конкурентів і партнерів по ринку;

• інформація про контрагентів і клієнтів;

• інформація про особисте життя співробітників ПрАТ «МТС УКРАЇНА».

Співробітники Компанії – постійні учасники спортивних змагань і марафонів.

Кожен співробітник, як представник ПрАТ «МТС УКРАЇНА», повинен дотримуватися мінімальних стандартів соціально відповідальної поведінки по відношенню до користувачів інформаційного простору.

Всі Співробітники прямо або опосередковано несуть відповідальність за маленьких абонентів Компанії та не повинні сприяти розміщенню і подальшому поширенню шкідливого і протиправного контенту. До такої інформації відносяться неетичні матеріали, що суперечать прийнятим у суспільстві нормам моралі і соціальним нормам: широко поширені в мережі зображення сексуального характеру, порнографія, агресивні онлайн-ігри, азартні ігри, пропаганда нездорового способу життя (вживання наркотиків, алкоголю, тютюну, навмисного розвитку анорексії, булімії), зображення насильства, нанесення шкоди здоров'ю і загрози життю, різних способів самогубства, нецензурна лайка, образи та інша подібна інформація.»

Компанія прагне забезпечити безпечні та комфортні умови праці для своїх співробітників. Однак збереження і підтримання здорової робочої обстановки залежить і від дотримання Співробітниками правил внутрішнього розпорядку.

Дисципліна праці – обов'язкове для всіх Працівників підпорядкування вимогам, встановленим правилами внутрішнього трудового розпорядку, трудовими договорами, в тому числі посадовими інструкціями, а також локальними нормативними актами. За порушення трудової дисципліни (вчинення дисциплінарного проступку), тобто невиконання або неналежне виконання з вини працівника покладених на нього трудових обов'язків, в ПрАТ «МТС УКРАЇНА» можуть застосовуватися дисциплінарні стягнення».

У п.4.3. викладені основи законодавчої політики в області конкуренції та антимонопольного законодавства, а саме: «...Законодавство про захист конкуренції існує у всіх юрисдикціях, де ведуть бізнес компанії Групи МТС. Вимоги такого законодавства зазвичай полягають у захисті вільної конкуренції і забороняють угоди між конкурентами, які ведуть до обмеження конкуренції, а також зловживання домінуючим становищем. Порушення цих положень законодавства може спричинити за собою штрафи та інші цивільні, адміністративні та кримінальні наслідки, аж до тюремного ув'язнення.

У своїй діяльності ПрАТ «МТС УКРАЇНА» і співробітники Компанії ніколи не будуть вступати ні в які переговори або угоди з конкурентами, формальні чи ні, спрямовані на встановлення цін

на послуги або товари, розподіл ринків і подібні дії. Тому співробітники ПрАТ «МТС УКРАЇНА» повинні завжди уникати обміну з конкурентами конфіденційною інформацією, до якої, в першу чергу, відносяться маркетингові плани і стратегії Компанії, а також конкретні плани щодо тарифної політики. Крім угод з конкурентами, законодавство про захист конкуренції також може регулювати взаємовідносини з постачальниками і клієнтами. ПрАТ «МТС УКРАЇНА» завжди прагне до справедливого і рівноправного ставлення з усіма своїми контрагентами у всіх аспектах свого бізнесу ».

Уважно викладено процес ознайомлення і використання інсайдерської інформації (див. п. 4.4), а саме: «Інсайдерська інформація – це інформація про компанію, яка не була публічно розкрита і при розкритті може вплинути на вартість цінних паперів компанії. Відповідно до законодавства у сфері регулювання ринку цінних паперів, співробітникам ПрАТ «МТС УКРАЇНА» забороняється використовувати інсайдерську інформацію:

- для здійснення операцій з цінними паперами, щодо яких така інформація стала відома. Заборона поширюється на операції з цінними паперами не тільки ПрАТ «МТС УКРАЇНА», а й будь-яких інших публічних компаній, які є або були клієнтами, замовниками, постачальниками та іншими контрагентами ПрАТ «МТС УКРАЇНА», а також конкурентами або протилежними сторонами в судових та інших розглядах, і службову інсайдерську інформацію про яких Співробітники отримали у зв'язку з їх роботою в ПрАТ «МТС УКРАЇНА»;

- шляхом передачі її іншій особі, за винятком осіб, яким вона необхідна в силу службових обов'язків і коли така передача дозволена діючими внутрішніми нормативними актами ПрАТ «МТС УКРАЇНА»;

- шляхом надання рекомендацій третім особам, що спонукає їх до придбання або продажу цінних паперів, а також до укладення договорів, які є похідними фінансовими інструментами, ціна яких залежить від таких цінних паперів або товарів.

Це можуть бути, наприклад:

– фінансові показники;

– інформація про угоди, що готуються, про злиття і поглинання (M&A);
– інформація про отримання ліцензії на вид діяльності;
– інформація про плановані дивіденди;
– інформація про великі судові розгляди...

...Співробітники ПрАТ «МТС УКРАЇНА», що володіють інсайдерською інформацією про ПрАТ «МТС УКРАЇНА», не повинні здійснювати операції з цінними паперами ПрАТ «МТС УКРАЇНА», передавати інформацію для здійснення таких угод або здійснювати аналогічні дії з інсайдерською інформацією про інші компанії, яка отримана внаслідок виконання посадових обов'язків».

Аспекти прозорості бізнесу і достовірного розкриття інформації, включаючи і облікові документи компанії викладені в п. 4.5 і п. 4.6, а саме: «ПрАТ« МТС УКРАЇНА» є приватною компанією і має згідно із Законом України надавати звіти про свої фінансові результати, а також розкривати значний обсяг фінансової та іншої інформації про свій бізнес засобам масової інформації, Комісії з цінних паперів і фондовому ринку, Антимонопольному комітету України та іншим органам.

Співробітники, відповідальні за ведення облікових записів і надання даних для складання звітності, повинні гарантувати, що всі господарські операції відображаються у фінансових звітах і поясненнях до них повністю, точно, своєчасно і в зрозумілій для користувачів формі.

Згідно застосовуваним правилам і нормам, ПрАТ «МТС УКРАЇНА» має негайно розкривати точну і повну інформацію про свій бізнес, фінансовий стан і результати діяльності. Неточна, неповна і несвоєчасна звітність з боку Працівників неприпустима, оскільки це може привести до серйозного збитку, юридичної, фінансової чи іншої відповідальності ПрАТ «МТС УКРАЇНА».

Розкриття інформації здійснюється з дотриманням розумного балансу між інформаційною прозорістю та забезпеченням комерційних інтересів Компанії. Для дотримання вимог законодавства, порушення яких може стати причиною істотних фінансових втрат і кримінального переслідування, як

Компанії, так і окремих співробітників, кожен співробітник повинен виконувати свою роль щодо участі в системі розкриття інформації. При цьому публічне розкриття інформації допускається лише особами, уповноваженими на це керівництвом Компанії, що закріплено внутрішніми документами Компанії.

У ПрАТ «МТС УКРАЇНА» єдиним підрозділом Компанії, який має право робити офіційні заяви, прес-релізи, коментарі, а також погоджує всі комунікації представників Компанії, уповноважених взаємодіяти зі ЗМІ, є Відділ зв'язків з громадськістю.

...Керівництво Компанії визначає склад, обсяг і порядок захисту інформації, що становить комерційну і службову таємницю. Обов'язок забезпечувати збереження конфіденційної інформації лежить на всіх співробітників компанії. Якщо запитувана інформація не є конфіденційною, вона підлягає розміщенню у відкритому доступі в засобах масової інформації, на офіційному сайті Компанії і т. п., посилання на які можна відправити знайомому співробітника ПрАТ «МТС УКРАЇНА».

Співробітникам може стати відома інформація про випадки несвоєчасного звітування, про які вони повинні повідомити в порядку, передбаченому цим Кодексом. До прикладів підозрілих обставин, про які слід повідомляти, відносяться:

- фінансові результати, які виглядають невідповідними щодо показників угод, у результаті яких вони отримані;
- неточності в облікових документах ПрАТ «МТС УКРАЇНА», такі як:
- завищення витрат у звітах і спотворення рахунків або неточний облік робочого часу;
- угоди, які здаються необґрунтованими з комерційної точки зору;
- прохання обійти звичайні процедури розгляду і затвердження угод чи інших дій, прийняті в ПрАТ «МТС УКРАЇНА».

Відносно облікової документації слід пам'ятати, що «Облікові документи повністю і точно відображають господарські операції, здійснювані Компанією, є основою для

складання різного роду звітностей і розкриттів інформації відповідно до вимог чинного законодавства та виходячи із загальноприйнятої практики.

Облікові записи є джерелом даних, що забезпечують прийняття важливих управлінських рішень щодо подальшого розвитку Компанії.

До облікових документів належать фінансова і управлінська звітність, облікові політики, первинні облікові документи, що підтверджують факт здійснення господарської операції, рахунки-фактури, документи про проведення перевірок фінансово-господарської діяльності, розрахунки по нарахуванню заробітної плати і багато інших.

Усі облікові документи ПрАТ «МТС УКРАЇНА» повинні містити повну, точну і достовірну в усіх суттєвих аспектах інформацію і відповідати всім діючим стандартам, законам і регламентам щодо бухгалтерської та фінансової звітності по угодах, кошторисах та прогнозах. Не повинні проводитися або затверджуватися неправильні, неповні, неточні або такі, що вводять в оману, угоди або записи в облікових документах. Крім того, суворо забороняється наявність в Компанії нерозкритих, неврахованих або неточно врахованих коштів, платежів або виручки.

У Компанії діють затверджені політики управління обліковими документами, вимоги до їх оформлення, подання, зберігання, передачі в архів і знищення. При фізичному знищенні документів Співробітники Компанії повинні керуватися наступними принципами:

- знищення завжди має бути санкціоновано;
- документи, пов'язані з майбутніми або актуальними судовими розглядами і розслідуваннями, не підлягають знищенню;
- знищення документів проводиться таким чином, щоб зберегти конфіденційність будь-якої інформації, що міститься в них;
- всі копії документів, дозволених до знищення, включаючи конфіденційні, страхові та резервні копії, також знищуються».

Таким чином, можна стверджувати (з високим рівнем вірогідності та акцентуючи увагу читача на тому факті, що весь Кодекс, викладений на 22 сторінках оригінального тексту, повністю відповідає законодавству України і наслідує загальноприйняті стандарти ділової етики), що безпосередній стан об'єкта інформаційної захищеності залежить від багатьох чинників, включно зі сферою його застосування та деструктивним впливом на потенційно значущі його інформаційні ресурси з боку терористичних і кримінальних структур у вигляді так званого «промислового шпигунства». Причому серед найнебезпечніших атак на інфраструктуру об'єкта, що захищається, слід насамперед вважати реалізацію негативного впливу з боку штатних співробітників цього підприємства, оскільки їм, як правило, відомі основні «больові точки» (вразливості) підвідомчого об'єкта на тлі уявної для них вседозволеності на робочому місці, що підкріплюється наявністю високої ймовірності здійснення таких атак із апріорі найбільшим рівнем їхньої скритності.

7.6. Аспекти профілактики кіберзлочинності в освітній сфері суспільства з позицій академічної доброчесності у вищих навчальних закладах

З раніше викладеного (див. п.7.3. Ключові моменти при підборі персоналу) випливає, що відомі загрози інформаційній безпеці підприємства і сучасні засоби їх захисту не можуть існувати без впливу на них так званого людського фактору, що вимагає (бажано заздалегідь прогнозованого і вчасно реалізованого) забезпечення кадрово-інтелектуальної безпеки. З цієї точки зору обов'язковим є моніторинг рівнів лояльності до кодексу корпоративної поведінки як кандидатів на вакансії, так і працівників підприємства, де управлінські функції кодексу полягає в регламентації

поведінки в складних ***етичних*** ситуаціях. При цьому корпоративна ***етика*** (культура) є складовою частиною організаційної політики функціонування і життєдіяльність будь-якого підприємства.

Нагадаємо, що ***етика*** за своєю родовою приналежністю відноситься до філософського знання поскільки зародилася в межах філософії. Як і філософія має справу з універсаліями, тобто найбільш загальними поняттями (наприклад, добра, зла, совісті, честі тощо) та підтверджує свій філософський характер, оскільки предметом філософського осмислення ***предмету етики*** (тобто ***моралі***) є загальні основи людського буття та відношення до світу в цілому.

В частности, в епоху Нового часу «філософія уподібнювалася людському організмові, де фізика — це «м'язова тканина», логіка — «скелет», етика — «серце». Такий метафоричний ряд підтверджує центральне, головне смислове навантаження саме етики у структурі філософського знання в цілому» [33].

Однак, якщо розглядати етику та філософію крізь призму стосунку частини та цілого, то етика не є однозначно підпорядкованою частиною, сутність котрої визначається сутністю цілого.

На сьогодні ***етика*** це особливе філософське знання, котре не може повною мірою емансипуватися від філософії на зразок цілої низки самостійних наук, що існують, а є «смислоутворюючою частиною цілого (філософії), втрата котрої руйнує смислову значимість цього цілого». ***Завдання етики полягає в тому, щоб не лише описати, пояснити мораль, а й навчити моралі.***

Трактування ***моралі***, виокремлення її своєрідності та призначення визначають ***зміст етики*** (див. рис. 7.5) [34, с.11]. Через призму розуміння моралі як діяльності етика виступає як наука про специфічну форму людської діяльності, філософська теорія моральності. Мораль це: - практично-оцінний спосіб ставлення людини до дійсності, що регулює поведінку людини; - реальне явище, що являє собою основу для людських вчинків; – сукупність вимог, норм, принципів до поведінки людини, її ставлення до інших людей і до себе; – системи мотивацій поведінки людини та ціннісно-смислове ядро культури (див. рис. 7.6) [34, с.12].

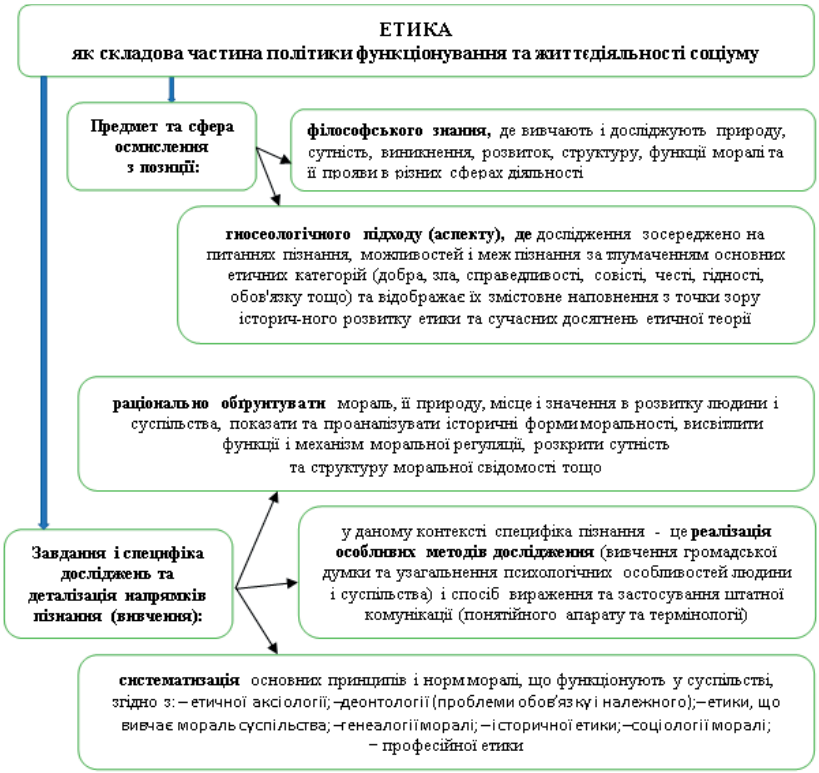

Рисунок 7.5. Специфіка, завдання та філософський підхід до тлумачення основних етичних категорій

До основних ***функцій моралі*** традиційно відносять *регулятивну, виховну, комунікативну*, *пізнавальну*, *світоглядну* (*ціннісно-орієнтаційну), мотиваційну* (гуманістичну) та ін. При цьому поняття моральної свідомості відіграють основну роль у духовно-практичному освоєнні дійсності, відображають моральне життя суспільства і характер людської життєдіяльності.

У свою чергу, від прояви етики у різноманітних сферах людської життєдіяльності, існують ***різні понятійні терміни етики***, наприклад [34]:

- ***етика професійна***, для позначення системи професійних моральних норм, напрямок етичних досліджень стосовно основ

професійної діяльності особи та являє собою систему моральних принципів, норм та правил поведінки спеціаліста із врахуванням особливостей його професійної діяльності та конкретної ситуації;

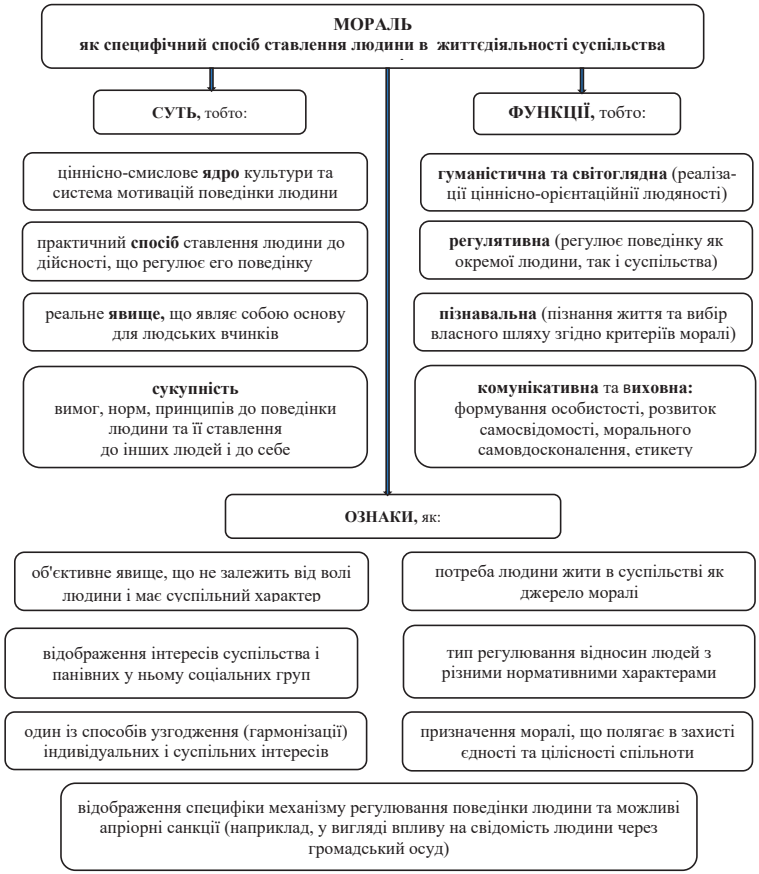

Рисунок 7.6. Розуміння моралі як регулятора людської поведінки та її ознаки

– ***етикет службовий,*** як загальноприйняті (або декларативно встановлені) правила етичної поведінки у професійному спілкуванні в конкретній установі чи сфері; система норм та атрибутів ділового етикету. Даний етикет

спрямований на естетизацію внутрішнього середовища установи, покращення стилю спілкування, дотримання визначених стандартів взаємостосунків, для забезпечення належної субординації між керівниками і підлеглими, піднесення культури партнерських відносин із суб'єктами зовнішнього співробітництва, належних способів формування іміджу організації.

Очевидно, що кожному з нас, свідомо чи ні, доводилося (або доводиться) робити моральний вибір щодо системи цінностей і способів їх реалізації в процесі своєї життєдіяльності в соціумі, де під впливом цього середовища поступово формується власний для нас ідеал. При цьому, освіченість, як основа моральної діяльності, кожної конкретної людини насамперед формується за рахунок [35]:

- світогляду дитини, що залежить від сформованих у сім'ї стосунків із соціумом і її (дитини) майбутнього в ньому;

- оволодіння строго визначеними соціальними навичками і манерою поведінки залежно від обставин існування в конкретному суспільстві;

- гідної освіти та самоосвіти за використання сучасних методів соціальної інженерії та навчання.

Причому кожен індивідуум цілеспрямовано або мимоволі знаходить і використовує строго певні соціальні навички, заготовлені відповіді, манери поведінки, які йому, як правило, нав'язують життєві обставини існування в конкретному соціумі. Це відбувається постійно, і повсюдно, і яке не слід ігнорувати, - бо інакше була б відсутня як адаптація в соціальному середовищі, так і гідне в ньому існування. Тому більшості індивідуумів соціуму, незалежно від їхніх природних здібностей і витрачених зусиль, характерне прагнення підніматися, утримуватися й перебувати якомога вище на щаблях соціальних сходів. А починати підйом цими сходами доводиться шляхом засвоєння азів освіченості (тобто сукупності знань, що набуваються, у вигляді набуття професійно-соціальної компетентності як системи адекватно сформованих знань, навичок міжособистісного й ділового спілкування, соціального іміджу, зумовленого не лише особливостями особистості, а й змістом та характером майбутньої професії з її креативністю й пошуком

творчих рішень) та подальших етапів безперервного її (освіченості) збагачення впродовж усієї життєдіяльності особи.

Таким чином, процес освіти набуває соціального характеру (державного, приватного, громадського чи іншого) і впливає як на профілі освіти (від загальної до фахової спеціальної професійної), так і на її рівні (від дошкільного до вищого у вигляді кваліфікацій магістра чи доктора наук), реалізація яких немислима без очевидної спадкоємності, одночасного функціонування та розвитку, які найчастіше використовують дуальність у термінології. При цьому у відриві від роз'яснювального контексту, невизначеність тлумачення понять і термінів у процесі реалізації безперервної освіти проявляється особливо значуще. У зв'язку з цим будь-яка професійна освіта має будуватися на понятійній чистоті використовуваних термінів, яким часто притаманна неоднозначність їхнього тлумачення, а саму неперервну освіту слід розуміти «як лінійне, послідовне сходження щаблями освіти, кожна з яких вирішує свій комплекс завдань. Це дає змогу опановувати щаблі з розривом у часі, обирати тип освіти, тобто змінювати сфери діяльності виходячи з її потреб та інтересів життєвого етапу» [36]. Така цілісність освіти реалізується, перш за все, за рахунок академічнії доброчесності (як «сукупності етичних принципів та визначених законом правил провадження освітньої (освітньо-творчої) та наукової (науково-технічної) діяльності, які є обов’язковими для всіх учасників (суб’єктів) такої діяльності та мають на меті забезпечувати довіру до результатів навчання, творчості, науково-дослідної діяльності» [36] та стабільності (за відсутності

дуалізму) термінології, що забезпечує збереження логіки процесу пізнання розділів класичної науки, в основі яких: - практика - відомий критерій істини.

Однако, велика кількість здобувачів освіти має вельми поверхневе уявлення про академічну доброчесність та не ототожнюють себе як долучених до процесу виконання правил академічної доброчесності, не розуміють в повній мірі своїх обов’язків та подальших наслідків у випадку академічної недоброчесності [37]. На сьогодні у здобувачів освіти, і не тільки технічних спеціальностей, за рідким виключенням, відсутня культура неможливості несамостійного виконання поточного

завдання, відповідей на тести контрольних робіт. Студенти не вважають списування за недолік, а використання поняття «плагіату» сприймають як допустиме цитування та посилання на них в своїх роботах. Але необізнаність студенцтва у відповідних законодавчих актах МОН України, рекомендацій національного агентства із забезпечення якості вищої освіти (НАЗЯВО) [38-40] та обов'язкових внутрішніх положень в кожному ВНЗ, наприклад в [41], не знімає відповідальності. Тож, зокрема, традиційне використання поняття термінів «компіляції» та «плагіату», повинно відповідати конкретній світоглядній матриці сприйняття (менталітету), що забезпечує точність, ясність і розуміння наукової думки, однак у даному випадку це досить проблематично, бо немає загальновизнаного визначення самого поняття «терміна», незважаючи на значну кількість варіантів його смислового визначення. Зокрема, поділяючи точку зору низки вчених, можна погодитися з трактуванням «терміна» як «слова або словосполучення», співвіднесеного зі спеціальним поняттям, явищем або предметом у системі будь-якої галузі знання. Отже, поняття узагальнює пізнання, а термін - класифікує його шляхом конкретного розмежування. Тому, не виходячи за рамки «класичної науки», пропонуємо задовольнятися положеннями наукової парадигми, тобто вибудовувати формулювання сприйняття «терміна» з огляду на його відповідність і науковим критеріям, і ціннісним вподобанням, і фундаментальним законам (вербальним і/або у вигляді математично доказових співвідношень, які акцентують істинність явища, визнаного науковим співтовариством на конкретному етапі розвитку науки), і навіть поняттям у вигляді «уявлень, що містять у собі вимоги сталості, досконалої визначеності, загального визнання, однозначного мовного вираження» [42].

На підставі викладеного вище, з позицій вимог понятійної чистоти в термінології, доцільно розглянути смислову неоднозначність термінів «компіляція» і «плагіат», які в багатьох випадках (наприклад, при виконанні рефератів, курсових і дипломних робіт) сприймаються як синоніми [43].

Нагадаємо, що слово «компіляція» утворено від латинського «compilatio» і буквально перекладається як «пограбування або

крадіжка», але не має (при вказівці авторства першоджерел) негативного характеру на перших та наступних стадіях реалізації безперервної освіти, що необхідно при формуванні, розвитку та засвоєнні процесу пізнання в етичній, природній та професійних сферах буття, що забезпечують гідне становлення того, хто навчається на його ієрархічних сходах. Слово «плагіат» (фр. plagiat від латів. plagiatus – викрадений) раніше трактувалося як наслідування чи копіювання творчості, тобто могло бути віднесеним як до галузі цитування (дослівної частини будь-якого тексту, взятої в лапки) або до ремінісценції (творчого осмисленого) цитування без лапок), які, у свою чергу, не є плагіатом. Однак, у міру запозичення результатів чужої роботи з метою затвердження власного авторства та отримання відповідної вигоди, термін «плагіат» набув негативного характеру. Зазвичай у вигляді важливої складової у протиборстві як з плагіатом, так і з іншими порушеннями прав інтелектуальної власності є відповідна профілактика як на рівні міжнародного співробітництва, так і у процесі професійних дискусій даного профілю. Причому очевидно, що слід підтримати реалізацію як ефективних методів виявлення загальних ознак, так і механізми адекватної боротьби з таким негативним явищем у сучасній освітній та академічній сфері, включаючи і заходи покарання за їх широкого обговорення у відкритому друці з акцентом як на надзвичайну подію в освітньому соціумі.

Нині це явище - це не тільки порушення авторських прав, а й підрив як наукової діяльності, так і брутальне посягання на суміжні права соціуму, передусім у сфері культурних та мистецьких цінностей. Тому боротьба з плагіатом завжди актуальна, а сам «захист авторського права і суміжних прав здійснюється в порядку, встановленому адміністративним, цивільним і кримінальним законодавством» [44, Ст. 50, 51, 52]. При цьому важливою складовою успіху в протиборстві як з плагіатом, так і з іншими порушеннями прав інтелектуальної власності є і відповідна профілактика на рівні міжнародного співробітництва [45, с. 121; 46, с. 288], і значуща конкретизація потенційних порушень академічної доброчесності (доброчесності) в Законі України «Про освіту » [40, Ст.42, п. 4] у вигляді: академічного плагіату, самоплагіату, фабрикації,

фальсифікації, списування, обману, хабарництва, необ'єктивного оцінювання, допомога або створення перешкод здобувачам під час оцінювання їхніх результатів навчання, вплив у будь-якій формі (прохання, вмовляння, вказівка, погроза, примус тощо) на науково-педагогічного працівника з метою здійснення ним необ'єктивного оцінювання результатів навчання. Згідно з [40, Ст.42, п. 2] також озвучено аспекти «дотримання академічної доброчесності педагогічними, науково–педагогічними та науковими працівниками, що передбачає: посилання на джерела інформації у разі використання ідей, розробок, тверджень, відомостей; дотримання норм законодавства про авторське право і суміжні права; надання достовірної інформації про досліджень, методики і результати джерела використаної інформації та власну педагогічну (науково–педагогічну, творчу) діяльність; контроль за дотриманням академічної доброчесності здобувачами освіти; об'єктивне оцінювання результатів навчання».

Крім того, згідно з Кодексом академічної доброчесності та забезпечення якості вищої освіти, Законом України «Про освіту» та внутрішніми ВНЗ-аналогічними положеннями, однозначно спрямованими на викорінення (знищення) плагіату (навмисне привласнення авторства чужого академічного тексту) серед наукових і педагогічних працівників, передбачені [40, Ст. 42, п. 5]: «відмова в присудженні ступеня освітньо-наукового чи освітньо-творчого рівня або присвоєнні вченого звання; позбавлення присудженого ступеня освітньо-наукового чи освітньо-творчого рівня або присвоєного вченого звання; відмова в присвоєнні або позбавлення присвоєного педагогічного звання, кваліфікаційної категорії; позбавлення права брати участь у роботі певних законом органів або обіймати певні законом посади». Тож з огляду на сучасні масштаби плагіату академічного тексту, його шкідливий вітчизняний та міжнародний характер, слід підтримати реалізацію як ефективних методів виявлення загальних ознак, так і механізми адекватної боротьби з таким негативним явищем у сучасній освітній та академічній сфері, включно з заходами покарання за умови їхнього широкого обговорення у відкритому друці з акцентом як на надзвичайну подію в освітянському соціумі.

Відповідно до чого доцільно відслідковувати будь-які прояви плагіату в даній сфері та постійно оптимізувати антиплагіатне програмне забезпечення (АПЗ) з рейтинговою оцінкою оптимальності їх реалізації. Принцип роботи більшості АПЗ зводиться до аналізу критерію технічної унікальності досліджуваного матеріалу за допомогою залучення конкретних програм або онлайн-сервісів із мережі інтернет. В їхній основі, як правило, один принцип дії: розбивка досліджуваного тексту на окремі частини з кількох слів і подальшого використання різних процедур контент-аналізу з підрахунком коефіцієнта Яніса [47]. Зокрема, одним із найпоширеніших вважається метод шинглів [48] (від англ. Shingle - «луска»), де частини з невеликою кількістю слів (це і є шингли), у кожному з яких є і спільні слова, шифруються своїм хешем у вигляді (тільки для нього унікального) набору букв і цифр. При цьому має виконуватися умова, за якої в одному тексті не повинно бути шинглів з одним і тим самим унікальним хешем. Далі реалізується порівняння на їхній збіг із тексту, що підлягає експертизі на плагіат, з аналогічними з базового тексту, обраного, наприклад, за ключовими словами. Очевидно, що чим більше буде зареєстрованих збігів, то нижчою буде оцінка унікальності, хоча й вона може бути піддана сумніву через програмні прорахунки, що виникають через цитування, надмірне використання стандартної термінології, законів, статей і положень законодавчого і галузевого рівнів і т. д., а також авторських хитрощів. У вишівському середовищі заведено орієнтуватися на ресурси, рекомендовані самими ВНЗ. При цьому вимоги щодо оригінальності тексту варіюються в межах 70-80% (для курсових поріг трохи нижчий, для дипломних робіт вищий), а перелік програмних продуктів онлайнівської перевірки стабільно розширюється. Як безкоштовні програми перевірки тексту на плагіат широко використовуються такі: Advego Plagiatus; Etxt Antiplagiat; ANTIPLAGIAT; CONTENT–WATCH; TEXT.RU; UNPLAG; StrikePlagiarism.com та багато інших сервісів [48].

Очевидно, що будь-яка антиплагіатна програмна продукція жодним чином не зупинить розробку ще більш ефективних способів їхнього нівелювання. Зокрема, вже в мережі Інтернет на різних спеціалізованих сайтах розміщено десятки методів обходу

антиплагіату, що дають змогу підвищити оригінальність тексту до 80-90% через нехитрі дії з документом. Як бачимо, студентство та їхні «співчуваючі» не дрімають, що слід враховувати і навіть частково вітати: у такий спосіб розширюється освітня база та її пізнавальні галузі. Наприклад, для пошукової оптимізації SEO (search engine optimization) можлива розробка комплексу заходів, спрямованих на оптимізацію конкретного сайту за цільовим пошуком, зокрема й антиплагіатного спрямування, користувацьких запитів, зокрема й поради щодо відбиття інформаційної атаки.

Таким чином, на відміну від плагіату, обов'язковою ознакою якого є присвоєння авторства, компіляція в сучасній безперервній освіті заслуговує на виправдання при чіткому зазначенні конкретних даних про першоджерела, особливо тих, які забезпечують необхідне пізнавальне орієнтування в термінологічному просторі професійного соціуму. В якості ж профілактики та повного викорінення академічного плагіату необхідно розвивати програмно-захисні заходи по виявленню та припиненню крадіжки інтелектуальної власності. У відсутності до нашого часу штучного інтелекту, гіпотетично призначеного для безпомилкового виявлення плагіату академічного тексту та оцінки його вагової сутності, слід очікувати як зростання антиплагіатних заходів, так і відповідного їм протиборства. но головне у цій галузі освіти – це виховання нетерпимості до плагіату як ганебному прояву слабкості людини, претендує високий інтелектуальний рівень, а тим паче відповідального за педагогічну діяльність.

Проте, на жаль, інтенсивність поширення плагіату розширюється і значною мірою підживлюється у процесі надання різного виду комерційних послуг у сфері освіти: від написання та продажу рефератів, курсових та дипломних робіт, аж до рівня дисертацій на здобуття доктора наук. Очевидність наявності корупційної складової при цьому не потребує доказів у сучасному соціумі. Стосовно особистості корупціонера часто розглядається лише його потяг до хабарно-залежного комплексу, що призводить у своїй заключній стадії до «придбання форми взяткоманії, пояснюючи, що сучасний соціум, в умовах роздвоєння між реальним та віртуальним, об'єктивно схильний

до "трансформації різних структур особистості" - їх установки, цілі, мотиви і т.д. Причому, якщо відсутня можливість такого збагачення, то депресивний синдром «скасування» через відсутність такої дози тривожно турбує, на противагу радісній ейфорії, коли вона отримана. Звідси – найчастіше виникають і виправдувальні мотивації, які базуються на тому, що «***манія***» - це психічно-інстинктивний процес потягу до придбання певної конкретної цінності без реалізації особистісних витрат на її придбання і, отже, до неї необхідно ставитися до якоїсь хвороби, яка потребує відповідного лікування. У зв'язку з цим у вишах часто не аналізують причини наявного плагіату, списуючи його на результат прояву психічної патології - клептоманії [49], яка підвладна лише медицині. На щастя, це явище абсолютно не притаманне нашому університету, що переконливо підтверджується, наприклад, низкою публікацій [50-54]. Проте, тим не менш, згідно з соціологічними дослідженнями, люди, які часто спілкуються з керівниками, схильними до проявів таких «маній», самі, згідно з технологією соціальної інженерії, швидко набувають досвіду вседозволеності та, врешті-решт, можуть завдати серйозної шкоди репутації свого вишу. То як же бути і що виділити у проблемі знищення академічного плагіату?

З боку педагогічного соціуму насамперед, детально з'ясовуючи причини виникнення плагіату, без формальної оцінки вже існуючих та реалізованих заходів профілактики не дивлячись на передбачені (у тому числі і на законодавчому рівні держави різні види покарання), необхідно поновлювати матеріально-технічну базу навчальних закладів та знаходити хоча б часткове фінансування публікацій, що індексують у Scopus, Web of Science, або при отримання патенту. Крім того потрібно більше уваги приділяти як пізнавальної сфері особистості, здійснюючи об'єктивну експертизу її публікацій, а й оцінювати її психічний стан у процесі зміни соціально-економічної, політичної, педагогічної та інших форм буття. Також очевидно, що для забезпечення психологічної безпеки освітньої сфери не існує однозначного алгоритму з апріорного виявлення схильностей щодо реалізації плагіату, оскільки особистісні, поведінкові, емоційні мотивації та зовнішні зміни (щодо трудомісткості поставлених завдань, стресонебезпечності та рівня професійного

навантаження, емоційної діяльності навантаженості) принципово неоднозначні, у зв'язку з чим і виявляються різні види плагіату: дослівний плагіат, авто- або самоплагіат, плагіат з перефразуванням, неточне авторство, мозаїчний плагіат, випадковий плагіат . При цьому, якщо на чолі кута не визнана клептоманія, то слід визнати, що реалізація плагіату властиво особам, у яких немає чітких моральних та етичних орієнтирів і вони відчувають власну недооціненість внаслідок нечіткої політики з боку керівництва (насамперед кафедри). Тому необхідно, як профілактику плагіату, підтримувати серед педскладу здорову позитивну мотивацію щодо виконання своїх освітньо-педагогічних, науково-дослідних та виховних функцій. Слід прагнути не допускати виникнення соціальної напруги в колективі, та розбіжності між декларованими та реально реалізованими міжособистісними відносинами з боку керівництва кафедри, де насамперед має сформуватися психологічна атмосфера, за якої плагіат неможливий, як і будь-який інший непристойний вчинок.

З позицій студентського соціуму в рамках формування їх світогляду, що докорінно не допускає явища корупції, необхідне сучасне педагогічне осмислення змісту та реалізація конкретних методів та засобів етичного антиплагіатного виховання. Щоб такий вибір був більш продуктивним, необхідно використовувати об'єктивну інформацію, в нашому випадку, наприклад, опубліковану в роботах [50-54], конструктивний аналіз негативних наслідків яких на законодавчому рівні аргументовано вказує на необхідність реалізації умов виховання серед студентства громадянської відповідальності, правової самосвідомості та моральності. На цій основі (правової освіти та морального відторгнення плагіату), реалізуючи навчальну програму, слід продовжувати як професійну освіту, так і розвиток духовних цінностей соціуму. В результаті, вже незабаром, можливо отримати такий моральний настрій мислення та поведінки студентства, який не здатний принести собі, навколишнім і середовищі усвідомлену шкоду.

Таким чином, головне в галузі освіти – це не лише підготовка професіоналів, а й формування їхнього антикорупційного світогляду. Тому, за аналогією з клятвою Гіппократа, у кожному

ВНЗ. Наприклад у [41] слід запроваджувати відповідний Кодекс доброчесності, взявши за основу рекомендації Національного агентства із забезпечення якості вищої освіти [38, 39], та, побудувавши таким чином, деякі рамкові угоди не лише з педагогічним, а й студентським колективом, що легко можна реалізувати шляхом чіткого розмежування понять компеляції, плагіату, цитування та інших аналогічних творчо-професійних аспектів, забезпечуючи захист від занурення нашої освітньої сфери у світ різних «аддікцій (залежностей): нарко-, алко-, ігро-, фанато-, бого-, клепто-, хабаро-, кредито-, нафто-, доларо-, інтернет-маній. Більше того, вінцем такого формування світогляду (і не лише у студентства) слід вважати таку набуту здатність подальшого вдосконалення та самореалізації, при якій обирається конкретна ідеологія чи релігія та здійснюється гідна ієрархічна упорядкованість різних видів життєдіяльності (виробничих, економічних, політичних, етичних та інших). В даному випадку - це виховання прояву нетерпимості до будь-якого виду плагіату як ганебного прояву слабкості людини, яка претендує на високий інтелектуальний рівень, а тим більше для індивіда, який претендує або вже відповідає за педагогічну діяльність.

Контрольні запитання до Розділу 7

1. Що таке ситуаційний (адаптивний або альтернативний) менеджмент?
2. Які прийнято розглядати етапи розвитку проблемної ситуації?
3. Що прийнято розуміти під звичайною виробничою ситуацією, кризовою та надзвичайною ситуаціями?
4. Поясніть суть концептуальної моделі ситуаційного менеджменту
5. Які основні чинники формують реакцію особи що приймає рішення щодо проблемної ситуації?
6. Поясніть поняття соціальної інженерії в сучасної інфраструктури
7. Що таке фрод на мережах зв'язку?

8. Які механізми впливу під час реалізації хакерських атак з метою досягнення необхідного інформаційного впливу можуть використовувати зловмисники з арсеналу соціальної інженерії?
9. Що таке етичний («білошапочний») хакінг і які використовують при цьому етапи

для виявлення потенційних вразливостей сучасної інфраструктури?

10. Що таке крекері та з якою метою вони використовують хакінг?
11. Що таке інсайдер і які існують їхні види (групи)?
12. Що розуміють під кадрово-інтелектуальною безпекою?
13. Поясніть ключови моменти, що визначають кадрову безпеку організації
14. Що таке потенційний конфлікт інтересів та реальний конфлікт інтересів?
15. Що таке рекрутинг, із яких етапів він складається?
16. Поясніть, що таке моніторинг рівнів лояльності, організаційні та міжособистісні конфлікти?
17. Що таке Кодекс корпоративної поведінки та его основні функції?
18. Ваше розуміння етики (професійної, службової, юридичної) та моралі як регуляторів людської поведінки
19. Що таке академічна доброчесність (недоброчесность), компіляції, плагіат, допустиме цитування та посилання при формуванні, розвитку та засвоєнні процесу пізнання в етичній, природній та професійних сферах буття?
20. Що таке антиплагіатне програмне забезпечення та метод шинглів?

Список використаних джерел під час підготовки тексту розділу 7

1. * Василенко В.О., Шостка В.І. Ситуаційний менеджмент. Нав. пос. – К.: ЦУЛ, 2003. - 356
2. Концептуально-гносеологічні аспекти інформаційної безпеки (захищеності) з позицій соціальної інженерії [Текст] /

Ю.С.Тарасенко, Соляніков В.Г., Калюжний О.Е. // Системи та технології. – 2020. – № 2(60). С. 92-101.

3. Зниження стороннього деструктивного кібернетичного впливу за допомогою соціальної інженерії. / Тарасенко Ю.С. Кузьменко Д.С. // International scientific conference "Innovative technologies, models Cyber Security Management, ITCSM-2020 ANNUAL SCIENTIFIC CONFERENCE ITCSM-2020 Dnipro, 2020. с. 96-98.

4.** Кузнєцов, М.В. Соціальна інженерія та соціальні хакери / М.В.Кузнєцов, І.В.Сімдянов. – СПб.: БХВ-П, 2007. – 368 с.: іл.

5.* Стюарт, І.; Джоїнс В. Сучасний транзактний аналіз - 2 видання / пров. з англ. Дмитра Касьянова. - СПб.: Метаною, 2017. - 444 стр. с ил. ISBN 978-5-901724-24-8

6.** Породін Д. Захист ключових систем інформаційної інфраструктури Журнал "Information Security / Інформаційна безпека " №3, 2012. АМТ-ГРУП, ЗАО. М., E-mail: info@amt.ru www.amt.ru.

7.*** Думки про ідеальну анонімність / Блог компанії Whoer.net, ...https://habr.com › company › whoer › blog. 13 04. 2016 г.

8.* Бурячок, В. Л. Інформаційна та кібербезпека: соціотехнічний аспект. [Підручник]. / В. Л. Бурячок, В.Б. Толубко, В. О. Хорошко, С. В. Толюпа /. Львів: «Магнолія 2006», 2018 – 320с.

9.* Поташніков А.М. Методи виявлення та відстеження об'єктів у системах відеоспостереження на основі систем комп'ютерного зору // Технології інформаційного суспільства. Зб. "Технології інформаційного суспільства". М.: ТОВ «ІД Медіа Паблішер», 2017 с.149.

10.* Тарасенко Ю.С. Фізичні основи радіолокації. Дніпро: Пороги, 2011. 487 с.

11. Яшин М.В., Толмачов А.А. Методи розпізнавання образів з метою оцінки характеристик пішохідних потоків // Технології інформаційного суспільства. Там же «ІД Медіа Паблішер», 2017 с.466.

12. * Грем Деніел Г. Етичний хакінг. Практичний посібник зі злому. - СПб.: П., 2022. — 384 с.

13.* 2021 by Daniel G. Graham. Ethical Hacking: A Hands-on Introduction to Breaking In, published by No Starch Press Inc. 245 8th Street, San Francisco, California United States

14** Згідно: А.Рябчук, Т.Хурцидзе. «Застосування дискурс-аналізу в сучасних соціальних дослідженнях». ISSN 2617-9067. Наукові записки НаУКМА. Соціологія. 2023. Том 6. С. 3-15. Мета визначення дискурсу (дискурсаналітичного дослідження) – це охарактеризувати, як сконструовано звичне/«природне»/будь-яке знання або об'єкт, та деконструювати його. С. 12.

15. Махмудова І.М., Методи забезпечення кадрової безпеки під час добору персоналу: організація бізнес-процесу. Економічні науки Випуск № 11(65) Листопад 2017

16. Бакшт, К. Вербування: альтернативний варіант підбору персоналу / К. Бакшт // HR-portal. – [Електронний ресурс] URL.: http://hr-portal.ru/article/verbovka-alternativnyy-variant-podbora-personala. Дата обращения 29.08.2017

17. Бєляєв, С. Агресивний рекрутинг: Партизанські методи підбору персоналу / С. Бєляєв // HR-portal. – [Електронний ресурс] URL.: http://hr-portal.ru/article/agressivnyy-rekruting-partizanskie-metody-podbora-personala Дата обращения 27.08.2017

18. Бізнес-розвідка: законні методи та заборонені прийоми [Електронний ресурс] – URL.: http://hr-portal.ru/article/biznes-razvedka-zakonnye-metody-i-zapreshchennye-priemy. Дата обращения 27.08.2017.

19. Роз'яснення «Питання, що стосуються обробки персональних даних працівників, претендентів на заміщення вакантних посад, і навіть осіб, які у кадровому резерві» // [Електронний ресурс]. URL: http://www.rsoc. Дата обращения 01.04.2013.

20. Ющенко, Д. Вербування у бізнесі / Д. Ющенко, Н. Царьова // Кадровик. Рекрутинг для кадровика. - 2012. - № 12. [Електронний ресурс] URL: http://hr-portal.ru/article/verbovka-v-biznese. Дата обращения 29.08.2017

21. Bossong, R. EU cooperation on terrorism prevention and violent radicalization: frustrated ambitions or new forms of EU security governance? / R. Bossong // Cambridge Review of International Affairs. – 2014. – № 27 (1). – P. 66-82

22. Camacho, E.T. The development and interaction of terrorist and fanatic groups / E.T. Camacho // Communications in Nonlinear Science and Numerical Simulation. – 2013. – № 18 (11). – P. 3086-3097

23. Jeff Haden Інтерв'ю під прикриттям. Хитрий спосіб говорити кандидата / Haden Jeff // HR-portal. – [Електронний ресурс] URL: http://hr-portal.ru/blog/intervyu-pod-prikrytiem-hitryy-sposob-razgovorit-kandidata . Дата обращения 27.08.2017

24. Скриль, В.В. Методи відбору персоналу для підприємства як інструмент реалізації кадрової політики / В.В. Скріль. – [Електронний ресурс]. - URL.: http://sci-article.ru/stat.php?i=1429596549. Дата звернення 27.08.2017.

25. Організація підбору персоналу: типові проблеми та помилки // Директор з персоналу. №8. 2016. - [Електронний ресурс]. – URL.: https://www.hr-director.ru/article/66205-qqq-16-m8-02-08-2016-organizatsiya-podbora-personala-predpriyatiya. Дата обращения 29.08. 2017.

26. Корольова, Н. Як швидко підібрати десятки чи навіть сотні співробітників. Використовуйте для масового підбору нестандартні та дієві методи / Н. Корольова, // Директор з персоналу. №9. 2013. - [Електронний ресурс]. – URL.:http://e.hr-director.ru/article.aspx?aid = 317825& utm_medium=refer&utm_source=e.hr-director.ru&utm_campaign=e.hr-director_ 7Block&utm_content=7. Дата обращения 02.08. 2017

27. Hofmann, D.C. Quantifying and qualifying charisma: a theoretical framework for measuring the presence of charismatic authority in terrorist groups / D.C. Hofmann // Studies in Conflict and Terrorism. – 2015. – № 38 (9). – P. 710-733)

28. Бочаєва Г. В. Кодекс корпоративної поведінки як елемент системи корпоративного управління// Молодий учений. — 2016. — №10. — С. 630-634. — URL https://moluch.ru/archive/114/30047/ (дата обращения: 07.07.2018).

29. Костіков І. В. Кодекс корпоративної поведінки. Корпоративна поведінка/ За заг. ред. І. В. Костікова. - М.: Економіка, 2014.

30. Гришина Н. В. Організація комплексної системи захисту інформації. - М.: Геліос АРВ, 2007. – 256 с.

31. Голдовський Ігор Ще раз про фроду. Чергові кроки міжнародних платіжних систем, спрямовані на підвищення безпеки карткових транзакцій // Журнал "ПЛАС". 2009. № 2(142). С. 3-5.

32. Голдовський Ігор Ще раз про фроду. Частина II. Мощування у сфері обслуговування карт // Журнал "ПЛАС". 2009. № 3(143). С. 9-19.]

33.* Етика. Естетика. [текст]: навч. посіб. / за наук. ред. Панченко В. І. – К.: «Центр учбової літератури», 2014. – 432 с.

34. Адаптовано згідно Етика та естетика: навчально-методичний посібник (у схемах і таблицях) / за наук. ред. проф. В. С. Бліхара. Львів: ПП «Арал», 2018. 204с.

35.* Тарасенко Ю.С., Клим В.Ю., Смирнов В.В. Plagiat as an Element of Negative and Criticality of Such Education «Science and education for sustainable development. Part 2. Innovative and Information Technologies in Education: Applied Aspects».p.665-674. 20-21 січня 2022 р. Monograph 50. Publishing House of University of Technology, Katowice, 2022.

36. Лаптєва О. І. Історико-наукові передумови визначення поняття безперервної освіти. Професійна освіта у сучасному світі. №3 (18), 2015. С. 39 – 47. с. 44.

37.** Закон України. Про академічну доброчесність. URL: https://naqa.gov.ua/wp-content/uploads/2020/12

38. Кодекс академічної доброчесності Національного агентства із забезпечення якості вищої освіти. URL: https://naqa.gov.ua/wp-content/uploads/2019/07/Кодекс-академічної- доброчесності.

39. Рекомендації для закладів вищої освіти щодо розробки та впровадження університетської системи забезпечення академічної доброчесності URL: https://naqa.gov.ua/wp-content/uploads/2019/10/Рекомендації-ЗВО-система-забезпечення-академічної-доброчесності.

40. Про освіту: Закон України від 05.09.2017 р. Вісник Верховної Ради. 2017. № 38□39.

41 Положення про академічну доброчесність та етику академічних взаємовідносин в Університеті митної справи та фінансів URL: http://umsf.dp.ua/index.php/about/publichna-informatsiia/dobrochesnist.

42* Зігварт Х. Логіка. Том 1: Вчення про судження, поняття та виведення / пров. з ним. І. А. Давидова. М: Видавництво. будинок «Територія майбутнього», 2008. 464 с.

43**Формування антиплагіатного світогляду в освітній сфері суспільства Ю.С.Тарасенко, В.Ю.Клим

44.* Про авторське право і суміжні права: Закон України від 23.12.1993 № 3792-XII. Відомості Верховної Ради, 1994. № 13.

45. Семенюк Т.В. та ін. Академічна доброчесність у сучасному цивілізованому світі та в Україні. International scientific conference «International scientific integration '2021»: conference proceedings. Series «SWorld–US Conference proceedings». No 8, Washington, October 19. USA, 2021. P.121 – 130.

46. Ульянова Г.А. Поняття та ознаки плагіату за законодавством держав - учасниць СНД. Науковий вісник Ужгородського національного університету, Серія ПРАВО. Вип. 21. Част. II. Т. 1. 2013. С.286 – 288

47.** Абраров Р. Д. Розробка методів пошуку плагіату. Текст: безпосередній. Молодий вчений. 2016. № 12.4 (116.4). С. 5 – 7. URL: https://moluch.ru/archive/116/32119/ .

48. Антиплагіату.Ні: веб-сайт. URL: https://antiplagiatu.net

49. Ткаченко Т. (2015) Медичний діагноз: клептоманія. Фармацевт Практик. Доступ он-лайн: https://fp.com.ua › meditsinskiy-diagnoz-kleptomaniya

50.* Ю.С.Тарасенко, В.Ю.Клим, С.В.Гарагатая. Актуальність освітньо-професійного процессу з позицій академічної доброчесності. Збірник матеріалів міжнародної наукової конференції «Інноваційні технології, моделі управління кібербезпекою - «ІТМК-2021», Дніпро, 13 – 15 грудня 2021 р. С. 32 – 34.

51. Ю.С.Тарасенко, В.Ю.Клім, Є.І.Панченко. Парадигма термінології: компіляція та/або плагіат. Participation in the IV International Scientific and Practical Conference International Scientific Discussion: problems, tasks and prospects. February 19-20, 2022. Brighton, Great Britain. https://www.interconf.top info@interconf.top.

52. Ю.С.Тарасенко, В.Ю.Клім, С.В.Гарагатая. Пізнавальний процес освіти без плагіату. VI International Scientific and Practical

Conference Scientific Community: interdisciplinary research held on January 26-28, 2022 in Hamburg, Germany.

53. Тарасенко Ю.С., Клим В.Ю., Смирнов В.В. Plagiat as an Element of Negative and Criticality of Such Education Міжнародна наукова конференція «Science and education for sustainable development. Part 2. Innovative and Information Technologies in Education: Applied Aspects. p.665-674. April 5 – 6, 2022. Monograph 50. Publishing House of University of Technology, Katowice, 2022.

54. Ю.С.Тарасенко, В.Ю.Клим. Формування антиплагіатного світогляду в освітній сфері суспільства. International Conference «Science and education for sustainable development. Part 2. Innovative and Information Technologies in Education: Applied Aspects». Publishing House of University of Technology, Katowice, 15.09.22. Monograph.

8. ОСНОВИ СТРАТЕГІЧНОГО МЕНЕДЖМЕНТУ КАДРОВОЇ АТЕСТАЦІЇ ПРИ ДОСЯГНЕННІ ПОЗИТИВНОГО ЕФЕКТУ В ІНФОРМАЦІЙНО-ЛОГІСТИЧНІЙ БЕЗПЕЦІ ОРГАНІЗАЦІЇ

8.1. Визначення поняття інформаційної логістики та стратегічного управління

Доцільно нагадати (см. рис.1.6), що «залежно від сфери дії виділяються різні види менеджменту: загальний або адміністративний, галузевий, організаційний, функціональний, підприємницький, міжнародний та інші. Зокрема, можна вести мову про маркетинговий менеджмент, фінансовий, кадровий, виробничий (операційний), транспортний, ситуаційний, ***стратегічний менеджмент*** тощо» [1]. При цьому (див. п.4.4), розвиток управління підприємств різної сфери діяльності дозволяє розглядати нові самостійні галузі управління, пов'язані з управлінням інформаційними ресурсами, впровадженням і використанням інформаційних технологій в діяльності підприємств і організацій, управлінням процесами опрацювання інформації в організаціях [2, с. 9]. Тобто в Україні в різних галузях народного господарства, використовуя терміни

«менеджмент» та «управління», дуже часто ці поняття ототожнюють, що призводить до плутанини.

На думку авторів [3,4] управління є цілеспрямованою дією на об'єкт (наприклад, технічними системами, літаком, комп'ютерними мережами тощо) з метою змінити його стан або поведінку у зв'язку зі зміною обставин. Менеджмент є різновидом управління та означає управління людьми (працівниками, колективами працівників, групами, організацією та ін.). При цьому, важливу роль в управлінні відіграють принципи менеджменту маркетингу і логістики, які тісно пов'язані між собою. Відмова від одного чи декількох принципів або неналежне їх врахування в управлінні знижує якість управлінських рішень [5] [*,36],.

На жаль, у науковій літературі не існує єдиного визначення поняття “логістика”. Лише у вітчизняних літературних джерелах їх налічується понад три десятки [6]. Тоді, в контексте даного навчального посібника, логíстика (англ. logistics, від грец. λογιστική — облік) може розглядатися як: оптимальне управління матеріальними, інформаційними та фінансовими потоками в економічних адаптивних системах із синергічними зв'язками; або функція в корпорації, завданням якої є забезпечення переміщення та зберігання продукції та сировини для забезпечення виробництва та продажу.

Оскільки логістика охоплює комплексне (див. рис. 8.1) управління *матеріальними та інформаційними потоками* в межах системи макро-мето-микрологістики, необхідно з’ясувати ці межі як види функціональних галузей логістики: закупівельну, виробничу, розподільчу, транспортну та інформаційну.

Остання (інформаційна логістика) тісно пов’язана з усіма іншими функціональними галузями логістики та забезпечує організації інформаційних потоків всередині підприємства, а

*[36] Згідно [5]: «Управління - це суспільний інститут, створений людьми. Сутність його полягає у взаємозв'язках, взаємодії та взаємодопомозі людей у розв'язанні особистих, суспільних і планетарних завдань. Якщо в земній природі, у рослинному і тваринному світі, у космосі відбувається об'єктивна саморегуляція, то людина, створивши свій світ, повинна свідомо регулювати процеси, що відбуваються в ньому».

також товарно-матеріальних цінностей, які розглядаються в часовому інтервалі при виконанні логістичних операцій.

Управління матеріальними потоками в логістиці пов'язане з плануванням, регулюванням, контролем, обліком та аналізом. Кожна з цих позицій є функцією логістики з певними завданнями, які, у свою чергу, поділяються на операції.

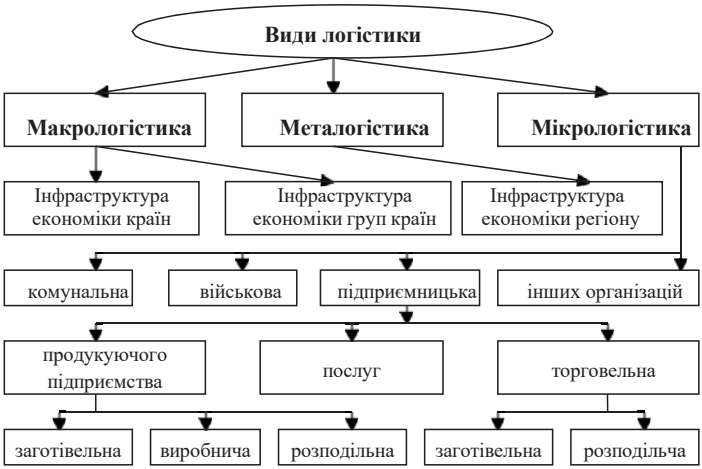

Рисунок 8.1. Види функціональних галузей логістики згідно [6]

Інформаційний потік — це сукупність інформації (зовнішньої, внутрішньої), необхідної для управління логістичними операціями і їх контролю. Інформаційний потік відповідає матеріальному і може здійснюватися у вигляді паперових і електронних документів. При цьому необхідно усвідомити, що основна мета інформаційної логістики полягає в забезпеченні логістичних систем інформацією в потрібний час потрібного обсягу й у потрібному місці. Тому інформаційні потоки можуть мати важливе самостійне значення для оперативного управління і вироблення стратегічних рішень, а можуть відповідати матеріальним і управляти ними. Різниця швидкостей матеріальних та інформаційних потоків може за наявності відповідності призводити до часового зсуву між ними.

Для обробки інформаційних потоків сучасні логістичні системи мають у своєму складі інформаційний логістичний центр. Завдання такого центру - накопичення одержуваних даних та їх прагматична фільтрація, тобто перетворення на інформацію, необхідну для вирішення логістичних завдань. При цьому зв'язок центру з джерелами інформації може бути одностороннім, двостороннім і багатостороннім. Сучасні логістичні системи використовують останній спосіб зв'язку. Таким чином, логістика оперує численними показниками і характеристиками інформаційних потоків:

- номенклатурою переданих повідомлень, типами даних, документами, масивами даних;
- інтенсивністю і швидкістю передачі даних;
- спеціальними характеристиками (пропускною спроможністю інформаційних каналів, захистом від несанкціонованого доступу, перешкодозахищеністю тощо).

Між інформаційним і матеріальним потоком відсутня ізоморфність (тобто однозначна відповідність, синхронність у часі виникнення). Як правило, інформаційний потік або випереджає матеріальний, або відстає від нього. Зокрема, саме зародження матеріального потоку зазвичай є наслідком інформаційних потоків під час, наприклад, переговорів за угодами купівлі-продажу товарів, складання контрактів тощо. Типовим є наявність кількох інформаційних потоків, що супроводжують матеріальний потік. Інформаційні потоки в логістиці утворюються у вигляді потоків масивів електронних даних, певним чином оформлених паперових документів, а також у вигляді потоків, що складаються з обох цих типів (квантів інформації). До такої інформації належать [7]:

- телефонограми і факси та накладні, що надходять разом із товаром;
- інформація про надходження та розміщення вантажів на складах;
- дані про транспортні тарифи, про можливі маршрути і типи транспорту та про зміни в динамічних моделях стану запасів;
- бібліотеки керуючих програм для технологічного обладнання з числовим програмним управлінням і каталоги цих бібліотек;

- різна нормативно-довідкова виробнича інформація;

- зміни в динамічних моделях ринку і в його сегментування;

- поточні відомості про виробничі потужності, про постачальників і продуцентів;

- зміни в динамічних моделях портфеля замовлень та поточні відомості про незавершене виробництво;

- дані про плани випуску, поточні дані про склади, про обсяги та види готової продукції, про фактичний збут продукції та фінансові потоки.

Таким чином, інформація, що створюється, зберігається, циркулює і використовується в логістичній системі, може бути визнана корисною, якщо можливе її включення в поточні виробничо-збутові процеси. Для успішної та ефективної реалізації логістичного управління на основі аналізу інформаційних потоків необхідні певні чинники та передумови, а саме:

- наявність відповідних інформаційних характеристик процесу;

- адекватний рівень систематизації та формалізації процесу логістичного управління;

- організаційні форми і система методів логістичного управління;

- можливість скорочення тривалості перехідних процесів і оперативного отримання зворотного зв'язку за результатами логістичної діяльності.

При цьому деталізацію (селекцію) інформаційних потоків здійснюють за даними: джерел виникнення; напрямку руху (адреси); швидкості передачі та загального обсягу переданої інформації. Причому інформаційні потоки можуть випереджати, відставати або бути синхронними з відповідними матеріальними потоками, а у зв'язку з опрацюванням збільшуваного обсягу інформації, необхідної для планування та контролю логістичних заходів, а також із розвитком комунікацій та комп'ютеризацією господарської діяльності, виникла (як одна з допоміжних підсистем логістики) *інформаційна логістика* з її інформаційними технологіями (див. мал. 8.2, який адаптований згідно [7]) у вигляді: управління даними (datamanagment — DM); електроного обміну даними (electronic data interchange — EDI);

штрихового кодування (barcoding— BC); штучного інтелекту / експертної системи (artificial inteligence/expert systems — AI/ES); дистанційного доступу та комунікації (remote accessand communication — RA&C).

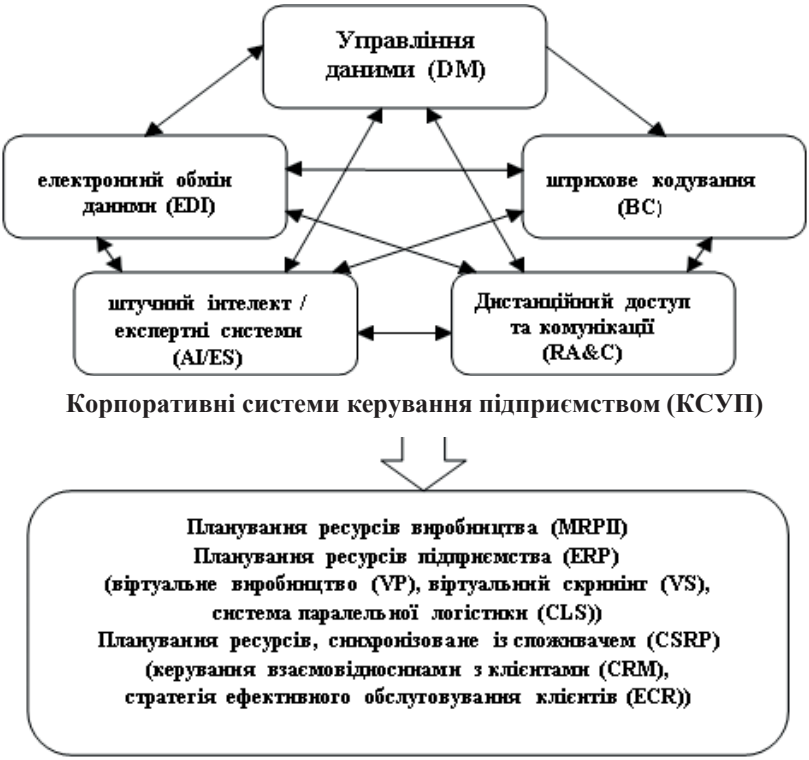

Рисунок 8.2. Сучасні інформаційні технології в логістиці

Управління даними являє собою процес накопичення і систематизації в необхідному обсязі даних (потоку) з метою доступу до них цільових користувачів у потрібний час. Сучасні інформаційні технології орієнтовані не на локально організовані дані, а на бази даних, що являють собою спеціально організоване зберігання інформаційних ресурсів у вигляді *інтегрованої*

сукупності, призначеної для багатоцільового використання і модифікації різними користувачами.

Ці сукупності працюють під управлінням СУБД - системи управління базою даних, основне призначення якої, поряд з управлінням даними, забезпечення доступу до них, організація і зв'язок з користувачем, що значно скорочує і прискорює шлях переміщення продукції від виробника до споживача, зокрема завдяки швидкому переказу інформації як усередині підприємства, так і в зовнішньому середовищі.

Електронний обмін даними. Залежно від фінансової ситуації підприємствам (фірмам) необхідно впроваджувати спочатку внутрішню систему обміну даних за допомогою локальних інформаційних джерел із широким використанням засобів EDI - для виключення паперового обігу документації, а потім за фінансового зростання інтегрувати її з Internet для широкого доступу до можливих клієнтів. Зарубіжний досвід показує, що ті фірми, які роблять ставку на використання стандартів EDI, що функціонують на ринкі, мають шанси ефективного функціонування в майбутньому. Ця необхідність досить лаконічно реалізована у вислові «EDI or DIE», тобто «електронний обмін даними або смерть».

Штрихове кодування - один із видів автоматичної ідентифікації, за якого використовують метод оптичного зчитування інформації, що позначає товар у вигляді комбінації паралельних темних штрихів і світлих смуг згідно з певною системою. Головним завданням позначення товарів штрих-кодами є раціоналізація продажу та розподілу товарів, незалежно від країни їхнього походження, місця збуту та розташування складського господарства.

Дистанційний доступ до комунікації базується на використанні супутникового зв'язку та сучасних комунікацій, що забезпечують аудіо зв'язок у режимі реального часу і дають змогу підприємствам віддалені ринки зробити частиною однієї мережі розподілу.

Програми штучного інтелекту насамперед використовують у процесі телемаркетингу - при прийнятті замовлення та обслуговуванні покупців. Основна їхня перевага в адаптуванні спілкування із замовником телефоном до реальної

ситуації під час персонального продажу. При цьому менеджер за допомогою комп'ютера отримує підказки про цінові знижки, можливості доставки, пропозиції заміни за відсутності необхідного товару на підприємстві, перелік товарів, що регулярно купуються, тощо.

Узагальнюючи сказане, можна констатувати, що сучасні інформаційні системи в логістиці сприяють (призначені для) швидкої адекватної реакції на вимогу ринку, забезпечуючи у своїй сукупності так необхідну сферу ***компетентного управління*** виробництвом (підприємством).

Вважаємо за доцільне уточнити відмінності в поняттях *компетентність* і *компетенція* (професійна компетенція) [8]. ***Компетенція*** - це набір знань, навичок, поведінкових характеристик, які дають змогу ефективно виконувати певну роботу**.** ***Компетентність*** - це здатність застосовувати ці компетенції на практиці, що підтверджується реальними результатами. Отже, компетенція - це теоретичний набір якостей, а компетентність - їхнє успішне використання в реальних умовах. Тож ***професійна компетенція*** - це не просто володіння знаннями та навичками, а цілий комплекс характеристик, що дають змогу виконувати необхідні завдання на високому рівні завдяки: *глибокому розумінню своєї професії,* використовуючи знання стандартів, процесів, технологій; *ефективній комунікації* у вигляді вміння взаємодіяти з колегами та клієнтами; *саморозвитку й адекватній адаптивності*, тобто здатності підвищувати свій рівень знань, вмінь та навичок адаптації до змін; *відповідальності,* тобто усвідомлення наслідків своїх рішень та інших дій; *стресостійкості*, - як можливості працювати в напружених умовах без втрати продуктивності.

Так, серед ключових сфер *компетентності* логістики [7] виокремлюють такі: управління запасами (УЗ); транспортування (Т); логістичну інфраструктуру (І); складське господарство (СГ); вантажопереробку та пакування (ВП) і логістичну інформацію (ЛІ). Причому успіхи в кожній із зазначених сфер мають сенс тільки в разі реалізації позитивного ефекту синергетики, тобто тоді, коли вони забезпечують зростання загальної ефективності логістичних процесів, де елементу А відповідає максимальний, а елементу Е - мінімальний рівень ефективності.

Виходячи з цих міркувань побудовано (див. рис. 8.3, який адаптовано згідно [7]) інтегровану модель інформаційного забезпечення логістики підприємства. Слід особливо виокремити ЛІ - *логістичну інформацію*, яка становить найважливіший стратегічний ресурс логістики в моделі «постачальник - споживач».

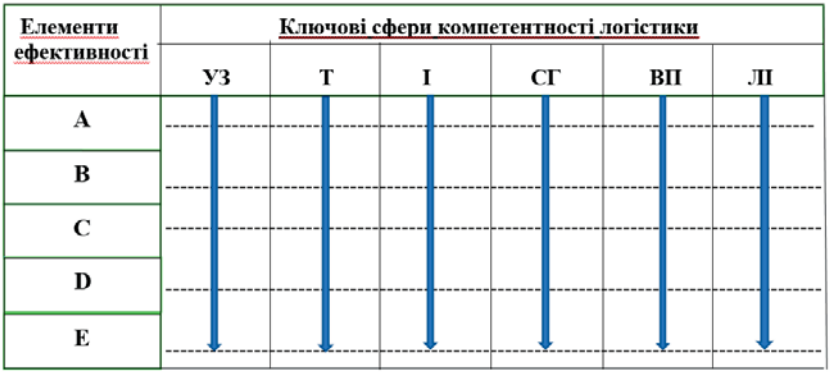

Рисунок 8.3. Модель інформаційного забезпечення логістики на підприємстві в площині елементів рівня ефективності та ключових компетентностей логістики

Використання сучасної обчислювальної техніки дає змогу серйозно знизити виробничі витрати завдяки ефективнішому управлінню інформаційними потоками за рахунок збільшення їхньої швидкості опрацювання і подальшої їхньої координації (коригування). При цьому, логістичні інформаційні системи зазвичай ділять за трьома групами:

1. *Планові інформаційні системи,* які створюються на адміністративному рівні управління і служать для прийняття довгострокових ***рішень стратегічного характеру.*** Серед розв'язуваних завдань можуть бути такі: створення й оптимізація ланок логістичного ланцюга; управління умовно-постійними даними, тобто тими, що мало змінюються; планування виробництва; загальне управління запасами; управління резервами та інші завдання;

2. *Диспозитивні інформаційні системи*, які створюються на рівні управління складом або цехом і служать для забезпечення налагодженої роботи логістичних систем. Тут можуть розв'язуватися такі завдання: детальне управління запасами (місцями складування); розпорядження внутрішньоскладським (або внутрішньозаводським) транспортом; відбір вантажів за замовленнями та їхнє комплектування, облік вантажів, що відправляються, та інші завдання;

3. *Виконавчі інформаційні системи,* які створюються на рівні адміністративного або оперативного управління. Оброблення інформації в цих системах проводять у темпі, який визначається швидкістю ее надходження в ЕОМ, у так званому режимі роботи в реальному масштабі часу, що дає змогу одержувати необхідну інформацію про рух вантажів у поточний момент часу та вчасно видавати відповідні адміністративні й управлінські впливи на об'єкт управління. Цими системами можна розв'язувати різноманітні завдання, наприклад, пов'язані з контролем матеріальних потоків, оперативним управлінням обслуговування виробництва, управлінням переміщеннями тощо.

Причому під час реалізації логістичних інформаційних систем необхідно дотримуватися певних принципів:

1. *Принцип використання апаратних і програмних модулів.* Дотримання цього принципу дає змогу: ***забезпечити*** сумісність обчислювальної техніки та програмного забезпечення на різних рівнях управління; ***підвищити*** ефективність функціонування логістичних інформаційних систем; ***знизити*** їхню вартість; ***прискорити*** їхню побудову.

2. *Принцип можливості поетапного створення системи.* Логістичні інформаційні системи, побудовані на базі сучасних електронних систем, як і інші автоматизовані системи управління, є системами, що постійно розвиваються. Це означає, що під час їхнього проектування необхідно передбачити можливість постійного ***збільшення кількості*** об'єктів автоматизації, можливість ***розширення складу*** реалізованих інформаційною системою функцій і ***кількості*** розв'язуваних завдань.

3. *Принцип чіткого встановлення місць стику*, в яких матеріальний та інформаційний потоки переходять або через

межі правомочності та відповідальності окремих підрозділів підприємства, або через власні межі самостійних (незалежних) організацій. Тому забезпечення плавного подолання місць стику є одним із важливих завдань логістики.

4. *Принцип гнучкості системи* з погляду специфічних вимог конкретного застосування.

5. *Принцип прийнятності системи* для користувача діалогу «людина - машина».

Очевидно, що реалізація описаних вище принципів у сфері *логістичних інформаційних систем* не обходиться без використання сучасної обчислювальної техніки, яку в сукупності та за аналогією з традиційною логістикою, заведено називати ***електронною логістикою*** [9], під якою розуміють управління та оптимізацію електронних інформаційних потоків, що виникають у ланцюгах постачань.

Дуже часто електронну логістику трактують як використання IT у логістиці, що справедливо лише частково. Наріжним каменем електронної

логістики є міжнародні стандарти. Дотримання стандартів дозволяє торговим партнерам з різних країн (або в одній країні) обмінюватися інформацією за допомогою простих, швидких і точних транзакцій, яки у даний час насамперед акцентовано за чотирма основними напрямками:

1) коди товарної нумерації (штрихове кодування);

2) електронний обмін даними (EDI, Electronic Data Interchange);

3) глобальна мережа синхронізації даних (GDSN, Global Data Synchronization Network);

4) електронний код продукції (EPC, Electronic Product Code).

Перші два напрямки в електронній логістики існують давно, і сьогодні вони є основою оптимізації інформаційних потоків в ланцюгах поставок. При цьому сучасні інформаційні технології дозволяють реєструвати надходження та реалізацію товарно-матеріальних цінностей практично в режимі "on-line". Наприклад, для застосування в оптово-роздрібній торгівлі призначений штрих-код EAN/ UPC, в промисловості, виробництві та складах (особливо у сфері управління матеріалами) використовуються стандарти Code 2/5 Interleaved;

Code 128 та EAN 128. Двомірні штрих-коди (Code 49; Code 16к; Codablock; PDF 417; Data Matrix; QR-код; MaxiCod) містять закодовану інформацію в двох вимірах, що дозволяє підвищити ємність коду та зменшити його розміри. Завдяки цьому, автоматична ідентифікація (сканування) штрихових кодів продукції в процесі виконання логістичних операцій і функцій дозволяє досягти серйозних переваг. При цьому удосконалення створення, передавання, приймання та оброблення інформації здійснюється на підставі концепції «Electronic Data Interchange» (EDI) або електронного обміну даними. EDI – це комп'ютерний обмін інформацією між користувачами із застосуванням стандартного формату відомостей та сучасних інформаційних технологій; завдяки йому прискорюється час руху інформації, скорочуються витрати на інформаційну логістику, підвищується продуктивність праці робітників, які беруть участь в інформаційній логістиці.

Використання EDI покращує достовірність, своєчасність і якість логістичної інформації. Для реалізації всіх переваг EDI необхідно пов'язати всі ланки логістичної системи, а також споживачів та інших зовнішніх користувачів логістичної інформації телекомунікаційними каналами. Цей зв'язок здійснюється за рахунок фірмових локальних мереж, комерційних і некомерційних телекомунікаційних мереж, що діють в межах регіону, країни або глобальних.

Безпосередня вигода застосування EDI в логістичних системах проявляється в наступних основних моментах:

• зростанні продуктивності в операційному менеджменті, яка досягається за рахунок швидкої передачі і обробки інформації, а точності і достовірності даних – за рахунок зменшення кількості паперових документів і можливості помилок введення даних;

• поліпшення канальних взаємин між ланками логістичної системи - це підвищення та зростанні продуктивності зовнішніх підсистем;

• зростанні здатності до повної інтеграції дій ланок логістичної системи способствует зменшення операційних та адміністративних витрат та скорочення логістичних витрат, що досягається за рахунок зменшення частки живої праці і матеріальних витрат, пов'язаних з друком, поштою, процедурами

паперового документообігу; скорочення телефонних, телексних і факсимільних комунікацій; зменшення адміністративних витрат.

Для EDI істотними є комунікаційні і інформаційні стандарти. Комунікаційні стандарти визначають технічні характеристики таким чином, щоб комп'ютери могли коректно інтерпретувати обмін інформацією.

Комунікаційні стандарти визначають характеристики прийому, перетворення і швидкість передачі даних.

Інформаційні стандарти регламентують структуру і вид документів, які повинні бути передані.

Найбільш часто використовувані в EDI комунікаційні стандарти – це ASC X. 12 (стандарт Американського комітету стандартів X.12) і стандарт UN/EDIFACT, стандарт TDK / EDIA і інші.

Для повноцінного вирішення завдань логістичного управління особливого значення набувають корпоративні мережі обміну інформацією. Вони, як правило, створюються на основі інформаційної технології INTRAnet і забезпечують доступ до інформаційних ресурсів мережі INTERNET та інших інформаційних мереж. При цьому є можливість обміну даними між будь-яким кінцевим обладнанням: комп'ютерами будь-яких моделей (в режимі електронної пошти і в режимі OnLine), факсимільними апаратами, телексами і телеграфними пристроями з використанням будь-яких протоколів передачі логістичних даних (TCP / IP, Frame Relay, X.25 та ін.). Особливо з точки зору автоматизації управління, більш перспективним є режим OnLine, при якому проводиться безпосередня передача інформації від відправника до її споживача або зчитування інформації споживачем з різноманітних Web-серверів або хостів в адресних просторах IP і X.25. В інформаційних системах, які здійснюють оперативне управління матеріальним потоком, особливо важливо фіксувати і обробляти інформацію в темпі проходження матеріального потоку. Рішення завдань, що виникають при цьому, найчастіше можливо лише за умови застосування сучасної техніки і технології збору, обробки і передачі інформації в режимі реального масштабу часу.

Сьогодні більшість територіально-розподілених корпоративних мереж все більше інтегруються з глобальною

мережею Internet, що вимагає стандартизації мережевих служб і протоколів. Фактично об'єднання стає необхідною умовою для оперативного обміну даними і ефективного управління. Так, всесвітня мережа синхронізації даних (англ. Global Data Synchronisation Network, GDSN) – це розподілена мережа електронних каталогів та Всесвітнього Реєстра (GS1 Global Registry™), яка надає компаніям у всьому світі можливість організувати обмін синхронізованими та стандартизованими даними зі своїми діловими партнерами. Мережа GDSN гарантує точність і відповідність стандартам даних, якими обмінюються ділові партнери. Вона складається з інформаційних систем торгівельних партнерів (постачальників та торгових мереж), каталогів даних (служб, що зберігають та обробляють дані торгових партнерів) та Всесвітнього Реєстру GS1 (всесвітній довідник, що допомагає спільноті GDSN визначати місцезнаходження інформаційних ресурсів та керувати синхронізацією зв'язків між торговими партнерами). GDSN забезпечує стандартизовані, надійні дані для ефективного обміну діловою інформацією на локальному і глобальному ринках, оптимізуючи фінансові витрати у ланцюзі постачання.

Можливість відстежити весь шлях товару в процесі товаропостачання, запобігти затримкам та втратам під час складування та транспортування, зробити облік миттєвим та таким, що не вимагає ніякої участі людини, забезпечити постійний контроль наявності необхідного товару на полицях торгових підприємств – це лише окремі переваги, що забезпечує Електронний код продукту (від англ. Electronic Product Code™, EPC), яка є «системою наступного покоління» для ідентифікації і простежування товарів протягом всього ланцюжка постачання. Дана система EPC уможливлює автоматичну ідентифікацію і простежування товарів в реальному часі на всьому шляху від виробника до споживача. EPC - це універсальний відкритий стандарт для ідентифікації окремих об'єктів і розповсюдження інформації під час їх постачання. Фактично EPC являє собою набір унікальних ідентифікаторів, присвоєних матеріальним предметам, місцезнаходженням чи іншим об'єктам, що відіграють певну роль у ділових операціях. Номер EPC може бути побудований на основі глобального номера товарної позиції

(GTIN) із додаванням індивідуального номера для кожної одиниці продукції (серіалізація GTIN). Номери EPC можуть бути представлені у різних форматах, в т.ч. у формі бінарного коду, яка найкраще підходить для запису в пам'ять позначки для радіочастотної (РЧІ), та у текстовому форматі формі для поширення даних в інформаційних системах підприємств. Для зчитування номеру застосовується технологія радіочастотної ідентифікації. Кожна одиниця такого номера у вигляді мікроелектронного пристрою (чіпа-радіомітки), містить і може відображати записані в його пам'яті дані за допомогою радіохвиль, а штатні приймачі (як автоматичні зчитувачі) можуть з високою швидкодією зчитувати, передавати та зберігати цю інформацію (у вигляді даних чіпа) в пам'яті штатних систем зчитування, які реалізують етапи виявлення, розпізнавання, контролю, допуску та зберігання даних для ідентифікації об'єктів, що експертизуються. Тому важливою складовою мережі EPC є спеціальне програмне забезпечення, яке впорядковує інформацію, що надходить від автоматичних зчитувачів, та забезпечує відображення інформації про поточний стан об'єкту в зовнішніх інформаційних системах. Це забезпечує Служба найменування об'єктів (ONS), яка за номером EPC надає інформацію про те, де саме знаходиться поточна інформація про об'єкт.

Отже, логістичні інформаційні системи та їхні інформаційні потоки (внутрішні та зовнішні, вертикальні та горизонтальні, вхідні та вихідні), що потрібни у виконання функціональних завдань, згідно з вище наведенним, реалізуються, зазвичай, за допомогою функціональних підсистем, де інформаційний потік вимірюється за кількістю опрацьованої чи переданої інформації за одиницю часу, використовуючи: технічне забезпечення, тобто сукупність технічних засобів, які забезпечують опрацювання інформації і передавання інформаційних потоків; інформаційне забезпечення, яке охоплює довідники, класифікатори, кодифікатори, засоби формалізованого опису даних; математичне забезпечення, тобто сукупність методів розв’язання функціональних завдань. При цьому логістичної системи інформації (у процесі інформаційнії діяльністі) властиво виявлення та ретельній аналіз реальних потреб штатної

життєдіяльності підприємства, ідентифікації ***ключових рішень*** та планів їх освоєння.

Відповідно до Закону України «Про інформацію») [10] ***інформаційна діяльність*** — це сукупністі дій, спрямованих на задоволення інформаційних потреб громадян, юридичних осіб і держави. Згідно ДСТУ 2392-94 «Інформація і документація. Базові поняття. Терміни та визначення» [11] *поняття «інформаційна діяльність»* визначає постійне та систематичне збирання та оброблення інформації з метою її зберігання, пошуку, використання або пересилання. Тобто таку інформаційну діяльність доцільно представляти у вигляді інформаційного процесу, що складається з отримання інформації, її подальшого оброблення (узагальнення), накопичення (зберігання) і передання користувачеві (див. рис. 8.4. та 8.5, які адаптовані згідно [12, с. 23]).

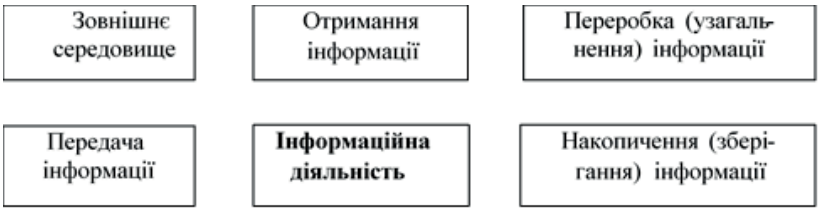

Рисунок 8.4. Схема інформаційного процесу у сучасному суспільстві

При ідентифікації ключових рішень водночас треба вирішити питання, яке рішення оптимальне. Очевидно, таке рішення повинно прийматися з урахуванням її вартості, тобто бути результатом балансу між потрібними для цього витратами і вигодами. Крім того, необхідно враховувати також можливі ризики операції інформаційній діяльності з огляду потреб, які можуть виникнути при реалізації таких угод, використовуючи ***інформаційно-довідкові*** та ***аналітичні*** матеріали (див. рис. 8.5).

Інформаційно-довідкові матеріали припускають доведення керівнику і спеціалістам інформації про юридичні документи (закони, укази, постанови, листи, розпорядження та ін.), а також

про порядок і правила підготовки й оформлення так званих процедурних документів (довідок, декларацій, угод та ін.).

Рисунок 8.5. Структура інформаційно-аналітичних матеріалів для ретельної підготовки і ефективного виконання операції у процесі інформаційній діяльності

В контексті викладеного вище, ретельно підготовані аналітичні матеріали, як основа (інструмент) розумової діяльності людей, дозволяють формувати якусь узагальнюючу (інтегральну) сферу інформаційнії діяльністі соціуму, секторіальні області якої цілком можна ототожнювати (розглядати) з точки зору сучасної реалізації діяльного, інституціонального, організаційного, ціннісного, гносеологічного, а також професійно-технологічних підходів. При цьому поняття аналітика й аналіз не є синонімами, що доказово викладено в нав. посіб «Основи інформаційно-аналітичної діяльності» Захаровой В. І. и Філіповой Л. Я. [12, с.29]. Там «під аналітикою розуміється задовольняюча деяким цінностям і стандартам діяльність щодо отримання знання про практичні проблеми, з якими стикається управління, і шляхи їх вирішення за допомогою застосування аналітичних методів». «Разом із тим аналіз — це робота з інформацією за допомогою методів, які можна класифікувати у три групи: методи пошуку і вибору інформації в Інтернеті, бібліотеках, базах і накопичувачах інформації; методи одержання інформації на основі використання життєвого і професійного досвіду; методи спеціальних досліджень».

На підставі узагальнення сформованого підходу фахівці [13 або 12, с.59] представляють триланкову модель аналітики (див. рис. 8.6). Подальший розвиток аналітики неминуче приводить до оформлення в ній організаційного аспекту, що означає цілеспрямовану діяльність різного роду аналітичних організацій, перетворення аналітичної діяльності в об'єкт організації і управління.

У контексті викладеного вище під аналітикою [13 або 12, с.30] слід розуміти діяльність окремих осіб або організацій (підрозділів, органів управління), що задовольняє певним цінностям і стандартам та орієнтована на здобуття знань щодо практичних проблем, з якими стикається управління, з метою вироблення алгоритму їх розв'язання, використовуючи аналітичні методи. Як свідчить практика, такий процес аналітичної діяльності доцільно формувати у вигляді сукупності таких етапів [12]:

1) етап розроблення алгоритму майбутнього проведення аналізу, спрямованого на забезпечення нівелювання конкретної проблеми, корельованої щодо об'єкта і предмета вивчення, поставлених цілей і завдань, апріорних гіпотез їх розв'язання та потенційного інструментарію аналізу;

Рисунок 8.6. Триланкова проблемно-методолого-ціннісно-нормативна природа аналітики

2) етап створення професійного колективу, здатного аналітично абстрагувати (виробити) робочу концепцію (модель) досліджуваного об'єкта (явища) з метою його подальшого вивчення і можливої оптимізації;

3) етап створення апріорної системи однозначно чітких показників і критеріїв, що забезпечують деталізацію сутності проблеми і зниження рівня невизначеності щодо пріоритетних властивостей досліджуваного об'єкта (явища);

4) етап збирання, систематизації та опрацювання інформації про властивості (статичні та динамічні) об'єкта (явища) відповідно до його параметрів, характеристик та критеріїв аналізу дослідження;

5) етап взаємно-кореляційного аналізу отриманої (апостеріорної) інформації з апріорною з метою перевірки прийнятих штатних гіпотез дослідження, виявлення наявності та можливих причин їхніх розбіжностей у рамках закономірностей потенційного розвитку явища (об'єкта);

6) етап вироблення практичних рекомендацій у вигляді звіту (доповідних) для органів управління за результатами розв'язання виниклої проблеми.

В такому контексті, під аналітикою варто розуміти задовольняючу деяким цінностям і стандартам інформаційну діяльність спеціальних організацій або підрозділів органів управління, або окремих спеціально підготовлених осіб з одержання знання про практичні проблеми, з якими стикається управління, і шляхи їх вирішення за допомогою застосування аналітичних методів [13]. Тоді, аналітична діяльність може бути класифікована за такими ознаками, як тип ціннісної орієнтації, тип об’єкта аналізу (сфери положення об’єкта), тип курируючої науки, тип домінуючого методу, рівень пізнання, місце в дослідженні, тип організації, тип кадрового забезпечення, ступінь відкритості для суспільства, а також тип часової детермінації. При цьому кожний різновид аналітичної діяльності має своє призначення в суспільстві та характеризується технологічною специфікою.

Таким чином існує багато визначень поняття «інформаційно-аналітичної діяльності» (ІАД). Зокрема, наприклад, будь-який вид виробничо-економічної діяльності

ґрунтується на відповідному інформаційному забезпеченні, в тому числі економічною, кон'юнктурною, науково-технічною, оглядово-аналітичною, фактографічною та іншою інформацією. Поширеними є такі, що *спрямовані на сферу управління*. Фахівці [12] розглядають інформаційно-аналітичну діяльність як процес у сфері управління, що являє собою процес пошуку, збору, переробки та подання інформації у формі, придатній для її використання; як інформаційно-аналітичну роботу у двох аспектах — інформаційну роботу та аналітичну роботу; як системне отримання, аналіз та накопичення інформації з елементами прогнозування з питань, що стосуються діяльності установи.

Управлінську інформацію можна умовно поділити на три категорії [12, с.55 або 14, с. 41]: інформація стратегічного планування, контрольна управлінська та оперативна. Там само [12, с.47] поняття «*інформаційно-аналітична робота*» розглядається як складова інформаційно-аналітичної діяльності, де під час проведення ІАД виділяють *два рівні* (або напрями) інформаційно-аналітичної роботи (ІАР):

1) *інформаційний рівень*, що полягає в пошуку, збиранні, зберігання, поширенні інформації;

2) *аналітичний рівень*, що полягає в узагальненні, класифікації інформації, її аналізі і перетворенні, розробці висновків, пропозицій, рекомендацій і прогнозів.

Доцільно озвучити, що в ІАР використовують сучасну методологію аналітичних досліджень, тобто сукупність принципів, методів, способів та підходів до організації та проведення таких досліджень. Уточнимо, що: принципи — вироблені наукою та практикою, сформульовані у концентрованому вигляді найбільш важливі ідеї, установки; метод — сукупність прийомів та способів пізнання; прийом — окрема дія для досягнення мети дослідження; спосіб — система дій, що застосовуються при виконання певного дослідження; процедура — встановлений порядок виконання прийомів та способів дослідження; методика — послідовність конкретних процедур, реалізація яких забезпечує досягнення мети досліджень; технологія (техніка) аналітичного дослідження — сукупність прийомів та способів, які входять до складу процедур.

Прийнято вважати, що з позицій прийняття рішень розрізняють оперативний, тактичний та стратегічний рівні ІАР, а його (ІАР) основними формами є: 1) моніторинг, що включає інформаційні зведення та огляди; 2) аналіз ефективності прийняття рішень; 3) дослідження актуальних проблем (інформаційні розробки, оперативні та аналітичні дослідження). При цьому основні принципи аналітичної роботи: — це цілеспрямованість; актуальність; активність; достовірність; повнота; альтернативність; обґрунтованість; системність; своєчасність; ініціативність; об'єктивність; неперервність; гнучкість [12, с. 47].

У загальному плані інформаційно-аналітична діяльність визначається як сукупність процесів збору, аналізу, синтезу, перетворення, зберігання, пошуку і розповсюдження інформації, систематично здійснюваних різними організаціями. Своєрідним продуктом діяльності ІАД є **консолідована інформація [15].**

Консолідована інформація є суспільним знанням, яке спеціально відібране, проаналізоване, просинтезоване, оцінене, реструктуризоване і видозмінене з метою придатності для безпосереднього вирішення проблем і задоволення інформаційних потреб окремих осіб або груп користувачів інформації, які по-іншому не мали б прямого доступу до цих знань і не могли б їх ефективно використовувати, тому, що вони розсіяні по багатьох документах і важко доступні у своїй оригінальній формі.

Під *реструктуризацією* інформації розуміються процеси її представлення і аналізу, що змінюють первинну структуру і форму та включають синтез інформації, підготовку оглядів, характеристику сучасного стану, спрощений або популярний виклад фізичної форми інформації (друкована, графічна, аудіовізуальна, машинозчитувана.

Уявлення про консолідовану інформацію, її місце та роль в ІАД і значення в інформаційному забезпеченні органів державної влади та інших споживачів дає рис. 8.7, згідно [12, с.58, 16.с.56], на якому показано збільшення цінності інформації для прийняття рішення і зменшення її об'єму в залежності від збільшення її консолідації. Основним методом підготовки консолідованої інформації є функціонально-інформаційний синтез (ФІС) предметної області.

Наприклад, у контексті підвищення ефективності управління регіоном, на сьогоднішній день особливої ваги набуває питання створення *регіональної інформаційно-аналітичної служби* (РІАС) при місцевих державних адміністраціях у їх прямому підпорядкуванні, метою діяльності якої є своєчасна, науково-обґрунтована підтримка процесів підготовки, прийняття управлінських рішень і забезпечення інформаційних потреб суспільства. РІАС можуть виконувати замовлення із інформаційно-аналітичного забезпечення організацій, установ різних форм власності, юридичних та фізичних осіб і на комерційній основі згідно з договором, що є альтернативним варіантом розв'язання питання низького рівня фінансування програм інформатизації та розвитку інформаційної сфери регіону.

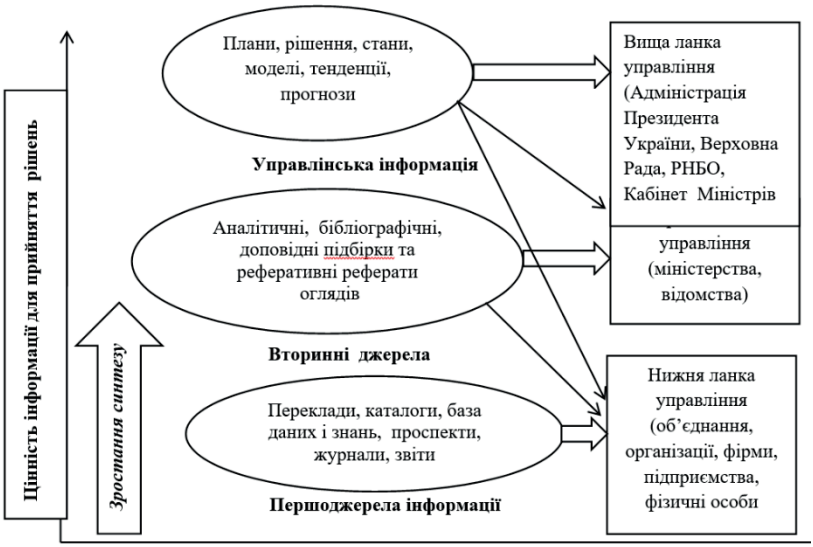

Рисунок 8.7. Місце консолідованої інформації в інформаційно-аналітичній діяльності та інформаційному забезпеченні органів державної влади

Функціонально інформаційно-аналітична служба в регіоні може складатися з таких базових підсистем (чи складових), які наведени на рис. 8.8. [12, с. 73 або 17]. Для реалізації вищенаведених функцій доцільно (див. рис. 8.9) в структурі інформаційно-аналітичної служби в регіоні створити відповідні відділи [12, с.74 або 17, с. 254]:

- аналітично-експертний відділ;
- відділ інформаційного пошуку та інформаційних ресурсів;
- відділ технічного забезпечення.

Рисунок 8.8. Функції регіональної інформаційно-аналітичної служби (РІАС)

Так, для порівняння з матеріалом рис. 8.9 на рис. 8.10 (який адаптований згідно [6, с. 309]) наведена узагальнена схема взаємодії учасників у процесі зовнішньоекономічної діяльності з метою аналізу інформаційно-аналітичних матеріалів для ретельної підготовки і ефективного виконання, наприклад, зовнішньоекономічної операції.

Ці матеріали дуже потрібні на всіх етапах підготовки і виконання операції, де алгоритм розв'язання експертно-аналітичних завдань підготовки і супроводу зовнішньоекономічної операції зображено на рис. 8.11, який адаптований згідно [6, с.311].

Очевидно, що крім зазначених прикладів і наведених служб інформаційно-аналітичної діяльності існує безліч інших перехресних зв'язків. Як правило у кожному блоці наведеного алгоритму розробляються і використовуються специфічні інформаційно-аналітичні матеріали, за допомогою яких керівник

відслідковує всі ключові аспекти, наприклад, зовнішньоекономічної операції і приймає обґрунтовані рішення.

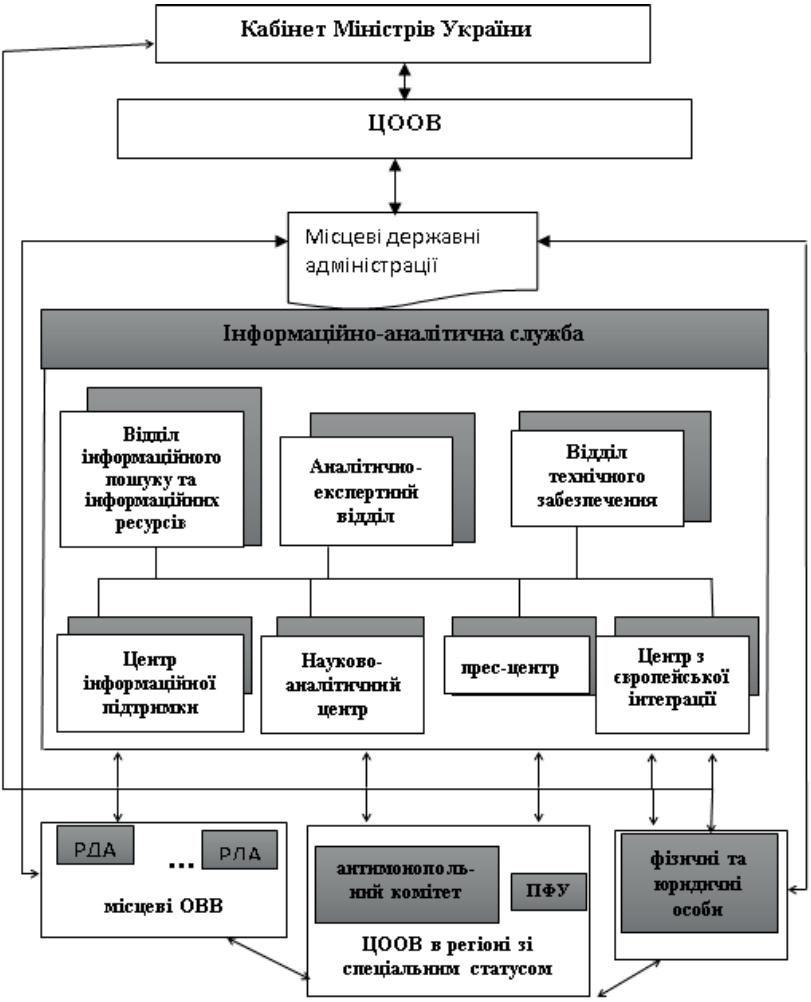

Рисунок 8.9. Структурна схема PIAC в системі органів виконавчої влади

При цьому вихідними даними є інформація з комерційної пропозиції (оферти) або юридично закріплені положення договору (контракту), а також додаткова інформація, необхідна для розрахунків, оформлена у вигляді вербальної (описової) постановки завдання.

Рисунок 8.10. Схему взаємодії учасників у процесі зовнішньоекономічної діяльності

У загальному випадку ефективність, наприклад, зовнішньоекономічної операції визначається сукупністю факторів, поданих на рис. 8.12 (згідно [6, с.313]), де кожний з

наведених факторів тією чи іншою мірою впливає на загальну ефективність зовнішньоекономічної операції.

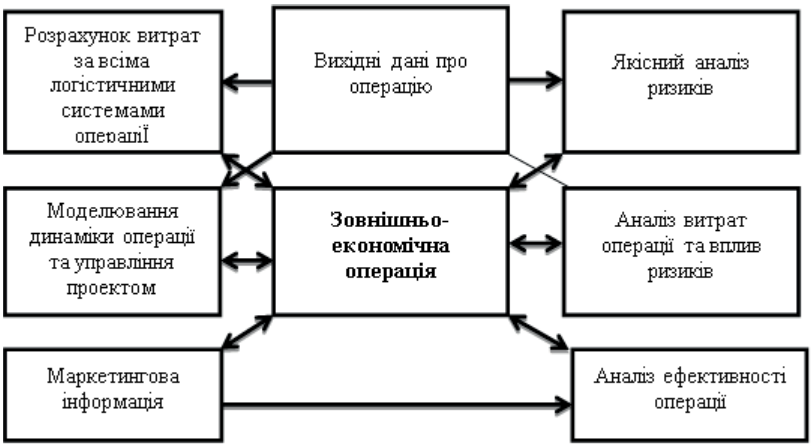

Рисунок 8.11. Схема аналізу та прийняття рішення у зовнішньоекономічної діяльності

Оскільки суть спрямованості реалізації логістики (закупівельної, виробничої, розподільчої, транспортної та інформаційної) полягає у формуванні та реалізації системи управління, яка має об'єднати послідовність дій управлінського персоналу та відповідних функціональних ланок, логістичних посередників та контрагентів у процесі управління потоками під час повного логістичного ланцюга «постачання-виробництво-збут» у межах логістичної системи на даний момент часу, то стратегічне управління розвитком сучасного підприємства, у сукупності з технологіями ситуаційного менеджменту та соціальної інженерії (див. п. 7.1), стають визначальними в конкретній сфері діяльності соціуму.

У таких випадках ***стратегію*** можна розглядати як мистецтво динамічної самоідентифікації підприємств щодо мінливих обставин зовнішнього середовища: конкурентів, партнерів, джерел ресурсів, правил взаємодії в освітній сфері тощо. При цьому слід зазначити, що універсального, придатного на всі випадки життя підходу до розроблення стратегії не існує,

хоча наукові дослідження в цьому напрямі та накопичений досвід підказують можливі напрями розроблення. На думку авторів цього навчального посібника надалі можна використовувати одне з двох основних визначень стратегії залежно від розуміння її суті [6].

Рисунок 8.12. Сукупність факторів, що впливає на ефективність операції

У першому випадку «стратегія - це конкретний довгостроковий план досягнення конкретної довгострокової мети, а вироблення стратегії - це знаходження мети та складання довгострокового плану».

У другому випадку «стратегія - це довгостроковий якісно визначений напрямок розвитку організації, що стосується сфери, засобів і форми її діяльності, системи взаємовідносин усередині організації, а також позиції організації в навколишньому середовищі, який приводить організацію до її цілей».

Причому, відповідність класифікаційних ознак і відповідних видів стратегій (див. рис. 8.13, який адаптований згідно [18, с. 18])) наведено в таблиці 8.1.

Зрештою, стратегія даної конкретної організації проявляється в системі її конкретних конкурентних переваг. Конкурентна перевага - це ті характеристики, які створюють для організації, що виробляє і/або реалізує цей продукт, певну перевагу над її конкурентами. Ці характеристики можуть бути найрізноманітнішими і стосуватися як самого продукту-товару

(базової послуги), так і додаткових послуг, що супроводжують базову, тобто форм виробництва, збуту, продажу тощо, специфічних для організації та/або її продукту.

Рисунок 8.13. Класифікаційні ознаки систематизації стратегій

При цьому, реальна конкурентна перевага досягається завдяки тому, як дана організація на практиці здійснює стратегічні види своєї діяльності та всю їхню інтегральну сукупність, адже оптимальний вибір стратегії та її успішна реалізація - очевидна запорука надійного процвітання і розвитку підприємства (організації).

Таблиця 8.1. Класифікація стратегій (адаптовано з [18, с. 16-18]

Ознака	Види стратегії
Концепція досягнення конкурентних переваг	**Стратегія мінімізації** витрат. Стратегія **диференціації.** Стратегія **фокусування.** Стратегія **інновацій.** Стратегія швидкого **реагування.** Стратегія **синергізму.**
Маркетингове середовище	**Інтеграційні стратегії:** макроекономічна; зовнішньоекономічна. **Регіональні стратегії:** виробничої сфери; невиробничої сфери; міжгалузева; галузева.
Функціональне призначення	**Стратегії факторів виробництва:** виробничих; інвестиційних; інноваційних; фінансових; трудових; інформаційних.
Цикл розвитку	**Стратегія зростання.** Стратегія **стабільності.** Стратегія **виживання,** у тому числі антикризова стратегія: запобігання неспроможності; вихід з кризи; ліквідація наслідків кризи.
Вид та масштаб ринку	**Стратегія розширення** ринку. Стратегія **проникнення** в глиб ринку. Стратегія **просування** товару нові ринки. Стратегія **формування та утримання** конкурентних переваг.
Пріоритет засобів маркетингу	**Товарна стратегія:** диференціація профілюючого товару; диверсифікація. **Цінова стратегія:** підвищення / зниження цін; цінова кон'юнктура. **Фірмова стратегія:** фірмового товару, іміджу, сервісу, стилю, дизайну.

Ознака	Види стратегії
	Рекламна стратегія: інформування про пере-ваги товару, переконання, мотивація, нагадування.
Ринкова кон'юнктура	**Стратегія попиту та пропозиції:** стимулююча, креативна, підтримуюча, протидіє.
Ринкова поведінка	**Стратегія дрібних організацій:** копіювання продуктів провід-них фірм, пристосування до потреб, інтеграція з більшими організація-ми. **Стратегія середніх організацій**: патентна (ринкових ніш), інноваційна, інтенсивного маркетингу. **Стратегія великих фірм:** широке проникнення, зняття вершків.
Ступінь реалізації	**Ретроспективна. Поточна. Перспективна.**
Ймовірність реалізації	**Реальна. Сумнівна. Нереальна**

Таким чином, узагальнюючи вищевикладене, ефективне підприємство можна розглядати як систему логістичного стратегічного менеджменту, тобто як єдину організаційно-господарську структуру із сучасною електронною логістикою, яка складається з власної конкурентно спроможної сфери діяльності, зовнішніх сумлінних постачальників сировини, матеріалів, комплектуючих виробів і споживачів готової продукції, де безпосередньо «стратегія не призначена для реалізації цілей, вона включає їх у себе, синтезує із засобами, і в цьому особливість стратегії та стратегічного планування, відмінність його від усіх інших видів планування» [18].

8.2. Аспекти стратегічного управління та формування процесу становлення стратегічного менеджменту підприємства (організації)

Пояснення суті стратегічного управління (СУ), що має бути в основі пріоритетних напрямів розвитку підприємства (організації), доцільно розпочинати з розгляду процесу реалізації СУ за структурно-функціональною схемою рис. 8.14 [19], здійснюваного за допомогою таких блоків:

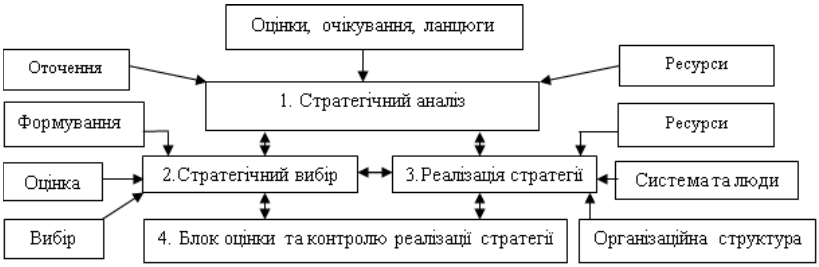

Рисунок 8.14. Структурно-функціональна схема стратегічного управління

1. ***Блок стратегічного аналізу,*** - це блок, за допомогою якого забезпечується чітке розуміння з боку керівництва того, на якій стадії розвитку перебуває підприємство, перш ніж вирішувати, куди рухатися далі. Для чого необхідна ефективна інформаційна система і відповідна ділова розвідка, що забезпечують професійними даними достовірність апріорних результатів, виходячи з професійного аналізу інцидентів і ситуацій минулих, теперішніх і за можливості майбутніх років. При цьому, добре проведена бізнес-діагностика сильних і слабких сторін діяльності власного підприємства і сторони-конкурента дає змогу дати реальну оцінку власних ресурсів і можливостей, що також є відправною точкою під час розроблення довготривалої стратегії. Важливими є знання як про внутрішні можливості в досягненні поставленої мети, так і результати моніторингу конкурентного оточення, в якому

працюють аналогічні підприємства (фірми). Як правило, такий аналіз (як для власної внутрішньої діяльності, так і для зовнішнього середовища) доцільно здійснювати в галузях економіки, політики, технології, ринку придбання та збуту, міжнародного та внутрішнього становища і конкуренції, а також у сфері соціально-культурної поведінки соціуму. Таким чином, стратегічний аналіз є найважливішим етапом управління під час вироблення ефективної стратегії, в основі якої закладено необхідність реалізації трьох складових у вигляді: - надійно обґрунтованих довгострокових цілей з високим рівнем імовірності їх досягнення; - достовірності й цілісності розуміння зовнішнього конкурентного оточення; - повноти й істинності реальної оцінки власних ресурсів і можливостей.

2. ***Блок формування стратегії та стратегічного вибору,*** - де під час формування забезпечується визначення (деталізація) ***місії***[*,37], та цілевказівки (довгострокових і короткострокових), а вибір (стратегічний) полягає в узагальненні всього аналітичного матеріалу стосовно власної внутрішньої та конкурентної у вищевказаних галузях діяльності з наступною оцінкою альтернативних напрямів розвитку власного підприємства (фірми). Очевидно, що тут ухвалюється найоптимальніший варіант рішення, використовуючи спеціальні методи прогнозування та оцінки можливих ситуацій, наприклад, на базі сценаріїв розвитку та портфельного ***аналізу*** **[19]**. Причому заведено вважати, що формування та оцінювання альтернативних варіантів розвитку представляє самостійну цінність для управління, і вона реалізується під час стратегічного планування, визначаючи часові межі, ресурси, джерела та обсяги фінансування, а також відповідальних з а реалізацію намічених заходів. При цьому, виокремлюють оперативне та перспективне планування. Перше покликане забезпечити ефективну організацію поточної діяльності підприємства, а друге - успішне виживання організації в майбутньому.

---

*[37] Миссия, или общественно значимая роль, предприятия представляет собой качественно выраженную совокупность основных целей, например, оптимизацию бизнеса.

3. *Блок реалізації стратегії, -* забезпечує процес, у якому стратегія перетворюється на дії на основі розроблених програм, бюджетів і процедур, а також оперативний процес проведення стратегічних змін в організації, що переводять її в такий стан, у якому організація буде готова до втілення запланованої стратегії в життя. У цьому разі реалізація обраної стратегії передбачає коригування двох попередніх етапів, де діяльність керівництва спрямована на модернізацію (за необхідності) системи управління, приведення її у відповідність до стратегічних цілей організаційної структури фірми, виділення необхідних ресурсів, а також на підготовку персоналу. До числа таких стратегічних рішень на даному етапі можна віднести: реконструкцію підприємства, упровадження нової продукції та технологій, організаційні зміни правової форми підприємства, структури виробництва та управління, оплати праці тощо, передбачаючи додатковий вихід на нові ринки придбання та збуту, зокрема і з метою злиття підприємств тощо.

4. *Блок оцінки та контролю реалізації стратегії,* - завдяки якому забезпечується стійкий зворотний зв'язок між реалізацією стратегії та цілями організації, де стратегічний контроль спрямований на з'ясування того, якою мірою реалізація стратегії призводить до досягнення цілей підприємства (фірми). У цьому разі заведено керуватися конкретним алгоритмом: що треба робити (концептуальний аспект, формування генеральної мети); як робити (технологічний аспект); з використанням яких засобів (ресурсний аспект); у які строки і в якій послідовності (часовий аспект); хто робитиме (кадровий аспект); якою має бути організаційна структура управління (організаційно-управлінський аспект).

Таким чином, відповідно до викладеного вище, процес розроблення стратегії, включно з її визначенням і вибором, має проводитися з урахуванням (на етапі) аналізу як внутрішнього, так і зовнішнього середовища, а її (стратегії) безпосередня оцінка може вимагати додаткового аналізу, підключаючи, за необхідності, ретельний моніторинг діяльності підприємства для подальшого (бажано щорічного) коригування стратегічних рішень і планів з реалізації довгострокових і короткострокових запланованих цілей. При цьому сфера стратегічних рішень

широка, а її конкретика у вигляді, наприклад, моделей стратегічного управління різноманітна і залежить від: вибору напрямів діяльності, пріоритету ресурсів, головних довготривалих партнерів, організаційної форми партнерства, способів розвитку потенціалу, можливостей використання сильних сторін підприємства, зниження негативних наслідків слабких і загроз зовнішнього середовища, конкурентної та інноваційної антикризової політики. Причому кожен із перелічених вище елементів та етапів успішної життєдіяльності соціуму має відповідати сучасним принципам добротного стратегічного управління.

Нагадаємо, що в контексті цього викладу в поняття ***принцип*** вкладено вимогу дотримання об'єктивного закону управління і відповідні правила його виконання. До принципів стратегічного управління заведено відносити [5]:

- принцип єдиноначальності, де влада законодавча, виконавча і судова зосереджена в руках однієї людини;
- принцип оптимального поєднання централізації та децентралізації у сфері управління, що дає змогу успішно розподіляти повноваження на ухвалення як рішень на кожному рівні ієрархії управління, так і стратегічних рішень (під час розроблення цілей, стратегії, політики) на вищому рівні управління організацією;
- принцип поєднання прав, обов'язків та відповідальності при визначенні повноти влади та відповідальності посадових осіб;
- принцип обґрунтованого і свідомого вибору цілей і стратегій розвитку організації;
- принцип відповідності.

Тому будь-які якісні зміни в керованому об'єкті мають супроводжуватися необхідними змінами в системі управління - в організаційних структурах, під час розподілу влади, у делегуванні повноважень, у штатному професійно-кваліфікаційному складі кадрів тощо. При цьому, функції і внутрішня структура системи управління узгоджуються зі структурою цілей організації (див. рис. 8.15, адаптованому з [22, с. 41]), що змінюється за умови збереження і відповідності прийнятим цілям того чи іншого рівня, як і якісні характеристики інформації в каналах управління.

Отже, цілі на всіх рівнях мають узгоджуватися між собою і за вертикаллю, і за горизонталлю, тобто будь-яка мета нижнього рівня повинна вносити свій внесок у реалізацію мети більш високого рівня і водночас не тільки не перешкоджати реалізації інших цілей одного з нею рівня, а всіляко сприяти їхньому досягненню. Причому цілі розвитку організації мають відповідати таким вимогам у вигляді:

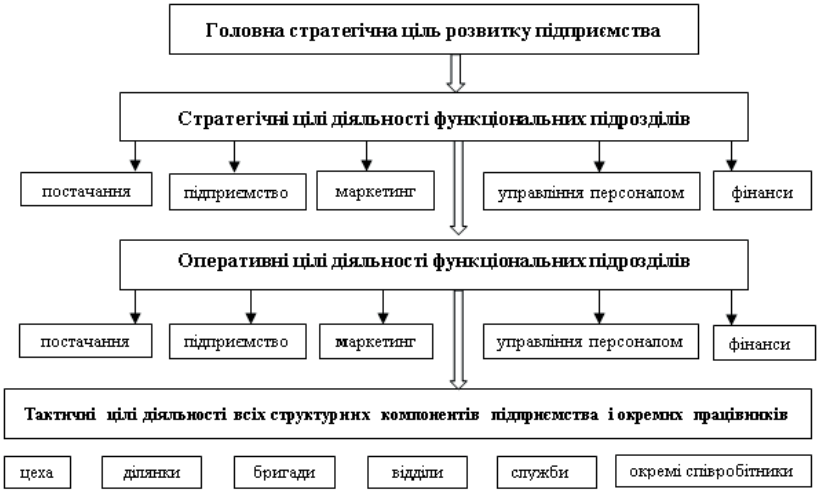

Рисунок 8.15. Організаційно-структурна система управління

– досяжності, коли стан організації, якого вона має досягти до кінця періоду реалізації стратегії, має відповідати реальним можливостям, спираючись на відповідні матеріальні та фінансові ресурси, а також потенціал персоналу, - оскільки саме недосяжні цілі відбивають у людей бажання працювати і зводять до мінімуму їхню мотивацію;

- вимірюваності, коли всі показники, які лежать в основі цілепокладання, виражаються в цифрових показниках, визначених об'єктивними розрахунками;

Отже, цілі на всіх рівнях мають узгоджуватися між собою і за вертикаллю, і за горизонталлю, тобто будь-яка мета нижнього

рівня повинна вносити свій внесок у реалізацію мети більш високого рівня і водночас не тільки не перешкоджати реалізації інших цілей одного з нею рівня, а всіляко сприяти їхньому досягненню. Причому цілі розвитку організації мають відповідати таким вимогам у вигляді:

– досяжності, коли стан організації, якого вона має досягти до кінця періоду реалізації стратегії, має відповідати реальним можливостям, спираючись на відповідні матеріальні та фінансові ресурси, а також потенціал персоналу, - оскільки саме недосяжні цілі відбивають у людей бажання працювати і зводять до мінімуму їхню мотивацію;

- вимірюваності, коли всі показники, які лежать в основі цілепокладання, виражаються в цифрових показниках, визначених об'єктивними розрахунками;

- однозначності (визначеності) у часі, коли часовий період, відведений на реалізацію мети, збігається з періодом реалізації стратегії (якщо йдеться про стратегію) або розв'язання будь-якої менш масштабної проблеми, запланованої в рамках реалізації цієї стратегії;

- гнучкості щодо здійснення корекції мети, яка стає або недосяжною у зв'язку з погіршенням ситуації, або, навпаки, в організації відкриваються додаткові можливості, і стара мета починає стримувати розвиток, чого не передбачалося під час формулювання мети через складність та дедалі більшу невизначеність довкілля, зміну багатьох чинників.

Саме тільки тоді цілі розвитку організації стають інструментом стратегічного менеджменту, коли вони чітко визначені та сформульовані, доведені до працівників, ними прийняті та можуть працювати для їх досягнення.

Класифікація цілей розвитку організації здійснюється за різними підставами. Залежно від важливості та ступеня впливу на результати діяльності організації виділяють цілі: - необхідні, тобто ті цілі, що визначаються у сфері основної діяльності організації та без досягнення яких неможливий її успішний розвиток, тобто це ті цілі, яких необхідно досягти обов'язково; - бажані, що додаються до необхідних цілей і дають змогу ще більше зміцнити становище організації, проте, якщо їх не буде досягнуто, то це не стане катастрофою для організації; - можливі,

тобто цілі, що безпосередньо не стосуються основної діяльності організації, проте здатні опосередковано вплинути на її ефективність.

Таким чином: 1. Визначення напряму розвитку організації містить у собі вирішення двох взаємопов'язаних завдань - формулювання місії та її конкретизацію. 2. Наслідком оформлення і подальшого поширення місії організації має сформуватися її позитивний імідж серед клієнтів, контрагентів і власних працівників. 3. Найпоширенішим способом формулювання цілей розвитку організації є професійне створення (побудова) «дерева цілей», що адекватно демонструє у такий спосіб визначення стратегічних, оперативних і тактичних цілей та їхнє узгодження як за вертикаллю, так і за горизонталлю.

Причому, з одного боку, цілі організації в системі менеджменту - це «прогнозовані, плановані та бажані результати, які повинні бути досягнуті організацією і на досягнення яких спрямована її діяльність [20]. З іншого боку, − "діяльність зі стратегічного управління, пов'язана з постановкою цілей, завдань організації та підтримкою останньою взаємовідносин із оточенням, що відповідають її внутрішнім можливостям, дають змогу домагатися поставлених цілей та залишатися чутливою до зовнішніх вимог», - а це вже сфера повноважень ***стратегічного менеджменту (strategic management)*** [21].

Отже, вищевикладеній стратегії цілком відповідає виконання необхідного комплексу правил щодо ухвалення рішень, якими організація керується для своєї успішної діяльності, де безпосередньо процес перетворення (трансформації) на якість стратегічного менеджменту (див. рис. 8.16, який адаптований згідно [21, с. 10]) передбачає реалізацію таких етапів:

1) визначення місії корпорації;

2) конкретизацію дій корпорації та постановку цілей;

3) формування стратегії для досягнення кінцевих цілей;

4) реалізацію стратегії, спрямованої на досягнення намічених цілей;

5) оцінку результатів і зміну в разі потреби стратегічного плану та методів його реалізації.

Перший етап. ***Визначення місії організації***

Місію організації можна розглядати в широкому і вузькому сенсах. Під місією організації в широкому сенсі можна розуміти свого роду життєву філософію - цінності, вірування і принципи, відповідно до яких ця організація має намір здійснювати свою діяльність. Під місією організації у вузькому сенсі розуміють чітко сформульоване твердження, що пояснює, для чого існує ця організація і чим вона відрізняється від інших, подібних до неї. Єдиних загальноприйнятих підходів до вирішення проблеми оформлення місії не існує. Тому будемо дотримуватися вже озвученого вище, де місія, або суспільно значуща роль, підприємства (організації) являє собою якісно виражену сукупність основних цілей, наприклад, оптимізацію бізнесу. Тоді вона (місія), як соціально орієнтована функція організації, характеризує спроможності підприємства у сфері своєї діяльності за наявності можливих негативних впливів як з боку конкурентів, так і деструктивних впливів

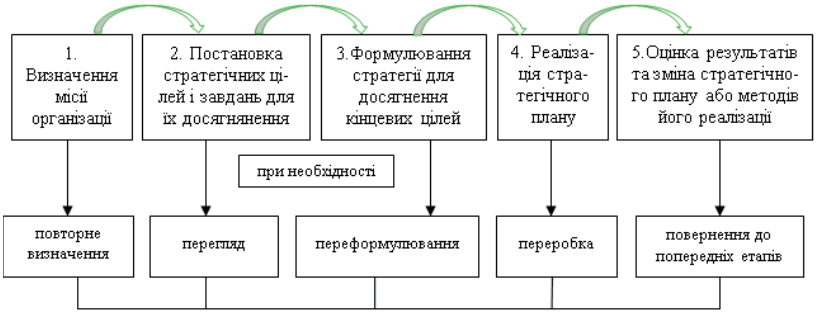

Рисунок 8.16. Процесс становления стратегического менеджмента

Задекларовані грамотні місії зазвичай враховують: загальні соціально-господарські цінності та принципи; оптимізацію своєї діяльності в площинах її ефективності та конкретних потреб соціуму; перспективні можливості позитивного розвитку виробництва та його соціальної сфери. Очевидно, що для довгострокової місії підприємства

знадобляться ще додаткові аспекти її реалізації, проте, тим не менш, наступним етапом процесу становлення стратегічного менеджменту є конкретизація (вибір) стратегічних цілей підприємства і завдань для їх досягнення.

Слід пояснити, що категорія «цілі» має загальнонауковий характер і не обмежується рамками менеджменту. Будь-яка свідома діяльність передбачає орієнтацію на досягнення результату і відповідно наявність цілей. У загальнонауковому плані мету можна розглядати як очікуваний результат свідомої діяльності. Тому слід (будемо) розглядати мету (або цілі) як категорії стратегічного менеджменту.

Тоді, мета розвитку організації - це конкретний стан організації в певному майбутньому, досягнення якого є бажаним, на що спрямовуються всі зусилля суб'єкта управління. При цьому показники, які можуть бути покладені в основу цілепокладання, слід визначати з огляду на те, що мета є значно конкретнішим поняттям, ніж місія, і, як правило, є вихідною категорією в процесі ухвалення управлінських рішень, здійснення планування та подальшого контролю. Так, наприклад, збільшення вартості активів організації - найпоширеніший показник підприємства. Збільшення прибутку є не менш поширеним показником. Позитивні зміни в діяльності працівників організації - ще один критерій, який може розглядатися як мета. Ці та інші показники можуть бути покладені в основу формування цілей розвитку організації [22].

Другий етап. ***Постановка стратегічних цілей і завдань для їх досягнення***

Однозначно зрозуміло, що на тлі благополучного розвитку підприємства (далеким від його виживання), безумовним пріоритетом, незримо присутнім у цільових настановах різної властивості, стає формулювання стратегічних цілей організації. При цьому принципова відмінність мети від місії (за їхньої органічної єдності, оскільки мета має випливати з місії) полягає в більшій динамічності першої (тобто мети) та істотно більшій невизначеності другої (тобто місії), оскільки конкретну мету можна позначити кількісними показниками. Якщо ж таких

показників не виявлено, то їх слід шукати більш професійно, або ж така мета сформульована неправильно. Правильно сформульована мета дає змогу розв'язувати завдання, що мають стратегічне значення для ефективної самоорганізації штатних співробітників, використовуючи: 1) деталізацію кінцевої мети (декомпозувавши її на складові) для кожного виконавця і 2) можливість, за необхідності, наскрізним способом реалізувати зворотний зв'язок у системі управління, створюючи в такий спосіб систему цілеорієнтованої мотивації трудової діяльності персоналу.

Цілі можна диференціювати за рівнями стратегії. Так, наприклад, у стратегічному менеджменті для сфери бізнесу розрізняють чотири рівні стратегії: ***перший (корпоративний)*** - притаманний компаніям, концернам, конгломератам, які функціонують у кількох сферах бізнесу, а їхні головні завдання - це вироблення рішень щодо видів та обсягів вироблюваного або закуповуваного товару, розробка планів диверсифікації, розрахунок стратегічної відповідності різних сфер бізнесу, глобальна оцінка фінансових ресурсів, з урахуванням якої будується управління цими ресурсами. Доцільно нагадати, що в широкому розумінні розуміння термін «диверсифікація» означає різноманіття, де, в контексті нашого викладу, його слід сприймати як процес проникнення організації в інші галузі виробництва і сфери діяльності з метою вберегти себе від потрапляння у надмірну залежність від якого-небудь обмеженого виду діяльності, неефективність у якому здатна призвести до неминучого провалу організації і навіть її загибелі; ***другий (бізнесовий),*** — це рівень перших керівників організацій (фірм), що входять до складу диверсифікованих організацій (компаній, конгломератів), головне завдання яких - забезпечити конкурентоспроможність своєї організації в рамках досягнення цілей корпорації; ***третій (функціональний)*** - це рівень керівників функціональних сфер, які розв'язують задачі у сфері маркетингу, управління персоналом, виробництва, фінансів, науково-дослідних, дослідницько-конструкторських робіт та ін.; ***четвертий (лінійний)*** - це рівень керівників підрозділів організації або її географічної мережі; четвертий (лінійний) - це рівень керівників підрозділів організацій або її географічно

віддалених частин - філій, представництв тощо, на якому розв'язуються завдання безпосередньо виробництва або реалізації продукції та послуг.

Основний принцип координації стратегічних цілей організації на всіх рівнях полягає в ієрархічній підпорядкованості цілей нижнього рівня цілям корпоративного рівня, де його (принципу) реалізація здійснюється за алгоритмом, коли стратегічні плани кожного наступного рівня узгоджуються з планами відповідного верхнього рівня. Причому, правильно сформулювати місію і стратегічні цілі організації без попереднього вивчення й аналізу як можливостей і потенціалу організації, так і зовнішнього середовища, що її оточує, дуже складно. Під час такого аналізу необхідно враховувати хоча б основні чинники, що впливають на процес стратегічного менеджменту організації з урахуванням зовнішнього середовища (див. рис. 8.17, який адаптований згідно [21, с. 14]). Останнє має велике значення і для третього етапу процесу стратегічного менеджменту.

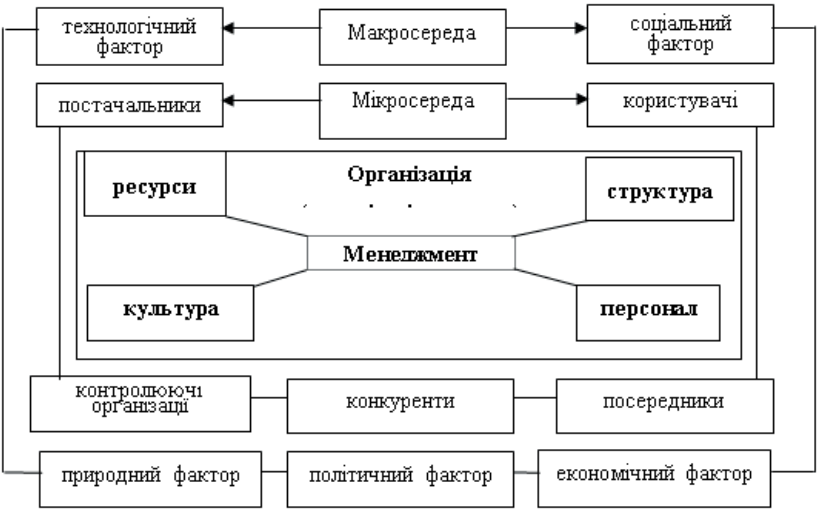

Рисунок 8.17. Основні фактори, що впливають на процес стратегічного менеджменту організації з урахуванням зовнішнього середовища

Третій етап. ***Формулювання стратегії для досягнення кінцевих цілей***, який найзручніше пояснити на прикладі діяльності комерційних організацій, що функціонують в умовах сучасної ринкової економіки (середовищі), де принципово важливим питанням (яке забезпечує процвітання, виживання або загибель цих організацій) є вибір оптимальної конкурентної стратегії у вигляді:

- лідерства за витратами, в основі якого одержання найбільшого прибутку при збереженні прийнятих стандартів якості та реалізації продукту або послуги за нижчою собівартістю, ніж у середньому по галузі;

- диференціації, де центральним моментом такої стратегії є розуміння потреб покупця, серед яких слід звертати увагу насамперед на цінову, прогресивно-модну унікальність і сезонність продукції. Усе це дає змогу збільшувати не тільки її ціну, але за оптимізації витрат підприємства, така надбавка до ціни сприяє збільшенню прибутковості.

- фокусування (фокусування), що має на увазі вибір сегмента або групи сегментів у галузі та задоволення потреб цього сегмента з більшою ефективністю, ніж конкуренти, які обслуговують ширший сегмент ринку. У зв'язку з цим можлива конкуренція за широким фондом (обслуговування декількох сегментів) або зосередження на вузькому напрямку (цілеспрямована дія). Обидва варіанти стратегії фокусування ґрунтуються на відмінностях між цільовими сегментами та рештою сегментів галузі.

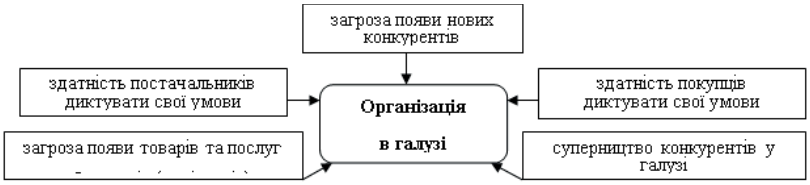

Рисунок 8.18. Структурно-функціональна схема дії п'яти сил (модель М. Портера), що визначають конкуренцію в галузі

Отже, наприклад, використовуючи структурно-функціональну схему дії п'яти сил, у вигляді моделі М. Портера (див. рис. 8.18, адаптованому з [21, с. 15]), можна цілком адекватно деталізувати конкурентну боротьбу в тій чи іншій галузі. Так фактично керівництву підприємства (організації) необхідно здійснити інформаційно-аналітичний вибір з альтернатив: чи застосовувати їм ухвалені стратегії на широкому ринку або на вузькому сегменті ринку, де сфокусована їхня діяльність. Ці можливості (альтернативи) в узагальненій формі наведено на рис. 8.19, який адаптований згідно [21, с. 16].

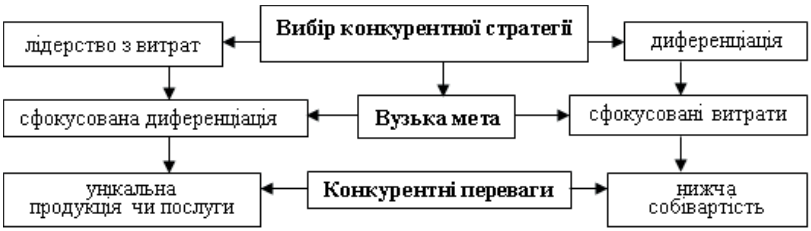

Рисунок 8.19. Конкурентні стратегії, адаптовано згідно [21, с.16].

Таким чином, головне на третьому етапі процесу стратегічного управління - сформулювати конкурентну стратегію, правильність вибору якої забезпечить організації успіх у конкурентній боротьбі. В іншому разі - такій організації (компанії, фірмі) загрожує стагнація, аж до її загибелі.

Четвертий етап. ***Реалізація стратегічного плану*****,** ефективність якої (реалізації) насамперед залежить від повноважень і компетенції керівника підприємства (організації), його здатності не тільки цілеспрямовано формувати добротну соціальну систему роботи з персоналом у процесі його життєдіяльності (у сфері освіти, освіченості й інших граней буття), а й забезпечувати гідне конкурентоспроможне функціонування підвідомчого підприємства, тобто бути його ***стратег-лідером***, який упроваджує й удосконалює штатну (задекларовану) концепцію ***стратегічного менеджменту***

підприємства на чіткій його ***методологічній основі*** (див. рис. 8.20, який адаптований згідно [21, с. 21]). При цьому роль стратега-лідера, повноваження якого адекватно збалансовані з відповідальністю, складно переоцінити.

У контексті викладеного доцільно викласти, а десь нагадати, що:

Рисунок 8.20. Структурно-функціональна схема основних складових системи стратегічного менеджменту організації

- під ***методологією стратегічного менеджменту*** слід розуміти сукупність узагальнених принципів, на яких будується система стратегічного управління організацією, де в менеджменті соціальної системи - це послідовність принципів: цільового управління організацією; доцільної діяльності персоналу; раціонального використання матеріальних ресурсів;

- під ***адекватною організаційною структурою*** слід розуміти таку, яка відповідає сучасній парадигмі організаційної структури, що забезпечує ефективність функціонування системи стратегічного менеджменту в організації;

- під ***адекватною управлінською культурою, стилем і цінностями*** в контексті рис. 8.20 перелічені складові системи стратегічного менеджменту в організації визначають насамперед необхідний (хоча часто далеко й не достатній) рівень компетенції керівника і стиль роботи задіяних підрозділів (структур) підприємства в його соціально-виробничій сфері;

- під ***системою роботи з персоналом*** слід розуміти реалізацію доцільної діяльності з персоналом, починаючи з його добору та розстановки, навчання та оцінки тощо в його (персоналу) виробничому процесі згідно з методологією стратегічного управління організацією.

П'ятий етап. ***Оцінка результатів і зміна стратегічного плану або методів його реалізації***, від результатів якого залежить зміст змін (або їх відсутність) на попередніх чотирьох етапах. На цьому етапі відслідковуються показники досягнення стратегічних цілей на всіх ієрархічних рівнях і плани розробок відповідних змін (модернізацій), за потреби починаючи з першого етапу - етапу визначення місії (див. рис. 8.16). Як правило, це бажано здійснювати вже тоді, коли поточна (планова або поза планом) оцінка одержуваних результатів та їхній адекватний аналіз формують достовірні підстави у правильності виробленої стратегії.

Таким чином, розглянуті питання стратегічного менеджменту в сучасній інтерпретації фахівців дають змогу одержати засадничі відомості щодо процесу стратегічного менеджменту в організаціях (на підприємствах) з урахуванням його взаємодії із зовнішнім середовищем і реалізації стратегічних задумів за допомогою внутрішнього механізму соціального управління. При цьому його (стратегічного менеджменту) поява і подальший процес становлення відбувався в умовах ускладнення зовнішніх чинників (передусім нестабільності та невизначеності зовнішнього середовища, посилення конкуренції, ускладнення потреб і відповідно виробництва цих потреб, підвищення впливу соціальних чинників тощо) на противагу та водночас на додаток до реактивного (оперативного) управління. Останнє, як відомо [21], зводиться до реакції тільки на поточні події, що часто призводить організації до важких ситуацій, яких усе ж таки можна було б уникнути за умови розвитку організаціями стратегічного менеджменту.

8.3. Стратегічні альтернативи розвитку підприємства та оцінка ефективності стратегій

Очевидно, що вже в процесі стратегічного аналізу керівництво організації схиляється до вибору одного з можливих варіантів стратегії - того, що найбільшою мірою відповідає умовам зовнішнього та внутрішнього середовища, а також обраним цілям діяльності організації, окреслюючи в такий спосіб подальші етапи її формування та реалізації. Зазвичай такий вибір стратегії розвитку підприємства (організації, фірми) може бути зведений до трьох основних типів стратегії: або до ***стратегії стабільності***, або ***зростання,*** або **скорочення** (див. рис. 8.21, який адаптований згідно [23, частина 2, с.3]). При цьому в кожної з цих альтернатив існують свої варіанти реалізації або экспансии. *,38,

Так: **- *стратегія стабільності*** зосереджена на наявних напрямах діяльності організації та збереженні конкурентної позиції на ринку. Застосовується в зрілих галузях промисловості зі статичною технологією, компаніями, задоволеними своїм становищем; **- *стратегія зростання*** відповідає збільшенню організації, часто шляхом проникнення і захоплення нових ринків з метою збільшення обсягу продажів, частки ринку, прибутку тощо, використовуючи перевищення (зростання) рівня свого розвитку над попереднім періодом; **- *стратегія скорочення*** є за своєю суттю стратегією відступу і застосовується в тих випадках, коли виживання організації перебуває під загрозою, у зв'язку з чим змушені передбачати встановлення рівня цілей організації, нижчого за досягнуті раніше.

Причому (див. рис. 8.22, який адаптований згідно [23, с. 6]):

---

*38 Звичайно використовують такі синоніми для експансії: розширення; розвиток; зростання; поширення; збільшення; підйом; розгортання; нарощування.

- ***стратегію інтенсивного зростання*** реалізують за рахунок проникнення на ринок, розширення меж ринків, шляхом підвищення конкурентоспроможності продукції (товару) тощо;

Рисунок 8.21. Структурно-функціональна схема стратегічних альтернатив

- стратегію інтеграційного зростання забезпечують або шляхом набуття власності, наприклад, за допомогою приєднання до неї або компаній-постачальників сировини, матеріалів і напівфабрикатів (стратегія зворотної вертикальної інтеграції), або збутових фірм (стратегія прямої інтеграції), або шляхом розширення (модернізації) зсередини. Коли одночасно реалізуються обидві ці стратегії, то заведено вважати, що створено вертикально інтегровану систему;

- ***стратегія диверсифікаційного зростання***, на відміну від інтеграційного зростання, передбачає вихід за рамки галузевого технологічного ланцюжка, використовуючи можливості, що відкриваються поза зоною традиційної діяльності підприємства (фірми), тобто за межами галузі.

Принято выделять три вида стратегии диверсификации*:*

- горизонтальную, которая предусматривает расширение существующего ассортимента продукции или услуг новыми товарами или услугами, которые не связаны с действующим ассортиментом, но представляют интерес для потребителей;

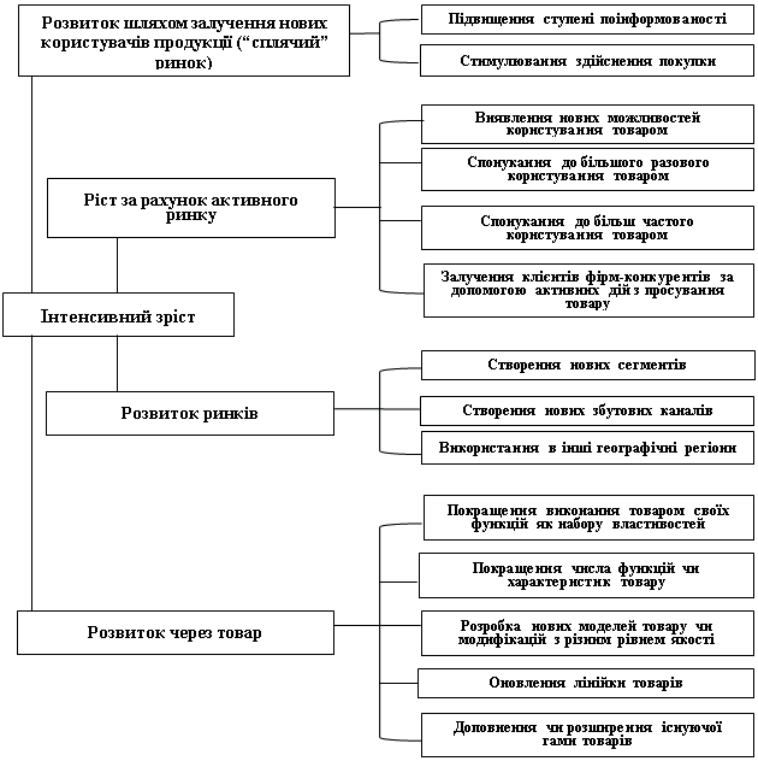

Рисунок 8.22. Джерела інтенсивного зростання

- ***концентричну,*** яка передбачає під час виходу фірми за рамки свого промислового ланцюжка наявність стратегічних відповідностей у технологічному та/або комерційному плані між наявною діяльністю та новими сферами бізнесу, розширюючи потенційний ринок і домагаючись ефекту синергії в такий спосіб;

- ***конгломератну,*** метою якої є оновлення господарської діяльності для отримання більшого прибутку та зниження

ризику, причиною якого може стати взаємопов'язаність і взаємозалежність окремих видів виробництва.

Таким чином, кожному підприємству зі своєю складною багатофункціональною системою потрібна адекватно збалансована стратегія його діяльності, яку (стратегію) можна назвати ***генеральною стратегією***. Останню деталізують за допомогою функціональних (робочих) стратегій, які відображають конкретні шляхи досягнення специфічних цілей підприємства, що стоять перед його окремими підрозділами і службами. Кожній такій робочій стратегії відповідає своя конкретна сфера функціонального впливу, унаслідок чого виокремлюють насамперед основні (хоча існують й інші) функціональні стратегії у вигляді:

- стратегії маркетингу, як способу досягнення оптимальної реалізації ринкової діяльності завдяки адекватному вибору стратегічних напрямів розвитку та стратегічних зон господарювання, у тому числі у сфері конкурентних переваг та опанування нових перспективних ринків***;***

- фінансової стратегії, як напряму і способу використання коштів для досягнення поставлених цілей управління фінансами підприємства, що не суперечать як ефективному використанню фінансових ресурсів, так і під час реалізації поставлених цілей, наприклад, у вигляді максимізації прибутку за мінімізації витрат, оптимізації структури активів підприємства, забезпечення фінансової стабільності підприємства в довгостроковій (осяжній) перспективі тощо;

- ***стратегії інновацій***, як взаємопов'язаного комплексу технічних, технологічних і організаційних дій, спрямованих на забезпечення конкурентоспроможності підприємства та сталого його розвитку в площині реалізації теорії життєвого циклу продукту, ринкової позиції фірми та науково-технічної політики, яку вона проводить;

- стратегії виробництва, як комплексу взаємопов'язаних заходів щодо вибору продукції (послуг), технології та організації конкурентноспроможного виробництва, що дають змогу забезпечити сталий ефективний розвиток підприємства.

- стратегії організаційних змін, реалізованої як багаторівнева система перетворень, що передбачають можливі

зміни в організаційній структурі управління, у методах роботи, в організаційно-соціальній культурі та життєдіяльності персоналу підприємства.

Очевидно, що наведений вище перелік (набір) функціональних стратегій, можна розширити, - проте їхній вибір та актуальність реалізації насамперед визначатиметься компетенцією керівництва, специфічними цілями підприємства та соціальним кліматом виробництва. При цьому неправильний вибір ***стратегічного рішення*** може призвести до наслідків, що не відповідають очікуваним. Крім прямого збитку, що мета стратегії не буде досягнута (а ресурси вже витрачено), проявляються додаткові негативні фактори, наприклад, у вигляді дискредитації не тільки особи (експертів), яка приймає рішення, а й інших осіб, відповідальних за розробку та реалізацію стратегії. У зв'язку з цим потреба в оцінюванні стратегічних рішень стає додатково вкрай необхідною, а її оцінювання зазвичай здійснюють за критерієм ефективності у вигляді комплексного показника ступеня досягнення цілей організації [18].

Для повноти й достовірності подальшого сприйняття того, що викладається, уточнимо такі поняття, що використовуються тут і далі:

- ***ефект*** (поза фізичним його сприйняттям - інтерпретацією) - це певний результат у його матеріальному, грошовому, соціальному вираженні, зафіксований у сфері життєдіяльності суспільства;

- ***ефективність*** - це сприйняття відносного ефекту як (у вигляді) результативності процесу (чи то операції, проєкту тощо), що визначається як відношення очікуваного (або вже досягнутого) результату до сумарних витрат (видатків), які зумовили його отримання;

- ***ефективність стратегічного управлінського рішення*** - це відношення результату виконання стратегічного управлінського рішення (РСУР - ефекту при досягненні мети) до витрат на його розроблення та реалізацію (див. рис. 8.23, який адаптований згідно [18, с. 85]).

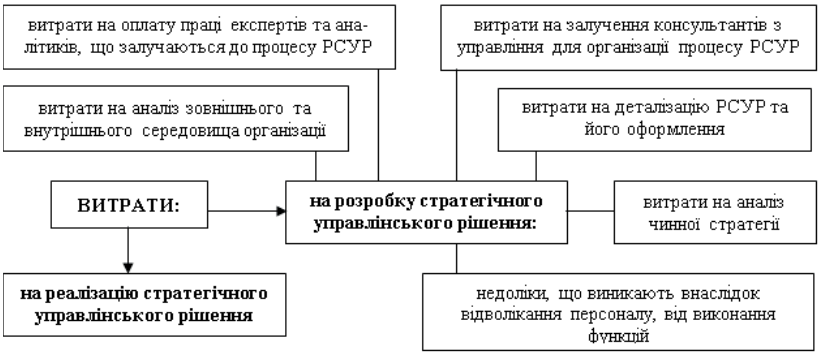

Рисунок 8.23. Витрати, пов'язані з розробленням і реалізацією стратегічного управлінського рішення (РСУР)

Як правило, оцінку ефективності реалізації стратегії проводять за трьома напрямами у вигляді:

1) ефективності реалізації стратегічної програми, шляхом аналізу (оптимізації) часткових від співвідношень за чотирма параметрами: - за вартістю реалізації програми порівняно з її вихідним бюджетом; - за термінами реалізації програми порівняно з первісно запланованими; за розміром отриманого ефекту від програми порівняно з очікуваними результатами; за обсягом сторонніх (несподіваних) ефектів, що виникли під час реалізації конкретної стратегічної програми;

2) ступеню досягнення поставлених стратегічних цілей, виокремлюючи середньо- і довгострокові показники, але в найзагальнішому вигляді;

3) ступеня відповідності поставлених стратегічних цілей інтересам стейкхолдерів: як власників (завдяки системі фінансових показників результативності) і держави, так і споживачів (включно зі штатними співробітниками та членами їхніх сімей).

Очевидно, що розроблення та реалізація рішень, які забезпечують довготривалу високу ефективність, - важке завдання навіть для ***досвідчених керівників,*** оскільки з багатьох причин (***ризиків***) ефект може не відповідати очікуваному результату, але прагнення до його максимізації має бути

постійним і продуктивним. У зв'язку з цим адекватну діяльність з боку, наприклад, вищого керівництва на стадії реалізації стратегії можна представити у вигляді п'яти послідовних етапів (рис. 8.24, який адаптований згідно [18, с. 91]).

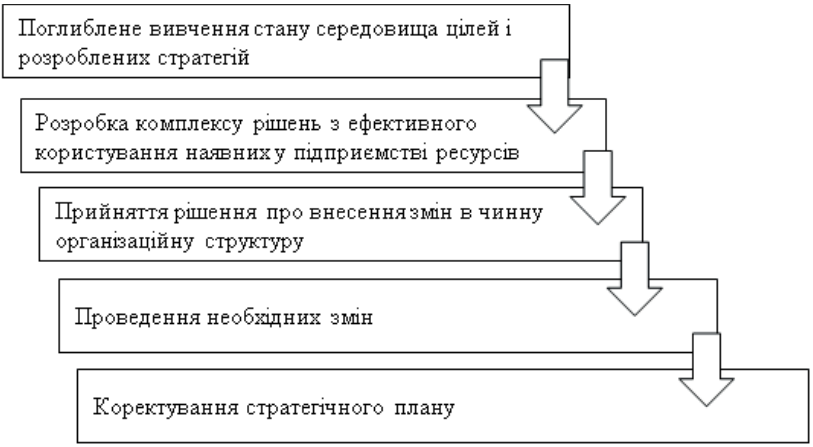

Рисунок 8.24. Етапи процесу реалізації стратегії з боку вищого керівництва

На першому етапі (*у вигляді поглибленого вивчення стану середовища, цілей і розроблених стратегій*) розв'язують переважно завдання: - з'ясування сутності планованих цілей, вироблених стратегією, їхньої коректності, взаємовідповідності та адекватності стану середовища; - коректного обговорення ідей і цілей стратегічного плану серед штатних працівників підприємства для підготовки оптимальних умов для їхнього залучення в майбутній процес реалізації стратегій. Фактично виявляються фактори та умови, які здатні вплинути на процес реалізації стратегії. Зокрема, під час аналізу таких факторів їх зазвичай класифікують за такими ознаками: 1) *за джерелом виникнення* або на внутрішні (ендогенні), тобто підконтрольні вищому рівню управління організацією, або на зовнішні (екзогенні), які перебувають поза сферою вищого рівня управління організацією; 2) *за ступенем об'єктивності* або переважно об'єктивні, або переважно суб'єктивні; 3) *за*

елементами організаційної системи як входи (ресурсні фактори), як процесори (процесні фактори), як виходи (результативні фактори); 4) *за характером впливу* на організацію у вигляді стимулюючих (що сприяють розвитку організації) або дестимулюючих (що перешкоджають розвитку організації).

На другому етапі (*у вигляді розроблення комплексу рішень щодо ефективного використання наявних у підприємства ресурсів*) проводять оцінювання ресурсів, їх розподіл і приведення у відповідність до реалізованих стратегій за допомогою створення та реалізації спеціальних програм, спрямованих на розвиток ресурсів, наприклад, для підвищення кваліфікації співробітників.

На третьому етапі вище керівництво *ухвалює рішення про внесення змін до чинної організаційної структури* та до процесів з метою досягнення найкращих результатів з реалізації стратегії, виділяючи при цьому чотири основні типи стратегічних змін: 1). *Реорганізацію (перебудову) підприємства*, починаючи зі зміни місії, організаційної культури, найчастіше навіть галузі і, відповідно, продукту, місця на ринку тощо; 2). *Радикальне перетворення підприємства,* яке здійснюють на стадії виконання стратегії в тому разі, якщо організація не змінює галузі, але водночас відбуваються зміни, наприклад, спричинені злиттям підприємства з аналогічною організацією, що загрожує сильними внутрішньоорганізаційними змінами. 3). *Помірне перетворення*, яке здійснюють, як правило, тоді, коли підприємство виходить на ринок із новим продуктом і, прагнучи завоювати для нього покупців, вимушене адаптувати під них свій виробничий процес і маркетинг; 4). *Звичайні зміни*, які не є істотними, оскільки пов'язані з проведенням перетворень у маркетинговій сфері для підтримання інтересу до продукту.

На четвертому етапі (*етапі проведення необхідних змін* на підприємстві, без яких неможливо розпочати реалізацію стратегії) складають апріорний сценарій можливого спротиву плановим змінам і розробляють відповідний алгоритм заходів щодо їхнього демпфірування, тобто зведення до мінімуму можливого опору, та закріплення проведених змін.

П'ятий етап - *коригування стратегічного плану*, який реалізується в тому разі, коли настійно цього вимагають обставини, що знову виникли (раніше не передбачені).

Зазначимо, що перелічені етапи процесу реалізації стратегії в будь-якій організації (підприємстві) хоч і є очевидними, але їхня ймовірність здійснення на тлі (див., наприклад, таблицю 8.2) невизначеності апріорних ризиків, що впливають на успішну реалізацію конкретної стратегії (особливо з позицій захисту і загальної безпеки від них), - це величезна поточна робота, починаючи з формулювання і місії, і цілей, і завдань, і т. ін., із необхідною подальшою їхньою реалізацією, наприклад, використовуючи SMART-технологію [18, с.93] під час формулювання тільки цілей стратегії. Значення абревіатури «SMART» наведено в таблиці 8.3., де Specific (конкретна), Measurable (вимірювана), Achievable (досяжна), Relevant (порівнянна), Timebound (визначена в часі).

Таблиця 8.2. Облік ризиків реалізації стратегії на прикладі відкриття SPA-салону[*,39],

Види ризиків	**Характеристика ризикової ситуації**	**Заходи профілактики**	**Варіанти виходу**
Комерційні	- зниження попиту; - посилення позицій конкурентів	– дослідження ринку; – реклама; - гнучка цінова політика; - стимулювання збуту	- зниження цін; – спеціальні акції, заходи, майстер-класи
Финансовые	- інфляція; - непередбачені витрати; - високі налоги	– податкове планування; - формування резервів;	підвищення цін

*[39] SPA або Sanitas Per Aquam латиною в буквальному перекладі означає «здоров'я через воду». Під словом SPA мають на увазі цілий комплекс процедур, кожна з яких впливає на відновлення гармонії між душею і тілом. Зазвичай це варіативні масажі, водні та косметичні процедури, методика яких спрямована на максимальне розслаблення.

Види ризиків	Характеристика ризикової ситуації	Заходи профілактики	Варіанти виходу
		- фінансове планування	
Виробничі	- вихід обладнання з ладу; - погіршення якості обслуговування	своєчасні планові огляди та міжремонтне обслуговування	– срочный ремонт; заключение новых трудовых договоров
Форс-мажорні	– пожежа; - крадіжка; – збій роботи комунальних мереж	- страхування; - встановлення пожежної та охоронний сигналізації	- отримання страхових виплат; - відновлення
Організаційні	- плинність кадрів, нестача майстрів; - конфлікти всередину колективу	– чітке розуміння мети; - формування ефективної системи мотивації; – підвищення рівня майстерності співробітників	- поліпшення умов праці; – пошук компромісів

На жаль, доволі часто цілі ототожнюють із завданнями, проте завданню властивий процес виконання конкретної послідовності операцій (алгоритму розв'язання), а цілі - відображення конкретного кінцевого стану. Тому постановка мети діяльності, наприклад, підприємства, є показником усвідомлених дій суб'єкта, тоді як завдання - це приписана робота або частина роботи (процедури), що має бути виконана заздалегідь встановленим способом і в обумовлені терміни.

Таблиця 8.3 - Критерії SMART

S - specific (конкретна)	Ціль повинна бути конкретною. Працівники, залучені до процесу її досягнення, повинні розуміти, в чому вона полягає.
M - measurable (вимірювана)	Ціль повинна бути вимірюваною. Працівники, залучені до процесу її досягнення, повинні розуміти, досягнута вона чи ні.
A - achievable (досяжна)	Ціль повинна бути досяжною. Працівники, залучені до процесу її досягнення, повинні мати відповідні ресурси (час, засоби, бюджет тощо).
R - relevant (релевантна / співвідносна)	Ціль повинна співвідноситися з більшою загальною стратегічною метою та спрямовуватися на її досягнення.
T - timebound (обмежена в часі)	Для кожної цілі повинні бути визначені часові рамки.

У контексті нашого викладу завдання - це конкретизація шляхів розв'язання проблемної ситуації і воно завжди виходить із мети, будучи засобом її реалізації. Тому спочатку обирають мету, як визначення напряму роботи, виходячи з якої, з урахуванням реальних можливостей, вибудовують послідовність (ланцюжок) завдань, успішна реалізація яких забезпечує досягнення планованої мети. Остання (тобто мета) має характеристику у вигляді конкретності кінцевого результату з притаманною йому часткою невизначеності і є безпосереднім наслідком потреби суб'єкта. Отже, мета вказує на кінцевий результат, а розв'язання кожного завдання наближає суб'єкта до цього результату. При цьому дуже важливим є процес формулювання і цілей, і завдань.

Перераховані вище критерії SMART - це відображення, мабуть, найпопулярнішої концепції сучасного менеджменту, що

має назву «Управління за цілями» або «Goal management» [18, с.69].

8.4. Основи управління персоналом та аспекти кадрової атестації у сфері інформаційно-логістичної безпеки

У практичній діяльності сучасної спільноти людей із розвиненою системою ситуаційного та стратегічного менеджменту безперечно беззаперечною вимогою залишається її безпека, особливо необхідна в процесі реалізації (з досить високим рівнем невизначеності) інформаційно-логістичної, виробничо-економічної та соціально-моральної сфер життєдіяльності соціуму. При цьому, особливо в галузі інформаційно-логістичної діяльності підприємства найбільш непередбачуваними і негативними впливами слід вважати атаки з боку штатних співробітників організації, так званого людського чинника. У зв'язку з чим, кадровий добір, особливо для підприємств (об'єктів) критичної інфраструктури, має бути не просто рутинною процедурою приймання до роботи з подальшими регулярно плановаными атестаціями (іноді вельми формальними), а дуже значущою інформаційно-аналітичною роботою в процесі створення адекватної сучасної сфери інституційної, організаційної, ціннісної, гносеологічної та професійно-технічної діяльності на виробництві.

На жаль, навіть у класичних моделях стратегічного управління виробництвом, серед яких найбільшого поширення набули моделі Ф. Девіда (рис. 8.25), Д. Томпсона (рис. 8.26), К. Ендрюса (рис. 8.27), Р. Лінча (рис. 8.28), В. Єфремова (рис. 8.29) [18, с.21], слабко приділяють увагу захисним заходам, які є вкрай необхідними для безпечного розвитку підприємства на основі безперервного контролю й оцінки змін, що відбуваються в його діяльності, з метою підтримання адекватної спроможності до виживання й ефективного функціонування в умовах апріорі нестабільного довкілля.

Як свідчить практика, у контексті людського фактора, реальний рівень забезпечення безпеки функціонування підприємства багато в чому визначається або недостатнім

моральним розвитком певної частини працівників підприємства, або можливою некомпетентністю керівників, або спільною реалізацією їхньої негативної сингулярності.

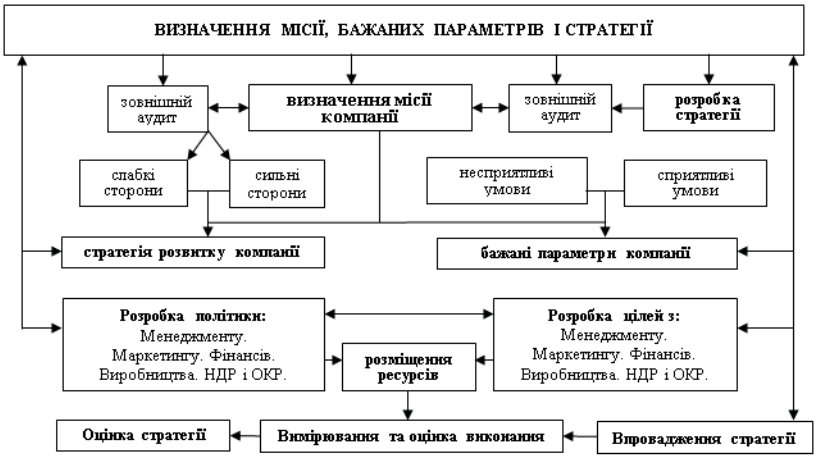

Рисунок 8.25. Модель стратегічного управління Девіда, яка, за його визначенням, має ефективно капіталізувати сильні сторони та забезпечувати подолання слабких сторін компанії

Особливо це позначається (загрожує) на рівень бездоганної роботи інформаційної системи підприємства, насамперед із боку підрозділів із засобами обчислювальної техніки, для якої режим її безпечної експлуатації та супутніх надійних засобів захисту вкрай необхідний.

Очевидно, що безпека багато в чому залежить як від структури персоналу, його безпосередніх штатних співробітників (кадрів), залучених до інформаційної логістики підприємства, так і від алгоритму їхнього прийому на роботу і подальших атестацій.

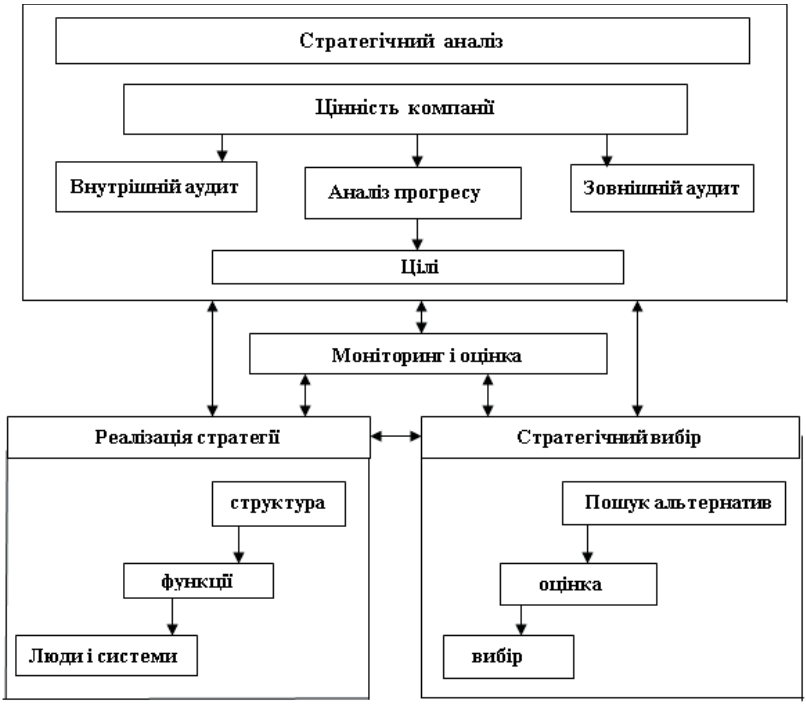

Рисунок 8.26. Модель стратегічного управління Томпсона як динамічна сукупність взаємопов'язаних етапів, що логічно слідують один за одним зі стійким зворотним зв'язком і взаємовпливом на етапи і процес управління

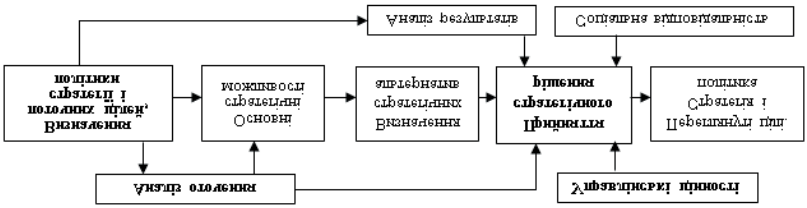

Рис. 8.27. Модель стратегічного управління Ендрюса яка розставляє акценти про зовнішню оцінку, що складається із загроз і можливостей у навколишньому середовищі, та про внутрішню оцінку сильних і слабких сторін організації

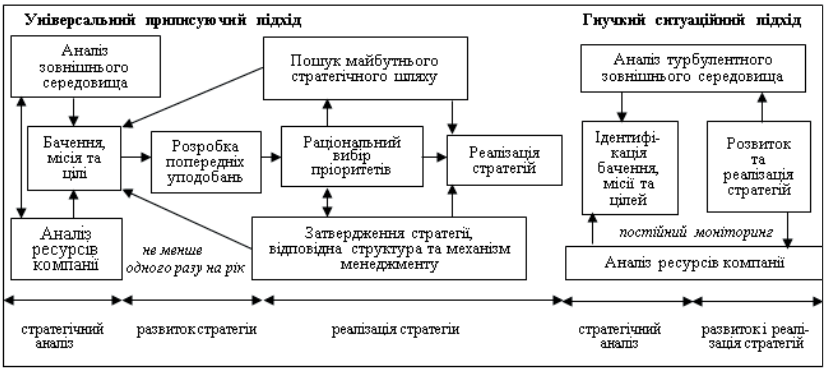

Рисунок 8.28. Модель стратегічного управління Р. Лінча у вигляді довгострокового моніторингу (як універсальний розпорядчий підхід) і постійного моніторингу (як ситуаційний підхід).

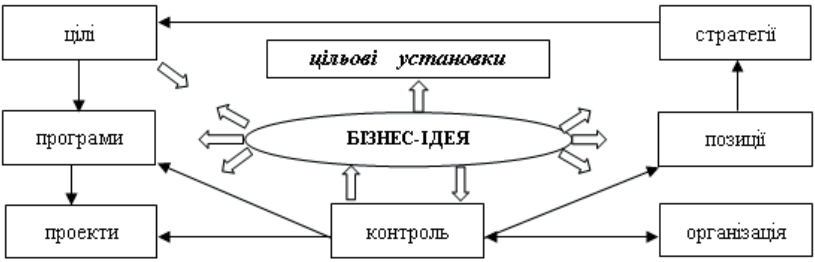

Рисунок 8.29. Модель стратегічного управління В. Єфремова, де вихідним пунктом є бізнес-ідея, як «душа» будь-якої виробничо-комерційної діяльності, що забезпечує цільові установки організації з контролем і аналізом, а за необхідності і з коригуванням програм, проектів та організаційного забезпечення

Як свідчить практика, персонал на підприємстві (як штатний склад працівників), що виконує його різноманітні виробничо-господарські функції, має свою статистичну та

аналітичну структуру, наприклад, у вигляді тієї, що наведена на рис. 8.30, який адаптований згідно [23, с. 4].

Рисунок 8.30. Структура персоналу

В основу структурування персоналу покладено їхню участь у виробничому або управлінському процесі, тобто характер трудових функцій (за обійманою посадою). У такому разі весь персонал можна розглядати за категоріями аналітичним і статистичним, де для останнього випадку (статистичного) передбачено додаткові ознаки участі у виробничому або управлінському процесі. Отже (див. рис. 8.29), за характером трудових функцій, а отже, і обійманої посади, весь персонал можна подати за такими категоріями: - **керівники,** які здійснюють функції загального управління, яким зазвичай передбачено три рівні: ***вищий*** (зазвичай це директор, генеральний директор, керуючий та їхні заступники), ***середній*** (керівники основних структурних підрозділів - відділів,

управлінь, цехів, а також головні фахівці) і ***низовий*** (ті, хто працює з виконавцями як керівники бюро, секторів; майстри). Крім того, до числа керівників належать особи, які обіймають посади **менеджерів**, зокрема менеджера з персоналу; - ***фахівці*** – це особи, які здійснюють економічні, інженерно-технічні, юридичні та інші функції, тобто економісти, юристи, інженери-технологи, інженери-механіки, бухгалтери, диспетчери, аудитори, інженери з підготовки кадрів, інспектори з кадрів тощо; - ***інші службовці (технічні виконавці)***, які здійснюють підготовку та оформлення документів, облік, контроль, господарське табельника та ін.; - ***робітники,*** які безпосередньо створюють матеріальні цінності або надають послуги виробничого характеру, у зв'язку з чим розрізняють основних і допоміжних робітників.

Крім того, в окрему категорію входять працівники соціальної інфраструктури, тобто особи, зайняті неосновною діяльністю (культурно- побутовим, житлово-комунальним обслуговуванням персоналу організації). До них належать працівники ЖКО та особи, які обслуговують дитячі садки, бази відпочинку тощо, що перебувають на балансі організації. Так, наприклад, у промисловості керівники, фахівці, інші службовці (технічні виконавці), робітники утворюють промислово-виробничий персонал, а працівники соціальної інфраструктури - непромисловий персонал. Причому очевидно, що будь-якій конкурентноздатній організації також необхідне адекватне управління своїм персоналом, яке, як правило, реалізується за допомогою сучасної ***системи управління персоналом (СУП).***

Система управління персоналом - передбачає формування цілей, функцій, організаційної структури управління персоналом, розроблення концепції та стратегії кадрової політики, сукупність принципів і методів управління кадрами в організації і може бути представлена структурною схемою рисунка 8.31, який адаптований згідно [23, с. 12]. При цьому безпосереднє формування системи управління персоналом здійснюють, як правило, відповідно до принципів у вигляді: - багатопланового підходу при створенні комплексної системи, яка зобов'язана відповідати вимогам підприємства і його співробітників, підтримуючи позитивну соціальну сферу їхнього буття; - чіткого

(бажано поетапного) алгоритму реалізації процесу управління персоналом, коли кожен співробітник розуміє свої завдання і терміни їх виконання, а також перспективи у своїй професійній кар'єрі.

Рисунок 8.31. Структурна схема системи управління персоналом

Очевидно, що в процесі позитивної реалізації зазначених вище принципів, керівництву підприємства вдається не тільки домогтися більших успіхів на підприємстві, а й удосконалювати свою ***кадрову стратегію і політику.*** На практиці *кадрова стратегія* (у рамках концепції досягнення головної мети організації під час розв'язання проблем і розподілу необхідних для цього ресурсів) являє собою систему управлінських та організаційних рішень, спрямованих на реалізацію місій, цілей і завдань підприємства. Типові завдання кадрової стратегії наведено на рис. 8.32, який адаптований згідно [23, с.13].

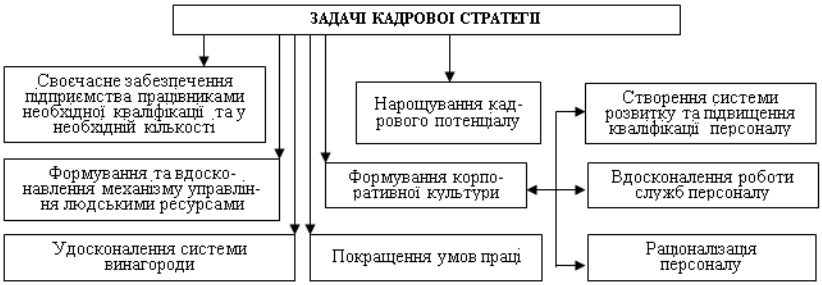

Рисунок 8.32. Завдання кадрової стратегії

Терміну *"кадрова політика"* подвійне тлумачення, або широке, у вигляді системи принципів і норм, що приводять людський ресурс у відповідність до стратегії підприємства (фірми), або вузьке - як набір конкретних правил, побажань та обмежень у взаємовідносинах людей і організацій.

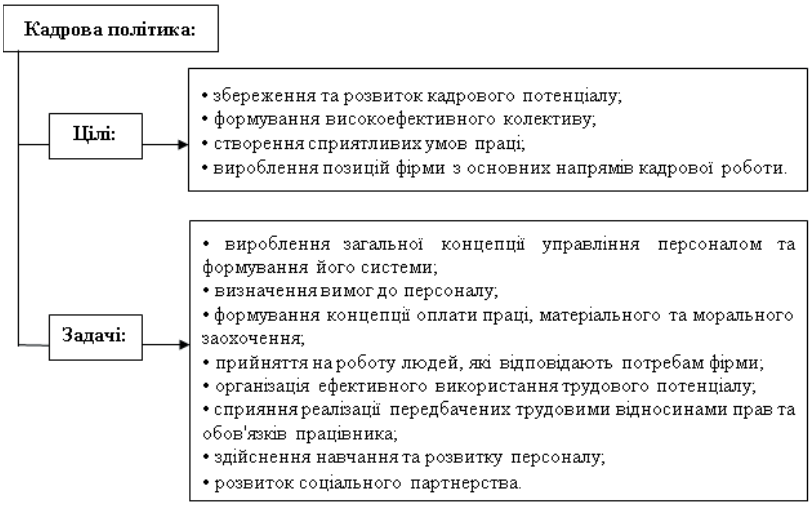

Рисунок 8.33. Цілі та завдання кадрової політики

Тому кадрова політика (як і будь-яка політика) у нашому випадку визначає генеральну лінію і принципові настанови в

роботі з персоналом на тривалу перспективу, а її основні цілі та завдання наведені на рисунку 8.33, який адаптований згідно [23, с.15]. При цьому, для успішної реалізації кадрової політики розроблено відповідні принципи управління персоналом (див. Табл. 8.4.), а зміст інформаційного забезпечення системи управління персоналом (СУП) представлено на рис. 8.34, згідно [23, с.32].

Отже, процес управління персоналом (його зміст) можна уявити у вигляді безлічі узгоджених, постійно ухвалюваних і реалізованих рішень, спрямованих зрештою на досягнення головної мети функціонування підприємства, де вироблення кожного з цих рішень має бути забезпечено відповідною службовою інформацією.

Таблиця 8.4.1 - Принципи побудови системи управління персоналом в організації.

1.1	обумовленості функцій управління персоналом цілями виробництва	функції управління персоналом формуються і змінюються не довільно, а відповідно до потреб і цілей виробництва.
1.2	первинності функцій управління персоналом	склад підсистем системи управління персоналом, організаційна структура, вимоги до працівників та їх чисельність залежать від змісту, кількості та трудомісткості функцій управління персоналом
1.3	оптимальності співвідношення інтрафункцій управління персоналом	визначає пропорції між функціями, спрямованими на організацію системи управління персоналом (інтрафункції), та функціями управління персоналом (інфрафункції)
1.4	оптимального співвідношення управлінських орієнтацій	диктує необхідність випередження орієнтації функцій управління персоналом на розвиток виробництва в порівнянні з функціями, спрямованими на забезпечення функціонування виробництва
1.5	потенційних імітацій	тимчасове вибуття окремих працівників не повинно переривати процес здійснення будь-яких функцій управління. Для цього кожен працівник системи управління персоналом повинен вміти імітувати функції вищестоящого, нижчестоящого співробітника і одного-двох працівників свого рівня

1.6	економічності	передбачає найбільш ефективну та економічну організацію управління персоналом, зниження частки витрат на систему управління в загальних витратах на одиницю продукції, що випускається, підвищення ефективності виробництва. У разі якщо після заходів щодо вдосконалення системи управління персоналом збільшилися витрати на управління, то вони повинні перекривати ефект у виробничій системі, отриманий в результаті їх здійснення.
1.7	прогресивності	відповідність системи управління персоналом передовим закордонним і вітчизняним аналогам
1.8	перспективності	при формуванні системи управління персоналом слід враховувати перспективи розвитку організації
1.9	комплексності	при формуванні системи управління персоналом необхідно враховувати всі фактори, що впливають на систему управління (зв'язки з вищими органами, договірні зв'язки, стан об'єкта управління тощо)
1.10	оперативності	своєчасне прийняття рішень щодо аналізу та вдосконалення системи управління персоналом, що попереджають або оперативно усувають відхилення
1.11	оптимальності	багатоваріантне опрацювання пропозицій щодо формування системи управління персоналом та вибір найбільш раціонального варіанту для конкретних умов виробництва
1.12	простоти	чим простіша система управління персоналом, тим краще вона працює. Безумовно, це виключає управління системи управління персоналом на шкоду виробництву
1.13	науковості	розробка заходів щодо формування системи управління персоналом повинна ґрунтуватися на досягненнях науки в галузі управління та з урахуванням змін законів розвитку суспільного виробництва в ринкових умовах
1.14	ієрархічності	у будь-яких вертикальних розрізах системи управління персоналом має забезпечуватися ієрархічна взаємодія між ланками управління (структурними підрозділами або окремими керівниками), принциповою характеристикою якої є несиметрична передача інформації

		«вниз» (дезагрегування, деталізація) «вгору» (агрегування) по системі управління
1.15	автономності	у будь-яких горизонтальних і вертикальних розрізах системи управління персоналом повинна забезпечуватися раціональна автономність структурних підрозділів або окремих керівників.
1.16	узгодженості	взаємодія між ієрархічними ланками по вертикалі, а також між відносно автономними ланками системи управління персоналом по горизонталі повинні бути в цілому узгоджені з основними цілями організації і синхронізовані в часі.
1.17	стійкості	для забезпечення сталого функціонування системи управління персоналом необхідно передбачати спеціальні «локальні регулятори», які при відхиленні від заданої мети організації ставлять того чи іншого працівника або підрозділ у невигідне становище і спонукають їх до регулювання системи управління персоналом.
1.18	багатоаспектності	управління персоналом, як по вертикалі, так і по горизонталі, може здійснюватися за різними каналами: адміністративно-господарським, економічним, правовим тощо.
1.19	прозорості	система управління персоналом повинна мати концептуальну єдність, містити єдину доступну термінологію, діяльність усіх підрозділів і керівників повинна будуватися на єдиних «несучих конструкціях» (етапах, фазах, функціях) для різних за економічним змістом процесів управління персоналом.
1.20	комфортності	система управління персоналом повинна забезпечити максимум зручностей для творчих процесів обґрунтування, розробки, прийняття та реалізації рішень людиною. Наприклад, вибірковий друк даних, різноманітність обробки, спеціальне оформлення документів з виділенням істотної інформації, їх гармонійний зовнішній вигляд, виключення зайвої роботи при заповненні документів тощо.

Таблиця 8.4.2 - Принципи, що визначають напрямки розвитку системи керування персоналом.

2.1	концентрації	розглядається у двох напрямках: концентрація зусиль працівників окремого підрозділу або всієї системи управління персоналом на вирішення основних завдань або як концентрація однорідних функцій в одному підрозділі системи управління персоналом, що усуває дублювання.
2.2	спеціалізації	розподіл праці в системі управління персоналом (виділяється праця керівників, фахівців і службовців). Формуються окремі підрозділи, що спеціалізуються на виконанні груп однорідних функцій.
2.3	паралельності	передбачає одночасне виконання окремих управлінських рішень, підвищує оперативність управління персоналом.
2.4	адаптивності (гнучкості)	означає пристосованість системи управління персоналом до мінливих цілей об'єкта управління та умов його роботи.
2.5	наступності	передбачає загальну методичну основу проведення робіт з удосконалення системи управління персоналом на різних її рівнях і різними фахівцями, стандартне їх оформлення.
2.6	безперервності	відсутність перерв у роботі працівників системи управління персоналом або підрозділу, зменшення часу пролежування документів, простоїв технічних засобів управління тощо.
2.7	ритмічності	виконання однакового обсягу робіт через рівні проміжки часу та регулярність повторення функцій управління персоналом.
2.8	прямо точності	впорядкованість і цілеспрямованість необхідної інформації для вироблення певного рішення. Вона буває горизонтальною і вертикальною (взаємозв'язки між функціональними підрозділами і взаємозв'язки між різними рівнями управління).

Таким чином, на загальному тлі існування *технічного забезпечення, правового забезпечення, соціального та інших видів (типів, засобів) забезпечення*, ***інформаційне забезпечення*** системи управління персоналом (ІОСУП) потребує серйозних ефективних заходів захисту. Оскільки ІОСУП складається з оперативної інформації, нормативно-довідкової інформації,

різних класифікаторів техніко-економічної інформації та систем документації (уніфікованих і спеціальних), то загалом така система є найушкодженішою для потенційно-ворожої атаки в напрямі всієї сукупності ухвалюваних та реалізованих рішень як за обсягом, розміщенням, формами організації інформації, так і способами її зберігання. При цьому, як уже неодноразово зазначалося, людський фактор у даному контексті стає найбільш значущим як у процесі її знищення або несанкціонованого доступу, так і в процесі забезпечення адекватних заходів захисту службової інформації, і не тільки щодо її достовірності, повноти та доступності. Тому нижче розглянемо процес підбору персоналу, оцінку його ефективності та подальшу його атестацію.

Рисунок 8.34. Зміст інформаційного забезпечення СУП

Сутність кадрового планування і найму персоналу полягає в наданні людям робочих місць у потрібний момент часу і в необхідній кількості відповідно до їхніх здібностей, нахилів і вимог виробництва. Зокрема, аналіз вимог, що висуваються до

робочих місць, формує систему вимог (див. табл. 8.5), які організація-роботодавець висуває до персоналу, що претендує на певні вакансії. Ці вимоги, (як достатньо необхідні якісні параметри претендента на роботу у вигляді його здібностей, властивостей і мотиваційних установок), визначають відповідно до характеру вакансії на тій чи іншій посаді або ж робочому місці. Своєю чергою, характер праці визначає ті вимоги, які висуваються до робочого місця. Вивчення вимог до робочих місць має відповідати стану або на даний час, або ж на майбутнє як прогнозу вимог, що особливо характерно для кадрового планування.

Таблиця 8.5. Вимоги до персоналу

Група	Зміст параметрів
Здібності	Рівень отриманої освіти; необхідні знання (основні та додаткові); практичні навички в певній сфері професійної діяльності; досвід роботи на певних посадах; навички співпраці та взаємодопомоги.
Властивості	Особистісні якості, необхідні для певного виду діяльності; здатність до сприйняття професійних навантажень; здатність до концентрації пам'яті, уваги, зусиль тощо.
Мотиваційні установки	Сфера професійних інтересів; прагнення до самовираження і самореалізації; здатність до навчання; зацікавленість у роботі на певній посаді, ясність професійних перспектив.

Кадрове планування - це цілеспрямована діяльність організації не тільки з добору персоналу, подальшої підготовки кадрів і його подальшого пропорційного та динамічного розвитку відповідно до прогнозованої (розрахункової) та реальної професійно-кваліфікаційної структури розвитку підприємства, а й штатна діяльність із визначення кадрової потреби та контролю за його використанням. При цьому, від якості відібраних кадрів залежить ефективність роботи організації та використання всіх її

інших ресурсів, тому помилки в доборі кадрів можуть дорого обійтися організації. Так, якщо підбір кадрів є вдалим, то вкладені при цьому фінансові кошти вважаються цілком виправданими, інакше і підбір, і подальше навчання (перепідготовка) працівників, які не підходять для виконання дорученої їм роботи, призводить до марної трати грошей.

Для оцінювання ефективності процесу пошуку і добору працівників на вакантні посади зазвичай використовують низку кількісних показників, що характеризують претендента, який приступив до роботи у вигляді штатного співробітника (див. рис. 8.35). При цьому кваліфікація претендента, його попередній досвід роботи за фахом і властиві йому мотиваційні установки відіграють істотну (а може навіть і визначальну) роль у процесі зайняття ним вакансії та подальшого його кар'єрного просування (зростання).

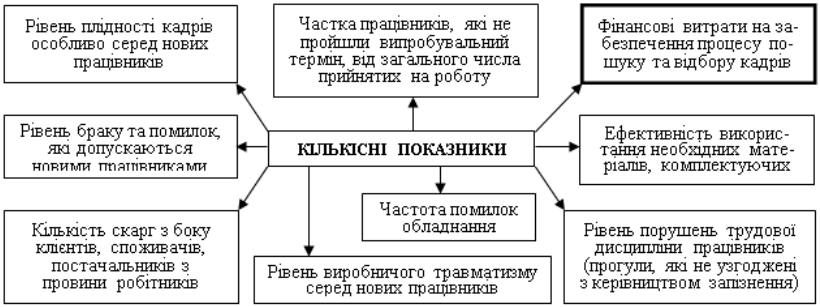

Рисунок 8.35. Кількісні показники ефективності процесу пошуку та підбору кадрів, адаптовано згідно [23, с.48].

Як правило, після проведення попередньої перевірки кандидата і прийняття його до роботи йому призначається випробувальний термін, під час якого виявляють його негативні якості. При цьому нових співробітників не поспішають допускати до службової інформації, - вони можуть використовувати тільки ту, яка необхідна для виконання їх функціональних обов'язків. Будь-які ж несанкціоновані спроби дізнатися більше повинні насторожувати і припинятися керівництвом або службою безпеки підприємства, хоча це

твердження повинно стосуватися і всього кадрового складу. Тому персонал повинен постійно перебувати під пильним наглядом і регулярно проходити спеціальні перевірки (контроль), які здійснюють фахівці (співробітники служби безпеки) або, в крайньому разі, менеджери з персоналу чи експерти, що працюють за контрактом

Перевірки (методи) можуть бути: - ***регулярними***, що проводяться за певним графіком; - ***оперативними***, у разі надзвичайної події, або розголошення конфіденційної інформації, або виникнення підозр щодо конкретних співробітників, або ж проводяться за змінним графіком, раптовим для тих, кого перевіряють; - ***спонтанними***, у вигляді незапланованої акції точкової перевірки. Такі акції зазвичай роблять для: - або перевірки конкретного параметра, який хоч і не потребує постійного контролю, але є базовою компетенцією керівника конкретного рангу у вигляді "лакмусового індикатора" його професіоналізму; - або для зниження рівня невизначеності в життєдіяльності виробництва, причину якої складно з'ясувати (визначити).

Перелічені перевірки можна проводити ***гласно*** або ***негласно,*** в основному використовуючи: ***- спостереження*** з боку співробітників служби безпеки, здійснюване як у робочий час, так і поза ним (наприклад, під час відпочинку, на спільних, святкових заходах тощо); - ***методи агентурної роботи*** для одержання інформації від осіб найближчого оточення (наприклад, від співробітників, які спільно працюють, друзів, товаришів, знайомих і родичів), найчастіше примушуючи їх до цих дій та оплачуючи їхні послуги як джерела (агента) інформації; - ***провокації*** як спеціальні заходи, під час яких шантажують тих, кого перевіряють (підозрюють) на розголошення конфіденційної інформації, використовуючи різні способи як соціальної інженерії (впливу) у вигляді підкупу, алкоголю, сексу, дружніх бесід тощо, так і реалізацію різного роду «оперативних пасток» (наприклад, у вигляді «випадкового» розголошення службової інформації з подальшим контролем її трафіку). Причому, в контексті нейтралізації можливих загроз безпеці підприємства, також слід враховувати мотивацію поведінки (праці) персоналу в процесі його трудової діяльності,

опосередковано пов'язаної також із захистом і безпекою підприємства.

Мотивація праці (як прагнення працівника задовольняти свої потреби за допомогою трудової діяльності) залежить від безлічі чинників, дуже індивідуальна, динамічна і реалізується за допомогою адекватного ***стимулювання праці*** кадрового складу успішного підприємства. Останнє передбачає створення умов (господарського механізму), за яких активна трудова діяльність, що дає певні, заздалегідь заплановані результати, стає необхідною і достатньою умовою як задоволення значущих і соціально зумовлених потреб працівника, так і формування у нього мотивів праці. Хороша робота з мотивації співробітників сприяє: - збільшенню обороту, прибутку та якості виробів; - підвищенню працездатності працівників, їхньої більшої згуртованості та солідарності; - покращенню репутації підприємства; - зменшенню плинності кадрів; - підвищенню конкурсу на вакантні посади; - прагненню до творчішого підходу та активності у впровадженні сучасних досягнень. При цьому, все це мотиваційне середовище, як і підприємство загалом, зобов'язане, з одного боку, бути добре захищеним від будь-якого внутрішнього і зовнішнього негативу (атак), а, з іншого боку, повинне сприяти отриманню позитивної адекватної оцінки апостеріорних наслідків за результатами тактичної або стратегічної діяльності співробітників. Причому, фактично кожен співробітник адекватність своєї виробничої оцінки (ефективності) визначає шляхом порівняння обсягу витраченої ним особистої праці (виробленого результату) до отриманої за неї винагороди. Однак, таке порівняння не завжди може бути сприйняте позитивно. Тому, щоб виправити ситуацію (в рамках мотиваційного профілю співробітника[*,40]) щодо поведінки працівника в організації (на підприємстві) існують певні ***форми стимулювання,*** які зазвичай класифікують (уявляють) як:

---

*[40] ***Мотиваційний профіль людини*** *характеризує ступінь присутності мотиваційних типів (люмпенізований, інструментальний, професійний, патріотичний і хазяйновитий) у співробітника та оцінюється від 0 до 100, де 0 - це повна відсутність відповідного характеру мотивації (див. нижче Табл.8.6).*

- ***негативні*** у вигляді незадоволення, покарання або загрози втрати роботи;

- ***грошові*** у вигляді заробітної плати, включно з усіма видами премій і надбавок;

- ***натуральні*** у вигляді покупок, оренди житла, надання автомобіля тощо;

- ***моральні*** у вигляді грамот, почесних знаків, представлення до відзнак тощо;

- ***піклування про працівника*** (патерналізм) у вигляді додаткового соціального і медичного страхування, створення умов для відпочинку та ін.;

- ***організаційні*** у вигляді створення певних умов праці, її змісту й організації;

- ***залучення*** до співволодіння та участі в управлінні.

Отримавши стимул, людина реагує на нього відповідно до свого мотиваційного профілю. Ця ***реакція*** може бути *позитивною*, і людина змінить свою поведінку так, як це планувалося*; нейтральною; негативною*, коли небажана поведінка співробітника тільки посилюється. Тому для забезпечення і подальшого підтримання необхідного ступеня задоволеності співробітників своїм матеріальним і моральним становищем потрібне не тільки оптимальне стимулювання праці в рамках мотиваційної політики підприємства і мотиваційного профілю співробітника, а й регулярна діагностика, моніторинг і корекція мотиваційної системи. Реалізації останньої передує мотиваційний аудит за системою оцінки рівня мотивації штатного персоналу щодо їхнього досягнення планованих рубежів у своїй виробничій кар'єрі.

Таблиця 8.6. Характеристика мотиваційних типів потенційних кадрів -ринку праці

Мотиваційний тип	Клас мотивації	Характеристика
Інструментальний	Ухильний	- все одно, яку роботу виконувати, немає переваг; - згоден на низьку оплату, за умови, що інші не отримували більше;

Мотиваційний тип	Клас мотивації	Характеристика
		- низька кваліфікація; - не прагне підвищити кваліфікацію, протидіє цьому; - низька активність і виступ проти активності інших; - низька відповідальність, прагнення перекласти її на інших; - прагнення до мінімізації зусиль.
Професійний	Досягальний	- цікавить зміст роботи; - не згоден на нецікаві для нього роботи, скільки б за них не платили; - цікавлять складні завдання - можливість самовираження; - вважає важливою свободу в оперативних діях; - важливе професійне визнання, як кращого в професії.
Патріотичний	Досягальний	- важлива ідея, яка буде ними рухати; - важливе суспільне визнання участі в успіху; - головна нагорода — загальне визнання власної незамінності.
Хазяйновитий	Досягальний	- добровільно бере на себе відповідальність; - характеризується загостреною вимогою свободи дій; - не терпить контролю.

У процесі реалізації мотиваційного аудиту прийнято перевіряти такі параметри:

- наявність і комплексність процедур із виявлення потреб персоналу;

- розподіл сфер відповідальності за мотивацію персоналу між вищим керівництвом, службою управління персоналом і лінійними керівниками;

- кількість і якість виконаних робіт із діагностики, здійснення та перевірки системи управління мотивацією працівників.

Причому при відборі способів мотиваційного аудиту важливо враховувати, що в його проведенні може бути зачеплений як весь персонал підприємства, так і окремі його категорії, до яких застосовні такі **методи у вигляді:**

- *настановних, експертних і структурованих інтерв'ю,* під час яких уточнюють принципи системи стимулювання, осіб і підрозділи, відповідальних за процес мотивації персоналу, стратегічні цілі організації, документацію, доступну для аналізу й оцінювання;

- *аналізу чинної документації* як основних джерел службової інформації, якими є розпорядчі, нормативні та організаційні документи підприємства, включно з наказами, положеннями, розпорядженнями, інструкціями, планами та навіть використовуваною періодикою (журнали, брошури);

- спостереження за роботою керівників, анкетування та тестування персоналу;

- формалізованого опису процедур і статистичних методів обробки.

Цілком очевидно, що цілі, завдання (див. рис. 8.36, адаптованому з [23, с. 122]) та результати мотиваційного аудиту можуть бути використані в різних сферах управління персоналом, - передусім для покращення або розроблення нової системи мотивації персоналу та для вдосконалення політики управління персоналом.

Як свідчить практика, ***конфліктна ситуація*** може виникнути в будь-якій спільній людській діяльності, в якій наявні неузгоджені інтереси та різні позиції як під час вироблення завдань, так і в процесі їх вирішення для досягнення поставлених цілей. Закріпощена на позиціях, зважаючи на їхню жорсткість, така ситуація здатна перешкоджати конструктивному розв'язанню проблем і навіть стимулювати силові підходи, трансформуючись у жорсткий конфлікт не тільки між співробітниками або їхніми групами, а й організаціями (підприємствами).

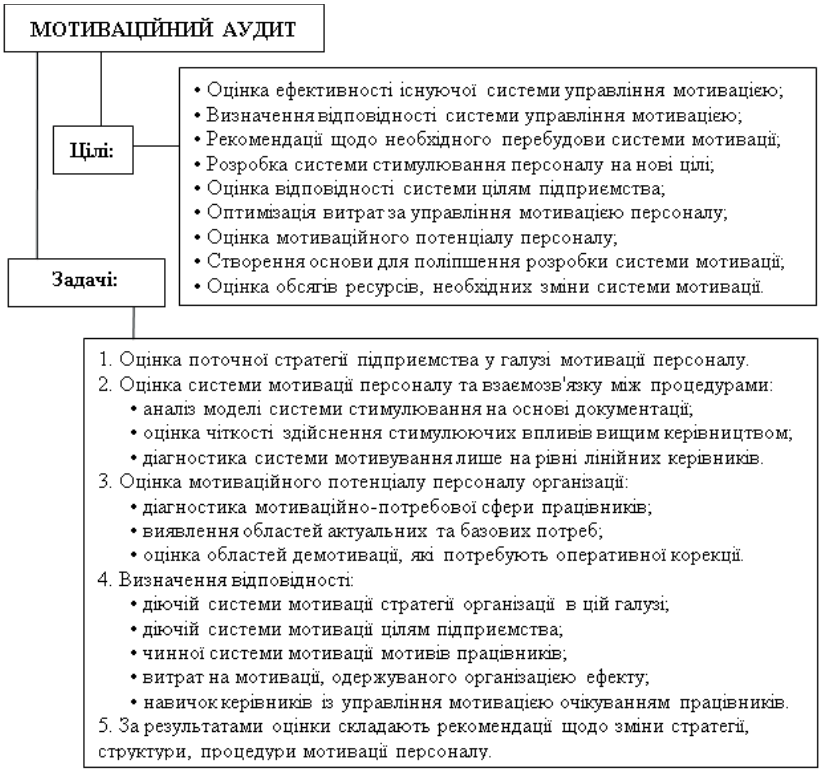

Рисунок 8.36. Цілі та завдання мотиваційного аудиту

Зазвичай **об'єктивними причинами** (про *суб'єктивні* трохи пізніше) **конфлікту** можуть виступати:

- ***управлінські чинники*** у вигляді недосконалої організаційної структури підприємства, нечіткого розподілу прав та обов'язків серед співробітників, суперечностей між функціональними та правовими обов'язками, закріпленими в посадових інструкціях, відповідальності й вимогами до працівника за результати його діяльності;

- ***організаційні чинники*** у вигляді незадовільної організації праці, порушення режиму праці й відпочинку, низького рівня трудової та виконавчої дисципліни, відсутності гласності,

надмірної завантаженості працівника, що призводить до постійного поспіху при виконанні завдань, неконкретності завдань, що ускладнює їхню реалізацію; - професійні чинники у вигляді недосконалості системи добору і розміщення кадрів, невизначеності перспектив професійного та посадового зростання, низького професійного рівня співробітників, що гальмує виконання завдань; санітарно-гігієнічні чинники у вигляді несприятливих умов праці та порушення режиму роботи;

- ***матеріально-технічні чинники*** у вигляді застарілого обладнання та технологій, а також дефіциту в забезпеченні необхідними сучасним засобами виробництва;

- економічні чинники у вигляді недосконалості системи оплати праці та преміювання, а також затримок зарплати**.**

Суб'єктивні причини конфліктів пов'язані з особистістю як самого керівника, так і співробітників підприємства. Зазвичай джерелами помилкових дій керівників, що сприяють конфліктам, є порушення службової етики та трудового законодавства, а також неадекватна оцінка підлеглих і результатів їхньої праці. Крім того, недостатня увага керівника до соціально-психологічних аспектів управління та його невміння зважати на узгодженість (злагодженість у роботі) співробітників - це ще одна з причин виникнення конфлікту. Причому, за спрямованістю впливу в колективі конфлікти поділяються на: - "горизонтальні" (між працівниками одного рівня); - "вертикальні" (між керівником і підлеглими); - "змішані".

Як свідчить практика, існують:

- *організаційні конфлікти*, які виникають унаслідок розбіжності формальних організаційних засад і реальної поведінки членів колективу;

- *міжособистісні конфлікти*, які відбуваються через психологічну несумісність співробітників або внаслідок емоційного неприйняття одним працівником іншого члена колективу. Такі конфлікти дуже затяжні та руйнівні, оптимальний вихід з яких - це розвести таких членів підприємства по різних структурних підрозділах, щоб їхні дії об'єктивно не перетиналися;

- *конфлікти між керівником і його заступником***,** які проявляються зазвичай на ґрунті несумісних стилів управління,

що зазвичай спричинено амбіціями та кар'єрними цілями цього керівництва, хоча їхня спільна діяльність (і керівника, і заступника) зобов'язана конструктивно об'єднувати їхні зусилля, гідно забезпечуючи роботу всього трудового колективу. Проте такий конфлікт швидко переноситься на підлеглих, бо кожен із конфліктуючих прагне мати переважну опору в трудовому колективі. У підсумку заведено розрізняти два типи конфліктів: ***конструктивні (творчі) і деструктивні (руйнівні).***

Конструктивний конфлікт може зароджуватися вже на етапі планування майбутньої діяльності колективу, проявлятися і навіть посилюватися в міру накопичення негативних наслідків. Однак, якщо колектив налаштований на прогресивні зміни в самій організації, то в принципових дискусіях і суперечках, у вільному обговоренні думок щодо об'єктивних суперечностей ситуації, яку обговорюють, завжди знаходять такий розв'язок конфлікту, що здатен привести до прогресивних змін у самій організації. ***Деструктивний конфлікт*** може бути спричинений як об'єктивними, так і суб'єктивними причинами, оскільки він (цей конфлікт), окрім ділової сфери виробництва, здатний проявитися і в зоні міжособистісних стосунків. У такому разі можливе навіть утворення протиборчих угруповань, з присутніми в них чварами і скандалами. Зокрема, соціологічними дослідженнями встановлено, що втрата робочого часу від такого роду конфліктів і післяконфліктних переживань становить близько 15%, а продуктивність праці знижується до 20%.

Слід зазначити, що будь-який різновид конфліктів можна здійснювати у двох формах: ***прихованій і відкритій***. *Відкритий конфлікт* - це конфлікт, коли зрозумілі його мотиви і протиборчі сторони його не приховують. *Прихований конфлікт* - це конфлікт, мотив якого ретельно маскують більш/менш правдоподібним приводом, через який він нібито виник.

Очевидно, що в діяльності підприємства будь-який конфлікт є вкрай небажаним, а якщо він уже проявив себе, то вибір найоптимальнішого *способу завершення конфлікту*[*,41] і його

[*41] ***Поняття "завершення конфлікту" і "вирішення конфлікту" не є тотожними. Розв'язання конфлікту є окремим випадком, однією з форм завершення конфлікту, і виражається в позитивному, конструктивному***

подальшої адекватної реалізації є актуальним і досить складним професійним завданням для керівного складу підприємства.

Найтиповішими *способами завершення конфлікту*, залежно від ситуації на підприємстві, є:

- або усунення (знищення) об'єкта конфлікту, або опонента, або обох опонентів протиборства;
- зміна позицій обох або однієї зі сторін конфлікту;
- участь у конфлікті нової сили, здатної завершити його шляхом примусу;
- звернення суб'єктів конфлікту до арбітра та завершення його за посередництвом третейського судді;
- перемовини як один із найефективніших та найбільш поширених способів розв'язання конфлікту.

За своїм характером завершення конфлікту може бути: - переможним, компромісним або поразницьким із погляду реалізації цілей протиборства; - мирним або насильницьким із погляду форми розв'язання конфлікту; - конструктивним або деструктивним із погляду функцій конфлікту; - повністю й докорінно завершеним або відкладеним на певний (або невизначений) час із погляду ефективності та повноти розв'язання.

Контрольні запитання до Розділу 8

1. Дайте поняття інформаційної логістики, електронної логістики та стратегічного управління. Які прийнято розглядати види функціональних галузей логістики?
2. Що таке логістична інформаційна система, інформаційний логістичний центр та его основни функції (завдання)?
3. Якими численними показниками і характеристиками інформаційних потоків оперує логістика?

вирішенні проблеми основними учасниками конфлікту або третьою стороною. Крім цього формами завершення конфлікту можуть бути: - загасання (згасання) конфлікту; - усунення конфлікту, - переростання конфлікту в інший конфлікт

4. Які певні чинники та передумови необхідні для успішної та ефективної реалізації логістичного управління на основі аналізу інформаційних потоків?

5. Що таке консолідована інформація та яки сучасні інформаційні технології здійснюють в логістиці?

6. Що таке інформаційна діяльність, управління даними, електронний обмін даними та компетентне управління в логістиці?

7. З яких етапів доцільно формувати процес аналітичної діяльності?

8. Поясніть (уточнити) відмінності в поняттях компетентність і компетенція (професійна компетенція)

9. Що виокремлюють серед ключових сфер компетентності логістики?

10. Поясніть ключови моменти та місце консолідованої інформації в інформаційно-аналітичній діяльності та інформаційному забезпеченні органів державної влади

11. Що являє собою інтегрована модель інформаційного забезпечення логістики підприємства?

12. Яких певних принципів необхідно дотримуватися під час реалізації логістичних інформаційних систем?

13. Яку роль виконують комунікаційні та інформаційні стандарти в електронної логістики

14. Поясніть, чому суть спрямованості реалізації логістики (закупівельної, виробничої, розподільчої, транспортної та інформаційної) полягає у формуванні та реалізації системи управління, яка має об'єднати послідовність дій управлінського персоналу та відповідних функціональних ланок, логістичних посередників та контрагентів у процесі управління потоками під час повного логістичного ланцюга «постачання-виробництво-збут»

15. Що таке стратегія в системі її конкретних конкурентних переваг, в чем суть стратегічного управління і стратегічних альтернатив у розвитку підприємства?

16. Що таке SMART-технології під час формулювання цілей стратегії?

17. Поясніть, чі можна ефективне підприємство розглядати як систему логістичного стратегічного менеджменту,

18. Що таке стратегічнії менеджмент (strategic management) та що прийнято розуміти під процесом його становлення?

19. Які моделі стратегічного управління набули найбільшого поширення? Поясніть, будь ласка, її суть.

20. Що таке кадрова політика, завдання кадрової стратегії та їхня реалізація?

Список використаних джерел під час підготовки тексту розділу 8

1. Т.І.Балановська. О.П.Гогуля. А.В.Троян. Основи менеджменту, маркетингу та підприємництва. Навч. посібник. - Київ: ЦП «КОМПРИНТ», 2018. – 518с.

2. Спрінсян В. Г., Бірюкова Т. Л. Ресурси та технології інформаційного менеджменту : навчальний посібник. Одеса : ОНПУ, 2012. 248 с.

3. Карпов В.Е., Закревський П.Ф. Менеджмент безпеки. Навч. посібник – теорія. Кіровоград. МАУП. 2007. -380 с

4. Карпов В.Е., Карпов А.В. Менеджмент логістики. Навч. посібник. Кіровоград. МАУП. 2013. -493 с.

5. Колпаков В. М., Дмитренко Г. А. Стратегічний кадровий менеджмент: Навч. посібник. - К.: МАУП, 2005. — 752 с.

6. Гурч Л.М. Логістика. Навч. посібник. – К. МАУП. 2008. С - 560

7. Сучасні інформаційні технології у логістиці. Репозиторій Полоцького державного вузу.https://elib.psu.by › bitstream

8. Что такое компетенция? – HURMA hurma.work https://hurma.work 21 авг. 2024 г.

9.* Конспект лекцій з дисципліни «Логістика» для студентів IIIкурсу всіх форм навчання спеціальності «Підприємництво, торгівля та біржова діяльність». Частина 1 (Укл. Г.О. Пудичева, В.С. Малишко. – Одеса: ОНЕУ, ротапринт, 2018 р. – 191с.)

10. Про інформацію: закон України від 2 жовтня 1992 р. № 2657 — XII / Відомості Верховної Ради України. — 1992. — № 48. — Ст. 650. [Електронний ресурс]. — Режим доступу: URL: http://zakon.rada.gov.ua/ cgi- bin/laws/main.cgi?nreg=2657-12– Назва з екрану.

11. Інформація та документація. Базові поняття. Терміни та визначення : ДСТУ 2392-94. — [Чинний від 1995-01-01]. — К.: Держстандарт України, 1994.– 53 с. — (Державний стандарт України).

12. Основи інформаційно-аналітичної діяльності [текст] : нав. посіб. / Захарова В. І., Філіпова Л. Я. – К. : «Центр учбової літератури», 2013. – 336 с.

13. Сурмін Ю.П. Аналітика державного управління: сутність і тенденції розвитку / Ю.П.Сурмін. — Режим доступу: http://www.nbuv.gov.ua/e- journals/DUTP/2007-1/txts/06sypdsv.htm

14. Матвієнко О.В. Основи інформаційного менеджменту: навчальний посібник / О.В. Матвієнко. — К: Центр навчальної літератури, 2004. — 128 с.

15. Калитич Г.І. Інформаційно-дослідницька діяльність як основа підготов- ки, прийняття та реалізації управлінських рішень / Г.І. Калитич // Матеріали Всеукраїнської науково-практичної конференції «Інформація, аналіз, прогноз — стратегічні важелі ефективного державного управління». — К.: УкрІНТЕІ, 2000. — С.82-85.

16. Морозов А.О. Інформаційно-аналітичні технології підтримки прийнят- тя рішень на основі регіонального соціально-економічного моніторингу / А.О. Морозов, В.Л. Косолапов. — К.: Наукова думка, 2002. — 231 с/

17. Гаман Т.В. Створення регіональної інформаційно-аналітичної служби як складової вдосконалення інформаційної діяльності місцевих державних адміністрацій / Т.В. Гаман // Університетські наукові записки. — 2007. — № 1(21). — С. 252-258. — Режим доступу : http://www.univer.km.ua/visnyk/1253.pdf

18. Ємельянова Є. А. Стратегічний менеджмент: навчальний посібник / Є. А. Ємельянова. - 2-ге вид., Дод. - Томськ: Ель Контент, 2015. — 114 с/

19. Стратегічний менеджмент: навчальний посібник [Електронний ресурс] / за ред. д-ра економ. наук, проф. М. А. Чернишова. — URL : http://manage-ment61.ru/index.php?do=static&page=strategtitul

20. Словник з кібернетики / За ред. В. С.Михалевича. - К.: Гол.ред. Укр. сов. енцикл., 1989.

21. Дмитренко Г. А. Стратегічний менеджмент: цільове управління персоналом організацій: Навч. посібник. - К.: МАУП, 2006. — 224 с.

22. Мавріна, І. Н. Стратегічний менеджмент: навчальний посібник / І. Н. Мавріна. – Є.: УрФУ,2014— 132 с.

23. Орлянська Г.Л. Курс лекцій "Управління персоналом". Інститут менеджменту та інформаційних технологій (філія) Санкт-Петербурзького державного політехнічного університету (ІМІТ СПбДПУ) м.Череповець 2010 р. - 157с.

ЛІТЕРАТУРА

1. Бондаренко М. Перспективи застосування міжнародного стандарту ISO/IEC в Україні / Бондаренко М., Скрипник Л, Потій О. // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні: зб. наук. праць. – К., 2001. – Вип. 3. – С. 7-26.
2. Т.І.Балановська. О.П.Гогуля. А.В.Троян. Основи менеджменту, маркетингу та підприємництва. Навч. посібник. - Київ: ЦП "КОМПРИНТ", 2018. – 518с/
3. Захист інформації у телекомунікаційних системах / Конахович Г.Ф., Клімчик В.П., Паук С.М., Потапов В.Г. - К.: МК-Прес, 2005.–288 с
4. орошко В.А. Методи та засоби захисту інформації / Хорошко В.А., Чекатков О.О. - К.: Юніор,2003. – 504 с.
5. Щокін Г.В. Теорія соціального управління: Монографія/Щекін Г.В. К.: МАУП, 1996. 408 с.
6. Василенко В.О., Шостка В.І. Ситуаційний менеджмент. Навч. посібник. - К.:ЦУЛ, 2003. - 285 с.
7. Концептуально-гносеологічні аспекти інформаційної безпеки (захищеності) з позицій соціальної інженерії [Текст] / Ю.С.Тарасенко, Соляннiков В.Г., Калюжний О.Е. // Системи та технології. – 2020. – № 2(60). С. 89-98
8. * Тарасенко Ю.С. Ризик-орієнтовані процеси забезпечення безпеки об’єктів критичної інфраструктури // Ю.С.Тарасенко, Ю.В.Савченко // Системи та технології №1 (65), 2023. с.67-76.
9. . Плющ А. Н. Соціально-психологічні механізми інформаційного впливу: монографія / А. Н. Плющ. - Ніжин: «Видавництво «Аспект-Поліграф», 2017. — 244 с.
10. Бондар О. В. Ситуаційний менеджмент. Навч. посіб. Київ : Центр учбової літератури, 2012. 388 с.
11. І. Діордіца. Методологія дослідження кібербезпекової політики: кібернетичний, системний та матричний підходи. / Юридичний вісник, 2020/4, стор. 66-73.

12. Семенова К. Д. Обґрунтування господарських рішень та оцінювання ризиків: Навчальний посібник. – Одеса: ОНЕУ, ротапринт, 2013 р. – 194 с.
13. Toliupa S., Nakonechny V., Brailovskyi N.. Building cyber-security systems of information networks based on intellectual technologies. // Scientific and Practical Cyber Security Journal (SPCSJ) 1(1):10-19. Scientific Cyber Security Association (SCSA), 2017. p.11.
14. Спрінсян В. Г., Бірюкова Т. Л. Ресурси та технології інформаційного менеджменту: навчальний посібник. Одеса : ОНПУ, 2012. 248 с.
15. Матвієнко О. В., Цивін М. Н. Основи менеджменту інформаційних систем: навчальний посібник. Київ : Центр навчальної літератури, 2005. 176 с.
16. Низенко Е. І., Каленяк В. П. Забезпечення інформаційної безпеки підприємництва : навч. посіб. Київ : МАУП, 2006. 134 с.
17. Биткін С.В. Конкурентна розвідка у зовнішньоекономічній діяльності: інженерно-економічні методи/С.В. Биткін, В.М. Литвин. - Х.,2015. – 240 с
18. Тарасенко Ю.С. Нівелювання електромагнітної вразливості інформації з обмеженим доступом. // Системи та технології, 2023, 65 (1). С. 56-65. DOI https://doi.org/10.32782/2521-6643-5. 2023.1-65.8.
19. Юдін О.К., Бучик С.С. Державні інформаційні ресурси. Методологія побудови класифікатора загроз : монографія. Київ : НАУ, 2015. 214 с
20. Ліпкан В. А., Максименко Ю. Є., Желіховський В. М. Інформаційна безпека України в умовах євроінтеграції : навчальний посібник. Київ : КНТ, 2006. 280 с.
21. Вовк С.М., Гнатушенко В.В., Бондаренко М.В. Методи обробки зображень та компютерний зір : навчальний посібник. Д. : ЛІРА, 2016. 148 с.
22. Менеджмент безпеки: навч. посіб. / М. О. Левченко. — К. : ДП «Вид. дім «Персонал», 2013. — 406 с.
23. Тарасенко Ю.С. Фізичні основи радіолокації [Текст]: навч. посіб. Т 19 / Ю.С. Тарасенко. – Д.: «Пороги», 2011.– 487с.

24. Бурячок, В. Л. Інформаційна та кібербезпека: соціотехнічний аспект. [Підручник]. / В. Л. Бурячок, В.Б. Толубко, В. О. Хорошко, С. В. Толюпа /. Львів: «Магнолія 2006», 2018 – 320с.
25. Bossong, R. EU cooperation on terrorism prevention and violent radicalization: frustrated ambitions or new forms of EU security governance? / R. Bossong // Cambridge Review of International Affairs. – 2014. – № 27 (1). – P. 66-82
26. Camacho, E.T. The development and interaction of terrorist and fanatic groups / E.T. Camacho // Communications in Nonlinear Science and Numerical Simulation. – 2013. – № 18 (11). – P. 3086-3097
27. Hofmann, D.C. Quantifying and qualifying charisma: a theoretical framework for measuring the presence of charismatic authority in terrorist groups / D.C. Hofmann // Studies in Conflict and Terrorism. – 2015. – № 38 (9). – P. 710-733)
28. Етика. Естетика. [текст]: навч. посіб. / за наук. ред. Панченко В. І. – К.: «Центр учбової літератури», 2014. – 432 с.
29. Етика та естетика: навчально-методичний посібник (у схемах і таблицях) / за наук. ред. проф. В. С. Бліхара. Львів: ПП «Арал», 2018. 204с.
30. Тарасенко Ю.С., Клим В.Ю., Смирнов В.В. Plagiat as an Element of Negative and Criticality of Such Education «Science and education for sustainable development. Part 2. Innovative and Information Technologies in Education: Applied Aspects».p.665-674. 20-21 січня 2022 р. Monograph 50. Publishing House of University of Technology, Katowice, 2022.
31. Положення про академічну доброчесність та етику академічних взаємовідносин в Університеті митної справи та фінансів URL: http://umsf.dp.ua/index.php/about/publichna-informatsiia/dobrochesnist.
32. Основи інформаційно-аналітичної діяльності [текст] : нав. посіб. / Захарова В. І., Філіпова Л. Я. – К. : «Центр учбової літератури», 2013. – 336 с.
33. Морозов А.О. Інформаційно-аналітичні технології підтримки прийняття рішень на основі регіонального

соціально-економічного моніторингу / А.О. Морозов, В.Л. Косолапов. — К.: Наукова думка, 2002. — 231 с.
34. Дмитренко Г. А. Стратегічний менеджмент: цільове управління персоналом організацій: Навч. посібник. - К.: МАУП, 2006. — 224 с.
35. Захист інформації у телекомунікаційних системах / Конахович Г.Ф., Клімчик В.П., Паук С.М., Потапов В.Г. - К.: МК-Прес, 2005.–288 с
36. Якименко І.З. Менеджмент інформаційної безпеки. Конспект лекцій. Тернопіль. 2019. -136 с.
37. Менеджмент інформаційної безпеки / О.Г. Корченко, М.Є. Шелест, С.В. Казмірчук, Ю.М. Ткач, Є.В. Іванченко. – Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея», 2019. – 408 с. : іл.

Додаток А.
Звід основної сучасної міжнародної нормативної бази згідно зі стандартами ISO менеджменту інформаційної безпеки та супровідної логістики

Процес активного впровадження та розвитку сучасних інформаційних технологій (ІТ) в Україні значною мірою обумовлений недосконалістю його законодавчої бази (тобто частковою неузгодженістю, суперечливістю, неповнотою законодавчих і нормативно-підзаконних актів у сфері телекомунікацій, використання Інтернет-технологій, реалізації електронних інформаційних ресурсів і продуктів, впровадження електронного документообігу та електронного цифрового підпису, інформаційної безпеки та захисту інформації тощо).[*42] Фактично до останнього часу даному процесу притаманна понятійна невизначеність різних аспектів використання менеджменту інформаційної безпеки[**43] та супутньої логістики в інформаційній сфері суспільних і галузевих відносин соціума. У зв'язку з цим доцільно керуватися сучасною міжнародною нормативною базою за стандартами ISO-менеджменту інформаційної безпеки, взявши за основу сімейство стандартів ISO/IEC 27000 для подальшої адаптації та розробки національного їх впровадження у вигляді ДСТУ, постанов, нормативних актів тощо. Причому основні поняття та особливості змістовного наповнення і впровадження менеджменту інформаційної безпеки викладені нижче в наведеній серії міжнародних стандартів:

– **ISO/IEC 27000** – IT. Методи забезпечення безпеки. СМІБ. Огляд і словник (Information technology. Security techniques. Information security management systems. Overview and

---

[42*] Адаптовано з навч. пос. Менеджмент інформаційної безпеки / О.Г. Корченко, М.Є. Шелест, С.В. Казмірчук, Ю.М. Ткач, Є.В. Іванченко. – Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея», 2019. – 408 с. : іл.

[43**] Нагадаємо, що система менеджменту (management system) є сукупністю взаємопов'язаних і взаємодіючих елементів організації для розробки політик і цілей, а також процесів для їх досягнення

vocabulary.) Введення в сімейство стандартів, а також глосарій загальних термінів;

– **ISO/IEC 27001** – IT. Методи забезпечення безпеки. СМІБ. Вимоги (Information technology. Security techniques. Information security management systems. Requirements). Стандарт для створення, реалізації, контролю та вдосконалення СМІБ (на основі британського стандарту BS 7799 Частина 2);

– **ISO/IEC 27002**, BS 7799-1: 2005, BS ISO/IEC 17799: 2005 – IT. Методи забезпечення безпеки. Практичні правила управління ІБ. Кодекс правил СМІБ (Information technology. Security techniques. Code of practice for information security management), (раніше відомої як ISO/IEC 17799 сам заснований на британському стандарт BS 7799 Частина 1, останній раз переглядався в 2005 і перейменований ISO / IEC 27002: 2005 в липні 2007 року);

– **ISO/IEC 27003** – IT. Методи забезпечення безпеки. Керівництво по впровадженню СМІБ (Information Technology. Security Techniques. Information Security Management Systems Implementation Guidance);

– ISO/IEC 27004 2009 – IT. Методи забезпечення безпеки. Вимірювання ефективності СМІБ (Information technology. Security techniques. Information security management. Measurement);

– ISO/IEC 27005 – IT. Методи забезпечення безпеки. Управління ризиками ІБ. Призначений для надання допомоги в оцінці ризику при впровадженні СМІБ – управління ризиками (Information technology. Security techniques. Information security risk management). Випущений в червні 2008р. Остання редакція стандарту випущена 19 травня 2011р.;

– ISO/IEC 27006 – IT. Методи забезпечення безпеки. Вимоги до органів аудиту і сертифікації СМІБ (Information technology. Security techniques. Requirements for bodies providing audit and certification of information security management systems);

– ISO/IEC 27007 – IT. Методи забезпечення безпеки. Керівництво з проведення аудиту СМІБ (Information technology – Security techniques – Guidelines for information security management systems auditing);

– ISO/IEC TR 27008 – IT. Методи забезпечення безпеки. Настанови для аудиторів з оцінки органів управління (Information technology – Security techniques – Guidelines for auditors on information security controls);

– ISO/IEC 27010 – IT. Методи забезпечення безпеки. Менеджмент забезпечення ЗІ між секторами і організаціями (Information technology – Security techniques – Information security management for inter–sector and inter–organizational communications);

– ISO/IEC 27011 – IT. Методи забезпечення безпеки. Настанови щодо управління ЗІ організацій, що пропонують телекомунікаційні послуги, на основі ISO / IEC 27002 (Information technology. Security techniques. Information security management guidelines for telecommunications organizations based on ISO / IEC 27002);

– ISO/IEC 27013 – IT. Методи забезпечення безпеки. Керівництво щодо інтегрованого впровадження ISO / IEC 27001 та ISO / IEC 20000-1 (Information technology – Security techniques – Guidance on the integrated implementation of ISO / IEC 27001 and ISO / IEC 20000-1);

– ISO/IEC TR 27015 – IT. Методи забезпечення безпеки. Структура забезпечення захисту. Настанови щодо менеджменту ІБ для фінансових операцій (Information technology – Security techniques – Information security management guidelines for financial services);

– ISO/IEC 27031 – IT. Методи забезпечення безпеки. Керівництво по забезпеченню готовності інформаційних і комунікаційних технологій до їх використання для управління безперервністю бізнесу. (Information technology. Security techniques. Guidelines for information and communications technology readiness for business continuity (FDIS));

– ISO/IEC 27032 – IT. Методи забезпечення безпеки. Настанови щодо кібербезпеки (Information technology – Security techniques – Guidelines for cybersecurity);

– ISO/IEC 27033-1 – IT. Методи забезпечення безпеки. Мережева безпека. Частина 1. Огляд та концепції (Information

technology – Security techniques – Network security – Part 1: Overview and concepts);

– ISO/IEC 27033-2 – IT. Методи забезпечення безпеки. Захист мережі. Частина 2. Настанови щодо проектування та впровадження захисту мережі (Information technology – Security techniques – Network security – Part 2: Guidelines for the design and implementation of network security);

– ISO/IEC 27033-3 – IT. Методи забезпечення безпеки. Мережева безпека. Частина 3. Еталонні мережеві сценарії. Загрози, методи проектування і питання управління (Information technology – Security techniques – Network security – Part 3: Reference networking scenarios – Threats, design techniques and control issues);

– ISO/IEC 27034-1 – IT. Методи забезпечення безпеки. Безпека застосування. Частина 1. Огляд та поняття (Information technology – Security techniques – Application security – Part 1: Overview and concepts);

– ISO/IEC 27035 – IT. Метод забезпечення безпеки. Управління випадковостями в системі ІБ (Information technology – Security techniques – Information security incident management);

– ISO / IEC 27037 – IT. Методи забезпечення безпеки. Настанови щодо ідентифікації, збору, придбання і збереження цифрових даних (Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence);

– ISO/IEC WD 27006 – IT – Методи забезпечення безпеки – Вимоги до органів, які проводять аудит і сертифікацію СМІБ (Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems);

– ISO/IEC DIS 27014 – IT – Методи забезпечення безпеки – Керівництво з ІБ (Information technology – Security techniques – Governance of information security);

– ISO/IEC PDTR 27015 – Proposal on an Information security management guidelines for financial and insurance services – Пропозиція з ІБ керуючі управлінські принципи для фінансових і страхових послуг;

– ISO/IEC PDTR 27016 – IT – Методи забезпечення безпеки – Управління ІБ – Організаційна економіка (Information technology – Security techniques – Information security management – Organizational economics);

– ISO/IEC WD 27017 – IT – Методи забезпечення безпеки – Безпеки Cloud computing і системи управління приватного життя – Безпека управління (Information technology – Security techniques – Information security management – Guidelines on information security controls for the use of cloud computing services based on ISO / IEC 27002);

– ISO/IEC WD 27018 – Code of practice for data protection controls for public cloud computing services;

– ISO/IEC 27036 – IT Security. Security techniques. Guidelines for security of outsourcing (DRAFT) – Керівництво з аутсорсингу безпеки;

– ISO/IEC 27033-4 – Забезпечення безпеки міжмережевих взаємодій за допомогою шлюзів безпеки – загрози, методи проектування та механізми контролю (Information technology – Security techniques – Network security – Part 4: Securing communications between networks using security gateways);

– ISO/IEC 27033-5 – IT. Методи забезпечення безпеки. Забезпечення безпеки Віртуальних Приватних Мереж – загрози, методи проектування та механізми контролю (Information technology – Security techniques – Network security – Part 5: Securing communications across networks using Virtual Private Network (VPNs));

– ISO/IEC 27033-6 – Information technology – Security techniques – Network security – Part 6: Securing IP network access using wireless – Конвергенція в IP мережах (Визначення загроз, методів проектування і механізмів контролю в IP мережах з конвергенцією даних);

– ISO/IEC 27034-2 – Organization Normative Framework (draft) – Нормативна база організації;

– ISO/IEC 27034-3 – Application Security Management Process (pre–draft) – Процес управління безпекою додатків; – ISO/IEC 27034-4 – Application security validation (pre–draft) – Оцінка безпеки додатків;

– ISO/IEC 27034-5 – Protocols and application security control data structure (pre-draft) – Протоколи і структура керуючої інформації для забезпечення безпеки додатків (XML схема);

– ISO/IEC 27034-6 – Security guidance for specific applications (pre-draft) – Керівництво по забезпеченню безпеки конкретних програм;

– ISO/IEC WD 27035-1 – IT. Методи забезпечення безпеки – ІБ управління інцидентами – Частина 1: Принципи управління інцидентами (Information technology – Security techniques – Information security incident management – Part 1: Principles of incident management);

– ISO/IEC WD 27035-2 – IT. Методи забезпечення безпеки – ІБ управління інцидентами – Частина 2: Керівні принципи щодо реагування на інциденти (Information technology – Security techniques – Information security incident management – Part 2: Guidelines for incident response readiness) ;

– ISO/IEC WD 27035-3 – IT. Методи забезпечення безпеки – ІБ управління інцидентами – Частина 3: Керівництво по CSIRT операціям (Information technology – Security techniques – Information security incident management – Part 3: Guidelines for CSIRT operations);

– ISO/IEC DIS 27036-1 – IT. Методи забезпечення безпеки – ІБ для відносин з постачальниками – Частина 1: Огляд та концепції (Information technology – Security techniques – Information security for supplier relationships – Part 1: Overview and concepts);

– ISO/IEC DIS 27036-2 – IT. Методи забезпечення безпеки – ІБ для відносин з постачальниками – Частина 2: Загальні вимоги (Information technology – Security techniques – Information security for supplier relationships – Part 2: Common requirements);

– ISO/IEC DIS 27036-3 – IT. Методи забезпечення безпеки – ІБ для відносин з постачальниками – Частина 3: Посібник з безпеки ІКТ ланцюжка поставок (Information technology – Security techniques – Information security for supplier relationships – Part 3: Guidelines for ICT supply chain security);

– ISO/IEC WD 27036-4 – IT. Методи забезпечення безпеки – ІБ для відносин з постачальниками – Частина 4: Посібник з

безпеки аутсорсингу (Information technology – Security techniques – Information security for supplier relationships – Part 4: Guidelines for security of outsourcing);

– ISO/IEC DIS 27038 – Information technology – Security techniques – Specification for Digital Redaction;

– ISO/IEC CD 27039 – Information technology – Security techniques – Selection, deployment and operations of intrusion detection systems;

– ISO/IEC CD 27040 – Information technology – Security techniques – Storage security; – ISO/IEC CD 27042 – Guidelines for the analysis and interpretation of digital evidence;

– ISO/IEC CD 27043 – Investigation principles and processes;

– ISO/IEC WD 27044 – Security Information and Event Management (SIEM).

Крім того, слід зазначити, що в сфері логістики стандарти ISO також відіграють важливу роль у підвищенні ефективності, якості та безпеки процесів (див. перелік із 133 стандартів системи менеджменту ISO) [*] [44], де основними стандартами логістики прийнято вважати ISO 9001 (управління якістю) та ISO 28000 (управління безпекою ланцюга поставок).

[44*] Перелік стандартів систем менеджменту ISO. / ISO - International Organization for Standardization https://www.iso.org › management-system-standards-list

Додаток Б.
КОРОТКИЙ СЛОВНИК ВИКОРИСТАНИХ ПОНЯТТІВ/ТЕРМІНОЛОГІЙ

AI/ES (artificial inteligence/expert systems) — штучний інтелект / експертна систем
BC (barcoding) — штрихове кодування
CALS - концепція «безперервного розвитку та підтримки життєвого циклу»
DM (datamanagment) —управління даними
ED (electronic data interchange) — електроний обмін даними
ETL репозиторій
GDSN (Global Data Synchronisation Network) - всесвітня мережа синхронізації даних
GPRS - General Packet data Radio Service
LTE - Long-Term Evolution
RA&C (remote accessand communication) — дистанційний доступ та комунікації
WAP - Wireless Application Protocol
Академічна доброчесність
Аналітичне та імітаційне моделювання
Архітектурні моделі захисту
Безпека
БЕК - безехова камера
Вибор критеріїв ризику

- відкрита, службова, конфіденційна

Відмовостійкість
Візуальний моніторинг
Вразливість
Вразливість
Гносеоло́гія
Деструктивний конфлікт
Джерела загроз
Ділова розвідка
Доступність інформації
Електрона логістика
Емерджентність або емергентність в теорії систем
Етика
Етика професійна

Етикет службовий
Ефективність стратегічного управлінського рішення
Живучість
Загроза
Загрози кадрової безпеки
Ієрархічній принцип
ІКТ - інформаційно-комунікаційни технології
Інформаційна діяльність
- інформації захист
- інформаційна безпека
- інформаційна війна
- інформаційна зброя

Інформаційна модель
- інформаційна система
- інформаційні протистояння
- інформаційні ризики

Інформація
Кадрова стратегія і політика
КДЦ - тріади конфіденційності, доступності, цілісності
Кібербезпека об'єкта
Кібербезпека України
Кібернетика (поняття, методи та підходи)
Кібернетична модель
Кіберпростір
Кіберстійкость
Класифікація порушників (виконавців загроз)
КМ - когнітивний менеджмент
Кодекс академічної доброчесності
Кодекс корпоративної поведінки
Комерційна розвідка
Комерційна таємниця
Компетентність, професійна компетенція
Компіляції
Конструктивний конфлікт
Конфіденційність інформації
Конфлікт інтересів (потенційний, реальний)
Конфлікти (організаційні та міжособистісні)
Конфліктна ситуація

Концепції безпеки підприємницької діяльності.
Концепція
Корпоративна етика (культура)
Кризова ситуація
Критерії SMART
Критична інфраструктура
Критично важливий об’єкт (КВО)
КСЗІ - комплексна система захисту інформації
КСІІ - ключові системи інформаційної інфраструктури
Логіко-семантична модель
Логістика
Менеджмент
Миссия
Моделі фізичної подібності (матеріальні); аналогові; символічні (математичні) та інфологічні (вербально-описові, тобто словесно-описові)
Модель концептуальна (змістовна)
Модель порушника
Модель фізична або математична
Моніторинг рівнів лояльності
Мораль
Мотиваційний аудит
Мотиваційний профіль людини
Надзвичайна ситуація
Об'єкт управління
Об'єкти кібербезпеки та кіберзахисту
ОІД - об'єкт інформаційної діяльності
ОКІ - об’єкти критичної інфраструктури
Організації та управління КСЗІ
Організаційна модель
Організаційної системи
Оцінювання ризику
Пентести (penetration test, pentest)
Плагіат
Повідомлення
Потенціал стримування
Принцип невизначеності
Принципи побудови математичних моделей

Причини конфліктів
Проведення тестів на проникнення
Промислове шпигунство
Рекрутинг (підбір персоналу)
Ризик
Рішення (поняття управлінське рішення, класи та методи)
Розвідувальна діяльність
РОМ - ризик-орієнтоване мислення
Семантика
Синергія
Система
Системи руйнування інформації
Системний аналіз
Ситуаційний менеджмент
Ситуаційний менеджмент
СІ - конкурентна розвідка
СКУД - системи контролю та управління доступом
Соціальна інженерія
Соціальне програмування
Соціальне хакерство
Соціум
Стадії побудови моделі
Стратегічний менеджмент
Стратегія диверсификации
Стратегія зростання
Стратегія скорочення
Стратегія стабільності
Структурна модель
Ступінь невизначеності з точки зору прийняття рішення
СУБД - система управління базами даних
Суб'єкт управління
Технологія комп'ютерного моделювання
Триланкова модель аналітики
Управління
Форми стимулювання
Фрод
Функції підприємництва
Функціональна модель

Функціональні стратегії
Хакерська атака
Хакінґ
Цілі та завдання мотиваційного аудиту
Цілісність інформації

АВТОРИ

ТАРАСЕНКО Юрій Станіславович – кандидат фізико-математичних наук, доцент, доцент кафедри транспортних технологій та міжнародної логістики Університету митної справи та фінансів.

САВЧЕНКО Юрій Володимирович – кандидат технічних наук, доцент, доцент кафедри кібербезпеки та інформаційних технологій Університету митної справи та фінансів.

ШАПОВАЛ Олександр Олександрович – доктор технічних наук, професор, професор кафедри машинобудування Кременчуцького національного університету імені Михайла Остроградського.

МОРОЗ Микола Миколайович – доктор технічних наук, професор, завідувач кафедри транспортних технологій Кременчуцького національного університету імені Михайла Остроградського.

Наукове видання

ТАРАСЕНКО Юрій Станіславович
САВЧЕНКО Юрій Володимирович
ШАПОВАЛ Олександр Олександрович
МОРОЗ Микола Миколайович

ОСНОВИ МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ ЛОГІСТИЧНОЇ ДІЯЛЬНОСТІ

Монографія

Підписано до друку 25.02.2026
Формат 60x84 1/16. Умовн. друк. арк. 27,6.
Наклад 300 прим. Замовлення № 21-26.
Папір офсетний. Гарнітура Times.
Електрографічний друк.

Видавець ПП «Видавництво «НОВАБУК»
Свідоцтво суб'єкта видавничої справи
ДК №7598 від 10.02.2025р.
www.novabook.com.ua
097 555 10 72

Віддруковано ФОП Щербатих О.В.
вул. Софіївська, 36-Б, м. Кременчук, 39601
Свідоцтво суб'єкта видавничої справи
ДК №2129 від 17.03.2005 р.

ISBN 978-617-639-578-2