УДК 681.321

В.С. Харченко[1], Ю.Л. Поночовный[2], А.А. Фурманов[2], К.А. Васильев[1]

[1] *Национальный аэрокосмический университет имени Н.Е. Жуковского "ХАИ", Харьков*
[2] *Полтавский национальный технический университет им. Ю. Кондратюка, Полтава*

МОДЕЛИ РАЗВИТИЯ УЯЗВИМОСТЕЙ IT-ПРОДУКТОВ: ПАТОЛОГИЧЕСКИЕ ЦЕПОЧКИ В КОНТЕКСТЕ МАРКОВСКОГО АНАЛИЗА

В статье рассмотрены вопросы развития уязвимостей IT-продуктов согласно концепции стандартов ISO15408 «Общие критерии» и ISO18045 «Общая методология». Проводится сопоставление стандартов серии ISO15408 и ISO61508 (функциональной и информационной безопасности) в контексте применения марковских моделей для оценивания безопасности. Дополнительно в модели развития уязвимостей включены уязвимости нулевого дня, неописанные в стандартах. Представлены 7 возможных вариантов событий при развитии уязвимостей, на основании которых сформированы 20 моделей в виде патологических цепочек. Рассмотрены вопросы взвешивания переходов в патологических цепочках на основании стандарта ISO18045.

Ключевые слова: *уязвимости IT-продуктов, эксплойт, патч, патологические цепочки.*

Введение

Возрастание числа, степени детализации и жесткости требований к информационной безопасности (и кибербезопасности) IT-продуктов обусловлено увеличением инцидентов в сфере так называемых safety critical и security critical систем (систем, критичных с точки зрения функциональной и информационной безопасности). Такая тенденция реализуется посредством разработки, и гармонизации и имплементации стандартов в области безопасности.

Положительным аспектом в сфере стандартизации является введение «Общих критериев» [1 – 3] и «Общей методологии» [4] оценки безопасности IT-продуктов. В концепции данных стандартов информационная безопасность связана с определением, достижением и поддержанием ценности IT-активов (в частности, конфиденциальности, целостности и доступности). Несмотря на достаточно жесткий формальный подход к определению и выполнению требований к информационной безопасности, «Общие критерии» не запрещают обоснованно вводить количественные оценки ценности активов в профили защиты и задания по безопасности. Наиболее применимыми на практике являются количественные модели оценки риска потери или повреждения активов информационной безо-

пасности. Стандарты в области оценки риска [5, 6] также являются достаточно гибкими и предлагают выбор более десяти различных методологий моделирования. В рамках этой работы авторы ограничатся вопросами применения марковских моделей в практике оценки информационной безопасности.

Постановка задачи

Следует отметить, что многие исследователи [7 – 9] отмечают близкие и смежные области концепций информационной и функциональной безопасности. Однако, если сопоставить серии стандартов ISO15408 [1-3] и ISO61508 [10,11], то в последней приводятся конкретные примеры применения марковских моделей оценивания показателей функциональной безопасности. Стандарты серии ISO15408 [1 – 3] и ISO18045 [4], к сожалению, не содержат примеров количественной оценки показателей информационной безопасности и ссылаются на модели оценки риска. В работе [7] указывается несколько причин такого разногласия:

– недоработка базы стандартов и сложившиеся традиции в сфере информационной и функциональной безопасности;

– сокрытие и, как следствие, нерепрезентативность данных об инцидентах в сфере информационной безопасности;

– сложность совмещения и идентификации временных и вероятностных параметров уязвимостей, атак и потери активов информационной безопасности.

На сегодня, с учетом прошедшего с момента издания работы [7] времени, сложилась достаточная информативная, стандартная и методологическая база для устранения указанных недостатков и применения марковского аппарата для оценивания показателей информационной безопасности. Это подтверждается тем, что рядом исследований успешно разработаны и исследованы такие модели [12 – 14]. При этом для исследования используется информация об уязвимостях, представленная в открытых базах данных.

Необходимо подчеркнуть, что для разработки таких моделей должно быть сформировано множество сценариев, отражающих атаковую обстановку и стратегию обслуживания уязвимостей (патч-менеджмента). В свою очередь, это множество должно базироваться на постулизации так называемых паталогических цепочек, определяющих логическую связь понятий и событий [8].

Целью данной работы является раскрытие патологических цепочек уязвимостей с целью построения моделей оценки входных параметров марковского анализа функционирования ИТ-продуктов с учетом угроз информационной безопасности.

Анализ терминологии в сфере уязвимостей информационной безопасности ИТ

В первой части стандарта ISO15408 [1] раскрыты виды уязвимостей, что позволяет детализировать типовой жизненный цикл уязвимостей. Основные термины, используемые в работе, сведены в табл. 1.

Таблица 1

Основные термины, раскрывающие события и переходы в жизненном цикле уязвимостей ИТ-продуктов

Термин	Описание
Слабое место, слабость, проблемное место (weakness, W)	Дефект или изъян в коде, проектировании, архитектуре или развертывании программного обеспечения, способный в определенный момент стать уязвимостью или приводить к возникновению других уязвимостей [16].
Уязвимость (vulnerability, V)	Слабое место объекта оценки, которое может быть использовано для нарушения функциональных требований безопасности в некоторой среде [1]. Любое слабое место в программном обеспечении, которое может быть использовано для нарушения системы или содержащейся в ней информации [15]
Эксплойт, эксплоит, сплоит (exploit)	Компьютерная программа, фрагмент программного кода или последовательность команд, использующие уязвимости в программном обеспечении и применяемые для проведения атаки на вычислительную систему [16].
Атака (attack)	Четко определенный набор действий, которые, в случае успеха, приведут либо к повреждению актива или нежелательным операциям [16].
Патч (patch) Обновление (update)	Информация, предназначенная для автоматизированного внесения определённых изменений в компьютерные файлы. Патчем или обновлением называется, в частности, содержащее такую информацию автоматизированное отдельно поставляемое программное средство, используемое для устранения проблем в программном обеспечении или изменения его функционала [16].
Обнаруженная потенциальная уязвимость (encountered potential vulnerabilities, EPV)	Потенциально слабое место объекта оценки, идентифицированные оценщиком при выполнении видов деятельности по оценке, которое может быть использовано для нарушения функциональных требований безопасности [1].
Пригодная для использования уязвимость (exploitable vulnerability, ExV)	Слабое место объекта оценки, которое можно использовать для нарушения функциональных требований безопасности в среде функционирования объекта оценки [1].
Потенциальная уязвимость (potential vulnerability, PV)	Подозреваемая, но не подтвержденная слабость [1].
Остаточная уязвимость (residual vulnerability, ResV)	Слабости, которые не могут быть использованы в среде функционирования объекта оценки, но которые могут быть использованы для нарушения функциональных требований безопасности нарушителем с более высоким потенциалом нападения, чем предполагается в среде функционирования этого объекта оценки [1].
Уязвимость нулевого дня (0day, zero day vulnerabilities, ZdV)	Неустранённые уязвимости (а также вредоносные программы) против которых ещё не разработаны защитные механизмы [16].

Типовой жизненный цикл уязвимостей

На данный момент в стандартах информационной безопасности рассматривается только жизненный цикл уязвимостей с учетом хранилищ так называемой белой зоны. Согласно Vulnerability Disclosure Framework [17] существует девять этапов жизненного цикла.

1. Исследование, результатом которого является превращение теоретической возможности совершить атаку через какую-либо дыру, в реальность, воплощенную т.н. эксплоитом (exploit).

2. Проверка позволяет удостовериться, что уязвимость – это не случайный результат функционирования системы, а свойство, которым можно воспользоваться в любой момент.

3. Уведомление владельца уязвимой системы, которое осуществляется с ним напрямую или через координатора.

4. Оценка владельца уязвимой системы позволяет подтвердить выводы исследователя.

5. Подтверждение является результатом положительной оценки и сигналом исследователю, что владелец будет поддерживать с ним дальнейший контакт для будущих исследований и обсуждения плана раскрытия информации.

6. Устранение заключается в разработке рекомендаций или патча для обнаруженной уязвимости.

7. Тестирование рекомендаций и патча подтверждает, что они негативно не повлияют на работу системы и ее окружения.

8. Выпуск патча и рекомендаций делает их доступными для пользователей.

9. Обратная связь и закрытие кейса завершают жизненный цикл уязвимости.

Уязвимость не всегда пройдет через все эти 9 этапов [12]. Это зависит от исследователя, которому может и не удастся повторить свои действия по идентификации уязвимостей. Это зависит от производителя, который может и не выпустить патч для уязвимости или не сообщить об этом разработчикам и пользователям. Период между созданием эксплоита и устранением уязвимости (разработкой патча) называют «окном возможности» (рис. 1), когда хакер может завладеть системой пользователя без его на то согласия, воспользовавшись обнаруженной незакрытой уязвимостью [12, 17].

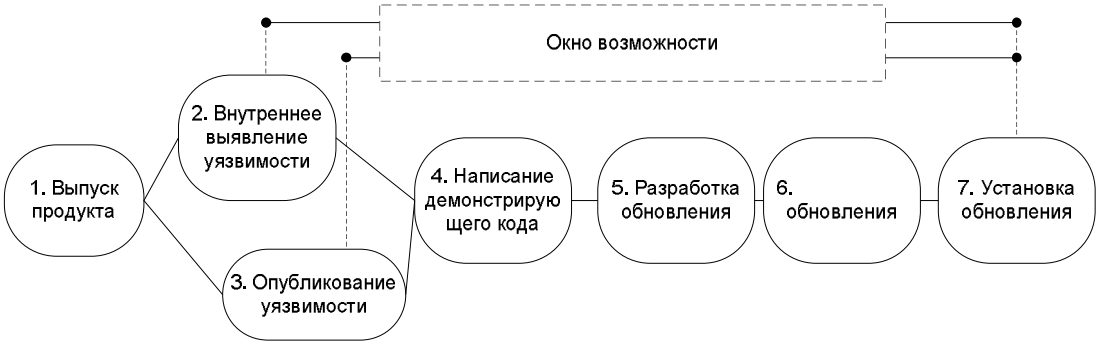

Рис. 1. Диаграмма жизненного цикла программной уязвимости и эксплойта

Простые цепочки событий в модели ЖЦ

На основании определений табл. 1 выделены следующие переходы между событиями жизненного цикла уязвимостей.

1. Слабое место – потенциальная уязвимость. Считается, что все ИТ-продукты имеют слабые места. В процессе идентификации, на основании анализа слабых мест конкретного ИТ-продукта, исследователь должен выделить множество потенциальных уязвимостей. При этом учитывается «глубина» поиска и прогнозируемый потенциал нападения злоумышленников.

2. Потенциальная уязвимость – обнаруженная потенциальная уязвимость. Данный переход моделирует процессы размещения информации про уязвимость в открытых источниках.

3. Потенциальная уязвимость – уязвимость нулевого дня. Переход происходит в случае неразглашения информации об уязвимости в открытых источниках.

4. Любая уязвимость: (обнаруженная потенциальная уязвимость, уязвимость нулевого дня, остаточная уязвимость) – пригодная для использования уязвимость. Данный переход моделирует разработку эксплоита, упрощающего использование уязвимости в случае атаки на ИТ-продукт.

5. Уязвимость – атака на уязвимость. Любая неустраненная уязвимость ИТ-продукта может быть проатакована злоумышленником. Естественно, что после атаки на уязвимость, она становится обнаруженной (переход «атака – обнаруженная потенциальная уязвимость»).

6. Обнаруженная уязвимость – патч (обновление). Переход моделирует устранение выявленных в ИТ-продукте уязвимостей. Характеристикой перехода служит временной промежуток разработки и установки патча (обновления). Важно, что патчем устраняются не все уязвимости, а только выявленные уязвимости с потенциалом нападения, не превышающим заданной величины (переход «патч – остаточная уязвимость»).

7. Уязвимость нулевого дня – обнаруженная уязвимость. Такой переход маловероятен, однако есть факты раскрытия уязвимостей нулевого дня до проведения атак на них [16].

На рис. 2 представлена диаграмма, иллюстрирующая объединение указанных простых цепочек в общую схему. Данная диаграмма позволяет разработать составные патологические цепочки жизненного цикла уязвимостей.

Составные цепочки жизненного цикла уязвимостей ИТ-продуктов

На основании перебора всех возможных вариантов сформировано 20 составных патологических цепочек уязвимостей. Десять из них заканчиваются полным устранением уязвимости после патчеризации, вторая половина приводит к переходу в группу остаточных уязвимостей, обусловленную недооценкой потенциала нападения (рис. 3). Двенадцать цепочек из 20 содержат атаки на уязвимости, остальные 8 благополучно ведут к закрытию уязвимости через патч или обновление.

По критичности для объекта атаки данные патологические цепочки имеют разный вес. Естественно, что первая половина (цепочки №1-10, в конце которых уязвимость полностью устраняется) имеет меньшую критичность по сравнению со второй половиной (цепочки №11-20). Наиболее критичными являются эксплойты уязвимости нулевого дня.

Внесение информации об уязвимости в реестр, с одной стороны, может ускорить разработку патча (что снижает критичность цепочки), с другой – способствовать разработке эксплойта (наоборот, повышает критичность).

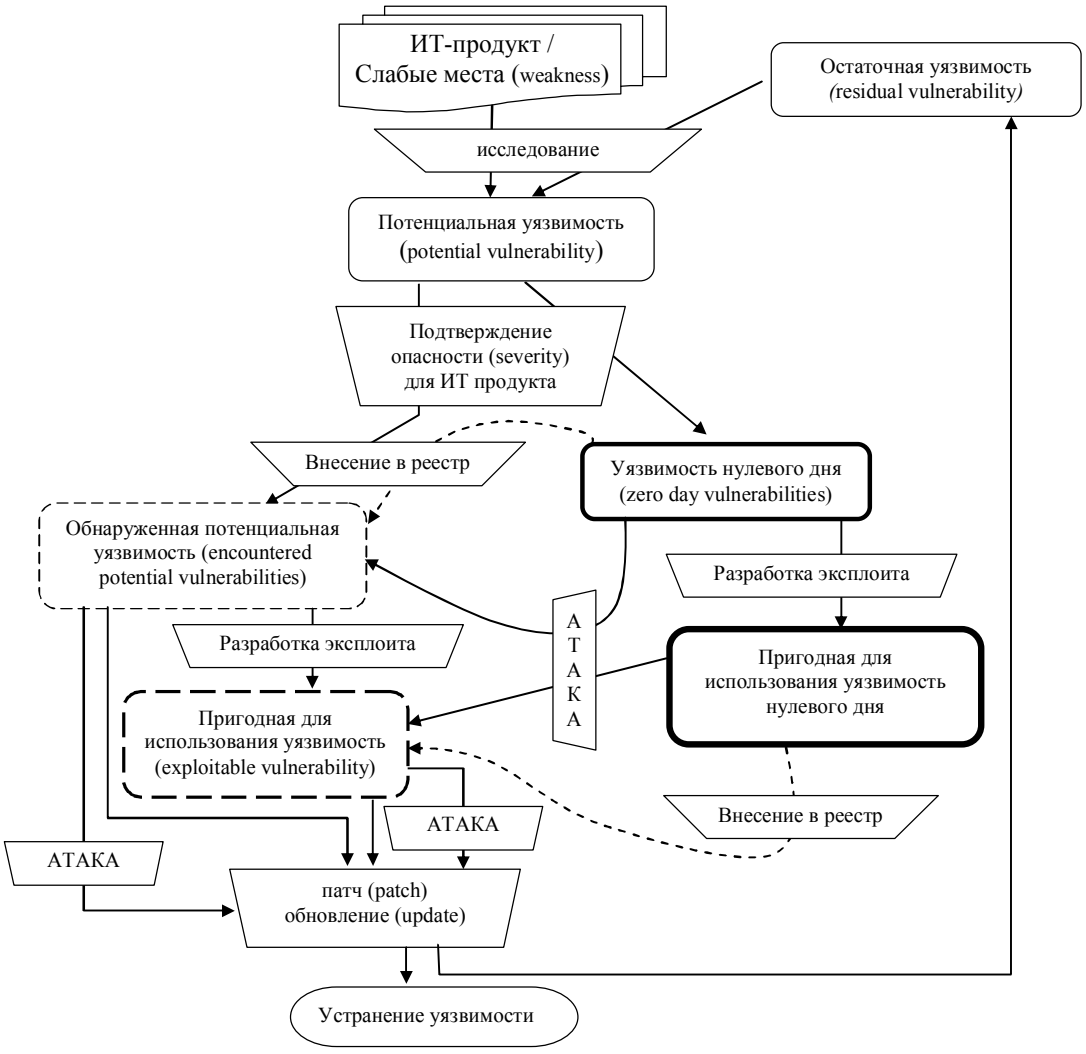

Рис. 2. Диаграмма расширенного жизненного цикла уязвимостей ИТ-продуктов согласно ISO15408 [1] и концепции уязвимостей нулевого дня

Существующие варианты «взвешивания» цепочек

В информативном приложении В стандарта ISO18045 [4] рассматривается пример вычисления потенциала нападения. Вначале указывается на зависимость потенциала нападения от компетентности, ресурсов и мотивации нарушителя.

Далее акцентируется связь третьего фактора – мотивации с вероятностью нападения, ценностью

актива в денежном или ином выражении, а также компетентностью и ресурсами нарушителя

Указывается на возможность указания методов и мер определения уровня мотивации в профиле защиты (ПЗ) на основании знаний автора ПЗ о среде функционирования, в которую будет помещен объект оценки.

В последующем зависимость потенциала нападения от мотивации не рассматривается. Вторая часть методики описывает зависимость потенциала нападения от 5 факторов:

1) общее затрачиваемое время;
2) компетентность;
3) знание объекта оценки;
4) возможность доступа к объекту оценки;
5) оборудование.

В зависимости от составляющих перечисленных факторов и их «аддитирования», вычисляется потенциал нападения, разделяемый на 4 условных уровня: базовый, усиленный базовый, умеренный и высокий. Отдельно выделен потенциал «за пределами высокого» (beyond high).

С точки зрения разработки и применения марковских моделей необходимо выделить временные и вероятностные факторы взвешивания патологических цепочек. Очевидно, что стандарт ISO18045 [4] выделяет явный временной фактор (общее затрачиваемое время) и вероятностные факторы компетентности, знания объекта оценки, возможности доступа, оборудования.

Однако, очевидна и практическая межфакторная взаимосвязь, нераскрытая в стандарте, но важная при построении моделей функционирования реальных ИТ-продуктов. Например, применение заказного оборудования нарушителями-профессионалами явно ускоряет процедуру идентификации уязвимостей в системе.

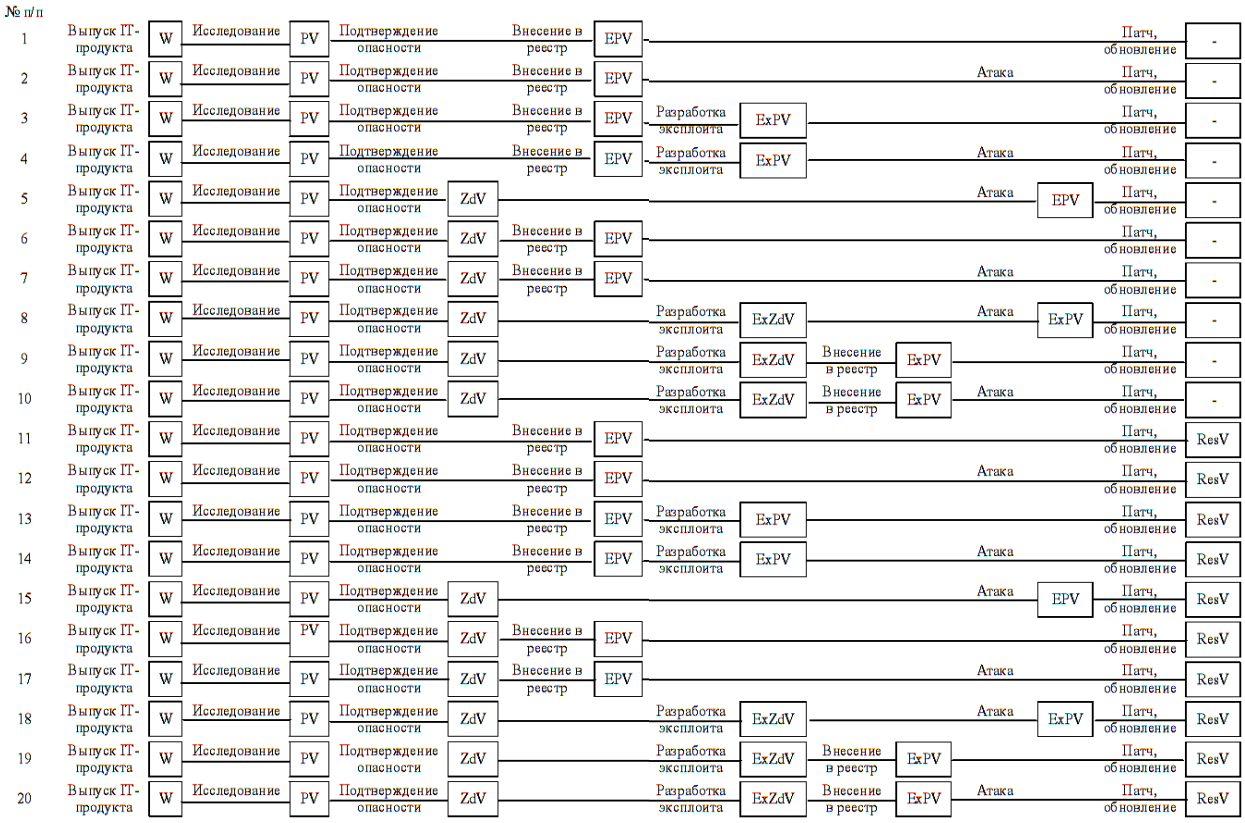

Рис. 3. Модели развития уязвимостей
в виде патологических цепочек

Выводы

В статье представлена расширенная модель жизненного цикла уязвимостей ИТ-продуктов. На основании допустимых комбинаций возможных переходов между состояниями уязвимостей разработаны 20 патологических цепочек развития уязвимостей, которые целесообразно использовать при разработке сценариев обслуживания уязвимостей и управления безопасностью систем.

Следует отметить, что в данной работе автор не ставили цель полной формализации описания соответствующих процессов. Необходимость такой формализации зависит от потенциала ее конструктивности, что может быть предметом дальнейших исследований.

Кроме того, важной задачей является обоснование, разработка и стандартизация методов определения параметров переходов между состояниями уязвимостей и других параметров для марковских

моделей безопасности ИТ-систем с учетом выявления и устранения уязвимостей и атак на них.

Список литературы

1. ISO/IEC 15408-1:2009. Information technology – Security techniques – Evaluation criteria for IT security –- Part 1: Introduction and general model [Text]. – impl. 15.12.2009. – Brussels: European Committee for Electrotechnical Standardization, 2009. – 64 p.

2. ISO/IEC 15408-2:2008. Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional components [Text]. – impl. 15.08.2008. – Brussels: European Committee for Electrotechnical Standardization, 2008. – 240 p.

3. ISO/IEC 15408-3:2008. Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance components [Text]. – impl. 15.08.2008. – Brussels: European Committee for Electrotechnical Standardization, 2008. – 188 p.

4. ISO/IEC 18045:2008. Information technology –- Security techniques – Methodology for IT security evaluation [Text]. – impl. 15.08.2008. – Brussels: European Committee for Electrotechnical Standardization, 2008. – 302 p.

5. IEC 31010:2009. Risk management – Risk assessment techniques [Text]. – impl. 12.01.2009. – Brussels: European Committee for Electrotechnical Standardization, 2009. – 176 p.

6. ГОСТ Р 51901.1-2002. Анализ риска технологических систем. [Текст]. – введ. 07.07.2002. – М.: Изд. стандартов, 2002. – 26 с.

7. Соммервилл Иан. Инженерия программного обеспечения, 6-е издание.: Пер. с англ. [Текст] / Иан Соммервилл. – М.: Издательский дом "Вильямс", 2002. – 624 с.

8. Avizienis A. Basic Concepts and Taxonomy of Dependable and Secure Computing / A. Avizienis, J.-C. Laprie, B. Randell, C. Landwehr // IEEE Transactions on Dependable and Secure Computing. – 2004. – Vol. 1, № 1. – P. 11-33.

9. Конорев Б.М. Прогнозирование вероятности скрытых дефектов критического ПО с заданной точностью [Текст] / Б.М. Конорев, В.В. Сергиенко, В.С. Харченко, Г.М. Жолткевич // Радіоелектронні і комп'ютерні системи. – 2014. – №5(69). – С. 50-54.

10. ISO/IEC 61508-1:2010. Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements [Text]. – impl. 01.05.2010. – Brussels: European Committee for Electrotechnical Standardization, 2010. – 68 p.

11. ISO/IEC 61508-6:2010. Functional safety of electrical/electronic/programmable electronic safety related systems - Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3 [Text]. – impl. 01.05.2010. – Brussels: European Committee for Electrotechnical Standardization, 2010. – 118 p.

12. Roy A. Cyber security analysis using attack countermeasure trees [Text] / A. Roy, Dong Seong Kim, K.S. Trivedi // In: Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research (CSIIRW '10), ACM, New York, 2010. – P. 1-4.

13. Kharchenko V. Web Systems Availability As-sessment Considering Attacks on Service Configuration Vulnerabilities / V. Kharchenko, Alaa Mohammed Abdul-Hadi, A. Boyarchuk, Y. Ponochovny // Seria "Advances in Intelligent Systems and Computing". Volume 286. W. Zamojski et al (editors), Springer International Publishing Switzerland, 2014. – P. 275-284.

14. Белобородов А.Ю. Применение аппарата теории массового обслуживания для исследования процессов выявления и устранения уязвимостей программных средств [Текст] / А.Ю. Белобородов, А.В. Горбенко, В.С. Харченко // Радіоелектронні і комп'ютерні системи. – 2014. – №5(69). – С. 65-69.

15. ISO/IEC 27000:2014. Информационные технологии. Методы обеспечения защиты. Системы управления защитой информации. Общий обзор и словарь [Текст]. – введ. 15.01.2014. – Женева: Международная организация по стандартизации, 2014. – 44 с.

16. Современные методы защиты от киберугроз: Взгляд интегратора [Электронный ресурс] // Александр Матенко, ITBiz – Режим доступа к ресурсу: http://www.itbiz.ua/prezentaczii.html – 26.11.2015 г.

17. NIAC, Vulnerability Disclosure Framework [Электронный ресурс] // National Infrastructure Advisory Council's – Режим доступа к ресурсу: http://www.dhs.gov/interweb/assetlibrary/vdwgreport.pdf – 26.11.2015 г.

Поступила в редколлегию 2.11.2015

Рецензент: д-р техн. наук, проф. Б.М. Конорев, Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Харьков.

МОДЕЛІ РОЗВИТКУ УРАЗЛИВОСТЕЙ ІТ-ПРОДУКТІВ: ПАТОЛОГІЧНІ ЛАНЦЮЖКИ У КОНТЕКСТІ МАРКОВСЬКОГО АНАЛІЗУ

В.С. Харченко, Ю.Л. Поночовний, О.А. Фурманов, К.О. Васильєв

У статті розглянуто питання розвитку вразливостей ІТ-продуктів згідно концепції стандартів ISO15408 «Загальні критерії» і ISO18045 «Загальна методологія».Аналізуються стандарти серії ISO15408 і ISO61508 (функціональної та інформаційної безпеки) у контексті використання марковських моделей для оцінювання безпеки. Додатково у моделі розвитку включено вразливості нульового дня, неописані у стандартах. Представлено 7 можливих варіантів подій при розвитку вразливостей, на підставі яких сформовані 20 моделей у вигляді патологічних ланцюжків. Розглянуто питання зважування переходів в патологічних ланцюжках на підставі стандарту ISO18045.

Ключові слова: *уразливості ІТ-продуктів, експлойт, патч, патологічні ланцюжки.*

MODELS DEVELOPMENT OF IT-PRODUCT VULNERABILITIES: PATHOLOGICAL CHAINS IN CONTEXT OF MARKOVIAN CHAIN-BASED ANALYSIS

V.S. Kharchenko, Y.L. Ponochovniy, A.A. Furmanov, K.A. Vasilyev

The article describes the development of vulnerability of IT-products in accordance with the concept of standards ISO15408 «Common Criteria» and ISO18045 «Common methodology». The series standards ISO15408 and ISO61508 (functional safety and information security) are compared in context of Markovian chain-based safety and security assessment. The model of vulnerability development has been added by zero-day ones, which are not described in the standards. 7 possible options for the event on the development of vulnerability are described, and 20 models in the form of pathological chains are suggested. The tasks of weighing for transitions in pathological chains are considered basing on the standard ISO18045.

Keywords: *vulnerability of IT-products, exploit, patch, pathological chain.*