УДК 004.051

О. В. Иванченко, кандидат технических наук,
доцент кафедры информационных систем
и технологий Университета таможенного дела
и финансов
А. П. Буланый, кандидат технических наук,
доцент кафедры информационных систем
и технологий Университета таможенного дела
и финансов
К. В. Смоктий, кандидат экономических наук,
доцент кафедры прикладной математики
и теории систем управления Донецкого
национального университета
О. В. Гавриш, студент Университета
таможенного дела и финансов

КОМПЛЕКСНЫЙ ПОДХОД К ОЦЕНКЕ УЯЗВИМОСТИ КОММЕРЧЕСКИХ ПРОГРАММНЫХ ПРОДУКТОВ

Рассмотрены актуальные вопросы оценки эффективности коммерческих программных продуктов по критерию уязвимости источников информации. Представлен комплексный подход, разработанный на основе использования известных информационных технологий, применение которого позволяет сравнивать соответствующие программные модули путем анализа и контроля их уровня защищенности от уязвимостей. В ходе исследований получены количественные оценки уязвимости различных программных продуктов, к которым относятся: количество уязвимостей, время исправления обнаруженных ошибок, показатель популярности продукта, степень серьезности найденных дефектов и т. д. Результаты исследований представлены в графическом виде.

Ключевые слова: *программные продукты; уязвимость; степень серьёзности дефектов.*

The work is devoted to the degree of software vulnerabilities and urgent issues of reliability of the software (including private). Until now there are no generally accepted measures of reliability programs. But there are tools that help in detecting vulnerabilities in the system. In this article we were selected software products for comparison based on the data about vulnerabilities from public sources. On the basis of the received data were constructed diagrams for visual presentation of the results.

Key words: *software products; vulnerability; degree of seriousness of the defects.*

Постановка проблемы. Необходимость оценки надежности и уязвимости соответствующих программных продуктов является одной из актуальных задач на пути дальнейшего развития IT-индустрии.

Под программным продуктом (далее – ПП) будем подразумевать самостоятельное, отчуждаемое произведение, представляющее собой публикацию текста программы или программ на языке программирования или в виде исполняемого кода [1]. В современных условиях создать идеальный (безошибочный) ПП достаточно сложно, особенно если учитывать проблемы, связанные с наличием уязвимостей и дефектов программного продукта. В рамках рассматриваемой проблемы уязвимость программного обеспечения может быть представлена как недостаток в системе, используя который внешний злоумышленник может намеренно нарушить её целостность и вызвать неправильную работу [2]. В сложившейся ситуации важно иметь возможность применять методический аппарат вероятностной оценки надежности программного обеспечения, использование которого направлено на выбор адекватной модели ПП, с помощью которой затем осуществляется прогнозирование показателей надежности программного обеспечения [3].

Анализ последних исследований и публикаций. Под надежностью программного обеспечения понимают способность ПП безотказно выполнять определенные функции при заданных условиях в течение заданного периода времени с достаточно большой вероятностью [4].

Исходя из указанного, можно сформулировать следующие цели и задачи исследований на уязвимость.

1. Обзор открытых источников информации об уязвимостях ПП.
2. Изучение структуры основных источников информации об уязвимостях.
3. Выбор ПП для сравнения и поиск информации, доступной по этим продуктам в различных источниках.
4. Приобретение навыков структурирования данных и использования их для оценки и сравнения показателей надежности ПП.
5. Выполнение оценки и сравнения продуктов на основе полученных данных, построение графиков и диаграмм для визуального представления результатов исследований.
6. Анализ возможных способов оценки и сравнение ПП на базе открытых источников информации.
7. Исследование зависимостей между различными показателями оцениваемых ПП на основе использования обобщенного критерия, который учитывает количество уязвимостей, время существования продукта, его популярность в IT-среде, степень серьёзности найденных дефектов и т. п.

Для того чтобы улучшить качество использования по назначению соответствующего программного обеспечения (далее – ПО), необходимо предварительно на различных этапах жизненного цикла ПО своевременно выявлять и устранять ошибки. Поэтому на протяжении многих лет проводились различные исследования, конечной целью которых являлся разносторонний анализ выявленных ошибок, изучение их свойств и условий, в которых они протекают.

Известно, что уязвимости ПО являются одной из основных проблем обеспечения компьютерной безопасности. Анализ различных методов оценки уязвимостей программного обеспечения, включая статистические методы, применяемые для тестирования соответствующих ПП, описаны в работе Бинг Чан Лю [5].

Следует отметить, что своевременное выявление и устранение уязвимостей ПО позволит предотвратить возможные атаки. Один из вариантов решения этой задачи представлен в работе В. А. Сердюка [6].

Цель статьи – комплексный анализ коммерческих программных продуктов на основе оценки их уязвимости и имеющейся в свободном электронном доступе информации об их дефектах.

Изложение основного материала. Для решения поставленной задачи был проведен анализ следующих программных продуктов: СУБД Oracle и Microsoft Access, а также web-браузеров Opera и Google Chrome. Выборка данных по качественной оценке уровня серьезности дефектов для соответствующих ПП с использованием известного ресурса NVD представлена в табл. 1–4. Фактически в указанных таблицах содержатся данные об уровне серьезности вскрытых дефектов (Low, Medium, High) для коммерческих программных продуктов, которые разработаны филиалами четырех IT-компаний, а именно: Oracle, Microsoft, Opera, Google Chrome.

В табл. 1–4 указано название ресурса, который представил данные в указанный срок; качественный уровень серьезности вскрытых дефектов; количественная оценка серьезности по 10-бальной шкале компании в целом; количественная оценка серьезности по 5-бальной шкале соответствующих филиалов приведенных компаний. Рассмотрим, каким образом можно использовать приведенные данные для получения соответствующих графических зависимостей.

Таблица 1

Выборка данных филиалов компании Oracle

CVEID	Опубликовано	Уровень серьёзности дефектов	CVSSScore	Branches Oracle
CVE-2007-0268	16.01.2007	Medium	6,5	2,0
CVE-2008-2992	04.11.2008	High	9,3	2,0
CVE-2009-0217	14.07.2009	Medium	5,0	2,0
CVE-2011-0808	19.04.2011	Medium	4,4	2,0
CVE-2014-3566	14.10.2014	Medium	4,3	2,0

Таблица 2

Выборка данных филиалов компании Microsoft

CVE ID	Опубликовано	Уровень серьёзности дефектов	CVSSScore	Branches Microsoft Access
CVE-2007-2240	15.08.2007	Medium	5,8	2,0
CVE-2008-5416	20.12.2008	High	9,0	2,0
CVE-2010-0806	10.03.2010	High	9,3	2,0
CVE-2012-4792	30.12.2012	High	9,3	2,0
CVE-2014-3566	14.10.2014	Medium	4,3	2,0

Таблица 3

Выборка данных филиалов компании Opera

CVE ID	Опубликовано	Уровень серьёзности дефектов	CVSSScore	Branches Opera
CVE-2007-0045	01.03.2007	Medium	4,3	2,0
CVE-2009-3555	09.11.2009	Medium	5,8	2,0
CVE-2011-3389	06.09.2011	Medium	4,3	2,0
CVE-2012-4600	31.08.2012	Low	2,6	2,0
CVE-2013-1489	31.01.2013	High	10,0	2,0

Таблица 4

Выборка данных филиалов компании Google Chrome

CVE ID	Опубликовано	Уровень серьёзности дефектов	CVSSScore	BranchGoogle Chrome
CVE-2017-0045	03.01.2007	Medium	4,3	2,0
CVE-2011-3389	06.09.2011	Medium	4,3	2,0
CVE-2013-1489	31.01.2013	High	10,0	2,0
CVE-2014-1568	25.09.2014	High	7,5	2,0

Результат очередного этапа исследований в виде графиков зависимостей суммарного количества выявленных уязвимостей за определенный период времени для различного ПО представлен на рис. 1–3. Соответствующие оценки получены с использованием методического аппарата и информационных технологий, изложенных в [3; 7].

Следует, что по показателю суммарного количества уязвимостей СУБД Oracle уступает Microsoft Access (рис. 1), что, конечно, вызывает определенные сомнения у активных пользователей ПП Oracle. Отметим, авторы не претендуют на “истину в последней инстанции”, тем более что исследования проводились для случая, когда тестирование Oracle было реализовано без применения утилиты Oracle Advanced Security [8]. Как не вызывает сомнения тот факт, что возможность использования указанной утилиты, безусловно, существенно улучшит показатели уязвимости программных продуктов Oracle.

Аналогичные исследования были выполнены для браузеров Opera, Google Chrome (рис. 2). Результаты комплексного оценивания свидетельствуют, что суммарное количество уязвимостей у браузера Google Chrome пусть не существенно, но все же ниже, чем у браузера Opera.

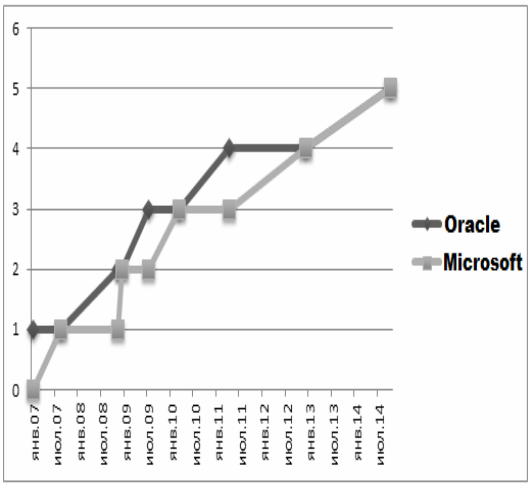

Рис. 1. Зависимость суммарного количества уязвимостей СУБД Oracle и Microsoft Access за фиксированный период времени

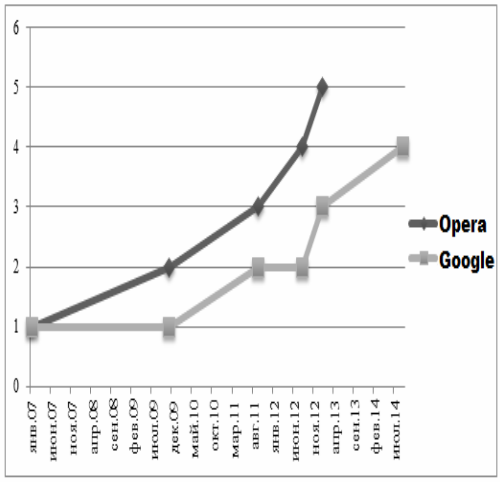

Рис. 2. Зависимость суммарного количества уязвимостей web-браузеров Opera и Google Chrome за фиксированный период времени

Обобщив полученные результаты исследований, отметим, что, начиная с 2007 г., СУБД Oracle и Microsoft Access,web-браузеры Opera и Google Chrome имели практически одинаковое количество уязвимостей. Однако в соответствии с полученными оценками уязвимости Microsoft Access и Google Chrome устранялись быстрее, чем у их оппонентов. Следовательно, по критерию уязвимости можно утверждать, что ПП Microsoft Access и Google Chrome более надежны, чем Oracle и Opera, соответственно.

Далее следует обратить внимание на уровень критичности обнаруживаемых дефектов [3; 7]. Используя информацию об уровне критичности ошибок, предоставленную базой NVD, получим результаты для СУБД и веб-серверов (рис. 3).

Нетрудно заметить, что большинство обнаруженных уязвимостей имеют средний рейтинг серьёзности. Самые критичные дефекты были обнаружены для СУБД Microsoft Access и web-браузера Google Chrome. Однако дополнительные исследования свидетельствуют, что время, затрачиваемое на устранение уязвимостей у Google Chrome, меньше, чем у Opera.

Одним из главных показателей надежности является время восстановления. Обнаружение и атака на уязвимости программных продуктов сходны с отказом системы. Поэтому в данном случае под временем восстановления можно понимать то время, которое проходит с момента обнаружения уязвимости до момента выпуска разработчиком patches (буквально, заплаты) или версии upgrade с исправлениями предыдущей версии [3].

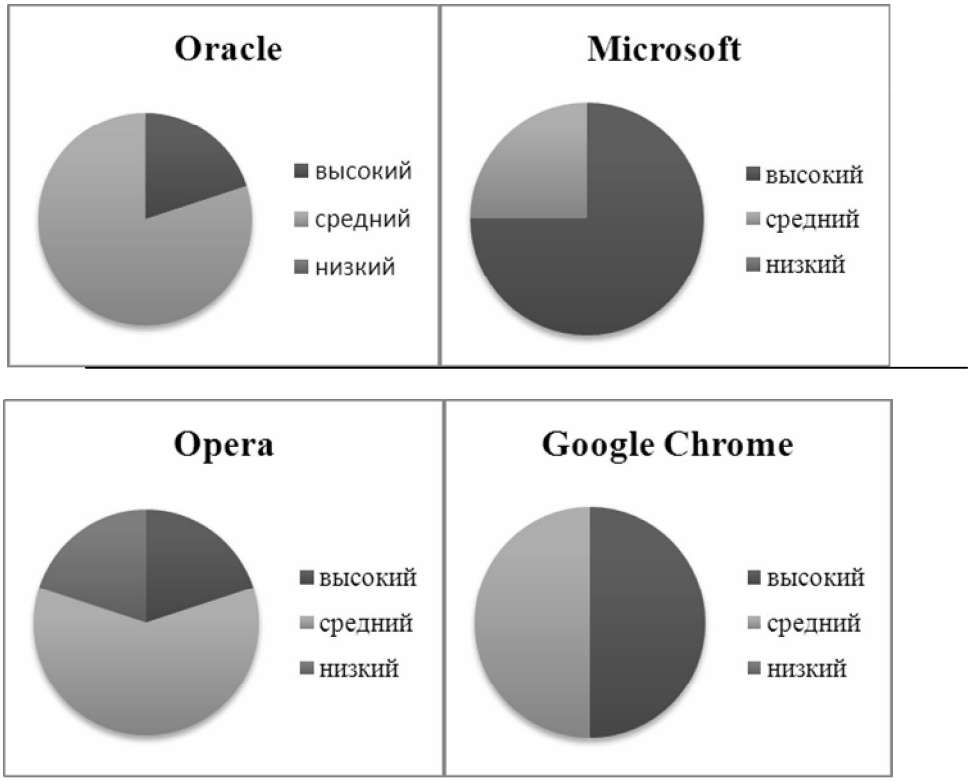

Рис. 3. Диаграммы распределения дефектов
с учетом уровня их серьёзности

Проанализируем, сколько времени требуется коммерческой корпорации Microsoft и Oracle, а также Opera и Google Chrome для того, чтобы исправить обнаруженные уязвимости в их продуктах.

Характеристика процесса обнаружения изложена в [3] и включает в себя следующие этапы:

- уязвимость обсуждается в списках рассылки, и, если она подтверждена, публикуется в качестве предупреждения об опасности;
- затем эта информация распространяется через Интернет-ресурс, в котором ведется учет уязвимости. Причем время появления этой информации на соответствующих сайтах варьируется как от нескольких дней, так и до нескольких лет.

Поэтому для начала необходимо исследовать потенциальные возможности каждого из ресурсов и найти достоверную дату обнаружения каждой уязвимости. Чаще всего уязвимости попадают в библиотеку CVE [3], на которой потом разворачиваются другие ресурсы.

Исправление обновления поддерживаются разработчиками ПП, поэтому дата выпуска исправлений может быть определена из официальных информационных изданий

Microsoft, Oracle, Opera, Google Chrome. То есть, имея всю необходимую информацию, можно расширить таблицы уязвимостей и выполнить соответствующие расчеты.

Результат очередного этапа исследований в виде графиков зависимостей суммарного количества выявленных уязвимостей за определенный период времени для различного ПО представлен на рис. 1–3.

Результаты очередного этапа исследований с использованием данных расширенных таблиц в виде графиков зависимостей суммарного количества выявленных уязвимостей за определенный период времени для различного ПО представлены на рис. 4, 5.

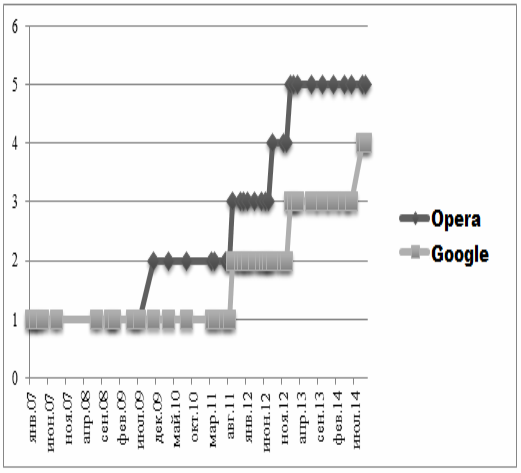

Рис. 4. Зависимость суммарного количества уязвимостей web-браузеров Opera и Google Chrome за фиксированный период времени

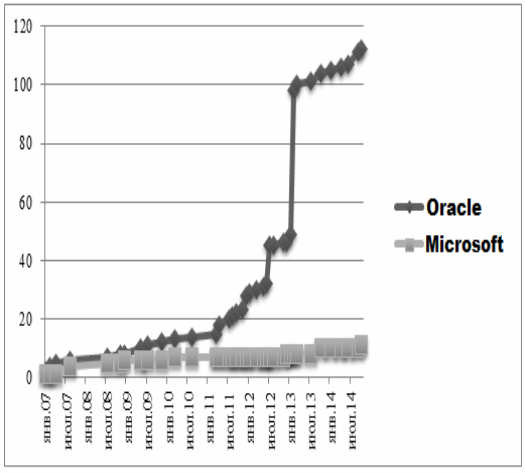

Рис. 5. Зависимость суммарного количества уязвимостей СУБД Oracle и Microsoft Access за фиксированный период времени

Следует (рис. 4), что web-браузер Opera – менее стабильный браузер, имеющий несколько брешей в безопасности, хотя его рейтинг близок Google Chrome. Анализируя представленные на рис. 2, 4 зависимости, можно сделать вывод, что оба браузера достаточно надежны и безопасны.

На рис. 5 представлены результаты исследований суммарной уязвимости соответствующих СУБД. Можно заключить, что по указанному показателю СУБД Oracle – менее стабильная версия с большим количеством брешей в безопасности, чем Microsoft Access. Поэтому СУБД Microsoft Access является достаточно надежной и безопасной по сравнению с СУБД Oracle.

Сравнивая время восстановления для web-браузеров Opera и Google Chrome, СУБД Oracle и Microsoft Access, можно констатировать, что, как правило, исправления обнаруженных уязвимостей выпускаются в течение следующего периода времени:

- Oracle – 122 дня;
- Microsoft Access – 96 дней;
- Opera – 62 дня;
- Google Chrome – 171 день.

Далее получим количественную оценку вероятности безотказной работы программных продуктов [3]. Для этого определим интенсивность отказов каждого ПП за год. По полученным значениям построим график зависимости интенсивности отказов (как число отказов N за период времени t) соответствующих ПП.

Результаты следующего этапа исследований в виде указанных графиков зависимостей представлены на рис. 6, 7. Представленные зависимости получены для ПП Oracle, Microsoft Access, Opera, Google Chrome. Графические зависимости получены в виде столбчатых гистограмм, параметры которых определялись на основе использования методического аппарата и информационных технологий, представленных в [3; 7].

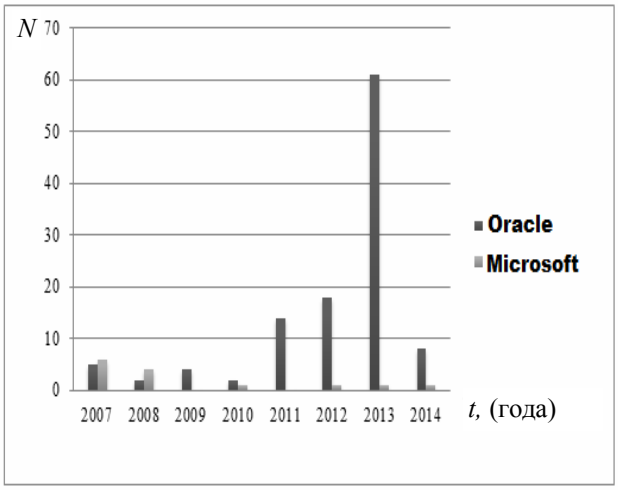

Рис. 6. Интенсивность отказов ПП Oracle и Microsoft Access

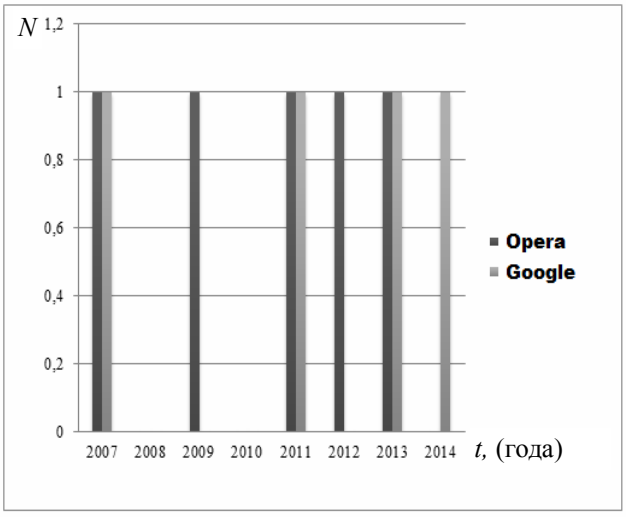

Рис. 7. Интенсивность отказов ПП Opera и Google Chrome

К сожалению, рис. 7 не позволяет выявить лидера по этому показателю среди web-браузеров, тем не менее, скачкообразный характер изменения интенсивностей отказов для СУБД (рис. 6) поддается анализу и может быть использован для сравнения надежности ПП Oracle и Microsoft Access на строго фиксированном интервале годовой периодичности использования программного продукта.

Выводы из данного исследования и перспективы дальнейших исследований в данном направлении. В работе выполнен анализ возможных способов оценки и сравнения программных продуктов по критерию уязвимости с использованием открытых источников информации. Результаты исследований для соответствующих ПП представлены с учетом количества и серьёзности уязвимостей, которые в последствии могут быть использованы для решения patch-задач (в буквальном смысле "накладывание заплат" на места предполагаемых уязвимостей) как в ручном, так и в автоматизированном режимах.

Подводя итог, отметим, что уязвимости ПП и угрозы их возникновения с каждым годом растут. Для эффективной борьбы с ними предприятиям и компаниям IT-сферы следует выделять больше финансовых, интеллектуальных, инновационных и других видов дополнительных ресурсов.

Список использованных источников:

1. Кабашов С. Ю. Делопроизводство и архивное дело в терминах и определениях [Электронный ресурс] : учебное пособие для вузов / С. Ю. Кабашов, И. Г. Асфандиярова. – М. : Флинта: Наука, 2009. – 296 с. – Режим доступа : http://clerical_work.academic.ru/777/ПРОГРАММНЫЙ_ ПРОДУКТ

2. Уязвимость (компьютерная безопасность) [Электронный ресурс] : Свободная энциклопедия, Википедия. – Режим доступа : https://ru.wikipedia.org/wiki/Уязвимость_(компьютерная_безопасность)

3. Скляр В. В. Оценка и экспертиза программного обеспечения. Лекционный материал / Скляр В. В. ; под ред. Харченко В. С. ; Министерство образования и науки Украины, Национальный аэрокосмический университет им. Н. Е. Жуковского "ХАИ", 2008. – 204 с.

4. Надежность программного обеспечения [Электронный ресурс] : финансовый словарь / Финансовый словарь Финам. Академик, 2000. – 2014. – Режим доступа : http://dic.academic.ru/dic.nsf/fin_enc/25453

5. Bingchang Liu Software Vulnerability Discovery Techniques: A Survey / Bingchang Liu, Liang Shi, Zhuhua Cai, Min Li // Fourth International Conference on Multimedia Information Networking and Security, Nanjing, 2–4 Nov., 2012. – P. 152–156.

6. Сердюк В. А. Практические аспекты выявления уязвимостей программного обеспечения [Электронный ресурс] / Сердюк В. А. – Режим доступа : http://dialognauka.ru/press-center/article/10023

7. Оценка качества и экспертиза программного обеспечения. Практикум / А. А. Андрашов, А. А. Гордеев, Е. И. Лобачева, В. С. Харченко ; под ред. В. С. Харченко / Министерство образования и науки Украины, Национальный аэрокосмический университет им. Н. Е. Жуковского "ХАИ", 2009. – 154 с.

8. Oracle Advanced Security [Электронный ресурс]. − Режим доступа : http://www.oracle.com/ru/products/database/options/advanced-security/overview/index.html