УДК 004.056

ОПРЕДЕЛЕНИЕ ВЕРОЯТНОСТИ НАРУШЕНИЯ КРИТИЧЕСКИХ СВОЙСТВ ИНФОРМАЦИОННОГО АКТИВА НА ОСНОВЕ CVSS МЕТРИК УЯЗВИМОСТЕЙ

Нурдинов Р.А.

Национальный исследовательский университет информационных технологий, механики и оптики, Санкт-Петербург, Россия (197101, г. Санкт-Петербург, пр. Кронверкский, д. 49), e-mail: org@mail.ifmo.ru

В наше время актуальной становится проблема управления уязвимостями информационной системы. Различные системы оценки уязвимостей, например CVSS, позволяют провести ранжирование уязвимостей на основании их уровней опасности. Возникает необходимость в определении целесообразности применения защитных мер и средств для устранения непропатченных уязвимостей. Для решения этой задачи предлагается использовать риск-ориентированный подход, который позволяет выбрать наиболее оптимальный способ для устранения обнаруженных уязвимостей. Риск предлагается оценивать как комбинацию вероятности нарушения критических свойств информационного актива и величины возникающего при этом ущерба. Для расчета вероятности нарушения конфиденциальности, целостности и доступности информационного актива предлагается использовать значения базовых и временных CVSS метрик уязвимостей информационной системы. Представленный метод позволяет определить вероятностную составляющую риска без привлечения экспертов, поэтому он может быть полезен при построении автоматизированной системы оценки рисков.

Ключевые слова: информационная система, управление уязвимостями, общая система оценки уязвимостей, информационный актив, риск информационной безопасности.

DETERMINING THE LIKELIHOOD OF INFORMATION ASSET CRITICAL PROPERTIES LOSING BASED ON CVSS METRICS OF VULNERABILITIES

Nurdinov R.A.

Research university of information technologies, mechanics and optics, St. Petersburg, Russia (197101, Saint Petersburg, Kronverkskiy pr., 49), e-mail: org@mail.ifmo.ru

Nowadays the problem of information system vulnerability management has become an actual. There are different vulnerability scoring systems, e. g. CVSS, which allow to rank detected vulnerabilities based on their severity values. It is necessary to determinate the feasibility of additional countermeasures using for elimination of unpatched vulnerabilities. To solve this problem the risk-oriented approach is offered, which allows choose the best way for detected vulnerabilities eliminating. It is proposed to assess the risk as combination of the likelihood of information asset critical properties losing, and the impact caused by this. To calculate the probability of information asset confidentiality, integrity and availability losing, it is offered to use base and temporal CVSS metrics of information system vulnerabilities. The presented method allows determine the probability component of risk without expert involvement, thereby it can be useful to build an automated risk assessment system.

Keywords: information system, vulnerability management, common vulnerability scoring system (CVSS), information asset, information security risk.

Введение

В последнее время всё больше конфиденциальной информации хранится и обрабатывается в различных информационных системах (ИС). Практически любой ИС присущи уязвимости, обуславливающие возможность реализации угроз обрабатываемой в ней информации [2]. Примером может служить недавний скандал, связанный с обнаружением уязвимости Heartbleed, которая позволила злоумышленникам получить информацию о банковских картах более чем 200 тысяч пользователей, осуществлявших покупку билетов на сайте РЖД [3].

Процесс управления уязвимостями включает обнаружение, классификацию, оценку и устранение уязвимостей. Для обнаружения уязвимостей используются специальные программные и аппаратные средства, называемые сканерами уязвимостей (MaxPatrol, Nessus, GFI LANguard и другие).

Большинство современных сканеров решают также задачу классификации найденных уязвимостей, используя данные из определённой базы уязвимостей, например Common Vulnerabilities and Exposures (CVE) [4]. Существуют различные системы оценки уязвимостей. Наиболее распространенная и проверенная на практике – Common Vulnerability Scoring System (CVSS). В CVSS для каждой уязвимости рассчитывается базовая оценка в интервале от 0 до 10. Затем определяется уровень опасности уязвимости по специальной шкале. Таким образом, CVSS позволяет ранжировать найденные уязвимости и определять приоритеты их устранения.

Некоторые уязвимости устраняются с помощью патчей. Использование патчей возможно в том случае, если производителем программного обеспечения (ПО) было выпущено обновление, позволяющее устранить обнаруженную уязвимость. Если такое обновление не было выпущено, то уязвимость можно частично или полностью устранить за счет использования дополнительных мер и средств защиты, что, в свою очередь, требует определённых финансовых затрат. Поэтому особо остро стоит задача определения эффективности их применения для устранения обнаруженных уязвимостей. Для решения данной задачи предлагается использовать риск-ориентированный подход.

Цель исследования – разработать метод для определения вероятности нарушения критических свойств информационного актива на основе CVSS метрик уязвимостей. Данный метод позволит оценить риск, связанный с эксплуатацией уязвимостей ИС, и определить эффективность использования дополнительных мер и средств защиты для их устранения.

Оценка риска для информационной системы

Согласно наиболее распространённому подходу, зафиксированному в стандарте ISO/IEC 27005 [1], значение риска может быть определено по формуле:

$$R = \sum_{j=1}^{n} P_r^j \cdot I^j , \qquad (1)$$

где R – значение риска;

P_r^j – вероятность реализации j-й угрозы;

I^j – значение ущерба от реализации j-й угрозы;

n – число угроз.

Формула (1) универсальна для всех типов объектов защиты, к которым могут относиться информационные активы (ИА), ПО, технические средства (ТС) и другие.

В стандарте NIST 800-37 представлен трехуровневый подход к оценке риска, в соответствии с которым выделяют уровень информационных систем (ИС), уровень бизнес-процессов и уровень организации [8]. На уровне ИС происходит идентификация ИА, уязвимостей и угроз, а также применяемых средств и мер защиты. Этой информации достаточно для определения вероятности возникновения ущерба.

Величина ущерба определяется преимущественно на уровнях бизнес-процессов и организации с привлечением владельцев бизнес-процессов, руководства компании и прочих заинтересованных лиц. На данном этапе исследования задача определения величины ущерба от нарушения свойств ИА не ставится, что позволяет не рассматривать два верхних уровня подхода, представленного в NIST 800-37, а остановиться на уровне ИС.

Процесс обеспечения информационной безопасности направлен на обеспечение критических свойств ИА, к которым чаще всего относят конфиденциальность, целостность и доступность. В методе предлагается отдельно определять значения риска от потери конфиденциальности, целостности и доступности ИА. При этом сумма значений риска, связанных с потерей отдельных критических свойств ИА, будет составлять полный риск ИА. С учетом этого формула для определения величины полного риска ИА приобретает вид:

$$R = P_c \cdot I_c + P_i \cdot I_i + P_a \cdot I_a , \qquad (2)$$

где P_c, P_i, P_a – вероятности нарушения конфиденциальности, целостности и доступности ИА соответственно;

I_c, I_i, I_a – значения ущерба, возникающего при нарушения конфиденциальности, целостности и доступности ИА соответственно.

Преимущество данного подхода в том, что нет необходимости для каждой пары «угроза-уязвимость» определять значение ущерба. Это позволяет отдельно оценивать вероятности нарушения критических свойств ИА и значения ущерба от нарушения этих свойств.

Обычно при оценке риска сначала определяется перечень актуальных угроз, а уязвимости лишь характеризуют возможность их реализации. В предлагаемом методе акцент смещается с угроз на уязвимости. Вместо вероятности реализации угрозы определяется вероятность эксплуатации уязвимости, которая учитывает как вероятность наличия уязвимости, так и вероятность её использования хотя бы одной из угроз.

Сам факт успешной эксплуатации уязвимости не обязательно влечёт за собой нарушение критических свойств ИА. Поэтому для каждой уязвимости необходимо определять вероятности того, что её эксплуатация приведет к нарушению критических свойств ИА. Считается, что уязвимости независимы друг от друга, поэтому эксплуатация

одной из них не обязательно приведёт к эксплуатации других. С учетом этого для расчета вероятностей нарушения критических свойств ИА предлагаются следующие формулы:

$$P_c = (1 - \prod_{j=1}^{m}(1 - P_e^j \cdot P_c^j)),$$
$$P_i = (1 - \prod_{j=1}^{m}(1 - P_e^j \cdot P_i^j)),$$
$$P_a = (1 - \prod_{j=1}^{m}(1 - P_e^j \cdot P_a^j)), \quad (3)$$

где P_e^j – вероятность эксплуатации j-й уязвимости.

Использование метрик CVSS для определения вероятности нарушения критических свойств ИА

Система CVSS включает три группы метрик: базовые, временные и контекстные (рисунок 1) [7].

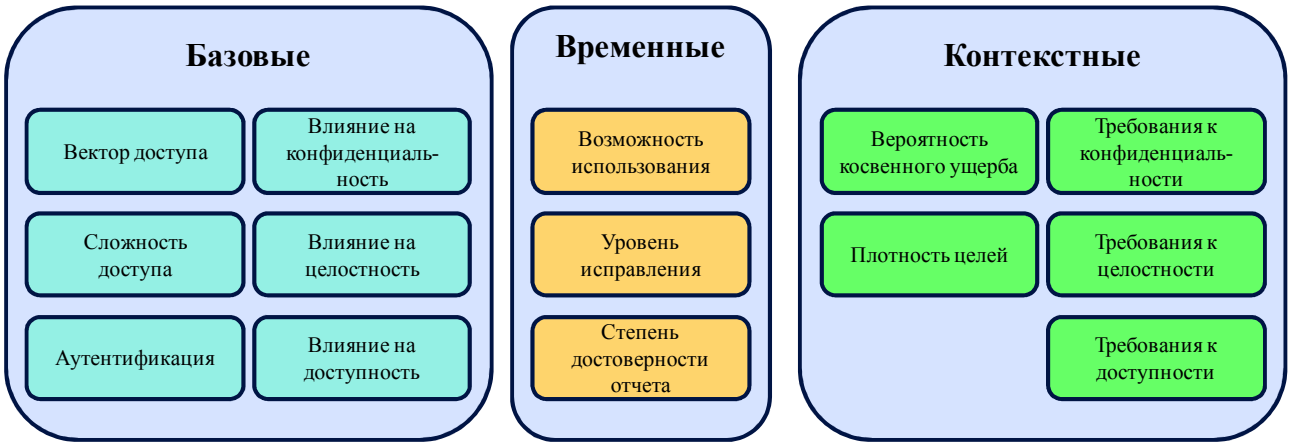

Рисунок 1 – Метрики CVSS

Базовые метрики отображают основные характеристики уязвимости, которые не изменяются со временем и не зависят от среды. Они подразделяются на метрики возможности эксплуатации и метрики воздействия. Временные метрики представляют характеристики уязвимости, изменяющиеся со временем и не зависящие от среды. Контекстные метрики представляют характеристики, связанные со средой пользователя, и позволяют оценить уровень ущерба в относительных величинах.

В методе определения вероятности нарушения критических свойств ИА используются базовые и временные метрики, значения которых определяются аналитиками, производителями продуктов в области ИБ или производителями приложений. Поскольку определение величины ущерба выносится за рамки данного исследования, контекстные метрики в работе не используются.

Для определения вероятности эксплуатации уязвимости предлагается использовать базовые метрики возможности эксплуатации, а также временные метрики (таблица 1).

Таблица 1 – Метрики, используемые для определения вероятности эксплуатации уязвимости

Наименование	Описание	Принимаемые значения

Базовые метрики CVSS		
Вектор доступа (AV)	Возможный способ эксплуатации уязвимости	Локальный (0.395) Локально-сетевой (0.646) Сетевой (1)
Сложность доступа (AC)	Уровень сложности атаки	Высокий (0.35) Средний (0.61) Низкий (0.71)
Аутентификация (Au)	Способ аутентификации для эксплуатации уязвимости	Многократная (0.45) Однократная (0.56) Отсутствует (0.704)
Временные метрики CVSS		
Возможность использования (E)	Наличие или отсутствие кода или техники эксплуатации	Непроверенный (0.85) Испытательный (0.9) Функциональный (0.95) Высокий (1) Не определено (1)
Уровень исправления (RL)	Наличие или отсутствие временного или постоянного исправления уязвимости	Официальное исправление (0.87) Временное исправление (0.9) Дополнительные действия (0.95) Не доступно (1) Не определено (1)
Степень достоверности отчета (RC)	Степень конфиденциальности информации о существовании уязвимости и достоверность известных технических деталей	Не подтверждено (0.9) Не доказано (0.95) Подтверждено (1) Не определено (1)

Представленные в таблице 1 метрики являются факторами, влияющими на вероятность эксплуатации уязвимости, которая находится по формуле:

$$P_e = AV \cdot AC \cdot Au \cdot E \cdot RL \cdot RC \qquad (4)$$

Для определения вероятности нарушения критических свойств ИА от эксплуатации уязвимости используются базовые метрики воздействия и дополнительно вводимая метрика взаимосвязи ИА и ПО, у которого была обнаружена уязвимость (таблица 2). Так, ИА может создаваться, изменяться, использоваться ПО, храниться с ПО на одном хосте, разных хостах с возможностью удаленного доступа, либо они могут быть не связанными.

Таблица 2 – Метрики, используемые для определения вероятности нарушения критических свойств ИА от эксплуатации уязвимости

Наименование	Описание	Принимаемые значения
Базовые метрики CVSS		
Воздействие на конфиденциальность (C)	Воздействие уязвимости на конфиденциальность данных системы	Нулевое (0) Частичное (0.275) Полное (0.66)
Воздействие на целостность (I)	Воздействие уязвимости на целостность данных в системе	Нулевое (0) Частичное (0.275) Полное (0.66)

Воздействие на доступность (A)	Воздействие уязвимости на доступность системы	Нулевое (0) Частичное (0.275) Полное (0.66)
Дополнительные метрики		
Взаимосвязь ИА и ПО (IR)	Отражает характер взаимосвязи ИА и ПО, у которого была обнаружена уязвимость	Не связаны (0) Удаленный доступ (0.2) Совместное хранение (0.4), использование (0.6) Изменение (0.8) Создание (1) Не определено (1)

Метрики, представленные в таблице 2, являются факторами, влияющими на значения вероятностей нарушения критических свойств ИА. С учетом этого вероятности нарушения конфиденциальности, целостности и доступности определяются по формулам:

$$P_c = C \cdot IR; \quad P_i = I \cdot IR; \quad P_a = A \cdot IR. \qquad (5)$$

Практические результаты

Метод определения вероятности нарушения критических свойств ИА был применен на практике. С помощью системы контроля защищенности MaxPatrol было проведено сканирование четырех узлов, входящих в состав одной корпоративной сети (рисунок 2).

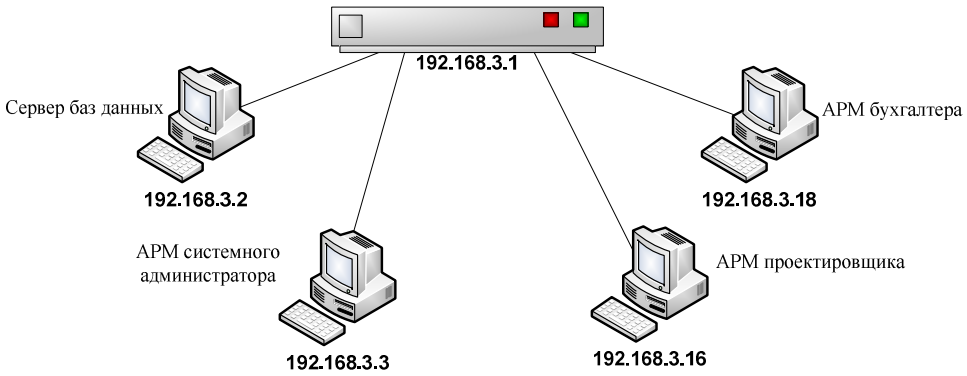

Рисунок 2 – Схема тестовой сети

На данных хостах было обнаружено 37 уязвимостей. На основании данных об этих уязвимостях были определены вероятности нарушения критических свойств, связанных с реализацией уязвимостей различного ПО (таблица 3) и хостов (таблица 4).

Таблица 3 – Вероятности нарушения критических свойств в результате использования уязвимостей программного обеспечения

Программное обеспечение	Критическое свойство	IP-адрес хоста			
		192.168.3.2	192.168.3.3	192.168.3.16	192.168.3.18
Microsoft SQL Server	К	0,528	-	-	-
	Ц	0,528	-	-	-
	Д	0,528	-	-	-
Open SSL	К	0,321	0,321	-	-
	Ц	0,31	0,31	-	-
	Д	0,38	0,38	-	-

Microsoft .NET Framework	К	-	-	0,29	-
	Ц	-	-	0,29	-
	Д	-	-	0,21	-
Microsoft Windows Server 2003	К	0	0,21	-	-
	Ц	0	0,21	-	-
	Д	0	0,21	-	-
Microsoft Windows XP	К	-	-	0,562	0,321
	Ц	-	-	0,507	0,31
	Д	-	-	0,684	0,51
1С Бухгалтерия	К	-	-	-	0,321
	Ц	-	-	-	0,244
	Д	-	-	-	0,244
Remove Desktop Client	К	-	0,21	-	-
	Ц	-	0,21	-	-
	Д	-	0,21	-	-

Таблица 4 – Вероятности нарушения критических свойств в результате использования уязвимостей хостов

Критическое свойство	IP-адрес хоста			
	192.168.3.2	192.168.3.3	192.168.3.16	192.168.3.18
К	0,68	0,576	0,689	0,539
Ц	0,674	0,569	0,65	0,478
Д	0,707	0,613	0,75	0,63

Для пяти ИА, размещенных на данных хостах, были рассчитаны значения вероятностей нарушения критических свойств (таблица 5).

Таблица 5 – Вероятности нарушения критических свойств информационных активов

Информационный актив	IP-адрес хоста	Вероятности нарушения критических свойств		
		К	Ц	Д
База данных	192.168.3.2	0,587	0,583	0,625
Учетные данные пользователей	192.168.3.3	0,373	0,369	0,522
Ключи ЭЦП	192.168.3.3	0,430	0,421	0,523
Проектная документация	192.168.3.16	0,449	0,422	0,522
Бухгалтерская отчетность	192.168.3.18	0,626	0,563	0,638

Выводы и задачи для дальнейшего исследования

Разработанный метод позволяет определить значения вероятностей нарушения критических свойств ИА, что было продемонстрировано на примере. Зная значения ущерба от нарушения критических свойств ИА в стоимостных величинах, можно по формуле (2) рассчитать значение полного риска.

Достоинством предложенного метода является его гибкость. Во-первых, он допускает использование дополнительных метрик. Во-вторых, эксперты в области ИБ могут изменять

числовые значения, соответствующие качественным значениям метрик. В-третьих, благодаря наличию различных сканеров уязвимостей, регулярно пополняемой базы уязвимостей CVE, а также инструментов для обработки данных возможно построение автоматизированной системы оценки рисков. При этом участие пользователей в процессе оценки рисков сводится к минимуму. Такая система может успешно применяться на многих современных коммерческих предприятиях.

Дальнейшее исследование будет направлено на решение второй основной задачи оценки рисков – определение величины ущерба от нарушения критических свойств ИА. Планируется в дальнейшем учитывать статистические данные по фактам эксплуатации различных уязвимостей для конкретной ИС, что позволит скорректировать количественные значения CVSS метрик с учетом особенностей ИС и повысить точность оценки риска.

Список литературы

1. ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности.
2. ГОСТ Р ИСО/МЭК 50922-2006. Защита информации. Основные термины и определения.
3. Хакер : интернет-журнал [Электронный ресурс]. – URL: http://www.xakep.ru (дата обращения: 28.05.2014).
4. CVE database [Электронный ресурс]. – URL: http://cve.mitre.org (дата обращения: 22.04.2014).
5. Joh H. and Malaiya Y.K. A Framework for Software Security Risk Evaluation using the Vulnerability Lifecycle and CVSS Metrics, Proc. International Workshop on Risk and Trust in Extended Enterprises, November 2010, pp. 430-434.
6. Houmb S.H. and Franqueira V.N.L. Estimating ToE Risk Level Using CVSS, International Conference on Availability, Reliability and Security, 2009, pp.718-725.
7. Mell P., Scarfone K., Romanosky S. A Complete Guide to the Common Vulnerability Scoring System Version 2.0, 2007 – 23 с.
8. NIST 800-37 Guide for Applying the Risk Management Framework to Federal Information Systems, 2011.

Рецензенты:

Ныркov А.П., д.т.н., профессор, заведующий кафедрой комплексного обеспечения информационной безопасности ГУМРФ им. адмирала С.О. Макарова, г. Санкт-Петербург.

Каторин Ю.Ф., д.в.н., профессор Национального исследовательского университета информационных технологий, механики и оптики, г. Санкт-Петербург.