УДК 004.75.05

А. Ю. БЕЛОБОРОДОВ, А. В. ГОРБЕНКО, В. С. ХАРЧЕНКО

Национальный аэрокосмический университет им. Н. Е. Жуковского "Харьковский авиационный институт", Украина

ПРИМЕНЕНИЕ АППАРАТА ТЕОРИИ МАССОВОГО ОБСЛУЖИВАНИЯ ДЛЯ ИССЛЕДОВАНИЯ ПРОЦЕССОВ ВЫЯВЛЕНИЯ И УСТРАНЕНИЯ УЯЗВИМОСТЕЙ ПРОГРАММНЫХ СРЕДСТВ

В статье предложены модели, позволяющие описать процессы выявления и устранения уязвимостей в программном обеспечении (ПО). В качестве базовой модели предлагается использовать марковскую цепь, описывающую процесс «гибель-размножение», где под размножением понимается обнаружение новой уязвимости, а под гибелью – устранение уязвимости. Параметры модели могут быть получены на основе статистического анализа баз данных уязвимостей CVE и NVD. Предлагаемые модели можно использовать для расчёта вероятностных показателей, например, вероятности нахождения в системе k уязвимостей, что позволяет количественно оценивать информационную безопасность ПО.

Ключевые слова: *моделирование уязвимостей, марковские цепи, процесс «гибель-размножение», оценка безопасности, программное обеспечение.*

Введение

Проблема информационной безопасности (ИБ) программного обеспечения (ПО) широко обсуждается в ежегодных отчётах международных институтов ИБ, в блогах, в научных работах [1-5].

Информационная безопасность является одной из составляющих гарантоспособности компьютерных систем [1, 6]. Основную угрозу безопасности таких систем представляют уязвимости, прежде всего, программных компонентов. Поиск уязвимостей в программных компонентах является актуальной и ресурсоемкой задачей, которой в последнее время занимаются крупные компании и исследовательские центры. Результаты их работы представляются в виде публичных отчетов и открытых баз данных, информирующих пользователей и производителей программных продуктов об обнаруженных уязвимостях и угрозах информационной безопасности. Например, в 2002 году при Совете по национальной инфраструктуре США (National Infrastructure Concil, NIAC) была создана рабочая группа по раскрытию информации об уязвимостях (Vulnerability Disclosure Working Group, VDWG),, результатом деятельности которой стала разработка 52-х страничного документа «Vulnerability Disclosure Framework» [4], описывающего жизненный цикл процесса раскрытия информации об уязвимостях, начиная с момента выявления отдельной уязвимости и заканчивая этапом ее закрытия с использованием патчей.

В настоящее время информацию об уязвимостях можно получить из общедоступных информационных источников, например Open Source Vulnerability Database (www.osvdb.org), Common Vulnerabilities and Explosures (www.cve.mitre.org), Natioal Vulnerability Database (www.nvd.nist.gov) и других баз данных уязвимостей.

Однако, несмотря на общедоступность информации об уязвимостях программных продуктов, имеющихся данных не достаточно, чтобы количественно оценивать и сравнивать безопасность программных продуктов по одному обобщённому критерию, а также прогнозировать их защищённость от информационных вторжений в будущем. Одна из основных проблем выбора наиболее защищенной конфигурации компьютерной системы заключается в сложности количественной оценки уровня информационной безопасности, а также выбора адекватных показателей для оценки, позволяющих в комплексе учесть все факторы, влияющие на успешное проникновение в систему и размер потенциального ущерба, который может быть нанесён при эксплуатации имеющихся угроз безопасности.

Целью данной статьи является исследование подходов к оценке и прогнозированию уровня информационной безопасности программных средств на основе моделирования процессов выявления и устранения уязвимостей с использованием аппарата марковских процессов.

1. Взаимосвязь между информационной безопасностью, надёжностью и гарантоспособностью компьютерных систем и программных средств

В работе [1] информационная безопасность (security) рассматривается как интегральное свойство, которое включает в себя готовность, целостность и конфиденциальность информации. При этом свойства готовности и целостности одновременно являются и составляющими гарантоспособности (dependability) компьютерных систем наряду со свойствами надежности (reliability), безопасности (safety) и обслуживаемости (maintainability).

Атака на информационную систему, в результате которой система становится недоступной либо должна быть временно приостановлена для обслуживания из-за нарушения целостности либо конфиденциальности данных, является фактически нарушением готовности, что сказывается на надёжностных показателях системы.

Вместе с тем, между информационной безопасностью и надёжностью программных средств можно провести параллель, перенося уже известные термины теории надёжности в область защищённости программных средств. Попытка провести данный анализ была сделана в [2]. Под критерием безопасности информационной системы в указанной работе предлагается рассматривать готовность системы обеспечить защиту информации в процессе эксплуатации, или вероятность того, что в произвольный момент времени информационная система находится в безопасном состоянии. Также в работе [2] предлагается трактовка таких понятий как «отказ защиты», «восстановление защиты», «интенсивность отказов защиты», «интенсивность восстановления защиты».

Угрозами надежности ПО являются отказы вследствие программных дефектов – ошибок, допущенных программистами. Условием проявления дефектов служат определенные данные, поступающие на вход программы в процессе её работы.

Угрозами информационной безопасности также являются отказы, нарушающие готовность системы, целостность или конфиденциальность информации. Причинами этих отказов являются уязвимости – специальный вид дефектов, которые активизируются вследствие злонамеренных действий (хакерских атак, воздействия вирусов, вредоносных программ и др.).

2. Моделирование процессов выявления и устранения уязвимостей с помощью аппарата СМО

Процессы выявления уязвимостей и выпуска программных обновлений (т.н. «заплаток»), устраняющих уязвимости, можно рассматривать как функционирование некоторой системы массового обслуживания, которая обрабатывает заявки на устранение уязвимостей.

Таким образом, в роли *обслуживающих каналов* могут рассматриваться субъекты, занимающиеся устранением уязвимостей. Зачастую в этой роли выступают сами производители ПО (группы разработчиков и инженеров, занимающиеся сопровождением выпущенных программных средств). Выявленные уязвимости, информация о которых распространяется через общедоступные базы данных уязвимостей (CVE, NVD и др.) можно рассматривать как некоторую *очередь ожидания* обслуживания. Обслуживание заявок (разработка и выпуск программных обновлений, устраняющих уязвимость) в очереди происходит либо случайным образом, либо по приоритету, который определяется уровнем критичности уязвимости.

Предварительный анализ процессов обнаружения и устранения уязвимостей показывает, что они могут быть описаны системой массового обслуживания с неограниченной длиной очереди. Параметры системы массового обслуживания могут быть получены и соотнесены с процессами и статистическими данными об обнаружении и устранении уязвимостей следующим образом:

– число обслуживающих каналов n соответствует количеству организаций или групп разработчиков, которые занимаются устранением уязвимости конкретного продукта. В простейшем варианте может быть рассмотрен только один обслуживающий орган;

– интенсивность поступления заявок λ, которая соответствует интенсивности обнаружения уязвимостей в рассматриваемом ПО или системе, может быть получена на основе анализа базы данных уязвимостей CVE (первичной базы) как количество уязвимостей, опубликованных за рассматриваемый промежуток времени (неделя, месяц, год);

– интенсивность обслуживания заявок μ, которая соответствует интенсивности устранения уязвимостей (выпуска обновлений, исправляющих уязвимости) может быть оценена с использованием информации из бюллетеней безопасности, публикуемых компаниями-производителями ПО, а также баз уязвимостей NVD и OSVDB (вторичные базы);

– время обслуживания $T_{обсл}$, которое соответствует параметру «количество дней риска» [2, 5], ко-

торый используется при оценке информационной безопасности компьютерных систем, определяется как усредненный период времени между появлением и устранением отдельных уязвимостей;

– вероятностью обслуживания поступившей заявки Q является вероятностью устранения уязвимости, которая теоретически равна единице; на практике же встречаются ситуации, когда отдельные уязвимости отдельных программных компонентов так и не устраняются;

– вероятность отказа $P_{отк}$ показывает вероятность того, что уязвимость не будет устранена;

– среднее число заявок в СМО $z_{ср}$ показывает среднее количество уязвимостей, которые присутствуют в системе в данный момент времени, и для которых еще не выпущено программное обновление - заплатка; данный показатель является одним из наиболее важных, поскольку определяет количество потенциальных возможностей для атаки информационной системы.

– среднее число заявок в очереди $r_{ср}$ определяет, сколько в среднем уязвимостей опубликовано и ожидает выпуска заплатки для их устранения;

– среднее время пребывания заявки в очереди $t_{оч.ср}$ показывает, сколько в среднем требуется времени для устранения уязвимости с момента её обнаружения;

– среднее число занятых каналов $k_{ср}$ говорит о том, сколько рабочих групп в среднем заняты устранением уязвимости.

3. Процессы выявления и устранения уязвимостей в терминах модели «гибель-размножение»

Рассмотренную выше систему массового обслуживания можно представить в виде системы состояний, в которой каждому состоянию будет соответствовать определённое количество обнаруженных уязвимостей, присутствующих в системе, для которых еще отсутствует рекомендация или программное обновление («заплатка») для устранения. Такие уязвимости будем называть активными.

Таким образом, при выявлении новой уязвимости система будет переходить в следующее состояние, а при выпуске заплатки система будет возвращаться в предыдущее состояние. Подобные процессы эффективно описываются марковскими цепочками «гибели-размножения».

Если принять допущения о том, что каждая уязвимость обнаруживается и исправляется индивидуально в отдельный момент времени, то соответствующая марковская цепочка «гибели-размножения» будет выглядеть так, как это представлено на рисунке 1.

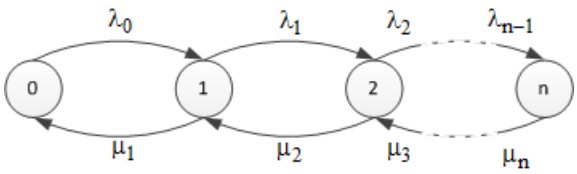

Рис. 1. Простая цепочка «гибели-размножения», описывающая изменения количества активных уязвимостей системы

При этом размножению будет соответствовать обнаружение новой уязвимости, а гибели – выпуск заплатки для её устранения. В рассмотренном случае вероятность нахождения системы в некотором состоянии P_k будет отражать вероятность того, что система имеет k уязвимостей и может быть вычислено по формуле [7]

$$P_k = \frac{\lambda_0\lambda_1...\lambda_{k-1}}{\mu_1\mu_2...\mu_k} P_0 \ (0 \le k \le n), \qquad (1)$$

где λ – частота обнаружения новых уязвимостей;

μ – частота выпуска заплаток;

Статистический анализ баз данных уязвимостей CVE и NVD позволяет сделать допущение о том, что для реальных программных продуктов интенсивность обнаружения новой уязвимости, как правило, не зависит от того, сколько активных уязвимостей в системе уже имеется на данный момент. В таком случае верными будут выражения 2 и 3.

$$\lambda_1 = \lambda_2 = \lambda_3 = ... = \lambda \qquad (2)$$

$$P_k = \frac{\lambda^k}{\mu^k} P_0 \ (0 \le k \le n) \qquad (3)$$

С учётом выражения 2 модель обретёт вид, представленный на рисунке 2.

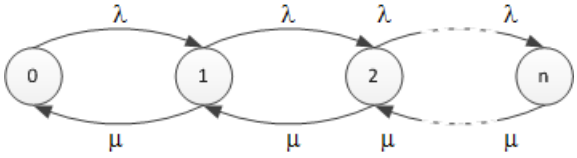

Рис. 2. Модель изменения количества активных уязвимостей системы с неизменной интенсивностью обнаружения новых уязвимостей

В то же время для реальных программных продуктов имеет место как одиночное обнаружение/устранение уязвимостей, так и групповое, когда, например, в базе данных CVE в один день публикуется «пакет» уязвимостей обнаруженных в некотором программном продукте или же вендором выпускается программное обновление, исправляющее сразу группу уязвимостей.

В случае группового обнаружения/устранения уязвимостей имеют место переходы не только в соседние состояния, но и в последующие (предыдущие) сразу на несколько состояний вперед (при

групповом обнаружении уязвимостей) или назад (при групповом исправлении уязвимостей). Примеры таких моделей представлены на рисунках 4 и 5.

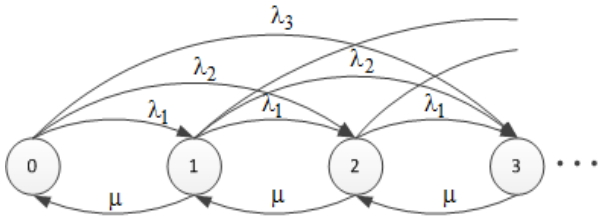

Рис. 4. Пример модели «гибели-размножения» при групповом обнаружении уязвимостей

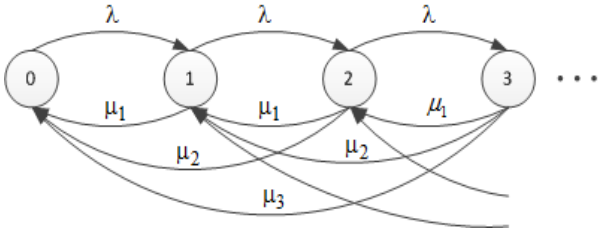

Рис. 5. Пример модели «гибели-размножения» при групповом устранении уязвимостей

Наиболее общим случаем можно считать групповое обнаружение и групповое устранение уязвимостей (см. рисунок 6).

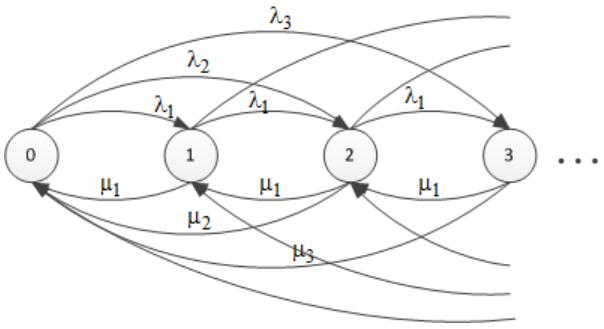

Рис. 6. Пример модели «гибели-размножения» при групповом обнаружении и групповом устранении уязвимостей

Запишем уравнение Колмогорова для состояния S_0 для графа, приведенного на рисунке 6 (см. формулу 4).

$$\frac{dP_0(t)}{dt} = -(\lambda_1 + \lambda_2 + \lambda_3)P_0 + \mu_1 P_1 + \mu_2 P_2 + \mu_3 P_3 + \ldots \quad (4)$$

Очевидно, что модель состояний и переходов, отображающая процесс обнаружения/исправления уязвимостей для реально существующей системы, может оказаться весьма сложной в силу множества возможных состояний и множества вариантов перехода из одного состояния в другое.

Для упрощения можно перейти к модели, показанной на рис. 2, при этом предположив, что существует некоторая $\lambda_э$, которая показывает обобщённую (эквивалентную) интенсивность переходов из состояний 0…i-1 в состояние i, а также некоторое $\mu_э$, показывающее обобщённую интенсивность перехода в состояние i из состояний i+1…n.

Заключение

В статье рассмотрена взаимосвязь между свойствами и понятиями информационной безопасности, надёжности и гарантоспособности компьютерных систем и программного обеспечения. Предложены модели описания процессов обнаружения и исправления уязвимостей с помощью марковских цепочек «гибели-размножения» и выполнено соотнесение между показателями систем массового обслуживания и показателями, оценивающими уровень информационной безопасности компьютерной системы с учетом уязвимостей программных компонентов.

Для практического использования моделей «гибели-размножения» с целью оценки информационной безопасности компьютерных систем актуальной является задача определения эквивалентных значений интенсивностей обнаружении и исправлении уязвимостей программных средств на основе статистического анализа информации из баз данных уязвимостей и бюллетеней безопасности, публикуемых вендорами.

В дальнейшем планируется получение аналитических выражений для оценки показателей информационной безопасности в рамках рассмотренных моделей, а также их развитие с учетом , критичности уязвимостей и вероятности совершения успешной атаки на уязвимость, которая зависит от наличия эксплоитов (программ, фрагментов программного кода или команд, автоматизирующих процесс использования уязвимостей) и других факторов.

Литература

1. Avizienis, A. Basic Concepts and Taxonomy of Dependable and Secure Computing [Текст] / A. Avizienis, J. C. Lapri, B. Randel // IEEE Transactions on Dependable and Secure Computing. – 2004. – Vol. 1, № 1. – P. 11–33.

2. Щеглов, А. Ю. Безопасность современных ОС «в цифрах» [Электронный ресурс] / А. Ю. Щеглов. – Режим доступа: http://blogs.csoonline.com/days_of_risk_in_2006 (2006)

3. 15th Annual CSI/FBI Computer Crime and Security Survey. Executive Summary [Text]. – CSI, FBI, 2010. – 17 p.

4.Vulnerability Disclosure Framework:Final Report and Recommendations by the Council [Text]. – Washington : NIAC, 2004. – 52 p.

5. Jones, J. Days-of-risk in 2006: Linux, Mac OS X, Solaris and Windows [Электронный ресурс] / J. Jones – Режим доступа: http://blogs.csoonline.com/days_of_risk_in_2006 (2006)

6. Горбенко, А. В. Гарантоспособные системы, сети и сервисы [Текст]: практикум / А. В. Горбенко, О. М. Тарасюк ; под ред. В. С. Харченко. – Харьков : Национальный аэрокосмический университет им. Н. Е. Жуковского «ХАИ», 2008. – 125 с.

7. Вентцель, Е. С. Прикладные задачи теории вероятностей [Текст] / Е. С. Вентцель, Л. А. Овчаров. – Москва : Радио и связь, 1983. – 414 с.

Поступила в редакцию 10.03.2014, рассмотрена на редколлегии 24.03.2014

Рецензент: д-р техн. наук, проф. В. А. Заславский, Киевский национальный университет им. Тараса Шевченко, Киев, Украина.

ЗАСТОСУВАННЯ АППАРАТУ ТЕОРІЇ МАСОВОГО ОБСЛУГОВУВАННЯ ДЛЯ ДОСЛІДЖЕННЯ ПРОЦЕССІВ ВИЯВЛЕННЯ ТА УСУНЕННЯ ВРАЗЛИВОСТЕЙ ПРОГРАМНИХ ЗАСОБІВ

О. Ю. Білобородов, А. В. Горбенко, В. С. Харченко

В статті запропоновані моделі, що дозволяють описувати процеси виявлення та усунення вразливостей в програмному забезпеченні (ПЗ). В якості базової моделі пропонується використовувати марковський ланцюг, що описує процес «загибель-розмноження», де під розмноженням розуміється виявлення нової вразливості, а під загибеллю – усунення вразливості. Параметри моделі можуть бути отримані на основі статистичного аналізу баз даних вразливостей CVE та NVD. Моделі, що пропонуються, можна застосовувати для розрахунку низки ймовірнісних показників, наприклад, ймовірності знаходження в системі k вразливостей, що дозволяє кількісно оцінити інформаційну безпеку ПЗ.

Ключові слова: моделювання вразливостей, марківські ланцюжки, процес «загибель-розмноження», оцінка безпеки, програмне забезпечення.

QUEUING THEORY APPLICATION TO STUDY DISCLOSURE AND ELIMINATION PROCESSES OF SOFTWARE VULNERABILITIES

O. Y. Biloborodov, A. V. Gorbenko, V. S. Kharchenko

The models which allow describing disclosure and elimination processes of software are proposed. Using Markov's chain «birth and death» is proposed as a basic model where under the birth is understood disclosure of a new vulnerability and under the death is understood elimination of a vulnerability. Parameters of the model can be got from static analysis of vulnerability databases such as CVE and NVD. The proposed models can be used to calculate a number of probabilistic marks, for instance probability of presence k vulnerabilities in a system that allow quantifying of software security.

Keywords: modeling of vulnerabilities, Markov's chains, «birth and death» chains, security assessment, software.

Белобородов Александр Юрьевич – аспирант кафедры компьютерных систем и сетей Национального аэрокосмического университета им. Н.Е. Жуковского «ХАИ», Харьков, Украина, e-mail: A.Beloborodov@csn.khai.edu.

Горбенко Анатолий Викторович – д-р техн. наук, профессор кафедры компьютерных систем и сетей Национального аэрокосмического университета им. Н.Е. Жуковского «ХАИ», Харьков, Украина, e-mail: A.Gorbenko@csn.khai.edu.

Харченко Вячеслав Сергеевич – д-р техн. наук, профессор, заведующий кафедрой компьютерных систем и сетей Национального аэрокосмического университета им. Н.Е. Жуковского «ХАИ», Харьков, Украина, e-mail: V.Kharchenko@khai.edu.