УДК 004.05

О. Е. ФЕДОРОВИЧ, Ю. А. ЛЕЩЕНКО

Национальный аэрокосмический университет им. Н. Е. Жуковского «ХАИ», Украина

РАЗРАБОТКА И ЭКСПЛУАТАЦИЯ КАЧЕСТВЕННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ В УСЛОВИЯХ КИБЕРПРЕСТУПНОСТИ

Рассматривается и решается задача разработки и эксплуатации качественного программного обеспечения (ПО) в условиях киберпреступности. Представлены две части для решения задачи. В первой части ставится и решается задача минимизации рисков, времени, затрат и ущербов для обеспечения устойчивости разрабатываемого ПО к возможным кибератакам методом целочисленного булевого программирования. Во второй части осуществляется моделирование во времени манипуляций киберпреступников и ответных действий специалистов ПО при эксплуатации систем методом имитационного событийного моделирования с использованием агентного представления основных модулей.

Ключевые слова: *последствия кибератак, оптимизация и минимизация ущербов, агентная модель.*

Введение

Разработка и эксплуатация современного программного обеспечения (ПО) осуществляется, в настоящее время, в условиях возрастания кибератак. Разработчики, на стадии проектирования и тестирования ПО, уделяют большое внимание поиску уязвимостей и минимизации риска последствий кибератак [1]. Существуют стандартные требования и процедуры защиты которых направлены на минимизацию уязвимостей. На это тратится значительное время, и выделяются добавочные финансовые ресурсы. В свою очередь совершенствуются методы и способы кибератак. Задача киберпреступников заключается в поиске уязвимостей и формировании «бреши» в эксплуатируемом ПО, локализации полученной «бреши» и организации устойчивой работы для кражи конфиденциальной информации, изменения функциональности решаемых задач, контроля за результатами работы ПО и нарушения задач управления (особенно это важно для систем критического применения) [2]. В данной публикации проводится оптимизация затрат и моделирование действий разработчиков ПО и киберпреступников для минимизации ущерба и последствий кибератак. Отсюда следует актуальность темы представленной публикации.

Постановка задачи исследования

Работа состоит из двух частей. В первой части ставится и решается задача минимизации рисков, времени, затрат и ущербов для обеспечения устойчивости разрабатываемого ПО к возможным кибератакам. Во второй части, с помощью агентного моделирования, осуществляется имитация во времени действий киберпреступников и ответных действий специалистов ПО при эксплуатации разработанных систем.

Опыт по созданию ПО в конкретной предметной области, а также наличие статистики действий киберпреступников позволяют выявить множество типовых уязвимых ПО [2].

Пусть для каждой i – ой ($i = \overline{1,n}$) уязвимости можно представить множество j_i – х ответных стратегий защиты $j_i = \overline{1,n_i}$, где n_i – количество возможных стратегий защиты для i – ой уязвимости. Каждая стратегия защиты характеризуется риском – r_{ji}, временем $-t_{ji}$, финансовыми затратами на её реализацию – v_{ji} и возможным ущербом от действий киберпреступников – w_{ji}.

Необходимо решить задачу оптимизации по выбору рациональной стратегии защиты ПО с учётом допустимого риска, времени и финансовых затрат на разработку, а также возможного ущерба.

После выбора множества рациональных стратегий необходимо провести моделирование стратегий разработчиков и специалистов по эксплуатации ПО в ответ на возможные действия киберпреступников.

Решение задачи исследования

I. Для задачи оптимизации выбора рациональных стратегий защиты ПО от киберпреступников воспользуемся методами целочисленного булевого

программирования [3].

Введём целочисленную булевую переменную x_{ij_i}, которая принимает значения из множества $x_{ij_i} \in \{0;1\}$, где $x_{ij_i} = 1$, означает, что для парирования i – ой уязвимости выбрана j_i – ая стратегия защиты, $x_{ij_i} = 0$ – в противном случае. При этом $\sum_{j_i=1}^{n_i} x_{ij_i} = 1$, что означает что для парирования i – ой уязвимости должна обязательно быть выбрана одна из стратегий защиты.

Тогда, с учётом переменных x_{ij_i}, критерии для оценки стратегий защиты ПО от киберпреступников будут представлены следующим образом:

1. Риск правильного выбора и стратегий защиты ПО от кибератак:

$$R = \sum_{i=1}^{n} \sum_{j_i=1}^{n_i} x_{ij_i} r_{ij_i}.$$

2. Время на разработку стратегий защиты от кибератак при проектировании (модернизации) ПО:

$$T = \sum_{i=1}^{n} \sum_{j_i=1}^{n_i} x_{ij_i} t_{ij_i}.$$

3. Дополнительные финансовые затраты, связанные с разработкой и организацией защиты ПО от киберпрестуников:

$$V = \sum_{i=1}^{n} \sum_{j_i=1}^{n_i} x_{ij_i} v_{ij_i}.$$

4. Возможный ущерб от действий кибепреступников:

$$W = \sum_{i=1}^{n} \sum_{ji=1}^{n_i} x_{i_{ji}} w_{i_{ji}}.$$

Сформулируем постановки задач минимизации затрат, связанных с борьбой с киберпреступностью.

1. Необходимо минимизировать риски, связанные с выбором стратегий защиты от кибепреступников:

$$\min\ R,\ R = \sum_{i=1}^{n} \sum_{j_i=1}^{n_i} x_{ij_i} r_{ij_i}.$$

С учётом ограничений:

$$T = \sum_{i=1}^{n} \sum_{j_i=1}^{n_i} x_{ij_i} t_{ij_i} \le T',$$

$$V = \sum_{i=1}^{n} \sum_{j_i=1}^{n_i} x_{ij_i} v_{ij_i} \le V',$$

$$W = \sum_{i=1}^{n} \sum_{j_i=1}^{n_i} x_{ij_i} w_{ij_i} \le W',$$

где T', V', W' – допустимые значения времени, затрат и ущербов.

2. Необходимо минимизировать время, потраченное на разработку программных средств защиты от киберпреступников:

$$\min\ T,\ T = \sum_{i=1}^{n} \sum_{j_i=1}^{n_i} x_{ij_i} t_{ij_i}.$$

С учётом ограничений:

$$R = \sum_{i=1}^{n} \sum_{j_i=1}^{n_i} x_{ij_i} r_{ij_i} \le R',$$

$$V = \sum_{i=1}^{n} \sum_{j_i=1}^{n_i} x_{ij_i} v_{ij_i} \le V',$$

$$W = \sum_{i=1}^{n} \sum_{j_i=1}^{n_i} x_{ij_i} w_{ij_i} \le W',$$

где R' – допустимое значение риска.

3. Необходимо минимизировать затраты, связанные с доработкой ПО для обеспечения защиты от киберпреступников:

$$\min\ V,\ V = \sum_{i=1}^{n} \sum_{j_i=1}^{n_i} x_{ij_i} v_{ij_i}.$$

С учётом ограничений:

$$R = \sum_{i=1}^{n} \sum_{j_i=1}^{n_i} x_{ij_i} r_{ij_i} \le R',$$

$$T = \sum_{i=1}^{n} \sum_{j_i=1}^{n_i} x_{ij_i} t_{ij_i} \le T',$$

$$W = \sum_{i=1}^{n} \sum_{j_i=1}^{n_i} x_{ij_i} w_{ij_i} \le W'.$$

4. Необходимо минимизировать ущерб от действий киберпреступников:

$$\min\ W,\ W = \sum_{i=1}^{n} \sum_{j_i=1}^{n_i} x_{ij_i} w_{ij_i}.$$

С учётом ограничений:

$$R = \sum_{i=1}^{n} \sum_{j_i=1}^{n_i} x_{ij_i} r_{ij_i} \le R',$$

$$T = \sum_{i=1}^{n} \sum_{j_i=1}^{n_i} x_{ij_i} t_{ij_i} \le T',$$

$$V = \sum_{i=1}^{n} \sum_{j_i=1}^{n_i} x_{ij_i} v_{ij_i} \le V'.$$

5. Многокритериальная постановка задачи. Для её решения необходимо, первоначально, определить важность «вес» α_k предложенных критериев $R, T, V, W,\ k = \overline{1,4}$.

Воспользуемся оценками экспертов по кибер-защите и назначим значение α_k с учётом условия:

$$\sum_{k=1}^{n} \alpha_k = 1.$$

После этого введём комплексный критерий для оценки ответных действий разработчиков ПО от киберпреступников:

$$Q = \alpha_R \hat{R} + \alpha_T \hat{T} + \alpha_V \hat{V} + \alpha_W \hat{W},$$

где $\hat{R}, \hat{T}, \hat{V}, \hat{W}$ – нормированные значения критериев (перевод в относительную шкалу $0 \div 1$):

$$\hat{R} = \frac{R - R'}{R' - R^*},$$

$$\hat{T} = \frac{T - T'}{T' - T^*},$$

$$\hat{V} = \frac{V - V'}{V' - V^*},$$

$$\hat{W} = \frac{W - W'}{W' - W^*},$$

где R^*, T^*, V^*, W^* – минимальные значения R, T, V, W, полученные в результате решения задач 1 – 4.

Необходимо найти:

$$\min Q',$$

$$Q' = \alpha_R \left(\frac{R - R^*}{R' - R^*} \right) + \alpha_T \left(\frac{T - T^*}{T' - T^*} \right) +$$

$$+ \alpha_V \left(\frac{V - V^*}{V' - V^*} \right) + \alpha_W \left(\frac{W - W^*}{W' - W^*} \right) =$$

$$= \frac{\alpha_R}{R' - R^*} \sum_{i=1}^{n} \sum_{j_i=1}^{n_i} x_{ij_i} r_{ij_i} + \frac{\alpha_T}{T' - T^*} \sum_{i=1}^{n} \sum_{j_i=1}^{n_i} x_{ij_i} t_{ij_i} +$$

$$+ \frac{\alpha_V}{V' - V^*} \sum_{i=1}^{n} \sum_{j_i=1}^{n_i} x_{ij_i} v_{ij_i} + \frac{\alpha_W}{W' - W^*} \sum_{i=1}^{n} \sum_{j_i=1}^{n_i} x_{ij_i} w_{ij_i} -$$

$$- \frac{\alpha_R \cdot R^*}{R' - R^*} - \frac{\alpha_T \cdot T^*}{T' - T^*} - \frac{\alpha_V \cdot V^*}{V' - V^*} - \frac{\alpha_W \cdot W^*}{W' - W^*}.$$

II. Моделирование кибератак и ответных действий специалистов, эксплуатирующих ПО.

Для моделирования во времени динамических процессов кибератак и действий специалистов ПО воспользуемся методом имитационного событийного моделирования с использованием агентного представления основных модулей [4]. Выделим следующие агенты моделирования:

– Агент кибератак. Формирует внешние к ПО «заявки», которые поступают в систему по заданному (случайному) закону распределения;

– Агент уязвимостей. Используемый для задания возможного вида уязвимости и для формирования «бреши» в ПО;

– Агент киберпреступник. Используется для формирования стратегии преступного воздействия на ПО (использования данных, нарушение функциональности, внешний контроль и управление ПО и т.д.);

– Агент защитник. Осуществляет выбор и имитацию ответной стратегии специалистов ПО к действиям агента киберпреступника;

– Агент диспетчер. Осуществляет координацию и взаимодействие во времени агентов (следит за временем и списком событий);

– Агент статистики. Собирает промежуточные и выходные результаты моделирования;

– Агент описания ПО. Используется для задания основных данных и характеристик исследуемого ПО.

Для моделирования используются локальные базы данных (ЛБД):

– ЛБД уязвимостей;

– ЛБД стратегий киберпреступника;

– ЛБД стратегий защиты.

Реализация агентной модели осуществляется с помощью платформы JADE [5].

На рис. 1 представлена структура агентной модели.

В результате моделирования можно получить выходные данные:

– количество кибератак за заданный интервал времени;

– количество и виды уязвимостей;

– перечень стратегий киберпреступника использованных на данном интервале времени;

– перечень ответных стратегий защиты и эффективность их применения;

– количество успешных кибератак;

– количество успешных защит.

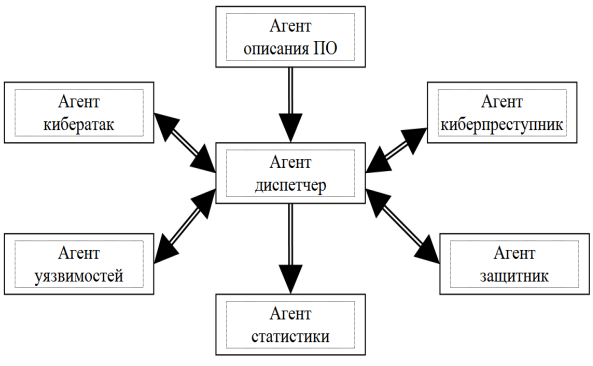

Рис. 1. Структура агентной модели

Заключение

Приложенный подход к разработке и эксплуатации ПО в условиях киберпреступности позволяет на стадии проектирования минимизировать возможные уязвимости в системе. На стадии эксплуатации – прогнозировать и осуществлять эффективные ответные действия по защите ПО от киберпреступников.

Литература

1. Номоконов, В. А. Киберпреступность: проблемы борьбы и прогнозы [Текст] / В. А. Номоконов, Т. Л. Тропина // Библиотека криминалиста. – 2013. – № 5. – С. 148 – 160.

2. Брюховецкий, А. А. Обнаружение уязвимостей в критических приложениях на основе решающих деревьев [Текст] / А. А. Брюховецкий, А. В. Скатков, П. О. Березенко // Радіоелектронні і комп'ютерні системи. – 2013. – № 5 (64). – С. 18 – 22.

3. Сеа, Ж. Оптимизация. Теория и алгоритмы [Текст] / Ж. Сеа ; под ред. А. Ф. Кононенко и Н. Н. Моисеевна ; перевод с фр. яз. Л.Г. Гурина. – М. : Мир, 1973. – 244 с.

4. Прохоров, А. В. Агентное имитационное моделирование процессов управления предприятиями нефтепродуктообеспечения [Текст] / А. В. Прохоров, Амен Соуд Абдалазез Мохаммед // Радіоелектронні і комп'ютерні системи. – 2011. – № 3 (51). – С. 37 – 43.

5. Java Agent DEvelopment Framework [Электронный ресурс] / JADE, сайт. – Режим доступа: http://jade.tilab.com. – 17.02.2014.

Поступила в редакцию 17.01.2014, рассмотрена на редколлегии 12.02.2014

Рецензент: д-р техн. наук, проф., зав. каф. инженерии программного обеспечения И. Б. Туркин, Национальный аэрокосмический университет им. Н. Е. Жуковского «ХАИ», Украина

РОЗРОБКА І ЕКСПЛУАТАЦІЯ ЯКІСНОГО ЗАБЕЗПЕЧЕННЯ В УМОВАХ КІБЕРЗЛОЧИННОСТІ

О. Є. Федорович, Ю. О. Лещенко

Розглядається і вирішується завдання розробки та експлуатації якісного програмного забезпечення (ПО) в умовах кіберзлочинності. Представлено дві частини для вирішення завдання. У першій частині ставиться і вирішується завдання мінімізації ризиків, часу, витрат і збитків для забезпечення стійкості ПО, що розробляється до можливих кібератак методом цілочисельного булевого програмування. У другій частині здійснюється моделювання в часі маніпуляцій кіберзлочинців і відповідних дій фахівців ПО при експлуатації систем методом імітаційного подієвого моделювання з використанням агентного представлення основних модулів.

Ключові слова : наслідки кібератак, оптимізація і мінімізація збитків, агентна модель.

DEVELOPMENT AND EXPLOITATION OF QUALITATIVE SOFTWARE UNDER CYBERCRIME

O. Ye. Fedorovich, Ju. A. Leshchenko

Considered and solved the problem of development and operation of quality software in terms of cybercrime. Are two parts to solve the problem. In the first part of the pose and solve the problem of minimizing risk, time, cost, and damages for the sustainability of the developed software for possible cyberattacks by integer boolean programming. In the second part of the simulation is carried out in time manipulation cybercriminals and response specialists in the operation of software systems by simulation event simulation using agent-based representation of the basic modules .

Keywords: effects of cyber attacks, optimization and minimization of damages, agent model.

Федорович Олег Евгеньевич – д-р техн. наук, проф., зав. каф. информационных управляющих систем, Национальный аэрокосмический университет им. Н. Е. Жуковского «ХАИ», Украина.

Лещенко Юлия Александровна – инженер каф. информационных управляющих систем, Национальный аэрокосмический университет им. Н. Е. Жуковского «ХАИ», Украина.