МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

УНІВЕРСИТЕТ МИТНОЇ СПРАВИ ТА ФІНАНСІВ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ПРАВА ТА МІЖНАРОДНО-ПРАВОВИХ ВІДНОСИН

ЦИВІЛЬНИЙ ЗАХИСТ, БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ ТА ОХОРОНА ПРАЦІ

Навчально-методичний посібник

Дніпро

Видавець Біла К. О.

2025

УДК 614.8:349.2(477)
С 91

Рекомендовано до друку вченою радою ННІ права та міжнародно-правових відносин (протокол № 10 від 23 листопада 2024 року)

Рецензенти:

Пиріг І. В., професор кафедри криміналістики та домедичної допомоги ННІППФПНП ДДУВС, д-р юрид. наук, професор;

Батраченко І. Г., професор кафедри психології, Дніпровського національного університету імені Олеся Гончара, д-р юрид. наук, професор.

Авторський колектив:

Сухацька І. Ю., канд. хім. наук, доцент (стаж судового експерта 25 років);

Батраченко Т. С., канд. юрид. наук, доцент;

Єфімова І. В., канд. юрид. наук, доцент.

Сухацька І. Ю.

С 91 Цивільний захист, безпека життєдіяльності та охорона праці : навч.-метод. посіб. / І. Ю. Сухацька, Т. С. Батраченко, І. В. Єфімова. – Дніпро : Біла К. О., 2025. – 112 с.

ISBN 978-617-645-524-0

Навчально-методичний посібник «Цивільний захист, безпека життєдіяльності та охорона праці» є комплексним виданням, що охоплює теоретичні основи та практичні аспекти забезпечення безпеки життєдіяльності, цивільного захисту та охорони праці. У ньому систематизовано основні нормативно-правові акти, що регулюють цю сферу в Україні, включаючи Кодекс цивільного захисту України, закони «Про охорону праці», «Про забезпечення санітарно-епідемічного благополуччя населення», а також міжнародні документи, що визначають правові засади безпеки в умовах надзвичайних ситуацій.

Посібник містить аналіз основних видів надзвичайних ситуацій, класифікацію небезпечних та шкідливих чинників, їхній вплив на людину та навколишнє середовище, а також рекомендації щодо забезпечення особистої безпеки в кризових ситуаціях. Особливу увагу приділено питанням вибухопожежної безпеки, електробезпеки, домедичної допомоги та організації евакуаційних заходів. Видання також розглядає питання інформаційної безпеки, захисту критичної інфраструктури та соціальної адаптації населення до умов воєнного часу та кризових ситуацій.

У навчальному посібнику представлено сучасні технології прогнозування та управління надзвичайними ситуаціями, включаючи геоінформаційні системи (GIS), методи моніторингу та оцінки ризиків, а також міжнародний досвід у сфері координації дій під час кризових ситуацій. Видання також містить практичні рекомендації, тестові завдання, ситуаційні кейси та аналіз реальних випадків, що сприяє закріпленню знань та формуванню необхідних компетентностей у здобувачів вищої освіти.

Цей навчально-методичний посібник рекомендований для викладачів, здобувачів вищої освіти, фахівців у сфері цивільного захисту, охорони праці, безпеки життєдіяльності, працівників правоохоронних органів, рятувальних служб та державних установ, відповідальних за управління ризиками та реагування на надзвичайні ситуації. Видання сприятиме поглибленню знань у сфері безпеки, підвищенню рівня підготовки спеціалістів та розвитку сучасних підходів до організації системи цивільного захисту в Україні.

УДК 614.8:349.2(477)

ISBN 978-617-645-524-0

ЗМІСТ

ПЕРЕДМОВА

Цивільний захист є невід'ємною складовою національної безпеки держави, яка забезпечує захист населення, територій, матеріальних і культурних цінностей у разі виникнення надзвичайних ситуацій. В умовах сучасних викликів, пов’язаних з воєнним станом, техногенними катастрофами, екологічними загрозами та інформаційними атаками, підготовка фахівців у сфері цивільного захисту набуває особливої актуальності.

Класичне визначення стверджує, що «Цивільний захист – функція держави, спрямована на захист населення, території, навколишнього природного середовища та майна від надзвичайних ситуацій шляхом запобігання таким ситуаціям, ліквідації їх наслідків і надання допомоги постраждалим у мирний час та в особливий період (Кодекс цивільного захисту України)».

Цивільний захист – це один з найважливіших аспектів діяльності людини. Всі прагнення людства спрямовані на вдосконалення існуючих здобутків науки та техніки. Всі галузі науки, в свою чергу, працюють над досягненням новітніх знань та технологій. Дійсно, перед науковцями стоять високі цілі, але, в усі часи, великі відкриття супроводжувалися шкідливим, так званим, «побічним продуктом» і використовувалися людиною проти людства.

Наш час продемонстрував як можуть змінити звичний стан природи та життя людей пандемія та війна. Ці страшні явища примушують нас розглядати «Цивільний захист» як одну з найважливіших учбових дисциплін.

Метою цього навчально-методичного посібника є надання здобувачам вищої освіти правового університету комплексних знань та практичних навичок, необхідних для розуміння та ефективного реагування на загрози, пов’язані з надзвичайними ситуаціями. Посібник структуровано відповідно до сучасних підходів у сфері цивільного захисту та включає не лише теоретичний матеріал, а й аналіз нормативно-правових актів, міжнародних стандартів, практичні рекомендації, тестові завдання, кейси та реальні приклади з практики.

Автори цієї збірки скомпонували теми та матеріали, які, з точки зору досвіду, мають бути корисними для студентів ВНЗ.

Посібник може бути використаний у навчальному процесі, а також слугувати основою для подальших досліджень і розробки практичних заходів у сфері цивільного захисту. Завдяки поєднанню наукової аргументації та практичної спрямованості він сприятиме формуванню у здобувачів здатності до аналітичного мислення, прийняття виважених рішень у кризових ситуаціях та ефективного застосування норм цивільного захисту на практиці.

РОЗДІЛ 1. Поняття про безпеку та нормативно-правові засади цивільного захисту.

Безпека людини та суспільства є основною умовою сталого розвитку держави, а її забезпечення передбачає сукупність правових, організаційних і технічних заходів, спрямованих на захист населення, територій, матеріальних цінностей і навколишнього середовища від надзвичайних ситуацій природного, техногенного, соціального та воєнного характеру. Цивільний захист є однією з ключових функцій держави, що включає комплекс заходів, спрямованих на запобігання, ліквідацію наслідків надзвичайних ситуацій, евакуацію населення, медичне забезпечення та відновлення критичної інфраструктури після катастроф.

1.1. Законодавство: «Про охорону праці», «Про забезпечення санітарноепідемічного благополуччя населення», «Про запобігання та протидію домашньому насильству», Кодекс цивільного захисту України.

Правовою основою цивільного захисту є **Конституція України**, Кодекс цивільного захисту України, а також акти Президента України та Кабінету Міністрів України. Нормативно-правове забезпечення та організаційно-функціональна структура системи захисту персоналу об’єктів господарювання та населення у надзвичайних ситуаціях ґрунтується на існуючій нормативно-правовій базі, що регламентує організаційну структуру системи управління безпекою та захистом у надзвичайних ситуаціях (НС).

Основні закони, що регулюють цю сферу:

Кодекс цивільного захисту України – визначає основні поняття та регулює відносини, пов’язані із захистом населення, територій, навколишнього природного середовища та майна від надзвичайних ситуацій.

Закон України «Про охорону праці» – містить положення щодо безпеки праці та заходів щодо запобігання виробничим аваріям і небезпечним ситуаціям.

Закон України «Про об'єкти підвищеної небезпеки» – регулює правові, економічні, соціальні та організаційні основи діяльності, пов'язаної з ОПН.

Закон України «Про промислову безпеку» – визначає стандарти роботи з небезпечними виробничими об'єктами.

Закон України «Про пожежну безпеку» – передбачає заходи пожежної безпеки для підприємств, установ та організацій.

Закон України «Про використання ядерної енергії та радіаційну безпеку» – регулює діяльність, пов'язану з використанням ядерних установок та джерел іонізуючого випромінювання.

Закон України «Про правовий режим воєнного стану» – визначає правові засади дій у період збройних конфліктів.

Закон України «Про мобілізаційну підготовку та мобілізацію» – встановлює норми щодо підготовки економіки до роботи в умовах НС.

Закон України «Про правовий режим надзвичайного стану» – встановлює порядок запровадження особливих заходів безпеки.

Крім зазначених нормативно-правових актів, цивільний захист в Україні регулюється численними підзаконними актами, державними стандартами та міжнародними угодами, які сприяють координації заходів із запобігання та ліквідації надзвичайних ситуацій.

1.2. Міжнародне співробітництво України у галузі цивільного захисту, програма «Партнерство заради миру».

Міжнародне співробітництво України у сфері цивільного захисту є важливим напрямом зовнішньої політики держави, спрямованим на інтеграцію у світову систему безпеки, обмін передовими практиками та зміцнення потенціалу щодо реагування на надзвичайні ситуації. Розвиток міжнародно-правової бази відіграє ключову роль у регулюванні механізмів спільного реагування на надзвичайні ситуації, передбачаючи укладання двосторонніх і багатосторонніх угод, що визначають принципи співпраці між державами. Україна активно

розвиває договірно-правову базу, спрямовану на створення ефективних механізмів обміну інформацією, взаємодопомоги та технічної підтримки у разі катастроф. Станом на 2025 рік Україна продовжує розширювати співпрацю у сфері цивільного захисту з міжнародними партнерами. Одним із ключових досягнень стало підписання оновленої угоди про співпрацю з Агентством Європейського Союзу з питань цивільного захисту та гуманітарної допомоги (ECHO), що передбачає розширення фінансування на покращення системи реагування на надзвичайні ситуації. Крім того, Україна приєдналася до нової ініціативи НАТО щодо покращення координації сил цивільного захисту в кризових умовах. Було підписано меморандум про взаємодію з Департаментом з надзвичайних ситуацій США (FEMA) щодо спільних навчань і розробки нових алгоритмів евакуації під час техногенних катастроф. Також у рамках співпраці з ООН у 2025 році запущено програму з моніторингу ризиків надзвичайних ситуацій за допомогою супутникових технологій, що дозволяє покращити прогнозування потенційних загроз і оперативність реагування.

Взаємодія з міжнародними організаціями є фундаментом ефективного цивільного захисту на глобальному рівні. Україна є активним учасником програм та ініціатив ООН, таких як Програма розвитку ООН (UNDP) у сфері підвищення стійкості до надзвичайних ситуацій, Глобальна ініціатива щодо зменшення ризику катастроф (UNDRR) та Координаційний механізм гуманітарної допомоги ООН (OCHA). У межах співпраці з НАТО Україна бере участь у Програмі «Наука заради миру та безпеки» (SPS), що включає розвиток новітніх технологій для моніторингу та ліквідації наслідків надзвичайних ситуацій. Рада Європи підтримує Україну у межах Програми Європейського Союзу «UCPM» (Механізм цивільного захисту ЄС), що забезпечує міжнародну координацію допомоги у разі надзвичайних ситуацій. Європейська комісія реалізує ініціативу «EU4Resilience» для підвищення адаптивної спроможності України до кризових ситуацій. ОБСЄ сприяє розбудові потенціалу цивільного захисту через Програму з безпеки навколишнього середовища, що спрямована на ліквідацію наслідків екологічних та техногенних катастроф., що сприяє

покращенню координації дій у випадку надзвичайних ситуацій. Важливим аспектом такої співпраці є залучення міжнародних експертів до оцінки ризиків, що дозволяє враховувати передовий світовий досвід у розробці стратегій цивільного захисту та підвищенні рівня готовності до надзвичайних подій. Спільні науково-дослідні ініціативи сприяють адаптації найкращих практик прогнозування ризиків та удосконаленню методологій реагування. Впровадження передових технологій моніторингу небезпек, зокрема використання супутникових систем, безпілотних літальних апаратів та штучного інтелекту, значно покращує швидкість і точність оцінки надзвичайних ситуацій. Це, у свою чергу, підвищує ефективність координації дій між міжнародними та національними органами цивільного захисту, забезпечуючи оперативне реагування, евакуацію та гуманітарну підтримку в критичних умовах.

Налагодження механізмів взаємодії з відповідними структурами інших держав сприяє підвищенню ефективності реагування на природні, техногенні та соціальні катастрофи. Створення спільних координаційних центрів, оперативне узгодження алгоритмів дій та розробка єдиних стандартів управління кризовими ситуаціями дозволяє швидко реагувати на надзвичайні ситуації. Крім того, міжнародне співробітництво в цій сфері передбачає проведення спільних тренувань та навчань, спрямованих на відпрацювання алгоритмів ліквідації наслідків катастроф та координацію рятувальних служб.

Обмін інформацією та досвідом є важливою складовою міжнародної взаємодії, оскільки дозволяє аналізувати причини та наслідки надзвичайних ситуацій у різних країнах, оцінювати ефективність застосованих заходів та адаптувати передові методи у власну систему цивільного захисту. У сучасних умовах, коли ризики глобальних катастроф значно зросли через збройні конфлікти, екологічні кризи, техногенні аварії та пандемії, оперативний обмін інформацією дозволяє країнам своєчасно виявляти загрози, покращувати механізми попередження і швидше мобілізувати ресурси для реагування. Використання спільних баз даних, проведення міжнародних наукових досліджень та інтеграція технологічних рішень значно підвищують рівень безпеки та ефективність роботи

структур цивільного захисту. Завдяки міжнародній взаємодії відбувається уніфікація стандартів реагування, що дозволяє державам працювати спільно у випадку катастроф глобального масштабу, забезпечуючи не лише національну, а й міжнародну безпеку. Розширення доступу до міжнародних баз даних, проведення спільних наукових досліджень та використання новітніх технологій прогнозування надзвичайних ситуацій сприяє підвищенню рівня безпеки населення. У сучасних умовах ці механізми використовуються для створення моделей прогнозування катастроф, що базуються на великих масивах даних та машинному навчанні. Наприклад, супутникові системи спостереження, такі як Copernicus Emergency Management Service (CEMS), дозволяють виявляти потенційні екологічні та техногенні загрози ще на ранніх етапах. Інтеграція в систему міжнародного обміну даними також дає змогу Україні оперативно отримувати інформацію про глобальні загрози, включаючи природні катаклізми, епідемії та військові конфлікти, що сприяє своєчасному реагуванню та оптимізації ресурсів. Ці заходи значно підвищують здатність держави до управління кризовими ситуаціями, що є критично важливим у сучасних геополітичних та екологічних реаліях.

Розвиток спільних навчальних програм, тренувань та навчань спрямований на вдосконалення професійної підготовки фахівців у сфері цивільного захисту, обмін найкращими практиками та стандартизацію методів реагування на катастрофи. У сучасних умовах Україна активно бере участь у таких міжнародних навчальних ініціативах, як спільні тренування з НАТО в межах Програми розширених можливостей (EOP), де українські рятувальники та військові проходять підготовку з кризового реагування. У 2024–2025 роках Україна також бере участь у європейській програмі «RescEU», що передбачає підготовку спеціалізованих команд для ліквідації наслідків стихійних лих, а також обмін досвідом із провідними європейськими структурами цивільного захисту. Крім того, у співпраці з Агентством США з міжнародного розвитку (USAID) реалізовано серію навчальних семінарів для українських рятувальників та медичних служб щодо дій у надзвичайних ситуаціях воєнного часу. Ці програми

не лише підвищують рівень професійної підготовки українських фахівців, а й сприяють адаптації найкращих міжнародних стандартів у систему цивільного захисту України. Участь українських рятувальних служб у міжнародних місіях і навчаннях дозволяє впроваджувати інноваційні методи роботи та підвищувати професіоналізм фахівців у надзвичайних ситуаціях.

Розширення співпраці у сфері наукових досліджень та інновацій сприяє створенню ефективних технологій запобігання та ліквідації наслідків надзвичайних ситуацій. Участь у міжнародних дослідницьких проєктах, розробка сучасних засобів захисту та впровадження штучного інтелекту у системи прогнозування загроз є важливими напрямками розвитку цивільного захисту України.

РОЗДІЛ 2. Загальні відомості про надзвичайні ситуації.

Основні поняття, класифікація та характеристики надзвичайних ситуацій, їхні причини та можливі наслідки для населення, інфраструктури та довкілля. Надзвичайні ситуації можуть мати природне, техногенне, соціальне або воєнне походження, і їхня поява вимагає негайного реагування для мінімізації шкоди. Важливим аспектом є аналіз механізмів прогнозування, запобігання та ліквідації наслідків НС, а також ролі державних органів, спеціалізованих служб і громадськості у забезпеченні ефективного цивільного захисту.

2.1. Види та джерела небезпеки при надзвичайних ситуаціях.

Надзвичайні ситуації (НС) – це події, що спричиняють порушення нормальних умов життєдіяльності населення та функціонування господарських об'єктів, призводять до загибелі або значного погіршення здоров'я людей, руйнування інфраструктури та значних матеріальних втрат. Вони класифікуються відповідно до їхнього походження та механізму виникнення.

Види надзвичайних ситуацій:

НС природного характеру – виникають унаслідок природних процесів та явищ, які мають значний вплив на довкілля, економіку та життєдіяльність населення. Ці явища можуть бути раптовими або розвиватися поступово, створюючи умови для потенційної катастрофи. Геофізичні та геологічні явища, такі як землетруси чи виверження вулканів, можуть спричиняти значні руйнування та зміну ландшафту, тоді як гідрометеорологічні катастрофи, такі як повені, урагани та засухи, загрожують сільському господарству, інфраструктурі та водним ресурсам. Біологічні НС, такі як пандемії або нашестя шкідників, можуть мати довготривалий вплив на громадське здоров'я, економічну стабільність та соціальну сферу. Попри те, що більшість природних НС неможливо повністю запобігти, сучасні методи прогнозування та раннього попередження дозволяють зменшувати їхній негативний вплив. До них належать: – геофізичні:

землетруси, цунамі, виверження вулканів; – геологічні: зсуви, обвали, карстові провали; – гідрометеорологічні: урагани, буревії, зливи, повені, селі, снігові лавини, посухи; – біологічні: епідемії серед людей, епізоотії серед тварин, епіфітотії серед рослин.

НС техногенного характеру – спричинені діяльністю людини, порушенням технологічних процесів, недотриманням норм безпеки, зношеністю інфраструктури та аваріями на промислових підприємствах і транспорті. Вони можуть виникати через технічні несправності, помилки персоналу, вплив зовнішніх факторів або недосконаліть технологічних систем. Особливо небезпечними є аварії на підприємствах, що працюють із токсичними, радіоактивними або вибухонебезпечними матеріалами, оскільки вони можуть мати довготривалі екологічні та соціальні наслідки. У транспортній сфері надзвичайні ситуації часто спричинені перевищенням швидкості, технічними несправностями транспортних засобів, несприятливими погодними умовами або людським фактором.

У сучасних умовах розвиток інноваційних технологій, автоматизованих систем контролю та посилення нормативного регулювання є ключовими заходами зменшення ризиків виникнення техногенних надзвичайних ситуацій включають: – **аварії на промислових підприємствах** включають вибухи на виробництвах із підвищеним рівнем небезпеки, хімічні аварії, що супроводжуються викидом отруйних речовин, пожежі, які можуть спричинити значні матеріальні збитки та загрозу для життя населення, а також радіаційні аварії, що мають довготривалий вплив на навколишнє середовище. Вони можуть виникати внаслідок недотримання правил безпеки, зношеності обладнання, людського фактору або впливу зовнішніх катастрофічних чинників. Наслідки таких аварій можуть мати масштабний екологічний, соціальний та економічний вплив, включаючи масові евакуації, зараження територій та потребу в довготривалих заходах ліквідації. – **аварії на транспорті** включають інциденти, пов’язані із залізничними, авіаційними, автомобільними, морськими та річковими перевезеннями, які можуть мати серйозні наслідки для життя та здоров’я людей, стану інфраструктури та навколишнього середовища; – з**алізничні аварії**

можуть бути спричинені сходженням потягів із рейок, зіткненням поїздів, несправністю колійного обладнання, порушенням сигналізації або помилками персоналу. Вони можуть спричинити масові людські жертви, значні матеріальні втрати та екологічні наслідки у разі перевезення небезпечних речовин; – **авіаційні катастрофи** відбуваються внаслідок технічних несправностей, погодних умов, помилок екіпажу або терористичних атак. Вони зазвичай мають високий рівень летальності та можуть призводити до руйнувань на місці падіння; – **автомобільні аварії** є найпоширенішими серед транспортних надзвичайних ситуацій та можуть включати зіткнення транспортних засобів, наїзди на пішоходів, злети з дороги, вибухи паливних баків. Основні причини – перевищення швидкості, водіння у стані сп'яніння, несправність транспорту та погані дорожні умови; – **морські та річкові аварії** пов'язані з зіткненнями суден, затопленням, пожежами на борту, порушенням навігаційних правил або стихійними явищами. Такі аварії можуть мати значний екологічний ефект, особливо у разі розливу нафти або інших небезпечних вантажів.

Запобігання транспортним аваріям потребує чіткого дотримання норм безпеки, впровадження сучасних систем контролю, підвищення рівня підготовки персоналу та використання новітніх технологій для моніторингу та управління транспортними потоками.

Енергетичні аварії включають відключення електропостачання, вихід з ладу систем теплопостачання, пошкодження об'єктів генерації та розподілу енергії. Такі ситуації можуть бути викликані технічними несправностями, перевантаженням мережі, терористичними атаками або природними катастрофами. Наслідки енергетичних аварій можуть мати довготривалий вплив на інші критично важливі сфери життєдіяльності, включаючи медицину, транспорт, водопостачання та безпеку об'єктів стратегічного значення.

Гідродинамічні аварії – це руйнування гідротехнічних споруд (гребель, дамб, каналів), що призводить до затоплення територій, руйнування інфраструктури та загрози для населення. Вони можуть виникати через природні фактори, такі як повені та землетруси, а також унаслідок технічних помилок,

навмисних диверсій або зношеності конструкцій. Такі аварії нерідко супроводжуються значними екологічними катастрофами, включаючи забруднення водних ресурсів і деградацію земель.

Аварії на системах життєзабезпечення охоплюють катастрофи в системах каналізації, газопостачання, водопостачання та теплопостачання. Вони можуть бути спричинені зношеністю інфраструктури, аварійними проривами мереж, терористичними актами або природними катастрофами. Наслідки таких аварій можуть включати перебої у постачанні питної води, витоки небезпечних газів, що створюють загрозу отруєнь і вибухів, а також порушення санітарно-епідемічної ситуації в регіоні. Для запобігання подібним ситуаціям необхідне регулярне технічне обслуговування мереж, використання сучасних технологій діагностики та впровадження аварійно-резервних систем.

НС соціального характеру – викликані свідомими діями людей або соціальними явищами, які порушують громадський порядок, створюють загрозу життю і здоров'ю населення та можуть мати дестабілізуючий вплив на суспільство. До таких ситуацій належать масові заворушення, страйки, акти тероризму, збройні конфлікти, незаконна міграція, етнічні чи релігійні протистояння, а також соціально-економічні кризи, що призводять до зростання злочинності та посилення соціальної напруженості. В умовах сучасного світу, де інформаційні та кібернетичні загрози набувають все більшої актуальності, значну небезпеку становлять також інформаційні маніпуляції, поширення дезінформації та кібератаки, спрямовані на розпалювання соціальної нестабільності та порушення критично важливих державних процесів. Подібні ситуації можуть мати довготривалий негативний ефект на суспільство, спричиняючи масові міграційні процеси, підрив економічної стабільності та погіршення рівня безпеки держави в цілому.

- **Масові заворушення, страйки, терористичні акти, збройні конфлікти,** що можуть призводити до значних жертв серед цивільного населення, руйнування критичної інфраструктури, погіршення економічної ситуації в країні та порушення функціонування державних органів влади. Такі

події створюють загрозу національній безпеці та можуть ускладнювати діяльність правоохоронних органів і служб цивільного захисту.

- **Незаконне переміщення небезпечних речовин, зброї, радіоактивних матеріалів або вибухонебезпечних речовин**, що становлять загрозу для населення та довкілля. Такі дії можуть бути пов'язані з терористичною діяльністю або контрабандою, що ускладнює контроль держави за безпековою ситуацією.
- **Нещасні випадки** з великою кількістю потерпілих, що можуть виникати внаслідок транспортних катастроф, обвалів будівель, техногенних аварій, терактів або стихійних лих. У таких ситуаціях особливого значення набувають оперативність рятувальних служб, координація медичної допомоги та організація евакуації постраждалих.
- **Масові епідемії**, викликані антисанітарними умовами, біотероризмом або поширенням нових інфекційних захворювань. Вони можуть мати серйозні наслідки для системи охорони здоров’я, економіки та безпеки країни. До таких випадків відносяться пандемії, локальні спалахи небезпечних вірусних інфекцій, а також навмисне поширення збудників інфекційних хвороб з метою дестабілізації суспільства.

НС воєнного характеру – виникають у результаті збройних конфліктів, терористичних актів, застосування сучасних методів гібридної війни або диверсійної діяльності. Вони можуть мати різні форми, від відкритих бойових дій із застосуванням звичайних озброєнь до інформаційних та кібернетичних атак, спрямованих на підрив державної безпеки та дестабілізацію економічної і соціальної систем. До таких ситуацій належить використання терористичних груп, підготовлених для проведення атак на критичну інфраструктуру, порушення систем управління військовими або цивільними об’єктами, організація інформаційних кампаній для дезорієнтації суспільства та поширення паніки. Крім того, війни та військові конфлікти можуть супроводжуватися великими гуманітарними кризами, масовими міграційними потоками, дефіцитом життєво необхідних ресурсів, а також значними екологічними наслідками у разі

руйнування промислових об'єктів, що містять небезпечні хімічні чи радіоактивні речовини: – **застосування зброї масового ураження** (ядерної, хімічної, біологічної), що може мати катастрофічні наслідки для населення, довкілля та інфраструктури. Використання ядерної зброї призводить до масових руйнувань, радіаційного зараження та довготривалих екологічних і гуманітарних криз. Хімічна зброя здатна спричинити отруєння великих територій та завдати шкоди здоров'ю населення на генетичному рівні. Біологічна зброя створює загрозу пандемій, які можуть швидко поширюватися, виходячи за межі однієї країни; – **збройні вторгнення, бойові дії, обстріли цивільних об'єктів,** що супроводжуються масштабними руйнуваннями, людськими втратами, порушенням функціонування систем життєзабезпечення та економічним колапсом. Військові конфлікти викликають масові переміщення біженців, що створює додаткові соціальні та гуманітарні проблеми для держави; – **кібератаки на критичну інфраструктуру**, які можуть паралізувати фінансові системи, енергетичні мережі, системи водопостачання, транспорт, зв'язок та державне управління. Кібератаки використовуються як елемент гібридної війни та здатні дестабілізувати країну без прямого застосування військової сили; – **диверсії** на об'єктах життєзабезпечення, транспорту, зв'язку, що спрямовані на створення хаосу, порушення обороноздатності та підрив соціально-економічної стабільності. Вибухи на підприємствах стратегічного значення, знищення мостів, дамб, підриви залізничних шляхів та комунікацій можуть значно ускладнити роботу рятувальних служб і вплинути на безпеку країни загалом.

Джерела небезпеки при НС:

Природні – неконтрольовані природні процеси, які виникають унаслідок геологічних, кліматичних або біологічних змін, що можуть загрожувати життю та здоров'ю населення, спричиняти значні матеріальні збитки, порушувати соціальну стабільність і екосистеми. Ці явища, зокрема землетруси, повені, урагани, посухи, можуть впливати на продовольчу безпеку, викликати дефіцит водних ресурсів, масові переміщення населення та погіршення санітарно-епідеміологічної ситуації. Умови глобального потепління та антропогенного

впливу збільшують частоту та масштабність таких подій, що вимагає розробки комплексних стратегій адаптації, запобігання та реагування на природні катастрофи.

Техногенні – аварії, спричинені людською діяльністю, що можуть виникати внаслідок технічних несправностей, помилок персоналу, недотримання норм безпеки, зношеності інфраструктури, навмисних диверсій чи впливу зовнішніх факторів. Такі аварії можуть включати промислові катастрофи, аварії на транспорті, пожежі, витоки небезпечних хімічних та радіоактивних речовин, техногенні вибухи, вихід з ладу критичних енергетичних та інженерних мереж. Вони можуть мати як локальний, так і глобальний характер, спричиняючи значні економічні збитки, людські жертви та довготривалий негативний вплив на довкілля.

Соціальні – умисні дії, що можуть спричинити дестабілізацію суспільства, загострення соціальних конфліктів, руйнування економічних зв’язків, погіршення рівня громадської безпеки та створення довготривалої нестабільності. До таких дій належать терористичні акти, масові заворушення, кібератаки, навмисне поширення дезінформації, маніпуляції суспільною свідомістю через соціальні мережі та засоби масової інформації. Також дестабілізуючий вплив можуть мати організовані економічні саботажі, блокування критично важливих ресурсів, створення штучного дефіциту продовольства чи енергетичних ресурсів. Наслідки таких дій можуть бути катастрофічними для політичної стабільності країни, її економічного розвитку та безпеки громадян, що вимагає ефективної протидії на рівні державної безпеки та стратегічного планування.

Воєнні – загрози, пов’язані з веденням бойових дій, диверсіями, кібератаками та інформаційними війнами. В умовах сучасних конфліктів бойові дії можуть супроводжуватися застосуванням високотехнологічної зброї, використанням безпілотних літальних апаратів, артилерійськими обстрілами населених пунктів та інфраструктури, а також операціями зі знищення об'єктів стратегічного значення. Диверсії можуть включати підривні дії на енергетичних об’єктах, транспортній інфраструктурі, промислових підприємствах та об'єктах критичної

інфраструктури. Кібератаки стають одним із головних інструментів гібридної війни, спрямованих на виведення з ладу державних інформаційних систем, банківської інфраструктури, телекомунікаційних мереж, а також на дестабілізацію роботи урядових органів через злам даних та поширення дезінформації. Інформаційні війни включають масові кампанії з використанням соціальних мереж та медіа з метою маніпуляції суспільною свідомістю, підриву довіри до державних інституцій та провокування соціальної нестабільності. Комплексний характер сучасних воєнних загроз вимагає ефективної системи національної безпеки, міжнародного співробітництва та розвитку механізмів кіберзахисту, а також стратегій інформаційної протидії агресору..

Розуміння видів та джерел НС дає змогу ефективно організовувати заходи з попередження, реагування та ліквідації їхніх наслідків, що є критично важливим для забезпечення національної безпеки та стабільного функціонування держави. Комплексний підхід до управління надзвичайними ситуаціями включає розробку ефективних систем раннього попередження, підвищення рівня підготовки сил цивільного захисту, створення стратегічних резервів ресурсів для ліквідації наслідків катастроф, а також впровадження сучасних інформаційних технологій для прогнозування можливих загроз. Посилення міжнародного співробітництва у сфері безпеки, обмін досвідом та інтеграція в глобальні системи моніторингу надзвичайних ситуацій є важливими складовими забезпечення стійкості держави перед викликами сучасного світу.

2.2. Класифікація надзвичайних ситуацій та аварій.

Класифікація надзвичайних ситуацій (НС) та аварій дозволяє систематизувати заходи з їх попередження, реагування та ліквідації наслідків. Відповідно до Кодексу цивільного захисту України, НС класифікуються за походженням, масштабом, характером впливу, рівнем небезпеки та специфікою наслідків. Це сприяє ефективному плануванню дій з метою мінімізації наслідків надзвичайних ситуацій, забезпеченню координації між органами влади, рятувальними службами

та громадськістю. Кожен із зазначених критеріїв класифікації відіграє важливу роль у визначенні заходів попередження, підготовки до можливих надзвичайних подій та оперативного реагування на них. Таким чином, систематизований підхід до аналізу та класифікації надзвичайних ситуацій є невід'ємною частиною державної політики у сфері цивільного захисту.

За характером впливу:

Хімічні – викликані викидом отруйних речовин у довкілля внаслідок аварій на хімічних підприємствах, транспортування небезпечних речовин, терактів або стихійних лих. Хімічне забруднення може призвести до масових отруєнь, загибелі людей, екологічних катастроф та тривалого негативного впливу на здоров'я населення.

Радіаційні – спричинені аваріями на атомних електростанціях, використанням ядерної зброї або витоком радіоактивних матеріалів під час транспортування. Наслідки таких ситуацій включають гострі та хронічні радіаційні ураження, генетичні мутації, довготривале забруднення довкілля і необхідність евакуації населення з великих територій.

Біологічні – пов'язані з поширенням небезпечних вірусів, бактерій, шкідників або зараженням продуктів харчування. Такі ситуації можуть виникати внаслідок природних епідемій або в результаті біотерористичних атак, що можуть викликати масові захворювання, пандемії та дестабілізацію економічної та соціальної ситуації.

Фізичні – пов'язані з механічними впливами, такими як вибухи, обвали, сейсмічні коливання, катастрофічні обвали ґрунту або руйнування будівель. Вони можуть призводити до значних жертв серед населення, руйнування інфраструктури та значних економічних втрат.

Кібератаки – викликані навмисним втручанням у роботу цифрових мереж та інформаційних систем. Це можуть бути зломи баз даних, порушення роботи критичних об'єктів інфраструктури, кібершпигунство, атаки на фінансову систему, що призводить до значних фінансових збитків, втрати контролю над державними ресурсами та загрози національній безпеці.

Комбіновані – поєднують кілька типів загроз одночасно (наприклад, воєнні дії, що супроводжуються техногенними катастрофами, екологічними лихами та епідеміями). Такі надзвичайні ситуації є найскладнішими для реагування, оскільки вимагають комплексних заходів ліквідації, залучення міжнародної допомоги та значних фінансових і людських ресурсів.

2.3. Наслідки надзвичайних ситуацій.

Надзвичайні ситуації мають багатовимірний вплив на суспільство, державні інституції, економіку, екологію та психічне здоров'я громадян. Їх наслідки можуть бути як безпосередніми, так і довготривалими, що змушує державні та міжнародні структури розробляти ефективні механізми попередження, реагування та ліквідації наслідків. У сучасному світі глобалізація, інтенсифікація промислового виробництва та технологічний прогрес роблять ризики виникнення НС ще більш значущими. Військові конфлікти, кліматичні зміни, техногенні катастрофи та біологічні загрози призводять до значних економічних, політичних і соціальних втрат, що впливають не лише на окремі регіони, а й на міжнародну стабільність. Вивчення та аналіз наслідків НС є важливим для формування стратегій управління ризиками та ефективного функціонування системи цивільного захисту.

Соціальні наслідки включають масову загибель людей, значне зростання рівня травматизму та погіршення стану здоров'я населення, а також погіршення умов життєдіяльності через знищення або пошкодження житлових будівель, комунальної інфраструктури та медичних закладів. Зростання рівня злочинності, соціального напруження, поширення паніки та деморалізації населення можуть стати додатковими негативними факторами, що сприяють виникненню нових конфліктів. Масові вимушені міграції населення створюють додаткове навантаження на економіку та соціальну інфраструктуру приймаючих регіонів чи країн.

Економічні наслідки включають руйнування промислових підприємств, об'єктів інфраструктури, транспортної мережі, що призводить до зупинки виробництва та втрати робочих місць. Дестабілізація фінансових ринків, значні економічні збитки можуть спричинити інфляцію, дефіцит товарів і ресурсів. Необхідність витрат на ліквідацію наслідків, відбудову зруйнованих об'єктів, компенсацію постраждалим може значно перевищувати резервні можливості держави. Втрата врожаю та продовольча криза внаслідок забруднення сільськогосподарських угідь, посухи, затоплення чи інших факторів також є серйозною загрозою стабільності економічного розвитку.

Екологічні наслідки полягають у забрудненні ґрунту, повітря та водних ресурсів внаслідок аварій на хімічних, нафтопереробних, атомних об'єктах. Винищення флори та фауни призводить до порушення екосистем і втрати біологічного різноманіття. Тривалі зміни кліматичних умов та ризик виникнення нових екологічних катастроф, зокрема внаслідок руйнування природних бар'єрів, лісових масивів, можуть мати непоправні наслідки для екологічного стану регіонів.

Політичні наслідки охоплюють дестабілізацію політичної ситуації, зниження довіри населення до влади через неефективні дії або відсутність своєчасного реагування на надзвичайну ситуацію. Посилення міждержавної напруженості може стати неминучим, якщо НС зачіпає кілька країн або пов’язана з військовими діями. Послаблення національної безпеки, підвищення ризику зовнішніх загроз та посилення соціальної напруженості всередині країни можуть стати фактором довготривалої нестабільності.

Психологічні наслідки проявляються у вигляді масових психологічних травм, посттравматичного стресового розладу (ПТСР), депресії, зростання рівня суїцидів серед постраждалих груп населення. Висока емоційна нестабільність, поширення страху негативно впливає на соціальну поведінку громадян. Зниження продуктивності праці через психологічне виснаження, емоційне вигорання працівників, особливо тих, хто працює в зонах ліквідації наслідків НС,

може мати суттєві наслідки для економіки та функціонування критично важливих сфер держави.

Зростання рівня злочинності, соціального напруження, поширення паніки та деморалізації населення під час надзвичайних ситуацій відбувається через кілька ключових факторів. **Нестабільність і руйнування соціальних інституцій** призводять до ослаблення контролю за дотриманням правопорядку, що створює сприятливі умови для зростання злочинності. В умовах хаосу, коли правоохоронні органи зосереджені на ліквідації наслідків катастрофи або війни, злочинні угруповання активізуються, використовуючи ситуацію для власної вигоди. **Погіршення економічної ситуації та злидні** штовхають частину населення до нелегальних способів виживання. Дефіцит продуктів, медикаментів, життєво важливих ресурсів провокує мародерство, контрабанду та нелегальну торгівлю. **Інформаційний вакуум або навпаки – інформаційні маніпуляції** сприяють поширенню паніки та дезінформації, що підвищує рівень соціального напруження. Недовіра до влади, поширення чуток, страх перед невизначеністю майбутнього можуть викликати масові протести, сплески агресії та насильства. **Психологічний стан населення** під впливом стресу та травматичних подій може спричиняти імпульсивні дії, агресію та деструктивну поведінку. Деморалізація населення відбувається через втрату почуття безпеки, руйнування звичних життєвих умов та постійне відчуття загрози.

Таким чином, наслідки надзвичайних ситуацій мають комплексний характер і потребують швидкої та скоординованої реакції з боку органів влади, громадських організацій, міжнародних партнерів та всього суспільства для мінімізації втрат та забезпечення швидкого відновлення країни після катастрофічних подій. з боку органів влади, громадських організацій, міжнародних партнерів та всього суспільства для мінімізації втрат та забезпечення швидкого відновлення країни після катастрофічних подій.

РОЗДІЛ 3. Небезпечні та шкідливі чинники в цивільному захисті.

Небезпечні та шкідливі чинники є основними загрозами для життя і здоров'я населення в умовах надзвичайних ситуацій, а їх ідентифікація, оцінка та мінімізація є ключовими завданнями цивільного захисту. Небезпечні чинники поділяються на природні, техногенні, соціальні та воєнні, а їхній вплив може бути як прямим, так і опосередкованим, що ускладнює ліквідацію наслідків надзвичайних ситуацій.

3.1. Класифікація небезпечних і шкідливих чинників.

Небезпечні речовини – це речовини, які за певних обставин можуть становити загрозу життю та здоров’ю людей, довкіллю, матеріальним і культурним цінностям. Вони включають хімічні та токсичні речовини, вибухові та окислювальні компоненти, горючі матеріали, а також біологічні агенти, що можуть викликати інфекційні захворювання чи забруднення довкілля. Залежно від хімічного складу та фізичних характеристик вони можуть поширюватися різними шляхами: через повітря, воду, ґрунт або безпосередній контакт. Особливу небезпеку становлять речовини з високою леткістю або стійкістю у довкіллі, оскільки вони можуть спричиняти довготривалі негативні наслідки.

У рамках системи цивільного захисту важливу роль відіграє **ідентифікація об’єктів підвищеної небезпеки**. Відповідно до постанови Кабінету Міністрів України, такі об’єкти визначаються за пороговими нормативами маси небезпечних речовин. Це дозволяє запроваджувати превентивні заходи контролю та регулювання, що сприяють зменшенню ризиків у разі виникнення аварійних ситуацій. Деякі речовини, зокрема аміак, хлор, формальдегід, ацетилен та нітрати, мають специфічні порогові значення, що вимагає розробки особливих заходів безпеки.

Забруднюючі речовини – це тверді, рідкі чи газоподібні хімічні компоненти, присутні в навколишньому середовищі у концентраціях, що перевищують

гранично допустимі норми. Вони можуть негативно впливати на здоров'я населення, спричиняти мутагенні, канцерогенні, алергенні ефекти, а також руйнувати екосистеми. До особливо небезпечних речовин, визначених ЮНЕСКО, належать бензол, азбест, ртуть та її сполуки, важкі метали, промислові барвники та агрохімікати. Їх присутність у повітрі, воді чи ґрунті може спричиняти довгострокові негативні наслідки для здоров'я, такі як хронічні захворювання органів дихання, онкологічні патології, порушення функцій нервової та ендокринної систем.

Шкідливі речовини можуть проникати в організм людини різними шляхами: інгаляційним, контактним або через травну систему. Найбільш небезпечним є інгаляційний шлях, коли токсичні гази та аерозолі потрапляють у кров через легеневу тканину, спричиняючи інтоксикацію організму. При контакті зі шкірою можливе проникнення рідких хімічних агентів, а через травну систему – забруднених продуктів харчування або води. Вплив шкідливих речовин може посилюватися під дією високої температури, вологості та фізичного навантаження. Особливо вразливими до їх дії є люди з ослабленим імунітетом, діти, вагітні жінки та особи похилого віку.

Контроль і регулювання небезпечних речовин у навколишньому середовищі є важливим елементом системи цивільного захисту. Одним із ключових показників, що визначають безпечність умов праці та проживання, є **гранично допустима концентрація (ГДК)** – максимально допустимий рівень шкідливих речовин у повітрі робочої зони, при якому їх вплив не спричиняє хронічних захворювань або професійних отруєнь. Відповідно до стандартів, шкідливі речовини поділяються на чотири класи небезпеки: надзвичайно небезпечні (ртуть, свинець, озон), високонебезпечні (фенол, хлор, кислоти), помірно небезпечні (метиловий спирт, толуол, ксилол) та малонебезпечні (аміак, бензин, ацетон). Контроль за ГДК є важливою складовою системи моніторингу промислових об'єктів та екологічної безпеки. Своєчасне виявлення перевищення допустимих рівнів забруднюючих речовин дозволяє запобігати їх негативному впливу на здоров'я населення та довкілля. Систематичний моніторинг дає змогу

оперативно реагувати на зміну концентрацій шкідливих речовин у повітрі, воді та ґрунті, що є особливо актуальним в умовах індустріалізації та зростання промислових викидів. Впровадження ефективної системи контролю ГДК дає можливість прогнозувати потенційні ризики, розробляти заходи щодо їх зменшення та впроваджувати сучасні технології очищення та фільтрації забруднюючих речовин. Таким чином, ретельний контроль за ГДК є не лише превентивним механізмом у сфері цивільного захисту, а й важливим елементом екологічної політики держави, спрямованої на збереження здоров’я населення та довкілля.

З огляду на значний вплив небезпечних та шкідливих речовин на здоров'я людини та навколишнє середовище, важливим напрямом захисту є застосування спеціальних засобів, що мінімізують їх негативний вплив. Одним із основних інструментів безпеки в умовах підвищеного ризику є **засоби індивідуального захисту (ЗІЗ)**, які є ключовим елементом запобігання впливу небезпечних факторів. Вони класифікуються за рівнями ризику: від поверхневих пошкоджень і контакту з мийними засобами (категорія I) до загроз життю та здоров’ю, таких як контакт із токсичними агентами, біологічна небезпека, електричний струм, падіння з висоти (категорія III). Використання ЗІЗ є обов’язковим, якщо конструкція обладнання або організація виробничого процесу не дозволяють повністю усунути ризики. Їх ефективність значною мірою залежить від правильного вибору, належного догляду та відповідного навчання персоналу.

Система цивільного захисту передбачає не лише засоби індивідуального захисту, а й комплексні превентивні заходи. До них належать технологічне вдосконалення виробництв, автоматизація небезпечних процесів, забезпечення ефективної вентиляції, контроль рівня забруднення повітря, а також інформаційна та освітня діяльність, спрямована на підвищення обізнаності населення про ризики та методи їх мінімізації.

3.2. Ризики в житті людини.

Ризики є невід'ємною частиною життя людини та супроводжують її у всіх сферах діяльності, від повсякденного побуту до професійної та суспільної активності. Вони можуть мати різне походження та впливати на фізичний і психоемоційний стан людини, її добробут, а також стійкість суспільства в цілому. Важливо усвідомлювати, що ризики можуть бути як контрольованими, тобто такими, на які можна впливати шляхом запобіжних заходів, так і не-контрольованими, які залежать від зовнішніх факторів і не завжди піддаються регулюванню. Їхні наслідки можуть варіюватися від незначних незручностей до масштабних катастрофічних подій, що суттєво загрожують безпеці людей та навколишньому середовищу.

Природні ризики є наслідком стихійних явищ, які можуть впливати на життя та діяльність людей. Вони охоплюють землетруси, повені, урагани, снігові лавини, посухи, а також глобальні зміни клімату, що збільшують частоту та інтенсивність цих явищ. Наслідки природних ризиків можуть бути руйнівними, адже вони призводять до масових руйнувань, порушення роботи інфраструктури та значних втрат серед населення. Саме тому важливим завданням цивільного захисту є розробка стратегій прогнозування природних катастроф, ефективна система оповіщення та заходи щодо мінімізації їхніх наслідків.

Техногенні ризики є результатом людської діяльності та впливають на суспільство через аварії на виробництвах, витоки небезпечних речовин, пожежі, вибухи, транспортні катастрофи, забруднення довкілля та збої в роботі критичної інфраструктури. Вони можуть бути спричинені зношеністю обладнання, порушенням технічних регламентів, людським фактором або надзвичайними подіями. Зменшення техногенних ризиків можливе через впровадження новітніх технологій безпеки, посилення контролю за станом небезпечних об'єктів та організацію системи оперативного реагування на аварії.

Соціальні ризики пов'язані з економічними, політичними та соціальними процесами, які можуть впливати на стабільність суспільства. Вони включають

економічні кризи, рівень безробіття, зростання злочинності, корупцію, терористичні загрози та військові конфлікти. У сучасних умовах, коли суспільства все більше стикаються з проблемами глобалізації, масової міграції та політичної нестабільності, соціальні ризики набувають особливого значення. Державна політика має бути спрямована на мінімізацію цих ризиків через економічні реформи, соціальні програми, боротьбу з корупцією та посилення правопорядку.

Особисті ризики залежать від способу життя, рівня обізнаності та відповідального ставлення людини до власної безпеки. До них належать ризики, пов'язані з професійною діяльністю, небезпечними видами спорту, дорожньо-транспортними пригодами, впливом шкідливих звичок і нехтуванням правилами безпеки. Зниження особистих ризиків можливе завдяки дотриманню норм охорони праці, веденню здорового способу життя, регулярним профілактичним заходам та розвитку культури безпеки серед населення.

Оцінка ризиків є ключовим етапом у розробці заходів з їх запобігання. Вона включає аналіз загроз, ідентифікацію критичних факторів, моделювання можливих сценаріїв розвитку подій та розробку стратегії управління ризиками. Цей процес дозволяє визначити пріоритетні напрями роботи для органів цивільного захисту та державних інституцій, які займаються питаннями безпеки населення. Завдяки ефективному прогнозуванню, швидкому реагуванню та застосуванню профілактичних заходів можна значно зменшити вплив небезпечних ситуацій на суспільство.

Таким чином, ризики є невід'ємним фактором сучасного життя, проте їхнє вчасне усвідомлення та правильне управління дозволяє значно підвищити рівень безпеки населення. Системний підхід до прогнозування ризиків, їхньої ідентифікації та розробки заходів щодо зменшення впливу є ключовим аспектом ефективної системи цивільного захисту, що сприяє стабільності та сталому розвитку суспільства.

3.3. Екологічна безпека.

Екологічна безпека є критично важливим елементом загальної системи цивільного захисту, оскільки забруднення навколишнього середовища, кліматичні зміни та виснаження природних ресурсів мають прямий вплив на здоров’я людини, соціально-економічну стабільність і національну безпеку. Глобальна екологічна криза зумовлена швидким зростанням населення планети, надмірним використанням природних ресурсів, забрудненням довкілля, зміною клімату та деструктивними технологічними процесами. Сучасні антропогенні впливи, такі як індустріалізація, урбанізація та інтенсивне сільськогосподарське виробництво, значно порушують екологічну рівновагу, що призводить до деградації біосфери, забруднення атмосфери та гідросфери, зменшення родючості ґрунтів і втрати біорізноманіття.

Основними глобальними екологічними проблемами, що становлять загрозу для людства, є забруднення атмосфери, води та ґрунтів, парниковий ефект, утворення озонових дір, опустелювання, деградація екосистем та накопичення токсичних відходів. Викиди промислових підприємств, спалювання викопного палива, масове вирубування лісів та неконтрольоване використання хімічних речовин призводять до накопичення шкідливих речовин у повітрі, воді та продуктах харчування, що негативно позначається на здоров’ї людей та природному балансі екосистем.

Забруднення атмосфери є однією з найсерйозніших екологічних загроз, оскільки воно впливає не лише на якість повітря, але й на глобальні кліматичні процеси. Викиди аерозолів важких металів, канцерогенних речовин, радіоактивних частинок та синтетичних сполук погіршують стан довкілля та спричиняють захворювання органів дихання, алергічні реакції, серцево-судинні патології та онкологічні захворювання. Основними джерелами забруднення повітря є теплоенергетика, металургія, нафтохімічна промисловість, транспортні засоби та сільськогосподарська діяльність, що сприяють накопиченню в

атмосфері таких речовин, як оксид вуглецю, двоокис сірки, оксиди азоту, вуглеводні та дрібнодисперсний пил. Наслідками такого забруднення є утворення кислотних дощів, смогу, погіршення прозорості атмосфери, зменшення рівня озонового шару та загальне потепління клімату через парниковий ефект.

Вплив атмосферного забруднення на людину є багатовимірним і охоплює не лише фізичне здоров'я, але й соціально-економічні аспекти. Високий рівень забрудненості повітря сприяє зростанню дитячої захворюваності, збільшенню частоти хронічних захворювань дихальної системи, ослабленню імунітету та загальному погіршенню якості життя. За оцінками Всесвітньої організації охорони здоров'я, забруднене повітря є причиною передчасної смерті мільйонів людей щороку, особливо в регіонах з високою концентрацією промислових підприємств та інтенсивним автомобільним трафіком.

Не менш серйозною проблемою є забруднення гідросфери, яке виникає через скидання промислових і побутових стічних вод, міграцію небезпечних речовин з ґрунтів і атмосфери, а також аварійні ситуації, пов'язані з розливом нафти та хімічних речовин. Забруднення води може бути фізичним, хімічним, біологічним і тепловим. Накопичення нерозчинних часток у водоймах зменшує їхню прозорість і негативно впливає на розвиток водної флори та фауни, тоді як хімічні забруднювачі, такі як пестициди, нафтопродукти, важкі метали та токсичні відходи, можуть мати кумулятивний ефект і спричиняти серйозні екологічні катастрофи. Біологічне забруднення є особливо небезпечним, оскільки воно сприяє поширенню інфекційних захворювань через забруднення водних джерел патогенними мікроорганізмами. Теплове забруднення, яке виникає через скидання у водойми нагрітих стічних вод, змінює екологічний баланс водойм, спричиняючи загибель багатьох видів водних організмів.

Забруднення та руйнування літосфери відбувається внаслідок хімізації сільського господарства, викидів важких металів, кислотних дощів, розробки корисних копалин та неконтрольованої урбанізації. Руйнування ґрунтового покриву призводить до зменшення площі лісів, втрати родючості ґрунтів,

процесів опустелювання та деградації екосистем. Це не лише знижує продуктивність агросистем, а й загрожує продовольчій безпеці та здоров'ю людей через накопичення токсичних речовин у продуктах харчування. Важливими наслідками руйнування літосфери є ерозія ґрунтів, забруднення підземних вод, зниження біорізноманіття та посилення кліматичних змін.

Однією з найнебезпечніших форм забруднення навколишнього середовища є енергетичне забруднення, яке включає вплив електромагнітних випромінювань, радіоактивного забруднення, шуму, вібрації, ультразвуку та інфразвуку. Іонізуюче випромінювання є особливо небезпечним для людського організму, оскільки воно впливає на функціонування центральної нервової системи, органів кровотворення та ендокринної системи, що може призводити до виникнення онкологічних захворювань та генетичних мутацій. Шумове забруднення та вібрація можуть викликати порушення сну, стресові стани та хронічну втому, тоді як ультразвук та інфразвук впливають на психоемоційний стан людини, спричиняючи підвищену дратівливість, тривожність та депресивні розлади.

Для подолання екологічної кризи необхідно впроваджувати комплексні заходи, спрямовані на зниження антропогенного впливу на природу. До основних методів екологічного захисту належать технологічні, економічно-правові та соціальні заходи. Важливими технологічними рішеннями є екологічний моніторинг, розвиток енергоефективних технологій, застосування безвідходного виробництва, попередження аварій та катастроф, використання сучасних систем очищення промислових викидів та стічних вод. Економічно-правові заходи включають екологічне законодавство, нормування викидів забруднюючих речовин, систему штрафів та екологічних податків, а також стимулювання екологічно відповідального бізнесу. Соціальні заходи охоплюють екологічну освіту, популяризацію еко-культури, підтримку громадських екологічних ініціатив та розвиток міжнародного співробітництва у сфері охорони довкілля.

Збереження екологічної безпеки є невід’ємною частиною національної безпеки, а вирішення екологічних проблем вимагає системного підходу, що об’єднує державні інституції, наукову спільноту, бізнес та громадськість. Лише шляхом впровадження інноваційних технологій, екологічного управління та свідомого ставлення до природи можна досягти гармонійного співіснування людини та довкілля.

РОЗДІЛ 4. Безпека людини та охорона праці.

Безпека людини та охорона праці є ключовими аспектами забезпечення фізичного, психічного та соціального благополуччя працівників у всіх сферах діяльності. Охорона праці включає в себе систему правових, соціально-економічних, організаційно-технічних, санітарно-гігієнічних, лікувально-профілактичних і профілактично-освітніх заходів, спрямованих на збереження здоров'я та працездатності людини в процесі трудової діяльності. Основною метою охорони праці є створення безпечних і комфортних умов роботи, запобігання виробничим травмам, професійним захворюванням та аварійним ситуаціям.

4.1. Класифікація праці (фізична та розумова праця).

Праця є основною діяльністю людини, що забезпечує її існування та розвиток суспільства в цілому. Вона поділяється на два основних види: **фізичну** та **розумову** працю.

Фізична праця передбачає виконання трудових операцій, які вимагають значних фізичних навантажень. Вона характерна для промисловості, сільського господарства, будівництва, транспорту тощо. Під час фізичної праці основне навантаження припадає на опорно-руховий апарат людини, серцево-судинну та дихальну системи. Тривале виконання фізичної праці може спричинити професійні захворювання, зокрема захворювання суглобів, м'язів та кісткової системи. Тому необхідне дотримання вимог ергономіки, належної організації праці, чергування навантажень та забезпечення безпеки на робочому місці. Важливу роль відіграє застосування засобів механізації та автоматизації процесів, що дозволяє зменшити фізичне навантаження на працівників.

Розумова праця пов'язана з інтелектуальною діяльністю та вимагає значного напруження мозку, концентрації уваги, пам'яті та мислення. Вона характерна для викладачів, науковців, програмістів, лікарів, юристів тощо. Важливими аспектами розумової праці є високий рівень психоемоційного

навантаження, необхідність швидкого прийняття рішень та обробки великих обсягів інформації. Виконання розумової праці в умовах постійного стресу може призвести до перевтоми, зниження працездатності, порушення сну та інших проблем зі здоров'ям. Тому важливим є правильний режим роботи та відпочинку, зниження стресових навантажень, раціональна організація робочого простору, дотримання гігієни праці, перерви для відпочинку та профілактичні заходи, спрямовані на підтримку психоемоційного стану працівників.

З розвитком науково-технічного прогресу та автоматизацією виробництва частка фізичної праці поступово зменшується, а роль розумової праці, навпаки, зростає. Однак, незважаючи на зміни у структурі зайнятості, кожен із цих видів праці має свої ризики, що потребують належного рівня охорони та забезпечення безпеки. Поєднання фізичної та розумової праці в різних сферах діяльності дозволяє досягти балансу між фізичним та інтелектуальним навантаженням, сприяючи загальному розвитку людини та підвищенню ефективності її діяльності.

4.2. Охорона праці.

Охорона праці є системою правових, соціально-економічних, організаційно-технічних, санітарно-гігієнічних та лікувально-профілактичних заходів, спрямованих на забезпечення безпечних умов праці, збереження здоров'я та працездатності працівників. Головною метою охорони праці є запобігання виробничому травматизму, професійним захворюванням, створення безпечних умов для виконання трудових обов'язків.

Законодавство України у сфері охорони праці передбачає обов'язкове дотримання встановлених норм безпеки, що включають проведення атестації робочих місць, організацію інструктажів, медичних оглядів, забезпечення працівників засобами індивідуального захисту. Важливу роль відіграє державний нагляд і контроль за дотриманням вимог охорони праці, який здійснюється органами Державної служби України з питань праці відповідно до сфери та виду

діяльності підприємств. Залежно від специфіки виробничих процесів, контроль включає проведення перевірок, аналіз стану умов праці, оцінку ризиків та відповідність роботодавців законодавчим вимогам. Особлива увага приділяється підприємствам з підвищеною небезпекою, таким як гірничодобувна, хімічна та будівельна галузі, а також сферам, де існує висока ймовірність професійних захворювань або травматизму.

Крім того, робоче середовище може містити низку небезпечних і шкідливих чинників, що впливають на безпеку працівників. До них належать фізичні, хімічні, біологічні, психоемоційні та інші фактори, які можуть викликати травми, захворювання або погіршення загального стану здоров'я. **Фізичні чинники** включають вплив екстремальних температур, шуму, вібрації, випромінювання (іонізуючого, електромагнітного тощо), недостатнього чи надмірного освітлення, що може призводити до професійних захворювань, зниження працездатності та підвищеного ризику нещасних випадків. Наприклад, тривалий вплив високого рівня шуму на виробництві може спричинити зниження слуху, а вібрація – професійні захворювання опорно-рухового апарату.

Хімічні чинники представлені токсичними, агресивними, вибухо-небезпечними та горючими речовинами, які можуть проникати в організм через органи дихання, шкіру або травний тракт. Дія таких речовин може призводити до гострих або хронічних отруєнь, розвитку алергічних реакцій, а в деяких випадках – до ураження внутрішніх органів та онкологічних захворювань. Особливу небезпеку становлять сполуки важких металів, пестициди, канцерогенні речовини, які можуть мати віддалені наслідки для здоров'я.

Біологічні чинники включають віруси, бактерії, гриби, паразити та продукти їхньої життєдіяльності, які можуть бути причиною інфекційних та алергічних захворювань. Працівники медичних закладів, лабораторій, сфери харчової промисловості та сільського господарства найбільш схильні до впливу цих факторів. Наприклад, робота з патогенними мікроорганізмами вимагає суворого дотримання заходів біозахисту, щоб уникнути зараження небезпечними інфекціями.

Психоемоційні фактори включають вплив стресу, перевантаження, ненормований робочий графік, високу відповідальність та несприятливий психологічний клімат у колективі. Надмірний рівень стресу може призводити до порушень психічного здоров'я, підвищеної втомлюваності, депресії та синдрому професійного вигорання, що, своєю чергою, знижує ефективність роботи і підвищує ризик помилок або нещасних випадків.

Важливо розуміти, що **вплив небезпечних і шкідливих чинників значною мірою залежить від сфери та виду діяльності**. Наприклад, у будівництві та промисловості головними загрозами є механічні травми, висока запиленість та контакт із токсичними речовинами, у медичних закладах – біологічна небезпека, а в офісних умовах – недостатня ергономіка робочого місця та психоемоційне навантаження. Саме тому заходи щодо забезпечення безпеки праці мають бути адаптовані до конкретних умов та професійних ризиків.

Для мінімізації впливу небезпечних і шкідливих чинників застосовуються сучасні системи управління охороною праці, що включають ідентифікацію ризиків, розробку та впровадження профілактичних заходів, використання засобів індивідуального та колективного захисту, медичне обстеження працівників та постійний контроль за умовами праці. Таким чином, забезпечення безпеки робочого середовища є комплексним завданням, що потребує взаємодії роботодавців, працівників, органів державного нагляду та професійних спілок.

Зменшення впливу небезпечних факторів досягається завдяки застосуванню технічних засобів захисту, організаційних заходів, контролю робочого середовища, навчання працівників щодо безпечних методів роботи.

Забезпечення ефективної охорони праці передбачає системний підхід, що включає не лише регламентацію виробничих процесів, а й комплексний аналіз умов праці, передбачення потенційних ризиків та запровадження ефективних механізмів їх попередження. Важливим завданням є постійне вдосконалення технологій, методів і стратегій, спрямованих на мінімізацію впливу шкідливих і небезпечних чинників на здоров'я та життя працівників.

Зокрема, одним із пріоритетних напрямів є **інноваційні технології у сфері охорони праці**. Сучасні підприємства дедалі частіше впроваджують автоматизовані системи контролю за робочим середовищем, що дозволяють оперативно відстежувати стан повітря, рівень шуму, концентрацію небезпечних речовин та фізичне навантаження на працівників. Наприклад, використання сенсорних технологій дозволяє в режимі реального часу отримувати дані про стан робочого середовища, а штучний інтелект аналізує ці дані та прогнозує можливі ризики. Також активно розвивається використання дронів та роботизованих систем для моніторингу потенційно небезпечних об'єктів, що мінімізує контакт людини з небезпечними зонами.

Інший важливий аспект – **психологічний комфорт та психоемоційна безпека працівників**. У сучасному світі зростає рівень стресу, зумовленого високою конкуренцією, швидкими темпами роботи, необхідністю постійного підвищення кваліфікації та адаптації до нових технологій. Психоемоційний стан працівників безпосередньо впливає на продуктивність, рівень помилок та ризик виникнення нещасних випадків. Для зменшення впливу цього фактору застосовуються програми психологічної підтримки, корпоративні тренінги з управління стресом, заходи з поліпшення комунікації всередині колективу та створення сприятливих умов праці. Впровадження політики work-life balance також є ефективним засобом зниження психологічного навантаження та збереження працездатності персоналу.

Ще одним важливим напрямом є **законодавче регулювання охорони праці**, яке постійно оновлюється відповідно до міжнародних стандартів та вимог безпеки. Україна, як учасниця міжнародних угод у сфері праці, імплементує норми та практики Європейського Союзу, Міжнародної організації праці (МОП), а також дотримується вимог національного законодавства. Дотримання міжнародних стандартів, таких як ISO 45001, сприяє підвищенню рівня безпеки на виробництві та адаптації національних підприємств до глобальних вимог.

Окремо варто розглянути **охорону праці в екстремальних умовах**, зокрема в зонах підвищеного ризику, на стратегічно важливих об'єктах, у зонах

ведення військових дій та в умовах надзвичайних ситуацій. У таких умовах особливої ваги набуває не лише фізична безпека працівників, а й розробка чітких алгоритмів дій у разі загроз. Для цього використовуються мобільні системи сповіщення, розробляються аварійні плани евакуації, проводяться спеціалізовані тренінги для персоналу. Наприклад, працівники, що працюють у зонах підвищеної небезпеки, проходять додаткову підготовку з надання першої домедичної допомоги, користування засобами індивідуального захисту та алгоритмів дій у разі надзвичайних ситуацій.

Значну роль відіграє також **індивідуальна відповідальність працівників за власну безпеку**, що включає дотримання правил техніки безпеки, використання засобів індивідуального захисту та своєчасне проходження медичних оглядів. Важливо, щоб кожен працівник усвідомлював ризики, пов’язані з його діяльністю, і мав необхідні навички для їх уникнення або мінімізації.

Таким чином, охорона праці – це не просто дотримання формальних норм, а комплексна система заходів, що охоплює правові, соціально-економічні, технічні, санітарно-гігієнічні та організаційні аспекти. Ефективне управління ризиками, впровадження новітніх технологій безпеки, підвищення рівня обізнаності працівників та адаптація до сучасних викликів дозволяють не лише знизити рівень виробничого травматизму, а й підвищити загальну ефективність праці та конкурентоспроможність підприємств.

Забезпечення ефективного управління охороною праці потребує системного підходу, що включає як організаційні, так і технічні заходи для зниження ризиків професійних захворювань та травматизму. Важливу роль у цьому процесі відіграє **розвиток нормативно-правової бази** та адаптація підприємств до міжнародних стандартів безпеки. Зокрема, імплементація стандарту ISO 45001 сприяє створенню системи управління охороною праці, що передбачає оцінку ризиків, моніторинг небезпечних чинників та реалізацію превентивних заходів.

Організаційні заходи в охороні праці включають ретельний аналіз виробничих умов, виявлення потенційних загроз та розробку програм профі-

лактики професійних ризиків. Важливим аспектом є впровадження системи оцінки ризиків (Risk Assessment System), яка дозволяє прогнозувати небезпечні ситуації та розробляти ефективні стратегії зменшення їхнього впливу. На сучасних підприємствах застосовуються **цифрові платформи для моніторингу безпеки**, що включають використання датчиків контролю шкідливих речовин, автоматизованих систем оповіщення та мобільних застосунків для моніторингу небезпечних зон.

Не менш важливою складовою є **застосування сучасних засобів колективного та індивідуального захисту**. Колективні засоби включають інженерні рішення, спрямовані на зменшення впливу шкідливих факторів, наприклад, установки для очищення повітря, шумопоглинаючі матеріали, спеціальні вентиляційні системи та протипожежне обладнання. Засоби індивідуального захисту (ЗІЗ) варіюються залежно від галузі та специфіки діяльності. Це можуть бути респіратори, протигази, захисні костюми, каски, навушники, рукавиці, окуляри тощо.

Охорона праці в умовах нових викликів набуває особливого значення в період глобальних змін, пов’язаних із розвитком технологій, екологічними ризиками та соціально-економічними трансформаціями. Наприклад, в епоху автоматизації та цифровізації значна частина професійних ризиків зміщується у сферу кібербезпеки та роботи з інтелектуальними системами. Для цього розробляються **політики безпеки цифрових середовищ**, що регулюють взаємодію людини з автоматизованими системами, забезпечують захист даних та мінімізують ризики помилок через людський фактор.

Психоемоційні аспекти охорони праці також набувають все більшої актуальності. У зв’язку з інтенсивним ритмом роботи, високим рівнем відповідальності та емоційним вигоранням, працівники потребують спеціалізованих програм підтримки. Корпоративні політики дедалі частіше включають психологічне консультування, гнучкий графік роботи, можливість віддаленої роботи, що сприяє покращенню загального рівня добробуту працівників та підвищенню їхньої продуктивності.

Інноваційні методи навчання та тренінги з безпеки стають невід'ємною частиною ефективного управління ризиками. Традиційні інструктажі доповнюються інтерактивними навчальними модулями, віртуальними тренінгами, моделюванням надзвичайних ситуацій у VR-середовищах, що дозволяє працівникам практично засвоювати навички реагування на потенційні загрози.

Моніторинг і аудит систем охорони праці відіграє ключову роль у забезпеченні дотримання стандартів безпеки. Регулярні перевірки умов праці, тестування рівня шкідливих факторів, контроль відповідності обладнання вимогам безпеки допомагають підтримувати високий рівень захисту працівників та зменшувати ризики виробничого травматизму.

Таким чином, охорона праці є комплексним багаторівневим процесом, що охоплює як правові, технічні, так і соціально-психологічні аспекти. Інтеграція сучасних технологій, підвищення рівня професійної культури безпеки, персоналізований підхід до оцінки ризиків та постійний контроль за робочими умовами є ключовими елементами ефективного управління безпекою праці.

РОЗДІЛ 5. Безпека в умовах надзвичайних ситуацій.

Забезпечення безпеки в умовах надзвичайних ситуацій є ключовим завданням цивільного захисту, яке включає комплекс заходів, спрямованих на мінімізацію людських жертв, збереження критичної інфраструктури, захист довкілля та забезпечення життєдіяльності населення. Надзвичайні ситуації можуть мати природний, техногенний, соціальний або воєнний характер, і кожна з них вимагає спеціальних підходів до реагування, евакуації, медичної допомоги та відновлення нормального функціонування суспільства.

5.1. Вибухопожежна безпека.

Вибухопожежна небезпека – наявність газоподібних, рідких та твердих речовин, матеріалів або їх сумішей, а також окислювачів, які здатні вибухати і горіти за певних умов.

Вибухи та пожежі в більшості випадків відбуваються на об’єктах, які виробляють вибухонебезпечні та хімічні речовини.

При горінні багатьох матеріалів утворюються високотоксичні речовини, від дії яких люди гинуть частіше, ніж від вогню.

При пожежах в повітря виділяється багато токсичних речовин: чадний газ, синильна, соляна й мурашкова кислоти, метанол, формальдегід та інших високотоксичних речовин.

Найбільш вибухо- та пожежонебезпечні суміші з повітрям утворюються при витоку газоподібних та зріджених вуглеводних продуктів метану, пропану, бутану, етилену, пропилену тощо.

Пожежі на підприємствах можуть виникати також внаслідок ушкодження електропроводки та машин, які знаходяться під напругою, опалювальних систем. За офіційною статистикою до основних причин пожеж та вибухів належать: несправність електрообладнання – 23 %; паління в неналежному місці – 18 %; перегрів унаслідок тертя в несправних вузлах машин – 10 %; перегрів пальних

матеріалів – 8 %; контакти з пальними поверхнями через несправність котлів, печей, димоходів – 7 %; контакти з полум'ям, запалення від полум'я газових горілок – 7 %; запалення від пальних часток (іскри) від установок та устаткування для спалювання – 5 %; самозапалювання пальних матеріалів – 4 %, запалювання матеріалів при різці та зварюванні металу – 4 %. Більше 63 % пожеж у промисловості обумовлено помилками людей або їх некомпетентністю.

Коли підприємство скорочує штати й бюджет аварійних служб, знижується ефективність їх функціонування, різко виростає ризик виникнення пожеж та вибухів, а також рівень людських та матеріальних втрат.

Оцінка вибухопожежонебезпеки об'єкта здійснюється за результатами відповідного аналізу пожежонебезпеки будівель, приміщень, інших споруд, характеру технологічних процесів та пожежонебезпечних властивостей речовин, які в них обертаються або знаходяться, з метою виявлення можливих обставин і причин виникнення вибухів і пожеж та їх наслідків. Таким чином, методика аналізу вибухопожежонебезпеки зводиться до виявлення й оцінки потенційних і наявних джерел запалювання, умов формування горючого середовища, умов виникнення контакту джерел запалювання й горючого середовища, умов і причин поширення вогню в разі виникнення пожежі або вибуху, масштабів можливої пожежі, загрози життю та здоров'ю людей, навколишньому середовищу і матеріальним цінностям.

Необхідність матеріальної оцінки вибухопожежонебезпеки потребує чітких критеріїв її визначення. Відомі два підходи до питань нормування у галузі вибухопожежонебезпеки: імовірнісний та детермінований. Імовірнісний підхід, заснований на концепції допустимого ризику, передбачає недопущення впливу на людей і матеріальні цінності небезпечних факторів пожежі з імовірністю, що перевищує нормативну.

Детермінований підхід ґрунтується на розподілі об'єктів за ступенем вибухопожежонебезпеки на категорії з позначенням їх конкретних кількісних меж залежно від параметра, що характеризує можливі наслідки пожежі та вибуху. Класифікація об'єктів за вибухопожежною та пожежною небезпекою

при використанні обох підходів здійснюється з урахуванням допустимого рівня їх пожежної небезпеки, а розрахунки критеріїв і показників її оцінки, у тому числі ймовірності пожежі (вибуху) – з урахуванням маси горючих та важкогорючих речовин і матеріалів, що знаходяться на об'єкті, вибухопожежонебезпечних зон, які утворюються при нормальних режимах ведення технологічних процесів та аварійних ситуаціях, можливих втрат для людей і матеріальних збитків. Основою для встановлення нормативних вимог до конструктивних та планувальних рішень на промислових об'єктах, а також інших питань забезпечення їх вибухопожежобезпеки є визначення категорій приміщень, будинків виробничого, складського й лабораторного призначення і зовнішніх установок за вибухопожежною та пожежною небезпекою.

Категорія виробничого і складського приміщення, будинку та зовнішньої установки за вибухопожежною та пожежною небезпекою є основним показником рівня їх пожежної небезпеки.

Категорійність за вибухопожежною та пожежною небезпекою зумовлює ступінь вогнестійкості будинку, граничні площі протипожежних відсіків, необхідність улаштування систем протипожежного захисту (пожежної сигналізації, пожежогасіння тощо).

Радіаційна небезпека. Питання захисту людини від негативного впливу іонізуючого випромінювання виникли майже одночасно з відкриттям рентгенівського випромінювання і радіоактивного розпаду. Це обумовлено наступними факторами: по-перше, надзвичайно швидкий розвиток застосування знову відкритих випромінювань у науці та на практиці, і, по-друге, виявлення негативного впливу випромінювання на організм.

Заходи радіаційної безпеки використовуються на підприємствах і, як правило, потребують проведення цілого комплексу різноманітних захисних способів, що залежать від конкретних умов роботи з джерелами іонізуючих випромінювань і, в першу чергу, від типу джерела випромінювання. Закритими називаються будь-які джерела іонізуючого випромінювання, обладнання яких виключає проникнення радіоактивних речовин у навколишнє середовище при

передбачених умовах їхньої експлуатації та зносу. Це – гамма-установки різноманітного призначення; нейтронні, бета- і гаммавипромінювачі; рентгенівські апарати і прискорювачі заряджених часток.

При роботі з закритими джерелами іонізуючого випромінювання персонал може піддаватися тільки зовнішньому опроміненню. Захисні заходи, що дозволяють забезпечити умови радіаційної безпеки при застосуванні закритих джерел, засновані на знаннях законів поширення іонізуючих випромінювань і характеру їхньої взаємодії з речовиною. Головні з них такі:

1) доза зовнішнього опромінення пропорційна інтенсивності випромінювання і часу впливу;

2) інтенсивність випромінювання від крапкового джерела пропорційна кількості квантів або часток, що виникають у ньому за одиницю часу, і обернено пропорційна квадрату відстані;

3) інтенсивність випромінювання може бути зменшена за допомогою екранів.

З цих закономірностей випливають основні принципи забезпечення радіаційної безпеки:

1) зменшення потужності джерел до мінімальних розмірів (“захист кількістю”);

2) скорочення часу роботи з джерелом (“захист часом”);

3) збільшення відстані від джерел до працюючих (“захист відстанню”);

4) екранування джерел випромінювання матеріалами, що поглинають іонізуюче випромінювання.

Відкритими називаються такі джерела іонізуючого випромінювання, при використанні яких можливе попадання радіоактивних речовин у навколишнє середовище. При цьому може відбуватися не тільки зовнішнє, але й додаткове внутрішнє опромінення персоналу. Це може відбутися при надходженні радіоактивних ізотопів у навколишнє робоче середовище у вигляді газів, аерозолів, а також твердих і рідких радіоактивних відходів. Джерелами аерозолів можуть

бути не тільки виконувані виробничі операції, але й забруднені радіоактивними речовинами робочі поверхні, спецодяг і взуття.

Основні принципи захисту:

1) використання принципів захисту, що застосовуються при роботі з джерелами випромінювання у закритому вигляді;

2) герметизація виробничого устаткування з метою ізоляції процесів, що можуть стати джерелами надходження радіоактивних речовин у зовнішнє середовище;

3) заходи планувального характеру;

4) застосування санітарно-технічних засобів і устаткування, використання спеціальних захисних матеріалів;

5) використання засобів індивідуального захисту і санітарного опрацювання персоналу;

6) виконання правил особистої гігієни;

7) очищення від радіоактивних забруднень поверхонь будівельних конструкцій, апаратури і засобів індивідуального захисту.

У випадку забруднення радіоактивними речовинами особистий одяг і взуття підлягають дезактивації під контролем служби радіаційної безпеки, а у випадку неможливості дезактивації – захороненню як радіоактивних відходів. Також використовують захист від медичних діагностичних джерел опромінення.

Рентгенорадіологічні процедури належать до найбільш ефективних методів діагностики захворювань людини. Це визначає подальше зростання застосування рентгенних радіологічних процедур або використання їх у більш широких масштабах. Проте інтереси безпеки пацієнтів зобов’язують прагнути до максимально можливого зниження рівнів опромінення, оскільки вплив іонізуючого випромінювання в будь-якій дозі поєднаний з додатковим, відмінним від нуля ризиком виникнення віддалених стохастичних ефектів.

У даний час з метою зниження індивідуальних і колективних доз опромінення населення за рахунок діагностики широко застосовуються організаційні і технічні заходи: 1) як виняток, необґрунтовані (тобто без доведень)

дослідження; 2) зміна структури досліджень на користь тих, що дають менше дозове навантаження; 3) впровадження нової апаратури, оснащеної сучасною електронною технікою посиленого візуального зображення; 4) застосування екранів для захисту ділянок тіла, що підлягають дослідженню. Ці міри, проте, не вичерпують проблеми забезпечення максимальної безпеки пацієнтів і оптимального використання діагностичних методів. Система забезпечення радіаційної безпеки пацієнтів може бути повною й ефективною, якщо вона буде доповнена гігієнічними регламентами допустимих доз опромінення.

5.2. Електробезпека та вплив електричного струму на організм людини.

Електробезпека – це комплекс організаційних, технічних та профілактичних заходів, спрямованих на захист людей від шкідливого та небезпечного впливу електричного струму, електричної дуги, статичної електрики та електромагнітного випромінювання. У сучасних умовах техногенного розвитку електрична енергія стала невід'ємною частиною всіх сфер людської діяльності, що підвищує ризик ураження електричним струмом. Високий рівень напруги, несправність електричних приладів, порушення правил безпечного користування електрообладнанням можуть спричинити серйозні травми, інвалідність або навіть летальний випадок.

З метою зниження цих ризиків розроблено комплекс заходів, що регламентуються нормативно-правовими документами, технічними стандартами та правилами електробезпеки. Оволодіння знаннями з електробезпеки є необхідністю для всіх категорій населення, особливо для осіб, які працюють в електротехнічній сфері або користуються електрообладнанням у промисловості, транспорті та побуті.

Дія електричного струму на організм людини. Вплив електричного струму на людину залежить від багатьох факторів, зокрема сили струму, напруги, частоти електричного сигналу, стану шкіри, шляху проходження

струму через тіло, тривалості контакту та загального стану організму. Основні види ураження електричним струмом включають:

Електричні травми виникають внаслідок прямого або непрямого впливу електричного струму на організм людини. Вони поділяються на кілька основних видів, кожен з яких має свої особливості прояву та наслідки. **Електричні опіки** виникають через проходження струму через тканини організму, що спричиняє нагрівання та руйнування клітин. Залежно від сили струму і тривалості контакту, опіки можуть бути поверхневими, глибокими або навіть уражати внутрішні органи. **Електричні знаки** є специфічними ураженнями шкіри у місцях контакту з провідниками струму, зазвичай не викликають болю, але мають характерний сіруватий або жовтий відтінок. **Електрометалізація шкіри** відбувається, коли під дією електричної дуги частки металу проникають у верхні шари епідермісу, що призводить до змін кольору шкіри та порушення її структури. **Електроофтальмія** виникає при тривалому впливі електричного розряду, зокрема ультрафіолетового випромінювання електричної дуги, що викликає подразнення слизової оболонки очей, почервоніння, біль та світлобоязнь.

Окрім прямих електричних уражень, небезпеку становлять **вторинні травми**, зокрема неконтрольовані судомні скорочення м’язів, що можуть призвести до падінь з висоти, ударів об тверді поверхні, переломів, вивихів та інших механічних пошкоджень. Особливо небезпечні ситуації, коли струм проходить через життєво важливі органи, такі як серце або головний мозок. Це може викликати **фібриляцію серця**, яка призводить до зупинки кровообігу, або параліч дихання, що потребує негайного медичного втручання. Високочастотні струми можуть також спричинити серйозні неврологічні порушення, включаючи втрату свідомості, судоми та параліч.

Ризик отримання електричних травм значно зростає при порушенні правил безпеки, використанні несправного електрообладнання або роботі у вологих умовах без належного захисту. Саме тому профілактика електротравматизму включає комплекс організаційних, технічних та індивідуальних заходів, таких як контроль стану електромереж, використання засобів захисту та регулярне

навчання персоналу. Усвідомлення потенційних небезпек та дотримання правил електробезпеки дозволяє значно зменшити ризик ураження електричним струмом та мінімізувати його наслідки., що спричиняють локальне пошкодження тканин (опіки, електричні знаки, металізація шкіри).

Електричні удари можуть спричинити серйозні порушення функціонування організму, серед яких найбільш небезпечними є зупинка серця, параліч дихання та порушення роботи центральної нервової системи. Дія електричного струму на організм викликає мимовільне скорочення м’язів, що у свою чергу може призвести до сильних судом, порушення координації рухів та втрати свідомості.

Вторинні механічні пошкодження виникають через неконтрольовані судомні скорочення м’язів, які можуть викликати вивихи, переломи кісток, ушкодження сухожиль і навіть розриви внутрішніх органів. Особливо небезпечними є випадки, коли уражена людина втрачає контроль над тілом у момент дотику до джерела струму, що може призвести до падінь з висоти або ударів об тверді поверхні.

Найбільша загроза для життя людини полягає у проходженні електричного струму через життєво важливі органи, зокрема серце та головний мозок. Це може спричинити фібриляцію серцевого м’яза – стан, при якому серце втрачає здатність до ефективного перекачування крові, що призводить до миттєвої втрати свідомості та смертельного наслідку, якщо не буде надано негайну медичну допомогу. Крім того, ураження головного мозку може викликати серйозні неврологічні розлади, такі як порушення свідомості, зупинка дихання та пошкодження нервових центрів, відповідальних за життєво важливі функції організму.

Захист людини від ураження електричним струмом забезпечується низкою заходів, що поділяються на **організаційні, технічні та індивідуальні**.

Організаційні заходи: 1) чітке дотримання нормативно-правових актів та стандартів електробезпеки; 2) проведення регулярних інструктажів та навчання

персоналу; 3) забезпечення контролю за станом електрообладнання; 4) призначення відповідальних осіб за електробезпеку.

Технічні заходи: 1) і**золяція електричних проводів** – застосування діелектричних матеріалів для покриття струмоведучих частин; 2) з**аземлення та занулення** – забезпечення безпечного відведення струму при несправностях; 3) з**ахисне вимкнення** – використання пристроїв автоматичного знеструмлення у разі замикання чи перевантаження; 4) р**озділові трансформатори** – застосування для зниження небезпеки приладів із високою напругою; 5) **система зрівнювання потенціалів** – запобігання утворенню небезпечних різниць потенціалів між металевими елементами конструкцій.

До індивідуальних засобів захисту відносять: 1) діелектричні рукавиці, калоші, килимки; 2) захисні окуляри для роботи з електричними дугами; 3) інструменти з ізольованими ручками.

Безпечна напруга. Для зменшення ризику ураження електричним струмом використовуються електромережі низької напруги.

SELV (Safety Extra-Low Voltage) – це напруга до 48 В змінного струму або до 120 В постійного струму, що застосовується в електричних колах для мінімізації небезпеки ураження. Найбезпечнішим вважається рівень напруги до 12 В.

Гальванічне розділення електричних кіл. Гальванічне розділення – це електричне відокремлення одного кола від іншого з метою запобігання проникненню небезпечного струму. Основний метод – використання розділових трансформаторів, що зменшують ризик ураження струмом.

Захист від випадкового контакту з електричними елементами. Для усунення небезпеки дотику до струмопровідних частин застосовуються такі заходи: – монтаж електрообладнання на висоті, недоступній для людини; – використання спеціальних огороджень, захисних кожухів, бар’єрів; – застосування електроустановок із подвійною або посиленою ізоляцією.

Перша допомога при ураженні електричним струмом. При наданні допомоги потерпілому необхідно:

1. **Знеструмити джерело напруги** – відключити вимикач, автоматичний запобіжник або використати діелектричні предмети для відокремлення потерпілого від джерела струму.
2. **Переконатися у власній безпеці**, перед тим як наближатися до потерпілого.
3. **Оцінити стан постраждалого** – перевірити наявність дихання, пульсу, реакції зіниць.
4. **Надати необхідну допомогу** – у разі зупинки дихання та серцевої діяльності негайно розпочати серцево-легеневу реанімацію.
5. **Викликати медичну допомогу** – навіть якщо потерпілий перебуває у свідомості, необхідно звернутися до лікаря, оскільки можливі приховані ураження внутрішніх органів.

Таким чином, електробезпека – це критично важливий аспект захисту життя та здоров’я людини у сучасному технологічному світі. Впровадження ефективних заходів захисту, навчання працівників, використання сучасних засобів контролю дозволяє мінімізувати ризики ураження електричним струмом та забезпечити безпечну роботу з електрообладнанням.

5.3. Домедична допомога.

Домедична допомога – це комплекс невідкладних заходів, спрямованих на збереження життя та здоров'я потерпілого до прибуття екстрених медичних служб. Вона охоплює дії, які виконуються особами без спеціальної медичної освіти, але які володіють базовими навичками порятунку життя. Домедична допомога є критично важливою, оскільки своєчасне реагування у перші хвилини після отримання травми чи раптового погіршення стану здоров'я значно підвищує шанси на виживання потерпілого та зменшує ризик ускладнень. Відповідно до сфери та виду діяльності, рівень підготовки осіб, які можуть надавати домедичну допомогу, варіюється. Працівники правоохоронних органів, рятувальники, педагоги та навіть водії громадського транспорту зобов'язані мати необхідні знання та навички для оперативного реагування у випадках над-звичайних ситуацій.

Загальні принципи надання домедичної допомоги. Основні принципи домедичної допомоги включають:

Безпека рятувальника та потерпілого. Перед наданням допомоги необхідно оцінити навколишнє середовище та переконатися, що немає загрози для життя рятівника та інших осіб.

Швидкість та ефективність дій. Час є критично важливим фактором, тому слід діяти оперативно, злагоджено та без паніки.

Достатній рівень підготовки. Навіть базові знання з надання першої допомоги можуть врятувати життя.

Принцип «не нашкодь». Якщо рятувальник не впевнений у своїх діях, краще утриматися від маніпуляцій, які можуть завдати шкоди потерпілому.

ЕТАПИ НАДАННЯ ДОМЕДИЧНОЇ ДОПОМОГИ:

Огляд місця події та забезпечення безпеки

- Оцінка навколишнього середовища на предмет потенційної загрози (вогонь, електричні дроти, хімічні речовини, нестабільні конструкції).
- Усунення факторів небезпеки, якщо це можливо, без загрози для власного життя.
- Визначення кількості потерпілих та ступеня їх ураження.

Виклик екстрених служб у разі необхідності (101, 102, 103, 112).

Оцінка стану потерпілого

- Визначення рівня свідомості шляхом голосового та тактильного контакту.
- Перевірка прохідності дихальних шляхів (виявлення сторонніх предметів, вивільнення ротової порожнини).
- Оцінка наявності самостійного дихання та його якості.
- Виявлення критичних кровотеч, видимих травм, деформацій кінцівок.

Зупинка критичних кровотеч

- Використання джгута у разі сильної артеріальної кровотечі (накладається вище місця кровотечі, обов’язково фіксується час накладання).
- Компресійна пов’язка або прямий тиск на рану для зменшення крововтрати.
- Використання гемостатичних засобів у разі складних ран.
- Перевірка серцевої діяльності за допомогою пальпації пульсу на сонній або променевій артерії.

Забезпечення прохідності дихальних шляхів	- Закидання голови назад та підняття нижньої щелепи для запобігання обструкції. - Видалення сторонніх предметів з ротової порожнини (при необхідності). - Використання спеціальних повітроводів (ротоглотковий або носоглотковий) при наявності відповідних навичок та засобів.
Серцево-легенева реанімація (СЛР)	- Проводиться у разі відсутності ознак життя (немає пульсу та дихання). - Виконання компресій грудної клітки (30 натискань на грудну клітку глибиною 5-6 см). - Виконання штучної вентиляції легень (2 вдихи після кожних 30 компресій). - Частота натискань – 100-120 разів на хвилину.
Переведення потерпілого у стабільне положення	- При збереженій свідомості та самостійному диханні потерпілого кладуть на бік. - Положення голови має бути нахиленим назад, щоб запобігти аспірації блювотних мас. - Забезпечення тепла (покриття термопокривалом або ковдрою).
Виклик екстреної медичної допомоги	**Місце події.** Чітко назвати адресу або орієнтири для швидкого прибуття бригади. **Кількість постраждалих.** Вказати вік, стать, особливі обставини (наприклад, дитина, вагітна жінка тощо). **Стан потерпілого.** Чи є свідомість, дихання, кровотеча. **Заходи, які вже виконані.** Наприклад, «проведена серцево-легенева реанімація», «накладено джгут» тощо. **Контактний номер телефону.** Щоб диспетчер міг уточнити інформацію. **Важливо!** Не кладемо слухавку, якщо не впевнені, що диспетчер зрозумів Вас правильно!
Контроль стану потерпілого до прибуття медичних служб	- Регулярна перевірка свідомості, дихання, пульсу. - Запобігання переохолодженню або перегріву. - Заспокоєння потерпілого, надання психологічної підтримки.

5.4. Евакуація населення у надзвичайних ситуаціях.

Загальні засади евакуації населення.

Евакуація населення є одним із найважливіших заходів у системі цивільного захисту, спрямованим на збереження життя та здоров'я громадян в умовах загрози або виникнення надзвичайних ситуацій природного, техногенного, соціального чи воєнного характеру. Евакуація дозволяє запобігти масовим жертвам, мінімізувати вплив небезпечних факторів на населення та забезпечити безпечне переміщення людей до зон, які не піддаються безпосередній загрозі.

Залежно від ситуації, евакуація може бути:

Аварійною – проводиться в екстреному порядку при раптовій загрозі життю та здоров'ю (землетруси, пожежі, аварії на хімічних підприємствах).

Попереджувальною – здійснюється завчасно, коли є ймовірність надзвичайної ситуації (загроза прориву греблі, наступ ворога, небезпека техногенної катастрофи).

Частковою – передбачає переміщення лише окремих категорій громадян (дітей, людей з інвалідністю, вагітних, військових).

Загальною – охоплює всіх мешканців певної території, коли залишатися там небезпечно.

Організованою – здійснюється державними структурами з використанням спеціального транспорту та ретельно розробленими маршрутами.

Самостійною – проводиться з ініціативи громадян, коли офіційні служби не можуть надати допомогу.

Евакуація населення проводиться відповідно до заздалегідь розроблених **планів евакуації**, які включають організаційні заходи, маршрути, пункти збору та методи розміщення людей у безпечних районах.

Медична евакуація для постраждалих.

Міністерство охорони здоров'я України у співпраці з Європейською комісією, ВООЗ та іншими міжнародними партнерами забезпечує евакуацію

важкопоранених громадян до закордонних клінік. Унаслідок тривалої війни та руйнування медичної інфраструктури доступ до спеціалізованої медичної допомоги в Україні є обмеженим, тому міжнародна медична евакуація стала критично важливим заходом.

Медична евакуація постраждалих українців до закордонних клінік регулюється низкою нормативно-правових актів України. Основним документом, що визначає критерії та порядок направлення громадян на лікування за кордон під час воєнного стану, є наказ Міністерства охорони здоров'я України №574 від 5 квітня 2022 року «Про затвердження Критеріїв направлення громадян України для лікування за кордон на період дії воєнного стану та Переліку закладів охорони здоров’я, які здійснюють координацію направлення громадян України для лікування за кордон на період дії воєнного стану». Цей наказ встановлює критерії відбору пацієнтів та визначає заклади охорони здоров'я, відповідальні за координацію процесу евакуації.

Відповідно до наказу, рішення про направлення пацієнта на лікування за кордон ухвалює сімейний або лікуючий лікар стаціонару. Підтвердження відповідності критеріям здійснюється за допомогою первинної облікової документації форми №027/о «Виписка із медичної карти амбулаторного (стаціонарного) хворого», яка заповнюється лікарем закладу охорони здоров'я, що координує направлення пацієнтів за кордон.

Процес медичної евакуації також передбачає співпрацю Міністерства охорони здоров'я України з міжнародними партнерами, зокрема Європейською комісією та Всесвітньою організацією охорони здоров'я. МОЗ подає запит на евакуацію, після чого отримує пропозиції від лікарень країн-членів Європейського Союзу та Європейської економічної зони. Координатори МОЗ взаємодіють з відповідними представниками країн, що приймають пацієнтів, узгоджуючи етапи та маршрути безпечного медичного транспортування. Перевезення пацієнтів з медичних закладів України до медичного евакуаційного хабу в Польщі забезпечують транспортні медичні команди обласних центрів екстреної медичної допомоги та медицини катастроф, медичні вагони

«Укрзалізниці», команда благодійної організації «Лікарі без кордонів», а також бригади парамедиків з європейських країн, залучені ВООЗ.

Процес медичної евакуації складається з декількох етапів:

1. МОЗ подає запит на евакуацію, після чого отримує пропозиції від лікарень країн ЄС та Європейської економічної зони.

2. Координація між державами – МОЗ України узгоджує маршрути транспортування з відповідальними структурами приймаючих країн.

3. Перевезення пацієнтів здійснюється транспортними медичними командами екстреної медичної допомоги, медичними вагонами Укрзалізниці, організацією «Лікарі без кордонів» та європейськими парамедиками, за-контрактованими ВООЗ.

Категорії пацієнтів, які направляються на лікування за кордон: – особи з важкими травмами, що потребують третинної медичної допомоги; – пацієнти з тяжкими опіками, які потребують комбустіологічного лікування; – діти та дорослі з онкологічними захворюваннями; – діти з орфанними (рідкісними) захворюваннями.

Процедура оформлення медичної евакуації. Направлення на лікування за кордон здійснюється на підставі наказу МОЗ №574 від 05.04.2022 р. «Про затвердження Критеріїв направлення громадян України для лікування за кордон на період дії воєнного стану».

Основні положення цього наказу: – критерії направлення на лікування за кордон: визначають категорії пацієнтів, які потребують високоспеціалізованої медичної допомоги, доступ до якої в Україні обмежений через воєнні дії; – перелік закладів охорони здоров'я: встановлює медичні установи, відповідальні за координацію процесу направлення пацієнтів на лікування за кордон.

Процедура медичної евакуації включає такі етапи:

1. **Прийняття рішення про направлення.** Сімейний або лікуючий лікар стаціонару, керуючись наказом МОЗ № 574, ухвалює рішення про необхідність направлення пацієнта на лікування за кордон.

2. **Підготовка документації.** Заповнюється форма первинної облікової документації № 027/о «Виписка із медичної карти амбулаторного (стаціонарного) хворого», яка підтверджує відповідність пацієнта встановленим критеріям

3. **Подання заявки.** Пацієнт або його законний представник може подати заявку через обласний департамент охорони здоров'я або безпосередньо через офіційний сайт МОЗ у розділі «Громадянам».

4. **Координація з іноземними клініками.** МОЗ надсилає запит до закордонних медичних установ, отримує пропозиції щодо прийому пацієнтів та узгоджує деталі транспортування.

5. **Організація транспортування.** Перевезення пацієнтів до медичних евакуаційних хабів, зокрема в Польщі, забезпечується транспортними медичними командами обласних центрів екстреної медичної допомоги, медичними вагонами «Укрзалізниці», благодійною організацією «Лікарі без кордонів» та бригадами парамедиків із європейських країн, залученими Всесвітньою організацією охорони здоров'я

Евакуація поранених з поля бою.

Підготовка до евакуації поранених з поля бою. За евакуацію поранених з місця поранення до медиків насамперед відповідальний командир підрозділу, всі інші – виконують наказ. Провідна роль у виконанні такого наказу належить бойовому медику. Проте, варто розуміти, що бойовий медик – один на взвод, а поранених може бути одночасно декілька, вони можуть перебувати в різних місцях, що іноді доволі віддалені від місцеперебування бойового медика. Тому, саме командир вирішує, як і кому займатися переміщенням кожного конкретного пораненого. Якщо поранений не може вести бій і самостійно відійти в укриття, тоді командир, виходячи з тактичної обстановки та додаткових факторів, визначає відповідального чи відповідальних за переміщення пораненого в укриття. Причому місця укриття, точки збору поранених і точки евакуації (місця під'їзду медиків) мають визначатися заздалегідь. Перед початком висування

необхідно спланувати процес, зважаючи на: – тактичну ситуацію; – вагу пораненого; – додаткові фактори (наприклад, наявність устаткування).

Далі визначається шлях до пораненого та ресурси, потрібні для його переміщення тощо.

Планування та відпрацювання наступних етапів евакуації проводиться до бою. Правильна підготовка поранених до евакуації допоможе забезпечити їх плавну передачу евакуаційному персоналу. Цей процес є складним з наступних причин: – тактичне середовище може бути небезпечним; складні навколишні умови: можуть включати погану видимість (наприклад, можливість евакуації виключно вночі), гучні звуки (наприклад, під гвинтом працюючого гелікоптера або біля хвостової частини евакуаційного літака) тощо. Евакуаційний засіб може злегка рухатися (наприклад, невеликий човен, що гойдається на хвилях).

1. Ретельна підготовка поранених до евакуації, попереднє планування, репетиції та ефективна комунікація сприяють плавній передачі поранених.

2. Враховуючи тактичну ситуацію та особливості поранених, спосіб підготовки до евакуації може відрізнятися. Однак, є деякі основні принципи, спільні для всіх ситуацій, які можуть забезпечити найкращий можливий результат для пораненого.

Підготовка до евакуації в укритті / точці передачі поранених. У більшості ситуацій першим кроком буде підготовка кожного пораненого в укритті до евакуації. Деякі кроки та індивідуальні завдання можуть відкладатися до етапу розміщення поранених у транспорті, проте зазвичай підготовка виконується до під'їзду евакуаційної бригади. Окрім надання допомоги згідно настанов, виконується також закріплення картки пораненого, вільних країв перев'язувальних матеріалів і засобів для попередження гіпотермії, затягування ременів нош перед завантаженням у транспорт тощо.

Розташування поранених для процесу евакуації. Один із наступних кроків після підготовки поранених – їх розташування для процесу евакуації. Це може бути зроблено двічі: один раз на місці надання допомоги (в укритті) та ще

раз у точці евакуації, якщо вона розташована на значній відстані від місця надання допомоги та є затримка в евакуації. Також на цьому етапі слід надати пораненим, особливо тим, які можуть ходити, певні інструкції, щоб зменшити робоче навантаження на евакуаційну бригаду під час завантаження поранених.

Безпека точки евакуації. Під час наближення засобів для евакуації важливо подбати про безпеку евакуаційної зони. Це мають забезпечити бійці, виділені командуванням підрозділу.

Завантаження евакуаційного транспорту. Після прибуття транспортних засобів, поранених необхідно належним чином завантажити під керівництвом евакуаційного персоналу. Бойовий медик команди (підрозділу), яка надавала допомогу в польових умовах, відповідальний за передачу поранених до евакуаційної бригади, що надаватиме допомогу на подальшому етапі.

Алгоритм евакуації поранених.

В залежності від тактичної ситуації або умовної зони перебування пораненого (відповідно до рекомендацій TCCC) алгоритми переміщення та евакуації будуть різні.

Загальний алгоритм переміщення та евакуації пораненого із зони «під вогнем» (зони прямої загрози) наступний:

1. Комунікація з постраждалим і командиром підрозділу (передати інформацію командиру про постраждалого).
2. Планування методів підходу, шляхів підходу та переміщення, розуміння необхідних ресурсів і методів комунікації, отримання дозволу на переміщення.
3. За можливості, попередити постраждалого, що медик / бійці підрозділу рухаються в його бік.
4. Наказати постраждалому відкласти зброю або роззброїти його (якщо постраждалий без свідомості).
5. Перемістити постраждалого в укриття згідно з планом.
6. Зробити запрос на евакуацію, доповідь командирові про ситуацію.
7. Провести сортування постраждалих, надати відповідну допомогу.

8. Підготовка до подальшої евакуації включає технічні моменти (фіксація, закріплення вільних кінців обладнання та перев'язувальних матеріалів), комунікацію, документацію, безпеку тощо.

Техніка пересування та переміщення пораненого з поля бою. Пересування та переміщення постраждалих на полі бою є початковим етапом евакуації поранених з поля бою та залежить від тактичної обстановки, а також додаткових факторів: місцевості, ваги та кількості спорядження тощо. Далі надаємо основні методи, рекомендовані ТССС. Але вибір та використання конкретного методу – на розсуд рятувальника. Дотримання цих методів не є обов'язковим, але є головні моменти, яких варто дотримуватися:

- метод має бути безпечним для рятувальників і пораненого;
- за можливості, не завдавати додаткових травм;
- виконувати максимально швидко.

Методи переміщення постраждалого в укриття:

1. Однією особою: – перетягування на шиї рятувальника (повзком); – за допомогою евакуаційних строп або ременя (повзком); – перетягування, тримаючи за спорядження (лямки бронежилета); – перетягування, тримаючи під пахви (швидше, ніж повзком, але з високим силуетом); – перенесення на спині (швидко й ефективно, але на повний зріст); – переміщення методом підтримування (тільки для ходячих постраждалих; швидко й ефективно, але на повний зріст).

2. Двома особами: – перетягування, тримаючи за спорядження (лямки бронежилета); – переміщення методом підтримування; – перенесення під пахви та за ноги.

Витягування поранених з техніки. Витягування поранених з техніки – елемент бойової підготовки, Цих методів повинні навчати у військових навчальних центрах.

Що потрібно мати медику під час евакуації пораненого з поля бою. Бойовому медику під час евакуації пораненого з поля бою необхідно мати: – індивідуальну зброю; – засоби зв'язку та захисту; – наплічник бойового медика.

РОЗДІЛ 6. Інформаційна безпека та захист критичної інфраструктури.

У сучасному світі інформаційна безпека та захист критичної інфраструктури відіграють ключову роль у забезпеченні національної безпеки. У періоди надзвичайних ситуацій, особливо в умовах війни чи масштабних криз, загрози інформаційній безпеці та кібератаки можуть мати катастрофічні наслідки, включаючи порушення державного управління, збої у роботі критично важливих об'єктів та дезорієнтацію населення.

6.1. Інформаційна безпека у надзвичайних ситуаціях.

Інформаційна безпека у надзвичайних ситуаціях охоплює захист інформаційних систем, персональних даних, критичних баз даних та урядових комунікаційних каналів від зовнішніх і внутрішніх загроз. У період війни, техногенних чи природних катастроф зростає ризик інформаційних атак, спрямованих на дестабілізацію ситуації, поширення паніки та порушення комунікаційних систем.

Основні загрози інформаційній безпеці у надзвичайних ситуаціях пов’язані з широким спектром атак, що спрямовані на дестабілізацію державного управління, порушення комунікацій та підрив довіри до офіційних джерел інформації. Однією з найнебезпечніших загроз є **дезінформація та поширення фейкових новин**, які можуть змінювати громадську думку, впливати на ухвалення рішень органами влади та дезорієнтувати населення в критичний момент. В умовах війни, природних катастроф або техногенних аварій створюються сприятливі умови для поширення викривленої інформації, оскільки люди перебувають у стані стресу, мають обмежений доступ до перевірених джерел та схильні до прийняття емоційних рішень. Використовуючи соціальні мережі, месенджери та інші цифрові платформи, зловмисники створюють масштабні інформаційні кампанії, що вводять громадян в оману, викликають паніку або формують негативний імідж державних інституцій. Основною метою

дезінформації є послаблення довіри до офіційних органів, дестабілізація суспільства та маніпуляція громадською думкою.

Не менш небезпечними є **кібератаки на державні установи**, які здійснюються з метою отримання несанкціонованого доступу до урядових баз даних, маніпулювання інформацією та порушення функціонування критично важливих державних структур. В умовах надзвичайних ситуацій, особливо під час війни, хакерські групи можуть атакувати сервери органів влади, системи комунікації рятувальних служб, медичних установ, військових командних пунктів. Злам таких ресурсів дозволяє зловмисникам отримати доступ до конфіденційних даних, викрасти секретні відомості або заблокувати роботу офіційних сайтів і порталів, що унеможливлює ефективну координацію дій підрозділів цивільного захисту. Крім того, кібератаки можуть включати впровадження шкідливого програмного забезпечення, що змінює чи знищує інформацію, порушує роботу державних і військових структур або поширює дезінформацію серед співробітників установ.

Перехоплення комунікацій є ще однією серйозною загрозою, особливо під час воєнного конфлікту або техногенних катастроф, коли необхідний швидкий і безперешкодний обмін інформацією між військовими, рятувальними службами, медичними установами та іншими державними структурами. Атаки на засоби зв’язку можуть здійснюватися шляхом глушіння сигналів мобільного зв’язку, блокування інтернет-мереж, зламу шифрованих каналів передачі даних. У багатьох випадках противник використовує технології, що дозволяють перехоплювати телефонні дзвінки, електронні повідомлення та навіть змінювати зміст переданої інформації, що може вводити в оману керівників підрозділів, відповідальних за координацію дій у кризових умовах. Крім того, технології глушіння можуть блокувати екстрені виклики, що унеможливлює своєчасну допомогу постраждалим під час надзвичайних ситуацій. В умовах війни такі методи застосовуються для дезорганізації військових і цивільних комунікацій, переривання командного управління та створення хаосу в інформаційному просторі.

Деструктивний інформаційний вплив є ще одним потужним інструментом, що використовується для підриву суспільної стабільності та деморалізації населення або військових підрозділів. Інформаційно-психологічні операції можуть включати поширення фальшивих повідомлень про великі втрати, наближення ворога, нестачу ресурсів чи неможливість ефективного реагування держави на надзвичайну ситуацію. Такі атаки спрямовані на створення атмосфери страху, зневіри у владу та ворожнечі серед населення. Використовуючи соціальні мережі, анонімні повідомлення та ботоферми, зловмисники здатні формувати хибну картину реальності, змушуючи людей приймати неправильні рішення, залишати свої домівки без реальної загрози, саботувати роботу державних установ або навіть сприяти ворогу. Психологічний вплив може бути особливо ефективним, якщо цільова аудиторія перебуває в стані стресу, коли критичне мислення знижується, а довіра до інформації формується на емоційному рівні.

Загалом, загрози інформаційній безпеці в умовах надзвичайних ситуацій становлять комплексний ризик, що включає маніпуляцію інформацією, злам державних систем, перехоплення критично важливих комунікацій та проведення інформаційно-психологічних операцій. Для їхньої ефективної нейтралізації необхідно використовувати комплексний підхід, що включає підвищення стійкості державних інформаційних ресурсів, удосконалення систем захисту даних, впровадження сучасних технологій шифрування, а також активну роботу з населенням у сфері медіаграмотності та критичного мислення.

Методи забезпечення інформаційної безпеки під час надзвичайних ситуацій охоплюють комплекс заходів, спрямованих на захист державних інформаційних систем, протидію дезінформації, збереження критичних даних і забезпечення безперебійної комунікації. В умовах кризових ситуацій особливу роль відіграють технологічні, організаційні та освітні механізми, що дозволяють нейтралізувати загрози та гарантувати стабільність інформаційного простору.

Контроль за інформаційними потоками є одним із ключових елементів забезпечення інформаційної безпеки, оскільки під час надзвичайних ситуацій

інформаційний простір стає об’єктом атак, спрямованих на створення хаосу, паніки та дезорієнтації населення. Моніторинг інформаційних ресурсів дозволяє виявляти фейки, неправдиві новини та маніпулятивний контент, що може призвести до панічних настроїв серед громадян. Наприклад, під час повномасштабного вторгнення в Україну у 2022 році російські пропагандистські канали поширювали неправдиву інформацію про нібито евакуацію керівництва країни та здачу Києва, що мало на меті посіяти хаос серед цивільного населення. Аналогічно, під час пандемії COVID-19 у 2020 році багато дезінформаційних кампаній спрямовувалися на дискредитацію вакцин, що спричинило відмову частини населення від щеплень та збільшення рівня захворюваності. Органи державної влади повинні впроваджувати системи швидкого реагування на поширення дезінформації, блокувати сайти та акаунти, які сприяють ворожій пропаганді, а також співпрацювати з технологічними компаніями для обмеження доступу до ресурсів, що поширюють маніпулятивний контент.

Захист державних баз даних є критично важливим завданням, адже під час надзвичайних ситуацій зростає загроза кібератак, спрямованих на знищення або викрадення конфіденційної інформації. Для запобігання таким атакам необхідно впроваджувати багаторівневі системи безпеки, які включають використання шифрування, технологій блокчейн, біометричної аутентифікації та розподілених обчислень. Наприклад, у 2017 році хакерська атака вірусу NotPetya, організована російськими спецслужбами, паралізувала роботу банків, енергетичних компаній та урядових структур в Україні, що спричинило масштабні збитки. Щоб уникнути подібних ситуацій, державні установи мають використовувати резервне копіювання даних у хмарних сервісах, як це зробив уряд України у 2022 році, перенісши частину своїх серверів у захищені дата-центри ЄС. Особливу увагу слід приділяти безпеці урядових комунікаційних каналів, адже витік інформації або злам системи прийняття рішень може мати катастрофічні наслідки для національної безпеки.

Розвиток системи інформаційного оповіщення є необхідним для оперативного реагування в кризових ситуаціях, оскільки своєчасне та достовірне

інформування населення дозволяє уникнути паніки, координувати дії екстрених служб і запобігати дезінформаційним атакам. Уряди багатьох країн використовують спеціальні системи раннього сповіщення, що базуються на мобільних технологіях, радіомовленні, супутникових системах та автоматизованих каналах зв'язку. Наприклад, в Японії після землетрусу та цунамі у 2011 році влада впровадила J-Alert – систему екстреного оповіщення, яка миттєво повідомляє громадян про загрози через мобільні мережі та телевізійне мовлення. Аналогічно, в Україні під час масованих ракетних атак 2022 року система оповіщення використовувала мобільні додатки «Повітряна тривога» та SMS-повідомлення, що дозволяло мінімізувати людські втрати. Крім того, важливим аспектом є захист систем екстреного зв'язку від кібератак – наприклад, у 2022 році російські хакери намагалися зламати систему сповіщення Києва, однак завдяки сучасним засобам шифрування атака була нейтралізована.

Медіаграмотність населення є не менш важливим інструментом забезпечення інформаційної безпеки, оскільки навіть найдосконаліші технології захисту не зможуть повністю зупинити потік фейків та маніпуляцій, якщо громадяни не володіють навичками критичного мислення. Наприклад, під час війни в Україні поширювалися фейки про «здачу» окремих міст, що спричиняло паніку серед місцевого населення. Проте своєчасна робота фактчекінгових платформ, таких як StopFake, та офіційних джерел інформації дозволяла швидко спростовувати маніпулятивні новини. Важливим є також навчання державних службовців та військових основам інформаційної безпеки, оскільки під час війни їхні дані можуть бути використані противником для проведення психологічних операцій. Наприклад, у 2022 році зафіксовано випадки, коли російські спецслужби розсилали SMS-повідомлення українським військовим із закликами до здачі, використовуючи зламані бази даних.

Таким чином, забезпечення інформаційної безпеки під час надзвичайних ситуацій є комплексним процесом, що включає контроль за поширенням інформації, посилений захист баз даних, розвиток системи екстреного оповіщення та підвищення рівня медіаграмотності населення. Впровадження цих заходів

дозволяє зменшити ризики, пов’язані з дезінформаційними атаками, кіберзагрозами та спробами маніпуляції суспільною свідомістю в умовах криз. Для ефективного функціонування державних структур та безпеки громадян критично важливо розробляти стратегії інформаційного захисту, вдосконалювати нормативно-правову базу та застосовувати передові технологічні рішення для протидії сучасним викликам у сфері інформаційної безпеки.

6.2. Кіберзагрози під час війни та кризових ситуацій.

Класифікація кіберзагроз у воєнний час охоплює широкий спектр атак, що спрямовані на підрив державної інфраструктури, дестабілізацію фінансової системи, порушення комунікацій та маніпулювання інформаційним простором. У сучасних конфліктах кібератаки стали невід’ємним елементом гібридної війни, а їхнє застосування може завдавати не меншої шкоди, ніж традиційні методи ведення бойових дій. Успішна кібератака може спричинити паралізацію урядових установ, фінансових систем та підприємств критичної інфраструктури, що значно послаблює обороноздатність держави та здатність громадян до організованого опору.

DDoS-атаки (атаки на відмову в обслуговуванні) є одним із найпоширеніших типів кібератак під час воєнних конфліктів, оскільки вони спрямовані на тимчасове або повне блокування доступу до важливих ресурсів. Ці атаки реалізуються через масове перевантаження серверів великою кількістю запитів, що унеможливлює нормальну роботу вебсайтів державних установ, фінансових сервісів та засобів комунікації. Наприклад, під час повномасштабного вторгнення росії в Україну у 2022 році українські урядові сайти та банки зазнали масштабних DDoS-атак, що тимчасово вивели з ладу портали «Дія», «ПриватБанк» і «Ощадбанк». Подібні атаки використовувалися також у 2007 році під час нападу на Естонію, коли хакери, пов’язані з російськими спецслужбами, паралізували роботу урядових установ та банківських систем країни.

Фішинг і соціальна інженерія є одними з найбільш ефективних методів отримання доступу до конфіденційної інформації, оскільки вони спрямовані на людський фактор. Нападники створюють підроблені сайти, надсилають електронні листи або телефонують від імені офіційних організацій, намагаючись змусити жертву передати логіни, паролі або інші чутливі дані. Наприклад, у 2022 році було зафіксовано масові фішингові атаки на військових та чиновників України, коли через електронні листи, що імітували офіційні звернення від Міністерства оборони, хакери отримували доступ до секретної інформації. Ще одним яскравим прикладом є фішингова кампанія, здійснена хакерською групою APT28, пов'язаною з російською розвідкою, яка атакувала урядові структури США та Європи, використовуючи підроблені документи та посилання.

Зловмисне програмне забезпечення (віруси, трояни, шкідливі програми) використовується для викрадення даних, шифрування систем або знищення баз даних. Одним із наймасштабніших прикладів використання шкідливого ПЗ є атака NotPetya у 2017 році, яка була спрямована на українські державні органи, енергетичні компанії, фінансові установи та транспортну інфраструктуру. Це шкідливе програмне забезпечення не лише шифрувало файли на заражених пристроях, а й робило їх відновлення неможливим, що призвело до збитків у сотні мільйонів доларів. Подібні атаки можуть мати руйнівний вплив на воєнну логістику, оскільки знищення даних про переміщення військ, склади з боєприпасами або мобілізаційні ресурси значно ускладнює ведення бойових дій.

Атаки на комунікаційні системи є критично важливими, оскільки вони спрямовані на підрив здатності військових, урядових установ та рятувальних служб ефективно координувати свої дії. Під час війни злам серверів телекомунікаційних компаній, блокування мобільного зв'язку та перехоплення радіосигналів можуть мати катастрофічні наслідки. Наприклад, у 2022 році Росія здійснила масовані атаки на українську систему супутникового зв'язку, намагаючись порушити роботу військових і урядових комунікацій. Аналогічно, у 2014 році під час анексії Криму російські спецслужби блокували зв'язок українських військових, що ускладнило організацію оборони.

Атаки на енергетичні системи можуть призвести до масштабних відключень електроенергії, що паралізує не лише військову інфраструктуру, а й лікарні, транспортні системи та цивільний сектор. У 2015 році Україна зазнала першої в історії підтвердженої кібератаки на енергетичну інфраструктуру, коли російські хакери зламали систему управління обленерго, що призвело до відключення електроенергії для 230 000 споживачів. Цей прецедент продемонстрував, наскільки вразливими можуть бути енергетичні системи, якщо вони не захищені належним чином.

Кібератаки стали одним із основних інструментів сучасної війни, а їхні наслідки можуть бути не менш руйнівними, ніж застосування традиційних озброєнь. Враховуючи ці ризики, держави повинні розробляти стратегії кібероборони, інвестувати в кібербезпеку критичної інфраструктури, проводити навчання персоналу та створювати резервні системи управління. Україна вже має значний досвід протидії кіберзагрозам, зокрема завдяки співпраці з міжнародними партнерами та впровадженню заходів кіберстійкості. Для ефективної протидії сучасним викликам необхідно розширювати технологічні можливості, впроваджувати автоматизовані системи моніторингу загроз та посилювати захист ключових державних і військових об’єктів.

Стратегії протидії кіберзагрозам під час війни передбачають комплекс заходів, спрямованих на зміцнення кіберзахисту держави, критичної інфраструктури та військових об’єктів. Кіберпростір став ключовим полем бойових дій у сучасних конфліктах, а успішні атаки можуть паралізувати системи управління державою, зв’язок, енергетичну інфраструктуру та навіть бойові операції. З огляду на це країни, що знаходяться у стані війни або гібридної агресії, повинні реалізовувати ефективні кіберстратегії, що поєднують технологічний захист, активний моніторинг загроз, збереження інформаційних ресурсів та підготовку фахівців до роботи в умовах інформаційного протистояння.

Захист державних і військових інформаційних систем є одним із найважливіших пріоритетів у боротьбі з кіберзагрозами під час війни. Для запобігання несанкціонованому доступу до урядових баз даних, серверів

військових штабів та критичних комунікаційних каналів застосовуються сучасні методи кіберзахисту, серед яких багаторівнева автентифікація доступу, сегментування мережі, використання віртуальних приватних мереж (VPN) та блокчейн-технологій. Наприклад, в Україні після серії атак у 2022 році було запроваджено посилені заходи захисту урядових серверів, включаючи їхнє перенесення на хмарні платформи за межами країни, що дозволило зберегти критично важливу інформацію навіть у разі фізичного знищення дата-центрів. Також важливим елементом захисту є впровадження політики нульової довіри (Zero Trust), яка передбачає перевірку кожного користувача та пристрою перед наданням доступу до державних систем.

Моніторинг кіберпростору є критично важливим для виявлення атак у реальному часі та запобігання масштабним кібератакам до того, як вони завдадуть значних збитків. Для цього використовуються аналітичні платформи, що аналізують поведінку мережевого трафіку, виявляють підозрілі дії та автоматично блокують потенційні загрози. Наприклад, під час російського вторгнення у 2022 році Україна активно співпрацювала з міжнародними компаніями з кібербезпеки, такими як Microsoft, Google та Amazon, які надали свої технології для моніторингу та протидії атакам. Одним із найефективніших інструментів є система SIEM (Security Information and Event Management), що дозволяє виявляти аномалії у поведінці користувачів і пристроїв у режимі реального часу. Також важливу роль відіграють розвідувальні платформи, що дозволяють відстежувати діяльність хакерських угруповань, зокрема таких, як Sandworm, Fancy Bear або APT29, які регулярно атакують українську та європейську кіберінфраструктуру.

Резервування та шифрування даних є обов'язковою практикою для захисту критичної інформації у воєнний час. Якщо зловмисникам вдається знищити або викрасти бази даних, це може мати катастрофічні наслідки для національної безпеки. Для уникнення таких ризиків використовується багаторівнева система резервного копіювання, що включає створення офлайн-резервів, зберігання даних у захищених дата-центрах та застосування хмарних рішень. Наприклад, у 2022 році уряд України переніс частину своїх серверів до дата-

центрів Європейського Союзу, що дозволило зберегти цифрові архіви, навіть коли фізичні сервери в Україні зазнавали атак. Одним із ключових методів шифрування даних є використання алгоритмів AES-256 та RSA, що забезпечують високий рівень криптографічного захисту. Важливо також запроваджувати системи автоматичного оновлення програмного забезпечення, адже застарілі версії можуть містити вразливості, які легко використовуються хакерами.

Кіберосвіта та підготовка фахівців є фундаментальним елементом стратегії кіберзахисту, адже навіть найсучасніші технології можуть бути марними, якщо користувачі не володіють базовими навичками безпеки. Відомо, що понад 80% усіх успішних атак здійснюється через людський фактор – наприклад, через використання слабких паролів, перехід за фішинговими посиланнями або нехтування правилами цифрової безпеки. Для вирішення цієї проблеми країни, що перебувають у стані воєнного конфлікту, активно розвивають систему навчання у сфері кібербезпеки. В Україні у 2022 році було створено урядову ініціативу «Кіберстійкість України», яка передбачає навчання державних службовців основам цифрової гігієни, проведення тренінгів із кіберзахисту та розвиток співпраці з міжнародними експертами. Крім того, важливу роль відіграють волонтерські ініціативи, такі як ІТ-армія України, що об’єднує тисячі добровольців, які беруть участь у відбитті ворожих атак та проведенні контрнаступальних кібероперацій.

Таким чином, протидія кіберзагрозам під час війни вимагає комплексного підходу, що включає технологічні, організаційні та освітні заходи. Використання захищених серверів, постійний моніторинг кіберпростору, резервне копіювання даних і розвиток кіберосвіти дозволяють зменшити ризики атак та мінімізувати їхні наслідки. Досвід останніх років показує, що країни, які інвестують у кібербезпеку та розвивають кіберстійкість, мають значно вищі шанси протистояти сучасним викликам у сфері інформаційної безпеки та забезпечити захист своїх громадян і критичної інфраструктури.

6.3. Методи захисту інформації та комунікацій у періоди надзвичайних ситуацій.

Основні **принципи захисту інформації** визначають фундаментальні підходи до забезпечення кібербезпеки та мінімізації ризиків втрати або компрометації даних. В умовах воєнного конфлікту, інформаційної війни та загроз, пов'язаних із кібератаками, ці принципи стають критично важливими для державних установ, військових структур, критичної інфраструктури, бізнесу та громадянського суспільства. Використання ефективних методів захисту дозволяє не лише запобігти несанкціонованому доступу до даних, але й забезпечити стабільність функціонування ключових цифрових систем навіть у кризових ситуаціях.

Конфіденційність є одним із ключових аспектів інформаційної безпеки, що передбачає захист персональних, службових і державних даних від несанкціонованого доступу. Це особливо актуально під час воєнних дій, коли противник може використовувати викрадену інформацію для проведення розвідувальних або дезінформаційних операцій. Наприклад, у 2022 році українські спецслужби викрили масштабну спробу російських хакерів отримати доступ до електронних листів військових та урядових чиновників через компрометацію поштових серверів. Для запобігання подібним загрозам впроваджуються багаторівневі системи аутентифікації, шифрування переданих даних і контроль за доступом до інформаційних ресурсів. Один із найефективніших методів захисту конфіденційності – використання end-to-end шифрування, що забезпечує безпечний обмін даними між відправником і отримувачем, виключаючи можливість перехоплення зловмисниками.

Цілісність інформації означає її незмінність та достовірність, що є особливо важливим у військових та кризових умовах. Зміна або фальсифікація даних може призвести до серйозних наслідків, таких як хибні накази в армії, маніпуляція фінансовими операціями, поширення дезінформації. Наприклад, у 2017 році вірус NotPetya, який атакував Україну, призвів до масового знищення

інформації в банківських, державних та комерційних системах, що викликало хаос і значні економічні втрати. Для захисту цілісності інформації використовуються такі технології, як блокчейн, цифрові підписи та контрольні хеш-суми, що дозволяють перевіряти справжність даних та запобігати їхній зміні несанкціонованими особами.

Доступність інформації є ще одним важливим принципом кібербезпеки, який передбачає безперебійну роботу інформаційних систем навіть під час надзвичайних ситуацій, кібератак або технічних збоїв. Противник може використовувати тактику масованих DDoS-атак для блокування роботи сайтів урядових органів, банків та комунікаційних платформ, що ускладнює управління державою та координацію між силовими структурами. Наприклад, на початку повномасштабного вторгнення в Україну у 2022 році було здійснено серію атак на сайти Кабінету Міністрів, Міністерства оборони та фінансових установ, що призвело до тимчасового збою їхньої роботи. Для забезпечення доступності інформації застосовуються методи розподіленого зберігання даних, дублювання серверів, впровадження захищених хмарних рішень та альтернативних каналів зв’язку, таких як супутниковий інтернет Starlink, який відіграв ключову роль у забезпеченні безперервної комунікації в Україні.

Технічні методи захисту інформації базуються на використанні передових технологій для забезпечення конфіденційності, цілісності та доступності даних. Одним із найважливіших методів є шифрування даних, що передбачає їхнє перетворення у вигляд, який неможливо прочитати без спеціального ключа. Найбільш поширеними алгоритмами є AES-256, який використовується для захисту військових та державних комунікацій, і RSA, що забезпечує надійне шифрування електронних підписів та файлів. Наприклад, месенджер Signal, який широко використовується військовими та журналістами, застосовує метод подвійного шифрування для забезпечення безпеки комунікацій.

Мережеві брандмауери (firewalls) відіграють ключову роль у блокуванні несанкціонованого доступу до систем, фільтруючи трафік та запобігаючи спробам проникнення зловмисників. Під час активної фази військових конфліктів

хакерські групи можуть здійснювати атаки на урядові та корпоративні сервери для отримання розвідувальних даних або порушення роботи систем управління. У 2022 році Україна значно посилила кіберзахист, впровадивши комплексні міжмережеві екрани, що блокували спроби проникнення до державних систем з IP-адрес, пов'язаних із ворожими хакерськими угрупованнями.

Захист електронної пошти та месенджерів є критично важливим для запобігання витоку конфіденційної інформації. Одним із головних методів атак є фішинг, коли зловмисники надсилають підроблені електронні листи, що імітують офіційну комунікацію, із метою викрадення облікових даних. Наприклад, у 2022 році було зафіксовано спроби зламу електронної пошти українських військових, коли хакери масово розсилали підроблені повідомлення про необхідність зміни паролів. Щоб запобігти таким атакам, державні та військові установи застосовують двофакторну аутентифікацію (2FA), що передбачає додаткове підтвердження особи через мобільний телефон або апаратний ключ.

VPN та TOR-мережі забезпечують анонімність і захист даних в умовах інформаційних загроз, дозволяючи уникати стеження, блокування сайтів і спроб перехоплення трафіку. У багатьох випадках під час військових конфліктів уряди-агресори намагаються обмежити доступ до інформації та контролювати комунікацію громадян. Наприклад, у Росії після початку війни в Україні було заблоковано доступ до незалежних новинних ресурсів, що змусило журналістів і громадян використовувати VPN для обходу цензури. У військових умовах VPN також застосовується для захищеного підключення до державних серверів та передачі конфіденційних даних.

Таким чином, основні принципи захисту інформації та технічні методи кібербезпеки є життєво необхідними в умовах сучасної війни та інформаційного протистояння. Використання шифрування, захист мережевої інфраструктури, контроль за доступом до даних, впровадження резервних копій та навчання персоналу цифровій безпеці дозволяє мінімізувати ризики атак і гарантувати стабільність функціонування інформаційних систем у критичних ситуаціях. Україна вже має значний досвід протидії кібератакам, і подальший розвиток

кібербезпеки стане ключовим фактором у забезпеченні її стійкості перед сучасними загрозами.

У сучасних умовах воєнних конфліктів, техногенних катастроф та інших кризових ситуацій **забезпечення безпеки** комунікацій є ключовим фактором ефективного управління державою, координації дій військових і рятувальних служб, а також підтримки стабільності суспільства. Противник часто використовує кібератаки, блокування зв'язку та інформаційно-психологічні операції для дестабілізації ситуації та обмеження доступу до достовірної інформації. Для ефективного захисту комунікацій необхідно впроваджувати комплексні стратегії, що включають резервні канали зв'язку, захист мобільних пристроїв, моніторинг інформаційного простору та організацію безпечного обміну даними між державними установами.

Створення резервних каналів зв'язку є критично важливим для забезпечення безперебійної комунікації під час кризи. В умовах війни або масштабних катастроф традиційні мережі зв'язку можуть бути виведені з ладу через ракетні удари, кібератаки або фізичне пошкодження інфраструктури. Наприклад, під час повномасштабного вторгнення в Україну у 2022 році Росія здійснювала систематичні атаки на вежі мобільного зв'язку та інтернет-мережі, намагаючись дестабілізувати ситуацію. Важливим рішенням стало впровадження системи супутникового інтернету Starlink, який забезпечив безперебійний зв'язок для військових, уряду та критичних об'єктів. Використання альтернативних операторів зв'язку та технологій, таких як радіозв'язок, супутникові телефони (Iridium, Inmarsat), дозволяє створювати незалежні комунікаційні мережі, що функціонують навіть у випадку знищення наземної інфраструктури.

Інформаційна безпека мобільних пристроїв є ще одним важливим аспектом, оскільки мобільні телефони та планшети можуть бути використані противником для шпигунства, збору персональних даних або прослуховування. Хакери використовують шкідливе програмне забезпечення, що може отримувати доступ до мікрофона, камери або GPS-модуля пристрою. Наприклад, відомий вірус Pegasus, який використовувався спецслужбами для стеження за

високопосадовцями, дозволяв непомітно зламувати смартфони та отримувати доступ до всіх їхніх даних. Для запобігання таким загрозам необхідно застосовувати спеціальні додатки для безпечного обміну інформацією, такі як Signal, Threema, Wire, що забезпечують наскрізне шифрування повідомлень та дзвінків. Крім того, важливими заходами є використання одноразових SIM-карток, відключення геолокації на пристроях військових і державних службовців, а також встановлення антивірусних програм і регулярне оновлення операційних систем.

Моніторинг та аналіз інформаційного простору дозволяють своєчасно виявляти потенційні загрози, такі як кібератаки, дезінформаційні кампанії та спроби перехоплення комунікацій. Противник може використовувати фейкові акаунти у соціальних мережах, ботоферми та маніпулятивний контент для дестабілізації ситуації. Наприклад, у 2022 році Росія активно поширювала через Telegram-канали та соціальні мережі неправдиву інформацію про «здачу українських міст» та «масовий відхід військ», що мало на меті посіяти паніку серед цивільного населення. Для боротьби з такими загрозами необхідно застосовувати системи аналізу інформаційних потоків, такі як OSINT (Open Source Intelligence), що дозволяють виявляти джерела дезінформації та нейтралізовувати їх через блокування або інформаційні спростування. Також активно використовуються платформи на основі штучного інтелекту, що аналізують велику кількість даних і прогнозують можливі інформаційні атаки.

Організація системи безпечного обміну інформацією між державними установами є необхідною умовою для збереження конфіденційності даних та забезпечення координації в кризових ситуаціях. Урядові структури та військове командування повинні використовувати захищені внутрішні платформи для передачі інформації, уникаючи відкритих каналів зв’язку, які можуть бути перехоплені противником. Наприклад, в Україні після серії атак на урядові сервери було впроваджено захищену систему комунікації СЕВ ОВВ (Система електронної взаємодії органів виконавчої влади), яка дозволяє безпечно передавати документи та оперативну інформацію. Використання закритих

мереж, шифрування даних за допомогою алгоритмів AES-256 та впровадження апаратних ключів доступу (HSM-модулі, USB-токени) дозволяє значно підвищити рівень безпеки державних комунікацій.

Таким чином, ефективний захист комунікацій у період кризових ситуацій вимагає комплексного підходу, що включає створення альтернативних каналів зв'язку, посилення інформаційної безпеки мобільних пристроїв, моніторинг загроз в інформаційному просторі та впровадження надійних методів обміну інформацією між державними установами. Враховуючи сучасні виклики та досвід ведення гібридної війни, країни повинні активно розвивати технологічні рішення для захисту комунікацій, що дозволить забезпечити безперервне управління в умовах надзвичайних ситуацій та мінімізувати загрози інформаційної безпеки.

РОЗДІЛ 7. Соціальна адаптація населення до кризових ситуацій.

Соціальна адаптація населення до кризових ситуацій є одним із ключових елементів стратегії цивільного захисту, оскільки здатність людей ефективно реагувати на надзвичайні обставини значною мірою визначає рівень стійкості суспільства. Війни, техногенні катастрофи, природні лиха та інші кризи створюють високий рівень стресу, вимагають швидкого ухвалення рішень та перебудови звичного способу життя. Успішна адаптація включає як **індивідуальну психологічну підготовку**, так і **колективну самоорганізацію громад**, що дозволяє мінімізувати негативні наслідки надзвичайних ситуацій та підвищити шанси на виживання.

7.1. Психологічна підготовка та стресостійкість у кризових умовах.

Психологічна стійкість у кризових умовах є важливою навичкою, що дозволяє людині зберігати раціональне мислення, контролювати емоції та діяти ефективно в екстремальних ситуаціях. Під час війни, терористичних атак чи природних катастроф багато людей переживають **гостру стресову реакцію**, яка може проявлятися у вигляді **паніки, паралізуючого страху, агресії або апатії**. Такий стан є природним механізмом реагування організму на небезпеку, проте якщо людина не має навичок подолання стресу, це може призвести до **емоційного виснаження, депресії або навіть психосоматичних розладів**. Наприклад, під час військових дій люди, які не були готові до кризової ситуації, часто відчували безпорадність та дезорієнтацію, що ускладнювало їхнє виживання.

Вчасна психологічна підготовка дозволяє мінімізувати ці негативні ефекти та забезпечити більш швидке повернення до нормального функціонування після пережитого стресу. **Дослідження показують**, що люди, які заздалегідь готували себе до можливих надзвичайних ситуацій, демонструють вищий рівень адаптації та ухвалюють більш ефективні рішення під час кризи. Наприклад, **під час**

терактів у США 11 вересня 2001 року було зафіксовано, що люди, які мали досвід проходження тренінгів з виживання та кризового реагування, залишали будівлі швидше, ніж ті, хто не мав такої підготовки.

Основними методами підготовки до кризових ситуацій є **тренування адаптаційних механізмів**. Наприклад, військові та рятувальники використовують методи **імітації критичних ситуацій** для формування навичок швидкого реагування. Одним із ключових підходів є **Box Breathing** (техніка контрольованого дихання), яка використовується у спецпідрозділах та рятувальних службах для швидкого зниження рівня тривожності. **Методика полягає у глибокому вдиху на 4 секунди, затримці дихання на 4 секунди, видиху на 4 секунди та знову затримці на 4 секунди.** Такий підхід дозволяє швидко стабілізувати серцебиття, покращити концентрацію та запобігти панічним реакціям.

Іншим ефективним методом є **психологічна десенсибілізація** – поступове звикання до стресових умов шляхом імітації кризових ситуацій. Наприклад, у країнах НАТО військовослужбовців перед відправленням у зону бойових дій тренують у спеціальних симуляційних центрах, де вони стикаються зі штучно створеними умовами реального бою (гучні звуки вибухів, задимлення, нестача світла), що допомагає адаптувати організм до екстремальних умов. В Україні **подібний підхід застосовується у центрах підготовки військових медиків та рятувальників**, де створюються максимально реалістичні умови для відпрацювання алгоритмів дій у критичних ситуаціях.

Крім того, важливим аспектом є **групова психологічна підтримка**. Відомо, що люди краще переносять кризові обставини, коли вони відчувають підтримку громади, рідних або колективу. **Під час бойових дій військові, які перебувають у згуртованих підрозділах, значно рідше стикаються з гострими психологічними розладами, ніж ті, хто перебуває у психологічній ізоляції**. Саме тому в арміях світу застосовується принцип **«бойового братерства»**, що сприяє формуванню почуття відповідальності та підтримки серед бійців.

Важливу роль відіграють **психологи кризового реагування**, які допомагають людям пережити шок після травматичних подій. Наприклад, після

звільнення територій, що перебували під окупацією, психологи мобільних бригад надавали допомогу місцевим жителям, які пережили тортури, голод і втрату рідних. Такі програми реабілітації діють у багатьох країнах світу. Наприклад, у США після урагану «Катріна» була запущена державна ініціатива з психологічної підтримки постраждалих, яка включала роботу кризових психологів, групові тренінги та програми реабілітації для дітей, які втратили родини.

В Україні у 2022 році було створено масштабні програми психологічної реабілітації для **військових, біженців та цивільного населення**, що дозволяють знизити рівень посттравматичного стресового розладу (ПТСР). Наприклад, ініціатива «Безбар'єрність» разом із Міністерством охорони здоров'я запустила серію тренінгів із психологічної стійкості для переселенців, а міжнародні організації, такі як ЮНІСЕФ, реалізують програми підтримки дітей, які втратили батьків через війну.

Таким чином, психологічна підготовка є не лише **індивідуальною навичкою**, а й **частиною комплексної стратегії держави**, спрямованої на збереження функціональності суспільства в умовах кризи. Стресостійкість можна розвивати за допомогою тренувань, психологічної освіти та підтримки громади. Для підвищення рівня готовності населення до надзвичайних ситуацій необхідно впроваджувати **масові тренінгові програми**, інтегрувати курси психологічної стійкості у систему освіти та активно розвивати кризові психологічні служби. Досвід показує, що суспільства, які мають високий рівень адаптивності до стресових умов, значно швидше відновлюються після катастроф та війн і демонструють більш ефективний опір загрозам.

7.2. Самоорганізація громад у періоди воєнного стану та інших НС.

В умовах надзвичайних ситуацій, коли держава або муніципальні служби не можуть швидко надати допомогу всім постраждалим, саме **громадська самоорганізація** стає ключовим фактором виживання. Організовані громади здатні **самостійно розподіляти ресурси, координувати дії, підтримувати порядок та забезпечувати безпеку** у кризові періоди. Колективна взаємодія дозволяє створювати ефективні механізми реагування на загрози, мінімізувати панічні настрої та допомагати вразливим категоріям населення, зокрема дітям, літнім людям та особам з інвалідністю.

Прикладом ефективної самоорганізації є **волонтерські рухи в Україні**, які під час війни 2022 року взяли на себе значну частину функцій державних структур: організацію евакуації, забезпечення продовольством, медичну допомогу, ремонт зруйнованої інфраструктури, гуманітарну підтримку цивільного населення та армії. В умовах війни такі ініціативи, як «Повернись живим», «Фонд Сергія Притули», «Help Ukraine Center», «Благодійний фонд Віктора та Олени Пінчук», «СпівДія», стали прикладом високої ефективності самоорганізації суспільства, де волонтери оперативно реагували на потреби військових та цивільних, компенсуючи нестачу ресурсів та координації з боку держави.

Одним із найяскравіших прикладів стало **самоорганізоване партизанське та волонтерське підпілля** на окупованих територіях, де громадяни допомагали з евакуацією, постачанням ліків та продуктів, надавали інформацію українським спецслужбам про пересування ворожих військ. Зокрема, у Херсоні під час окупації діяв Рух Опору «Жовта стрічка», який координував акції протесту, розповсюдження інформації та підтримку місцевого населення.

Основними етапами формування самостійних громадських структур є:

Створення структури управління в громаді є першочерговим завданням для ефективної самоорганізації. Визначення відповідальних осіб дозволяє чітко розподілити функції між учасниками: – координація допомоги та логістики – забезпечення доставки гуманітарних вантажів, транспортування постраждалих;

медична допомога – формування груп лікарів та парамедиків, організація аптечних пунктів, навчання навичкам домедичної допомоги; – безпека та охорона – організація патрулювань, створення територіальних загонів самооборони; – комунікація та інформаційна підтримка – встановлення каналів зв'язку для оперативного реагування, боротьба з дезінформацією.

Відтак, під час блекаутів у Києві внаслідок ракетних ударів по енергетичній інфраструктурі у 2022 році волонтери спільно з владою розгорнули «Пункти незламності», де можна було отримати електрику, зв'язок, тепло та медичну допомогу.

Розробка комунікаційної мережі. Під час кризових ситуацій традиційні засоби зв'язку можуть бути недоступними через збої в мобільних мережах, кібератаки або руйнування інфраструктури. Важливо заздалегідь налагодити альтернативні канали комунікації: – використання месенджерів з наскрізним шифруванням для захисту інформації; – радіозв'язок – радіостанції УКХ (VHF) та КХ (HF), СВ-радіозв'язок для дальніх комунікацій; – створення локальних мереж Wi-Fi, які працюють без інтернет-підключення (наприклад, на базі Mesh Network); – використання супутникового інтернету Starlink, що забезпечив зв'язок для військових та гуманітарних організацій в Україні після російського вторгнення.

Забезпечення логістики та ресурсів. Найбільші ризики в умовах блокади або гуманітарної кризи – нестача їжі, води, медикаментів, пального. Важливо заздалегідь створити резервні запаси та розробити систему розподілу ресурсів. Наприклад, під час облоги Маріуполя в 2022 році містяни змушені були добувати воду з технічних колодязів і талого снігу через знищення системи водопостачання. У таких випадках працюють альтернативні джерела енергії та автономні системи водозабезпечення, а також групи волонтерів, які займаються збором та розподілом допомоги.

Громадська безпека. Під час воєнних дій, стихійних лих або соціальних заворушень збільшується ризик мародерства, диверсій, злочинності. Для забезпечення правопорядку формуються територіальні громади самооборони,

що виконують такі функції: – патрулювання вулиць для запобігання злочинності; – ідентифікація диверсійних груп та мародерів; – охорона стратегічних об'єктів (джерела води, склади, пункти медичної допомоги). Прикладом таких ініціатив є **Рух опору в Київській області під час окупації Бучі та Ірпеня**, коли місцеві жителі допомагали ідентифікувати ворожі ДРГ (диверсійно-розвідувальні групи), передавали координати російської техніки Збройним силам України та охороняли свої громади.

Психологічна підтримка та інформаційна безпека. У кризових ситуаціях інформаційні війни та психологічний тиск можуть впливати на моральний стан населення. Противник може поширювати фейки, спрямовані на створення паніки та деморалізацію. Наприклад, під час оборони Києва у лютому-березні 2022 року російська пропаганда розповсюджувала неправдиву інформацію про «здачу столиці», що могло викликати хаос серед жителів.

Важливими заходами протидії є: – навчання населення правилам медіаграмотності (перевірка інформації через офіційні джерела); – створення закритих комунікаційних платформ для перевіреної інформації; – робота кризових психологів, які допомагають справлятися зі стресом та панікою.

7.3. Стратегії виживання в умовах тривалих надзвичайних ситуацій.

Коли надзвичайна ситуація триває тижнями або навіть місяцями, життєво необхідним стає **раціональне планування ресурсів, підтримка фізичного та психологічного здоров’я, а також адаптація до нових умов життя.** У таких випадках головними факторами виживання є забезпечення базових потреб, зокрема води, їжі, тепла, безпеки та інформації. Відсутність хоча б одного з цих елементів може призвести до критичних наслідків, тому важливо заздалегідь продумати стратегію автономного існування в умовах надзвичайних ситуацій.

Доступ до централізованого водопостачання та продовольства може бути ускладненим або повністю відсутнім. Прикладом є блокада Маріуполя у 2022 році, коли більшість жителів міста виживали завдяки заздалегідь зробленим запасам

їжі та можливості добути воду з колодязів, опадів або шляхом розтоплення снігу. Через відсутність гуманітарних коридорів у перші тижні облоги багато людей гинули від зневоднення та нестачі їжі. Для автономного водозабезпечення необхідно мати аварійний запас води мінімум 2-3 літри на людину на добу, використовувати альтернативні джерела, такі як дощова вода або природні джерела, і застосовувати методи очищення, зокрема кип'ятіння чи використання фільтрів для води. Продовольчий запас має включати продукти тривалого зберігання, такі як консерви, крупи, сухе молоко, горіхи, сухофрукти, сухі супи, а також їжу, що не потребує приготування, наприклад, енергетичні батончики та сублімовані продукти. В умовах відсутності електроенергії важливо мати альтернативні засоби приготування їжі, такі як портативні газові плити, спиртові пальники чи буржуйки.

Тривалі надзвичайні ситуації, особливо взимку, вимагають ефективного забезпечення тепла, оскільки холод може бути не менш небезпечним, ніж нестача їжі. Масові відключення електроенергії в Україні у 2022–2023 роках продемонстрували критичну необхідність альтернативних джерел обігріву. Використання буржуйок, твердопаливних печей, інфрачервоних обігрівачів або генераторів дозволяло зберігати життєво важливе тепло. Утеплення приміщень за допомогою заклеювання вікон, ущільнення дверей, використання термоковдр та спільного сну у закритому просторі допомагало людям виживати без доступу до централізованого опалення. Для забезпечення електропостачання можна використовувати портативні генератори, павербанки, сонячні панелі або акумулятори, які дозволяють заряджати мобільні пристрої та живити критично важливі прилади, такі як радіозв'язок чи медичне обладнання.

В умовах бойових дій або масштабних катастроф необхідно мати альтернативні джерела інформації, адже відсутність зв'язку може спричинити паніку і дезорієнтацію. Автономні радіоприймачі на батарейках або радіостанції дозволяють отримувати екстрені повідомлення навіть за відсутності мобільного зв'язку. Супутниковий інтернет, наприклад Starlink, або супутниковий телефон Iridium забезпечують стабільний зв'язок у зонах, де зруйнована інфраструктура.

Використання захищених месенджерів, таких як Signal або Briar, що можуть працювати навіть без доступу до інтернету, є ефективним способом збереження комунікації між людьми у кризових умовах. Організація фізичної безпеки передбачає зміцнення помешкань, зокрема посилення дверей, маскування вікон та мінімізацію використання світла у темний час доби. Захист від мародерства, патрулювання території разом із сусідами та створення груп самооборони дозволяють забезпечити базову безпеку громади.

Тривале перебування в умовах нестачі ресурсів, загрози життю та невизначеності створює ризик розвитку депресії, паніки та агресії. Люди, які не готові до тривалого перебування у кризовому стані, можуть ухвалювати небезпечні рішення, що погіршує ситуацію. Для підтримки психологічної стійкості необхідно дотримуватися режиму дня, виконувати фізичні вправи, підтримувати соціальні контакти навіть у складних умовах. Структурованість розпорядку дня допомагає знизити рівень стресу та підтримувати концентрацію. Фізична активність сприяє виробленню ендорфінів, які покращують емоційний стан і запобігають психологічному виснаженню. Спілкування з рідними, навіть через обмежені засоби зв'язку, дозволяє людям не відчувати себе ізольованими, що є ключовим фактором виживання у довготривалих кризових ситуаціях. Контроль емоцій можливий завдяки використанню спеціальних технік дихання, наприклад, методу «4-7-8», що передбачає вдих на 4 секунди, затримку дихання на 7 секунд та повільний видих на 8 секунд. Обмеження негативного інформаційного впливу також є важливим, адже надмірне читання новин може викликати підвищену тривожність, особливо якщо інформація є емоційно забарвленою або маніпулятивною.

Успішне виживання в умовах тривалих надзвичайних ситуацій залежить від рівня підготовки, наявності необхідних ресурсів та здатності адаптуватися до нових реалій. Практика показує, що люди, які заздалегідь готуються до можливих кризових сценаріїв, мають значно вищі шанси на виживання та підтримання нормального рівня життя навіть у найскладніших умовах. Готовність до кризових ситуацій включає як фізичні аспекти – наявність запасів, засобів обігріву,

альтернативних джерел енергії – так і психологічну підготовку, яка дозволяє зберігати критичне мислення та раціонально діяти в умовах загрози. В умовах війни та інших тривалих надзвичайних ситуацій стратегічне планування стає основою виживання, забезпечуючи можливість збереження здоров’я, безпеки та функціонування громад навіть у найскладніші періоди.

РОЗДІЛ 8. Технології прогнозування та управління надзвичайними ситуаціями.

Сучасні технології прогнозування та управління надзвичайними ситуаціями є критично важливими для забезпечення ефективного реагування та мінімізації наслідків природних, техногенних і соціальних катастроф. Використання аналітичних методів, геоінформаційних систем, штучного інтелекту та великих даних дозволяє завчасно виявляти потенційні загрози, прогнозувати їхній розвиток і координувати відповідні заходи. В умовах гібридних загроз особливе значення набувають інтегровані підходи до управління кризовими ситуаціями, що включають аналіз кіберризиків, дезінформаційних кампаній та використання новітніх військових і технологічних методів впливу.

8.1. Використання геоінформаційних систем (GIS) у прогнозуванні катастроф.

Використання геоінформаційних систем (GIS) у прогнозуванні катастроф є одним із ключових напрямів сучасного цивільного захисту, оскільки дозволяє отримувати точні дані про геопросторові фактори ризику, розраховувати сценарії розвитку катастроф та забезпечувати оперативне управління рятувальними операціями. **GIS-технології** поєднують аналітичні методи обробки великих даних, супутниковий моніторинг, цифрове картографування та прогностичне моделювання, що значно підвищує ефективність реагування на природні, техногенні та військові загрози.

Одним із найважливіших застосувань GIS є **моделювання поширення стихійних лих, таких як повені, пожежі, урагани та землетруси**. Використання просторового аналізу дозволяє прогнозувати, які території можуть бути уражені внаслідок катастрофи, оцінювати потенційні втрати, розробляти плани евакуації та визначати пріоритетні напрями для розгортання рятувальних операцій. Наприклад, у США Національне управління океанічних і атмосферних

досліджень (NOAA) активно застосовує GIS для прогнозування ураганів, використовуючи супутникові дані та кліматичні моделі для оцінки сили буревіїв та можливих маршрутів їхнього руху. В Японії подібні системи застосовуються для моніторингу сейсмічної активності, що дозволяє швидко визначати зони найбільшого ризику після землетрусів і запускати автоматизовану систему оповіщення про загрозу цунамі.

GIS є критично важливим інструментом також у системах раннього виявлення техногенних катастроф, зокрема аварій на хімічних, ядерних і гідротехнічних об'єктах. Наприклад, у країнах Європейського Союзу використовується інтегрована система Copernicus Emergency Management Service (EMS), яка дозволяє здійснювати супутниковий моніторинг промислових зон та миттєво оцінювати наслідки надзвичайних ситуацій. В Україні GIS-технології застосовуються для аналізу радіаційної безпеки навколо Запорізької АЕС, оцінки ризиків аварій на підприємствах хімічної промисловості, а також моніторингу стану великих гідроелектростанцій, таких як Дніпровська ГЕС.

GIS-технології широко використовуються для **управління гуманітарними кризами**, пов’язаними з військовими діями та евакуацією населення. У період повномасштабної війни в Україні геоінформаційні системи застосовуються для оцінки наслідків ракетних ударів, аналізу пошкодженої інфраструктури, координації розміщення тимчасових центрів для біженців та визначення гуманітарних коридорів. Наприклад, використання супутникових знімків, аерофотозйомки та даних із дронів дозволяє оперативно оцінювати масштаб руйнувань та визначати найбільш ефективні маршрути для рятувальних підрозділів. Завдяки використанню GIS можна швидко реагувати на зміну тактичної ситуації в зоні бойових дій, координувати логістику гуманітарних місій та уникати небезпечних ділянок, де тривають активні обстріли.

GIS також активно використовується у **плануванні інфраструктури та відновленні регіонів**, що постраждали внаслідок катастроф. Завдяки цифровим картам можливо швидко оцінити стан пошкоджених будівель, дорожньої інфраструктури, систем водопостачання та електропостачання. Наприклад, в Україні було

створено цифрові геоінформаційні платформи для оцінки руйнувань у Київській, Харківській, Донецькій та Херсонській областях, що дозволило уряду та міжнародним організаціям планувати ефективне виділення коштів на відновлення.

GIS-технології застосовуються також у **прогнозуванні екологічних загроз**, пов'язаних із лісовими пожежами, змінами рівня води у великих річках та забрудненням повітря. В умовах військових дій такі системи є особливо важливими, оскільки дозволяють контролювати рівень небезпечних викидів у повітря після знищення нафтобаз, промислових об'єктів та військових складів. Наприклад, після підриву Каховської ГЕС у 2023 році українські екологічні служби використали GIS для оцінки рівня забруднення води, змоделювали поширення шкідливих речовин та прогнозували довгострокові наслідки катастрофи для навколишнього середовища.

GIS-технології також є важливим інструментом для **оптимізації дій рятувальних служб** та координації між різними відомствами. Наприклад, у разі великомасштабної аварії або теракту GIS дозволяє організувати швидкий розподіл медичних ресурсів, визначити найкоротші маршрути для транспортування постраждалих та встановити пріоритетні зони для розміщення мобільних госпіталів.

Отже, використання геоінформаційних систем значно підвищує ефективність прогнозування та реагування на катастрофи, забезпечуючи точне моделювання ризиків, швидке ухвалення рішень та координацію рятувальних операцій. В умовах сучасних викликів GIS-технології стають не лише потужним аналітичним інструментом, але й необхідною складовою державних систем безпеки та управління кризовими ситуаціями.

8.2. Методи прогнозування та моніторингу надзвичайних ситуацій.

Методи прогнозування та моніторингу надзвичайних ситуацій базуються на використанні аналітичних моделей, статистичних методів, машинного навчання та обробки великих даних (Big Data). Сучасні технології дозволяють не

лише відстежувати та аналізувати наявні загрози, а й будувати прогностичні моделі, що дають змогу оцінювати ймовірність виникнення катастроф та їхній потенційний вплив на населення, інфраструктуру та екосистеми. Для ефективного прогнозування використовуються як традиційні математичні методи, так і новітні підходи на основі штучного інтелекту, що дозволяють аналізувати величезні масиви даних у реальному часі та швидко знаходити закономірності у виникненні кризових ситуацій.

Основні підходи до прогнозування поділяються на детерміністичні та ймовірнісні. Детерміністичні методи включають математичні моделі та комп'ютерні симуляції, що дозволяють розрахувати поведінку небезпечного явища на основі фізичних законів. Наприклад, моделювання поширення токсичних речовин у повітрі чи воді допомагає оцінити потенційну зону ураження під час хімічних аварій. Такі моделі враховують напрямок і швидкість вітру, рельєф місцевості, атмосферні умови, що дозволяє прогнозувати можливі сценарії розвитку подій та ухвалювати рішення щодо евакуації населення або нейтралізації загрози. Аналогічні моделі застосовуються для прогнозування поширення радіоактивного забруднення після аварій на атомних електростанціях, що було критично важливим після Чорнобильської катастрофи 1986 року та аварії на Фукусімській АЕС у 2011 році.

Ймовірнісні методи ґрунтуються на аналізі історичних даних і статистичних закономірностей, що дозволяє передбачати частоту виникнення стихійних лих на основі попередніх подій. Наприклад, аналіз даних про землетруси в певному регіоні дозволяє оцінити ймовірність повторного виникнення сейсмічної активності та ухвалювати рішення про посилення інфраструктури або зміну містобудівних стандартів. Вчені використовують великі бази даних, що містять відомості про історичні природні катастрофи, для визначення загрозливих тенденцій. Наприклад, Національна адміністрація з аеронавтики та дослідження космічного простору США (NASA) аналізує супутникові дані, щоб прогнозувати зміни клімату та ризики екстремальних погодних явищ, таких як урагани, повені та посухи.

Сучасні системи моніторингу надзвичайних ситуацій включають використання сенсорних мереж, що реєструють зміни в навколишньому середовищі, таких як підвищення температури, рівня води, сейсмічної активності або радіації. Сенсорні мережі застосовуються для виявлення лісових пожеж, аналізу стану гребель та мостів, моніторингу якості повітря та контролю рівня небезпечних речовин у довкіллі. Наприклад, у США система FireCAST дозволяє виявляти спалахи лісових пожеж, оцінювати швидкість їх поширення та прогнозувати можливі шляхи розвитку, що дає можливість своєчасно мобілізувати пожежні служби та мінімізувати наслідки. В Європі застосовується система Flood Forecasting, яка використовує дані гідрологічних станцій та метеорологічних супутників для передбачення паводків та оперативного оповіщення місцевих органів влади та рятувальників.

Важливу роль у ранньому виявленні загроз відіграють автоматизовані системи оповіщення, які надсилають сповіщення населенню та рятувальним службам через мобільні додатки, SMS або сигнальні сирени. Наприклад, у Японії система J-ALERT дозволяє автоматично інформувати громадян про наближення цунамі, землетрусів чи ракетних загроз, надсилаючи попередження на мобільні телефони, телебачення та радіостанції. Завдяки цьому у 2011 році багато жителів японського узбережжя встигли евакуюватися перед ударом цунамі, що врятувало тисячі життів. В Україні активно розвивається система «Повітряна тривога», яка через мобільні додатки миттєво повідомляє громадян про загрозу ракетного удару або артилерійського обстрілу. Важливою особливістю цієї системи є її інтеграція з міжнародними мережами раннього виявлення загроз, що дозволяє отримувати інформацію про запуски ракет, ворожі атаки безпілотників або потенційні техногенні аварії в реальному часі.

Окрему роль відіграє **розвиток кібербезпеки та моніторинг цифрових загроз**, оскільки у сучасному світі надзвичайні ситуації можуть бути викликані не лише фізичними, а й кібернетичними атаками. Наприклад, у 2015 році російські хакери атакували українську енергосистему, що спричинило масштабне відключення електроенергії в кількох областях. Відтоді Україна активно

впроваджує системи кіберзахисту для моніторингу потенційних загроз, використовуючи інструменти аналізу трафіку, виявлення аномальної активності в мережах та системи реагування на кіберінциденти.

Отже, прогнозування та моніторинг надзвичайних ситуацій є багатокомпонентним процесом, що включає аналіз даних, використання сенсорних мереж, автоматизованих систем оповіщення, штучного інтелекту та кіберзахисту. Поєднання традиційних та інноваційних підходів дозволяє не лише ефективно реагувати на надзвичайні ситуації, а й завчасно їх передбачати, що значно зменшує ризики для життя та безпеки людей. Впровадження сучасних технологій у сфері прогнозування надзвичайних ситуацій є одним із головних напрямів розвитку цивільного захисту в Україні та світі, адже своєчасна інформація є запорукою швидкого реагування та зменшення масштабів катастроф.

8.3. Цивільний захист у контексті гібридних загроз.

Цивільний захист у контексті гібридних загроз вимагає нових підходів до забезпечення безпеки, оскільки сучасні конфлікти часто поєднують військові, інформаційні, економічні та кібернетичні методи впливу. Гібридні загрози мають комплексний характер і можуть включати кібератаки на критичну інфраструктуру, поширення дезінформації, економічний тиск, диверсійні акції, маніпулювання громадською думкою та використання проксі-структур для дестабілізації держави. Особливістю таких загроз є їхня непередбачуваність і складність у виявленні, що ускладнює їхню нейтралізацію традиційними методами цивільного захисту.

Прикладом гібридної загрози є атаки на енергосистеми, такі як злам комп'ютерних мереж українських електростанцій у 2015 році, що призвело до масштабного відключення електроенергії в кількох регіонах країни. Цей випадок став першою у світі підтвердженою кібератакою на енергетичну інфраструктуру держави, що продемонструвало вразливість критичних об'єктів до цифрових загроз. У 2017 році Україна знову стала жертвою кібернападу, коли вірус-

шифрувальник **NotPetya** вразив тисячі комп'ютерних систем державних установ, банків, транспортних компаній і підприємств. Його наслідки були катастрофічними – паралізовано роботу бізнесу, завдано мільярдних економічних збитків, що стало частиною ширшої стратегії дестабілізації країни в межах гібридної війни.

Під час повномасштабної війни в Україні у 2022–2023 роках ворог активно застосовував інформаційно-психологічні операції, поширюючи фейки про «здачу Києва», «крах економіки», «невідворотність капітуляції» та інші маніпулятивні повідомлення, спрямовані на деморалізацію суспільства. Окрім інформаційної війни, відбувалися масові атаки на критичну інфраструктуру: знищення підстанцій, ударні дрони проти енергетичних об’єктів, диверсійні групи, які підривали залізничні шляхи та підприємства. Знищення об'єктів енергосистеми спричиняло масштабні відключення світла, водопостачання та зв’язку, що ставило під загрозу функціонування держави в цілому.

У відповідь Україна розробила **стратегії інформаційної безпеки**, що включають посилення кіберзахисту урядових систем, створення незалежних каналів комунікації та боротьбу з ворожою пропагандою. Зокрема, розширено можливості **Кіберполіції України** та Держспецзв’язку щодо моніторингу цифрових загроз, запущено інформаційні кампанії проти дезінформації та фейкових новин, а також активізовано співпрацю з міжнародними партнерами для зміцнення кіберзахисту критичних систем.

Системи прогнозування гібридних загроз базуються на методах аналізу великих масивів даних та штучного інтелекту, які дозволяють виявляти аномальні патерни у фінансових транзакціях, активності в соціальних мережах та поведінці користувачів у кіберпросторі. Наприклад, автоматизовані алгоритми здатні ідентифікувати скоординовані дезінформаційні кампанії, аналізуючи одночасне поширення фейкових новин у різних джерелах. Важливим інструментом є **платформи OSINT (Open Source Intelligence)**, що дозволяють виявляти джерела ворожої пропаганди, відстежувати дії диверсійних груп і розкривати фінансові махінації, спрямовані на підрив економічної стабільності.

Такі технології широко застосовуються у сфері національної безпеки для аналізу ворожої активності в інформаційному просторі, визначення потенційних загроз та відстеження переміщення ресурсів, які можуть бути використані для підтримки диверсійної діяльності.

Цивільний захист у контексті гібридних загроз також передбачає **підготовку населення до дій у кризових умовах**. Важливим елементом є розвиток навичок інформаційної гігієни, що включає вміння перевіряти джерела інформації, аналізувати контент на предмет маніпулятивних технік та уникати впливу ворожої пропаганди. Наприклад, у країнах Балтії активно проводяться **освітні кампанії з цифрової грамотності**, що навчають громадян виявляти інформаційні маніпуляції та методи соціальної інженерії. В Україні в умовах війни було посилено заходи щодо кібербезпеки та цифрової грамотності – запроваджено спеціальні навчальні програми, розроблено курси для державних службовців, військових та журналістів щодо розпізнавання дезінформації та захисту від кібератак.

Окрему увагу приділено **створенню незалежних інформаційних платформ**, що дозволяють громадянам отримувати перевірені дані у періоди кризових ситуацій. Наприклад, офіційні ресурси, такі як **«Сили оборони України», «Центр стратегічних комунікацій» та «StopFake»**, систематично спростовують фейки, пояснюють реальний стан справ і забезпечують об’єктивну оцінку ситуації. Такий підхід дозволяє зменшити вплив ворожої пропаганди та запобігти паніці серед населення.

Сучасні технології прогнозування та управління надзвичайними ситуаціями дають змогу ефективно реагувати на виклики сучасного світу, мінімізувати втрати та забезпечити стабільність у кризових умовах. Інтеграція геоінформаційних систем, методів прогнозування, штучного інтелекту та систем моніторингу дозволяє створити **ефективну систему цивільного захисту**, що здатна протистояти як природним, так і технологічним загрозам. У контексті гібридних воєн держава має розвивати **аналітичні центри**, що спеціалізуються

на виявленні новітніх загроз, створювати **стратегії інформаційного опору** та **зміцнювати кіберзахист критичної інфраструктури**.

Одним із ключових напрямів є розвиток **кіберрезерву держави**, що включає підготовку фахівців у сфері кібербезпеки, створення резервних цифрових систем для збереження державних даних та розвиток захищених платформ для комунікації державних структур. Важливу роль відіграє **співпраця з міжнародними партнерами**, такими як НАТО, Європейський Союз та великі технологічні компанії, що допомагають розробляти ефективні стратегії захисту від гібридних загроз.

Таким чином, цивільний захист у контексті гібридних загроз є багаторівневою системою, що охоплює цифрову безпеку, інформаційний захист, моніторинг потенційних загроз та підготовку населення до кризових ситуацій. Використання новітніх технологій, штучного інтелекту та аналітики великих даних дає змогу державам своєчасно виявляти гібридні загрози, мінімізувати їхні наслідки та забезпечувати стабільність навіть у найскладніших умовах.

РОЗДІЛ 9. Міжнародний досвід та координація цивільного захисту.

Цивільний захист є ключовим елементом системи національної безпеки кожної держави, що забезпечує готовність до надзвичайних ситуацій, їх запобігання та ефективне реагування. У сучасному світі загрози цивільному населенню стають дедалі складнішими через глобальні виклики, включаючи природні катастрофи, техногенні аварії, епідемії, терористичні акти та гібридні війни. Враховуючи транснаціональний характер багатьох з цих загроз, ефективна система цивільного захисту неможлива без міжнародного співробітництва, обміну досвідом, координації зусиль та гармонізації нормативно-правової бази.

У цьому розділі розглядається міжнародний досвід організації цивільного захисту, механізми міжнародної взаємодії, координація заходів з іншими країнами та міжнародними організаціями, а також вплив сучасних конфліктів на систему цивільного захисту. Окрему увагу приділено аналізу правових аспектів міжнародного регулювання у цій сфері, визначенню об’єктів критичної інфраструктури та механізмів їхнього захисту, а також розгляду ефективності міжнародної допомоги у подоланні кризових ситуацій. Спираючись на досвід провідних країн та міжнародних інституцій, у розділі наведено приклади успішних стратегій реагування на надзвичайні ситуації, міжнародні ініціативи у сфері цивільного захисту та перспективи удосконалення національних механізмів реагування на загрози.

Таким чином, аналізуючи міжнародний досвід та координацію цивільного захисту, можна визначити найефективніші моделі реагування, покращити міждержавну співпрацю та сприяти зміцненню глобальної безпеки через посилення стійкості суспільства до кризових ситуацій.

9.1. Роль цивільного захисту під час інформаційних війн.

В умовах сучасного інформаційного суспільства інформаційні війни набувають усе більшого значення як інструмент впливу на суспільну думку, стратегічне управління державою та міжнародні відносини. Вони спрямовані на

підрив довіри до державних інституцій, розповсюдження панічних настроїв, спотворення реальної картини подій та маніпулювання свідомістю громадян з метою ослаблення суспільної єдності та національної безпеки. У такій ситуації цивільний захист відіграє критично важливу роль у забезпеченні стійкості держави до інформаційних атак. Основними заходами є впровадження національної інформаційної політики, що базується на науково обґрунтованих методах боротьби з дезінформацією, створення державних та незалежних центрів фактчекінгу, активна взаємодія з міжнародними організаціями з питань інформаційної безпеки, а також підвищення рівня цифрової грамотності серед населення.

За даними досліджень Європейського центру боротьби з дезінформацією, близько 70% населення ЄС стикалося з фейковими новинами, а 40% зізналися, що не можуть відрізнити правдиву інформацію від маніпулятивної. В Україні, згідно зі звітом Центру стратегічних комунікацій, понад 60% населення вважають, що інформаційні атаки є серйозною загрозою національній безпеці. Це свідчить про необхідність удосконалення системи моніторингу інформаційного простору, що є першочерговим завданням цивільного захисту.

Моніторинг інформаційного простору є першочерговим завданням цивільного захисту, адже тільки через оперативне виявлення дезінформаційних кампаній можливо швидко реагувати та здійснювати спростування недостовірних даних. Для цього необхідне впровадження сучасних систем автоматизованого аналізу інформаційного потоку, що використовують технології штучного інтелекту та великі дані. Важливою складовою є підготовка кадрів, що здатні працювати з інформаційними загрозами, аналізувати дані та координувати міжвідомчу співпрацю для ефективного реагування. У зв’язку з глобалізацією інформаційних потоків державні структури повинні забезпечувати постійну взаємодію з провідними світовими центрами кібербезпеки, співпрацювати з організаціями, що займаються моніторингом маніпулятивного контенту, та активно залучати міжнародну допомогу в питаннях інформаційного захисту.

В умовах ведення інформаційних воєн необхідно впроваджувати ефективні стратегії кризової комунікації, які дозволяють не тільки оперативно

реагувати на інформаційні загрози, але й формувати довгострокову довіру громадян до державних органів та офіційних джерел інформації. Такі стратегії передбачають розробку комунікаційних протоколів на випадок інформаційних атак, створення єдиних центрів швидкого реагування, а також підготовку речників та аналітиків, які зможуть обґрунтовано та швидко відповідати на інформаційні виклики. Важливим аспектом є також співпраця з громадським сектором та незалежними ЗМІ, які можуть сприяти поширенню правдивої інформації та нівелюванню впливу дезінформаційних кампаній. Окрім цього, слід розглядати створення інформаційних платформ для інтерактивного обміну перевіреними даними між урядом та суспільством, що сприятиме підвищенню інформаційної стійкості держави.

Загалом, роль цивільного захисту у сфері протидії інформаційним війнам є комплексною та багаторівневою. Вона вимагає не лише технічного та правового забезпечення, а й зміни підходів до формування інформаційної культури населення, підвищення стійкості до маніпулятивного впливу, розвитку національних інформаційних стратегій та інтеграції міжнародного досвіду у сфері інформаційної безпеки. Успішна реалізація цих заходів дозволить не лише захистити населення від деструктивного інформаційного впливу, але й посилити загальну національну безпеку, що є стратегічним пріоритетом будь-якої держави у сучасному світі.

9.2. Захист критичної інфраструктури від диверсій.

Критична інфраструктура є стратегічно важливим елементом державної безпеки та функціонування суспільства, оскільки включає енергетичні об'єкти, транспортну систему, зв'язок, водопостачання, медичні заклади, телекомунікації, фінансову систему, логістику та стратегічні підприємства оборонного комплексу. В умовах сучасних загроз, зокрема кібератак, терористичних актів та військових конфліктів, необхідність посилення безпеки критичної інфраструктури стає одним із пріоритетів державної політики. Захист таких об’єктів

включає багаторівневий підхід, що охоплює правові, технічні, організаційні та міжнародні аспекти. Згідно з даними Національного центру кібербезпеки, у 2022 році зафіксовано понад 800 атак на об’єкти критичної інфраструктури в Україні, зокрема на енергетичні компанії, системи водопостачання та транспортні вузли. Такі дії призводять до значних економічних збитків, соціальної нестабільності та загрожують життю цивільного населення.

Об'єкт критичної інфраструктури – це об'єкт, система або мережа, руйнування або виведення з ладу яких може мати значний негативний вплив на національну безпеку, економічну стабільність, життєдіяльність суспільства або навколишнє середовище.

До об'єктів критичної інфраструктури належать енергетичні підприємства, водо- та теплопостачальні системи, об'єкти транспорту, телекомунікаційні вузли, фінансові інститути, державні інформаційні ресурси, стратегічні підприємства оборонного комплексу та медичні установи. Особливу роль відіграє міжвідомча координація, яка забезпечує ефективний обмін інформацією між силовими структурами, службами безпеки та комунальними підприємствами.

Нормативне регулювання захисту критичної інфраструктури здійснюється на основі міжнародних стандартів, а також відповідного національного законодавства. В Україні цей напрям регулюється Законом України «Про основи національної безпеки», Постановою Кабінету Міністрів України «Про затвердження Порядку визначення об'єктів критичної інфраструктури» та іншими нормативно-правовими актами, які встановлюють механізми управління ризиками, вимоги до безпеки та порядок реагування на надзвичайні ситуації.

Україна активно взаємодіє з ЄС, НАТО, США та іншими міжнародними партнерами, адаптуючи найкращі практики у сфері безпеки критичної інфраструктури. Ця співпраця охоплює розробку спільних стандартів безпеки, обмін інформацією про потенційні загрози, спільні тренування з реагування на кризові ситуації, а також участь у програмах міжнародної технічної допомоги. Зокрема, в рамках співпраці з НАТО Україна бере участь у програмі «Удосконалення кібербезпеки та захисту критичної інфраструктури», що

передбачає навчання фахівців, спільні кібернавчання та розробку протоколів швидкого реагування на надзвичайні ситуації. Також значну увагу приділено гармонізації національного законодавства з європейськими стандартами, що дозволяє інтегрувати найкращі практики у сфері управління ризиками та впроваджувати ефективні механізми захисту критично важливих об'єктів від диверсій та терористичних загроз.

Для забезпечення належного рівня захисту критичної інфраструктури застосовуються передові методи оцінки загроз та управління ризиками, що включають аналіз вразливостей, прогнозування потенційних атак, розвиток протоколів швидкого реагування, посилення фізичної охорони, а також впровадження сучасних технологій кібербезпеки. Особливу роль відіграє міжвідомча координація, яка забезпечує ефективний обмін інформацією між силовими структурами, службами безпеки та комунальними підприємствами. Україна активно взаємодіє з ЄС, НАТО, США та іншими міжнародними партнерами, адаптуючи найкращі практики у сфері безпеки критичної інфраструктури.

Таким чином, забезпечення безпеки критичної інфраструктури потребує комплексного підходу, що включає технологічне вдосконалення, міжнародне співробітництво, підготовку кадрів та посилення правового регулювання. Ефективна реалізація цих заходів дозволить зменшити вразливість критичних об'єктів до атак, підвищити рівень безпеки громадян та забезпечити стабільне функціонування суспільства навіть в умовах кризових ситуацій. Важливим аспектом залишається впровадження багаторівневих систем безпеки, що включають фізичні та цифрові заходи захисту, що у свою чергу потребує значних фінансових ресурсів та стратегічного планування.

9.3. Механізми міжнародної допомоги в умовах гібридних конфліктів.

Гібридні конфлікти поєднують традиційні військові дії з інформаційними, економічними та кібернетичними атаками, що створює нові виклики для системи цивільного захисту. У таких умовах міжнародна допомога стає важливим

елементом забезпечення стійкості держави до кризових ситуацій. Основні механізми міжнародної допомоги включають гуманітарну підтримку, фінансову і технічну допомогу, військово-технічне співробітництво, координацію дій між міжнародними організаціями, а також спільні навчання та обмін досвідом. Ці заходи допомагають зміцнити спроможність держави до ефективного реагування на загрози та мінімізації наслідків конфліктів.

Гуманітарна допомога є першочерговим елементом міжнародної підтримки та включає надання продовольства, медикаментів, води, тимчасового житла та інших критично важливих ресурсів для постраждалого населення. Наприклад, за даними ООН, у 2022 році внаслідок збройних конфліктів у різних країнах понад 274 мільйони людей потребували гуманітарної допомоги, що є найвищим показником за останні десятиліття. В Україні міжнародні організації, такі як Червоний Хрест та Всесвітня продовольча програма, забезпечили мільйони громадян необхідними ресурсами під час активних бойових дій.

Фінансова та технічна допомога спрямована на підтримку економічної стабільності держави, відновлення критичної інфраструктури, забезпечення доступу до енергетичних ресурсів та покращення умов життя населення. Вона включає як безповоротну гуманітарну допомогу, так і кредити з пільговими умовами повернення. Європейський Союз, Світовий банк, Міжнародний валютний фонд та інші міжнародні фінансові установи регулярно виділяють фінансові пакети для країн, що постраждали від військових конфліктів. Зокрема, у 2022-2024 році ЄС ухвалив виділення Україні понад 18 мільярдів євро для економічної стабілізації та розвитку, що стало найбільшим пакетом підтримки в історії Союзу для однієї країни.

Фінансова допомога також спрямовується на розвиток малого та середнього бізнесу, що є ключовим елементом економічної стабільності у постконфліктний період. Наприклад, через програму «Український фонд стійкості» понад 5000 підприємств отримали фінансування для відновлення діяльності. Значна частина коштів також спрямовується на модернізацію енергетичної інфраструктури, що дозволяє зменшити залежність від традиційних енергоресурсів і

впроваджувати інноваційні підходи до енергетичної безпеки. Наприклад, у рамках співпраці з Європейським банком реконструкції та розвитку було реалізовано програму «Зелена енергетика», що включає будівництво нових об'єктів сонячної та вітрової генерації для забезпечення енергетичної незалежності.

Крім безпосереднього фінансування, технічна допомога включає експертну підтримку та консультації щодо реформування економічних інститутів, оновлення системи державного управління, боротьби з корупцією та впровадження цифрових технологій у державний сектор. Так, за підтримки МВФ в Україні впроваджено комплексну програму з підвищення прозорості бюджетного процесу, що дозволяє ефективніше розподіляти міжнародні кошти та запобігати їхньому нецільовому використанню.

Військово-технічне співробітництво є важливим компонентом міжнародної допомоги в умовах гібридних конфліктів. Воно охоплює широкий спектр заходів, включаючи постачання сучасних оборонних технологій, надання зброї, підготовку військових фахівців, спільні військові навчання та розвиток технологічних систем для покращення обороноздатності. Така співпраця не лише підвищує оборонний потенціал приймаючих країн, але й дозволяє інтегрувати їх у міжнародні стандарти ведення бойових дій та стратегічного управління. Наприклад, програма військової підтримки України передбачає надання протитанкових комплексів Javelin, артилерійських систем та засобів протиповітряної оборони, що дозволяє значно зміцнити можливості Збройних сил України.

Окрім безпосередньої передачі техніки, важливу роль відіграють **навчальні ініціативи**. НАТО регулярно проводить тренування з кіберзахисту для країн-партнерів, що дозволяє підвищити їхню здатність протидіяти цифровим загрозам, особливо в контексті гібридних конфліктів. У рамках програми «Кіберщит» Україна отримала доступ до новітніх методів виявлення та ліквідації кібератак, що дозволяє не лише захищати критичну інфраструктуру, а й активно протидіяти ворожим інформаційним операціям. Також важливою складовою міжнародного військово-технічного співробітництва є обмін розвідданими, що

сприяє ефективнішому аналізу потенційних загроз і розробці тактичних рішень для їхньої нейтралізації.

Крім традиційних видів військової допомоги, значну роль відіграє розробка та впровадження систем автоматизованого управління військами, що дозволяє підвищити координацію між підрозділами та швидкість реагування на загрози. Наприклад, інтеграція України до загальноєвропейської системи обміну оперативною інформацією дозволяє покращити взаємодію з союзниками у сфері військового планування та оборонних операцій. Такі заходи є ключовими для підтримання оборонного потенціалу країн, що зазнають впливу гібридних загроз.

Координація дій між міжнародними організаціями є ключовим аспектом забезпечення ефективної міжнародної підтримки. Організація Об'єднаних Націй, Європейський Союз, ОБСЄ та НАТО регулярно організовують консультації та міжурядові зустрічі для розробки стратегій захисту цивільного населення, гуманітарного реагування та військової допомоги. Наприклад, у 2022 році ООН заснувала спеціальну платформу «Глобальна відповідь на конфлікти», яка спрямована на координацію гуманітарних місій у зонах конфліктів по всьому світу.

Спільні навчання та обмін досвідом дозволяють країнам, які зіткнулися з гібридними загрозами, адаптувати найкращі практики міжнародного реагування. Навчання, що проводяться під егідою НАТО, ЄС та інших партнерів, включають тренування з ліквідації наслідків надзвичайних ситуацій, протидії інформаційним атакам, розвитку навичок кризового управління та підготовки кадрів для гуманітарного реагування. Наприклад, навчання «Стійка Європа 2023» залучили понад 20 країн для розробки спільних механізмів реагування на потенційні гібридні загрози.

Законодавче регулювання міжнародної допомоги в умовах гібридних конфліктів здійснюється на основі міжнародних норм, включаючи Женевські конвенції, резолюції Ради Безпеки ООН, угоди міждержавного співробітництва, нормативно-правові акти Європейського Союзу та стандарти міжнародних

гуманітарних організацій. Одним з ключових документів є Глобальний гуманітарний договір, який визначає принципи надання гуманітарної допомоги в умовах збройних конфліктів, включаючи нейтральність, незалежність та ефективність розподілу ресурсів.

В Україні питання міжнародної допомоги регулюється низкою законодавчих актів, серед яких Закон «Про гуманітарну допомогу», який встановлює правові засади надання, отримання та розподілу міжнародної допомоги, а також співпрацю із міжнародними організаціями. Крім того, Законом «Про основи національної безпеки» визначено механізми стратегічної взаємодії України з міжнародними партнерами у сфері забезпечення обороноздатності та гуманітарного реагування. Важливу роль відіграє також Закон «Про міжнародні договори України», який регулює процедури укладання угод з міжнародними донорами, фінансовими організаціями та військово-технічними партнерами.

Значну увагу приділяють узгодженню національного законодавства із міжнародними стандартами. Так, постановами Кабінету Міністрів України запроваджено механізми оперативного контролю за отриманням та використанням міжнародної допомоги, а також створено координаційні центри при Міністерстві оборони та Державній службі з надзвичайних ситуацій для розподілу гуманітарних ресурсів у кризових ситуаціях.

Законодавче регулювання охоплює також фінансові аспекти допомоги. Наприклад, спеціальні положення Бюджетного кодексу України передбачають створення фондів міжнародної підтримки, які функціонують під контролем міжнародних аудиторських організацій для запобігання корупційним ризикам. Крім того, Національний банк України розробив механізм контролю за валютними операціями, пов'язаними з отриманням фінансової допомоги, що дозволяє мінімізувати можливості фінансових зловживань.

Отже, законодавче регулювання міжнародної допомоги в умовах гібридних конфліктів є багаторівневим і спрямованим на забезпечення ефективності, прозорості та відповідності міжнародним стандартам. Постійна адаптація правової бази до нових викликів, удосконалення механізмів контролю та

координації допомоги з міжнародними партнерами є важливими складовими підвищення стійкості держави до кризових ситуацій.

Таким чином, міжнародна допомога в умовах гібридних конфліктів є складним багаторівневим процесом, що охоплює гуманітарну, фінансову, військову та координаційну підтримку. Ефективна реалізація цих механізмів дозволяє країнам-реципієнтам зберігати стійкість перед викликами, швидко реагувати на кризові ситуації та мінімізувати їхні наслідки для населення і національної безпеки.

РОЗДІЛ 10. Рекомендований перелік нормативно-правових актів з питань цивільного захисту, безпеки життєдіяльності та охорони праці.

Нормативно-правові акти з питань цивільного захисту:

Кодекс цивільного захисту України : Закон України від 2 жовтня 2012 р. № 5403-VI. URL: https://zakon.rada.gov.ua/laws/show/5403-17

Про правовий режим надзвичайного стану : Закон України від 16 березня 2000 р. № 1550-III. URL: https://zakon.rada.gov.ua/laws/show/1550-14

Про правовий режим воєнного стану : Закон України від 12 травня 2015 р. № 389-VIII. URL: https://zakon.rada.gov.ua/laws/show/389-19

Про затвердження Положення про єдину державну систему цивільного захисту : Постанова Кабінету Міністрів України від 9 січня 2014 р. № 11. URL: https://zakon.rada.gov.ua/laws/show/11-2014-%D0%BF

Про затвердження Порядку класифікації надзвичайних ситуацій за їх рівнями : Постанова Кабінету Міністрів України від 24 березня 2004 р. № 368. URL: https://zakon.rada.gov.ua/laws/show/368-2004-%D0%BF

Про затвердження Класифікаційних ознак надзвичайних ситуацій : Наказ Міністерства внутрішніх справ України від 6 серпня 2018 р. № 658. URL: https://zakon.rada.gov.ua/laws/show/z0970-18

Про затвердження Положення про організацію оповіщення про загрозу виникнення або виникнення надзвичайних ситуацій та зв’язку у сфері цивільного захисту : Постанова Кабінету Міністрів України від 27 вересня 2017 р. № 733. URL: https://zakon.rada.gov.ua/laws/show/733-2017-%D0%BF

Нормативно-правові акти з питань охорони праці та безпеки життєдіяльності:

Про охорону праці : Закон України від 14 жовтня 1992 р. № 2694-XII. URL: https://zakon.rada.gov.ua/laws/show/2694-12

Кодекс законів про працю України : Закон України від 10 грудня 1971 р. № 322-VIII. URL: https://zakon.rada.gov.ua/laws/show/322-08

Про забезпечення санітарного та епідемічного благополуччя населення : Закон України від 24 лютого 1994 р. № 4004-XII. URL: https://zakon.rada.gov.ua/laws/show/4004-12

Про затвердження Положення про організацію роботи з охорони праці та безпеки життєдіяльності учасників освітнього процесу в установах і закладах освіти : Наказ Міністерства освіти і науки України від 26 грудня 2017 р. № 1669. URL: https://zakon.rada.gov.ua/laws/show/z0100-18

Про затвердження Порядку проведення навчання керівного складу та фахівців, діяльність яких пов'язана з організацією і здійсненням заходів з питань цивільного захисту : Постанова Кабінету Міністрів України від 23 жовтня 2013 р. № 819. URL: https://zakon.rada.gov.ua/laws/show/819-2013-%D0%BF

Про затвердження Порядку здійснення навчання населення діям у надзвичайних ситуаціях : Постанова Кабінету Міністрів України від 26 червня 2013 р. № 444. URL: https://zakon.rada.gov.ua/laws/show/444-2013-%D0%BF

Про затвердження Порядку утворення, завдання та функції формувань цивільного захисту : Постанова Кабінету Міністрів України від 9 жовтня 2013 р. № 787. URL: https://zakon.rada.gov.ua/laws/show/787-2013-%D0%BF

Про затвердження Порядку проведення евакуації у разі загрози виникнення або виникнення надзвичайних ситуацій техногенного та природного характеру : Постанова Кабінету Міністрів України від 30 жовтня 2013 р. № 841. URL: https://zakon.rada.gov.ua/laws/show/841-2013-%D0%BF

Про затвердження Положення про добровільні формування цивільного захисту : Постанова Кабінету Міністрів України від 21 серпня 2013 р. № 616. URL: https://zakon.rada.gov.ua/laws/show/616-2013-%D0%BF

Про затвердження Порядку утворення та функціонування пожежно-рятувальних підрозділів для забезпечення добровільної пожежної охорони : Постанова Кабінету Міністрів України від 7 квітня 2023 р. № 314. URL: https://zakon.rada.gov.ua/laws/show/314-2023-%D0%BF

ЛІТЕРАТУРА:

Labour Protection and Civil Defense [Electronic resource] textbook for undergraduate students O. Levchenko, O. Polukarov, O. Arlamov, Y. Polukarov, O. Zemlyanska edited by O. Levchenko. Electronic text data 1 file 3,28 Mb. Kyiv: Igor Sikorsky Kyiv Polytechnic Institute, 2021. 352 p. URL https://ela.kpi.ua/bitstream/123456789/42252/1/Levchenko-et-al_Labour-Protectionand-Civil-Defense_Textbook.pdf

Андреєв О. В., Гончарук С. І. Інноваційні підходи до забезпечення цивільного захисту: навчальний посібник. Харків: ХНУ, 2022. 180 с.

Безпека життєдіяльності та охорона праці підручник В. В. Сокуренко, О. М. Бандурка, С. М Бортник та ін. за заг. ред. В. В. Сокуренка. Харків нац. ун-т внутр. справ. Харків: ХНУВС, 2021. 308 с. URL http://dspace.univd.edu.ua/xmlui/bitstream/handle/123456789/10837/Bezpeka%20zhyttiediialnosti%20ta%20okhorona%20pratsi%20_pidruchnyk_Sokurenko_2021.pdf?sequence=1&isAllowed=y

Безпека життєдіяльності та цивільний захист [Електронний ресурс] підручник для студ. спеціальностей з природничих соціально-гуманітарних наук та інженерно-комунікаційних технологій О. Г. Левченко, О. В. Землянська, Н. А. Праховнік, В. В. Зацарний, КПІ ім. Ігоря Сікорського. Електронні текстові дані 1 файл 10,2 Мб. Київ: КПІ ім. Ігоря Сікорського, 2019. 267 с. URL https://ela.kpi.ua/bitstream/123456789/41133/1/Bezpeka_pidruchnyk.pdf

Безпека життєдіяльності та цивільний захист. Практикум [Електронне видання] для студентів бакалаврів спеціальностей 121 Інженерія програмного забезпечення 123 Комп'ютерна інженерія 126 Інформаційні системи та технології КПІ ім. Ігоря Сікорського уклад Е. В. Землянська, Н. Ф. Качинська, Н. А. Праховнік, М. О. Мітюк. Електронне видання 1 файл 3,58 Мб. Київ: КПІ ім. Ігоря Сікорського, 2021. 113 с. URL https://ela.kpi.ua/bitstream/123456789/42305/1/Bezpeka_ta_tsyvilnyi_zakhyst.pdf

Березуцький В. В. Управління охороною праці: навчальний посібник для студентів спеціальності «Цивільна безпека освітньої програми. Охорона праці» / В. В. Березуцький. Харків: ФОП Панов А М. 2021 412 с. URL http://repository.kpi.kharkov.ua/bitstream/KhPIPress/54108/1/Book_2021_Berezutskyi_Upravlinnia.pdf

Бєлов О. Г. Екологічна безпека та раціональне природокористування. Київ: Центр учбової літератури, 2021. 260 с.

Гладкий С. М., Матвійчук В. М. Цивільний захист у сучасних умовах: навч. посіб. Львів: ЛНУ ім. І. Франка, 2022. 240 с. https://ela.kpi.ua/server/api/core/bitstreams/07b44994-8442-45cb-afbd-489e8325d23a

Голінько В. І., Третякова Л. Д., Чеберячко С. І. Проектування засобів індивідуального захисту працюючих: навч. посіб. В. І. Голінько, Л. Д. Третякова, С. І. Чеберячко. М-во освіти і науки України, Нац гірн ун-т. Дніпро: НГУ, 2017. 181 с. URL https://ela.kpi.ua/bitstream/123456789/41917/1/NavchPosib_Proektuvannia-ZIZ.pdf

Грицай І. І., Попович О. В. Охорона праці у навчальних закладах. Навчальний посібник. Львів: ЛНУ, 2023. 256 с. https://kpdi.edu.ua/biblioteka/O/Охорона%20праці%20Грицай%20М.С..pdf

Гуменюк В. О., Карпова Т. С., Яковлєва Л. І. Безпека життєдіяльності. Навчальний посібник. Вид. 4-те. Київ: Видавничий дім «Академія», 2021. 320 с.

Забезпечення інженерного захисту територій будівель і споруд в умовах надзвичайних ситуацій практикум / О. В. Васильченко, О. В. Савченко, Ю. А. Отрош. Харків: НУЦЗУ, 2019. 220 с.

Капустін В. І., Мороз А. П. Техногенна безпека: основи теорії та практики. Дніпро: ДНУ, 2022. 220 с.

Кобець П. В., & Кравець Л. В. Основи охорони праці: підручник. Київ: КНТЕУ, 2021. 400 с.

Коваль В. П. Безпека життєдіяльності: практичний посібник. Дніпро: ДДУВС, 2023. 220 с. https://er.dduvs.edu.ua/bitstream/123456789/10901/1/макет_Підручник%20БЖД%20та%20ОП-1.pdf

Ковжога С. О., Тузіков С. А., Карманний Є. В., Зенін А. П. Цивільний захист і охорона праці в галузі: навчальний посібник. Харків: Право, 2020. 192 с. ISBN 978-966-458-405-7.

Кравченко О. В., Петренко І. М. Роль сучасних інформаційних систем у цивільному захисті. Науковий журнал «Цивільна безпека». 2022. № 5. С. 32–37.

Криворучко О. В., & Трофименко С. М. Цивільний захист: підручник. Харків: ХНУВС, 2022. 280 с.

Курепін В. М. Цивільний захист: Курс лекцій. 2021. URL: https://dspace.mnau.edu.ua/jspui/bitstream/123456789/8595/1/Tsyvilnyi_zakhyst_kurs_lektsii.pdf.

Литвиненко Г. М., Базилевич, І. І. Основи цивільного захисту: навчально-методичний посібник. Київ: Університет економіки і права, 2022. 192 с.

Мельник В. О., Горбунова Н. С. Адаптація міжнародних стандартів до системи управління безпекою праці в Україні. Журнал «Охорона праці». 2023. № 2. С. 15–20.

Мороз Л. Г., Соколова І. В. Системи безпеки життєдіяльності: навчальний посібник. Одеса: ОНМУ, 2022. 190 с.

Основи професійної безпеки та здоров’я людини: підручник / В. В. Березуцький та ін.; під ред. проф. В. В. Березуцького. Харків: НТУ ХПІ, 2018. 553 с. URL http://repository.kpi.kharkov.ua/bitstream/KhPIPress/37199/1/Book_2018_Berezutskyi_Osnovy_prof_bezpeky.pdf

Отрош Ю. А. Будівлі та споруди і їх поведінка в умовах пожежі: навчальний посібник. Отрош Ю. А. Черкаси: ЧІПБ ім Героїв Чорнобиля НУЦЗ України, 2016. 158 с. URL http://pb.nuczu.edu.ua/images/ppnp/MetodVudavnDiyal/2016_8___.pdf

Охорона праці та цивільний захист [Електронний ресурс]: навч посіб для студ спеціальностей 132 Матеріалознавство та 136 Металургія / О. Г. Левченко; КПІ ім. Ігоря Сікорського. Електронні текстові дані 1 файл 26,1 Кб. Київ: КПІ ім Ігоря Сікорського, 2019. 337 с. URL https://ela.kpi.ua/handle/123456789/31215

Охорона праці та цивільний захист Лабораторний практикум [Електронне видання] для здобувачів ступеня бакалавра спеціальностей 151 Автоматизація та комп'ютерно-інтегровані технології 152 Метрологія та інформаційно-вимірювальна техніка, 153 Мікро- та наносистемна техніка, 171 Електроніка, 172 Телекомунікації та радіотехніка, 162 Біотехнології та біоінженерія, 163 Біомедична інженерія, 227 Фізична терапія ерготерапія. Н. Ф. Качинська, О. В. Землянська, О. Ю. Арламов, А. І. Ковтун, Г. В. Демчук. Електронне видання 1 файл 1,46 Мб. Київ: КПІ ім Ігоря Сікорського, 2021. URL https://ela.kpi.ua/bitstream/123456789/45082/1/Posibnyk_OPTsZ_Lab-prakt.pdf

Охорона праці та цивільний захист: Підручник для студентів які навчаються за спеціальностями галузей знань «Автоматизація та приладобудування» / О. Г. Левченко, О. І. Полукаров, В. В. Зацарний, Ю. О. Полукаров, О. В. Землянська. За ред. О. Г. Левченка. Київ: КПІ ім Ігоря Сікорського, 2019 420 с URL https://ela.kpi.ua/handle/123456789/26895

Охорона праці та цивільний захист практикум [Електронне видання] для здобувачів ступеня бакалавра спеціальностей 151 Автоматизація та комп'ютерно-інтегровані технології, 152 Метрологія та інформаційно-вимірювальна техніка приладобудівного факультету / Н. Ф. Качинська. Електронне видання 1 файл 2,432 Мб. Київ: КПІ ім Ігоря Сікорського, 2021. 282 с. URL https://ela.kpi.ua/bitstream/123456789/45080/1/Posibnyk_OPTsZ_Prakt.pdf

Панасюк Т. В., Даниленко О. В. Основи охорони праці. Харків: ХАІ, 2021. 180 с.

Розрахунок залізобетонних конструкцій на вогнестійкість відповідно до Єврокоду 2: Практичний посібник / В. Г. Поклонський, О. А. Фесенко, В. Г. Тарасюк та ін. Київ: Інтертехнологія, 2016. 83 с. URL http://pb.nuczu.edu.ua/images/ppnp/MetodVudavnDiyal/12__.pdf

Семенюк О. Г. Організація охорони праці та безпеки життєдіяльності. Одеса: ОНУ, 2022. 256 с.

Сидоренко І. В., Шевченко Л. Г. Системи управління ризиками на підприємствах: навчальний посібник. Львів: ЛНУ ім. І. Франка, 2023. 240 с.

Спеціальне водопостачання: підручник, навчальне видання, виправлене та доповнене / О. А. Петухова, С. А. Горносталь, Ю. В. Уваров Харків: НУЦЗУ, 2015. 256 с. URL http://pb.nuczu.edu.ua/images/ppnp/MetodVudavnDiyal/2015_11___.pdf

Стиценко Т. Є., Пронюк Г. В., Сердюк Н. М., Хондак І. І. Безпека життєдіяльності: навч посібник. Т. Є. Стиценко, Г. В. Пронюк, Н. М. Сердюк, І. І. Хондак. Харків: ХНУРЕ, 2018. 336 с. URL https://os.nure.ua/wp-content/uploads/2021/04/posibnik-bgd_2018.pdf

Супрун Т. В. Профілактика професійних захворювань та травматизму: монографія. Одеса: ОНУ, 2021. 200 с.

Тимошенко Г. М., Литвиненко О. В. Мінімізація ризиків у надзвичайних ситуаціях природного характеру. Екологічна безпека. 2021. № 3. С. 40–45.

Ткаченко М. М., Зайченко О. П. Охорона праці: основи теорії і практики. Київ: НАУ, 2021. 280 с.

Шевчук Т. С. Організація навчання з питань безпеки життєдіяльності у закладах освіти. Безпека життєдіяльності. 2023. № 1. С. 12–17.

Яковенко І. Г., Сидорчук Л. В. Використання сучасних технологій для підвищення ефективності охорони праці. Науковий вісник цивільного захисту. 2022. № 4. С. 28–34.

Ярошенко Т. В. Основи охорони праці в системі освіти. Харків: ХНПУ ім. Г. Сковороди, 2023. 200 с.

Навчальне видання

Сухацька *Ірина Юріївна*

Батраченко *Тетяна Сергіївна*

Єфімова *Інна Веніамінівна*

ЦИВІЛЬНИЙ ЗАХИСТ, БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ ТА ОХОРОНА ПРАЦІ

Навчально-методичний посібник

Видання друкується в авторській редакції

Відповідальний редактор *Біла К. О.*
Технічний редактор *Біла К. О.*
Оригінал-макет *Батраченко Т. С.*
Дизайн обкладинки *Біла К. О.*

Здано до друку 24.02.25. Підп. до друку 10.03.25. Формат 60х84 1/16.
Гарнітура – Times. Папір офсетний. Спосіб друку – плоский.
Ум. друк. арк. 5,10. Обл.-вид. арк. 5,23. Тираж 50 пр. Зам. № 0325-03/2.

Видавець та виготовлювач СПД Біла К. О.
Свідоцтво про внесення до Державного реєстру
суб'єктів видавничої справи ДК № 3618 від 06.11.09

Надруковано на поліграфічній базі видавця Білої К. О.
Україна, 49000, м. Дніпро, пр. Д. Яворницького, 111, оф. 1
+38 (099) 7805049; +38 (067) 2100256
www.impact.dp.ua e-mail: impact.dnepr@gmail.com