УДК 004.56 DOI: 10.26102/2310-6018/2020.30.3.021

Метод оценки уровня рисков безопасности узлов сети для повышения эффективности размещения иммунных детекторов

В.Л. Токарев, А.А. Сычугов
Федеральное государственное автономное образовательное учреждение высшего образования «Тульский государственный университет», Тула, Российская Федерация

Резюме: Актуальность исследования обусловлена необходимостью повышения эффективности использования систем обнаружения вторжений, построенных на основе иммунных детекторов. Важное значение для эффективности применения таких систем имеет рациональное размещение иммунных детекторов по отдельным узлам сети. В качестве критерия выбора узлов для установки иммунных детекторов предлагается использовать уровень риска безопасности отдельных узлов сети. В данной статье предлагается метод оценки этой величины, позволяющий выделить наименее защищенные узлы. Оценка риска безопасности узлов сети осложняется тем, что уязвимость часто бывает не единственной. Основная идея, положенная в основу метода - использование статистической формальной модели на основе Марковских цепей в сочетании с графом возможных траекторий и метриками анализа уязвимостей. В качестве метрик анализа уязвимостей используются скоринговые оценки, которые используют три вида метрик: базовые, временные и контекстные. Приведен расчетный пример. Полученная модель может быть использована для определения критических узлов на пути доступа к целевому узлу, в которых нарушители могут быть наиболее опасны. Основываясь на получаемой с помощью модели информации, сетевой администратор может на этих узлах установить иммунные детекторы, что позволит существенно улучшить систему защиты.

Ключевые слова: информационная безопасность, системы обнаружения вторжений, иммунные детекторы, Марковские цепи.

Для цитирования: Токарев В.Л., Сычугов А.А. Метод оценки уровня рисков безопасности узлов сети для повышения эффективности размещения иммунных детекторов. *Моделирование, оптимизация и информационные технологии.* 2020;8(3). Доступно по: https://moit.vivt.ru/wp-content/uploads/2020/08/TokarevSychugov_3_20_1.pdf DOI: 10.26102/2310-6018/2020.30.3.021

Method for assessing the level of security risks of network nodes to improve the efficiency of placement of immune detectors

V.L. Tokarev, A.A. Sychugov
Federal State Autonomous Educational Institution of Higher Education "Tula State University", Tula, Russian Federation

Abstract: The relevance of the study is due to the need to improve the efficiency of the use of intrusion detection systems based on immune detectors. The rational placement of immune detectors on separate network nodes is of great importance for the effectiveness of the use of such systems. It is proposed to use the security risk level of individual network nodes as a criterion for selecting nodes for installing immune detectors. In this article, we propose a method for estimating this value, which makes it possible

to single out the least protected nodes. Assessing the security risk of network nodes is complicated by the fact that the vulnerability is often not the only one. The main idea underlying the method is the use of a statistical formal model based on Markov chains in combination with a graph of possible trajectories and metrics for analyzing vulnerabilities. Scoring scores are used as metrics for analyzing vulnerabilities, which use three types of metrics: basic, temporal, and contextual. A design example is given. The resulting model can be used to identify critical nodes along the path of access to the target node, in which intruders can be most dangerous. Based on the information obtained using the model, the network administrator can install immune detectors on these nodes, which will significantly improve the protection system.

Keywords: information security, intrusion detection systems, immune detectors, Markov chains.

For citation: Tokarev V.L., Sychugov A.A. Method for assessing the level of security risks of network nodes to improve the efficiency of placement of immune detectors. *Modeling, Optimization and Information Technology*. 2020;8(3). Available from: https://moit.vivt.ru/wp-content/uploads/2020/08/TokarevSychugov_3_20_1.pdf DOI: 10.26102/2310-6018/2020.30.3.021 (In Russ).

Введение

Одним из наиболее эффективных средств своевременного обнаружения атак в компьютерных сетях являются системы обнаружения вторжений (СОВ), построенные на основе иммунных детекторов [1, 2]. Такие системы позволяют обнаруживать атаки различных классов, включая и еще неизвестных.

Однако важное значения для эффективности применения таких СОВ имеет рациональное размещение иммунных детекторов по узлам сети. Показано [3], что состав и размещение иммунных детекторов тогда позволяют достичь наибольшего эффекта, когда они контролируют узлы со сравнительно высоким риском нарушения информационной безопасности.

Оценка риска сетевой безопасности осложняется тем, что уязвимость часто бывает не единственной. Она может быть многоступенчатой, многовариантной и охватывать несколько узлов.

Для решения этой проблемы, предложено использовать статистическую формальную модель на основе Марковских цепей в сочетании с метриками анализа уязвимостей, что позволяет определить критические узлы, в которых нарушители могут быть наиболее опасны. Основываясь на получаемой с помощью модели информации, сетевой администратор может именно на этих узлах установить иммунные детекторы, что позволит существенно улучшить систему защиты, то есть снизить значение показателя общей защищенности.

Предлагаемая формальная модель может быть использована для оценивания рисков информационной безопасности сетей различных топологий.

Метрики оценивания уязвимостей

В качестве оценок уязвимостей часто используются скоринговые оценки CVSS [4, 5], которые используют три вида метрик: базовые, временные и контекстные. Основные показатели метрик и их качественные значения приведены в Таблице 1.

Для получения оценок в диапазоне от 0 до 10, качественные значения показателей преобразуются в количественные с помощью логистической кривой [3], а итоговые оценки метрик получаются с помощью формул:

$$Exp = \phi_1(AV, AC, AU); \quad \text{Imp} = \phi_2(C, I, A); \quad Base = \phi_3(\text{Imp}, Exp), \quad (1)$$

Например,

$\text{Exp} = 20 \cdot \text{AV} \cdot \text{AC} \cdot \text{AU};\ \text{Imp} = 10{,}41 \cdot [1 - (1 - C) \cdot (1 - I) \cdot (1 - A)];$

$\text{Base} = 0{,}6 \cdot \text{Imp} + 0{,}4 \cdot \text{Exp}.$

При этом узлы с диапазоном баллов от 0 до 3,9 считается с низкой уязвимостью, 4,0 - 6,9 - со средней уязвимостью, а 7,0-10 - с высокой уязвимостью.

Таблица 1 – CVSS метрики уязвимостей
Table 1 – CVSS vulnerability metrics

Наименования показателей		Качественные значения
Базовая метрика (BASE)		
Характеристики доступа – «эксплойтность» (Exp)	способ получения доступа (AV)	Локальный, через смежную сеть, сетевой
	сложность получения доступа (AC)	Высокая, средняя, низкая
	Аутентификация (AU)	Множественная, единственная, отсутствие
Влияние (Imp) на:	Конфиденциальность (C)	не оказывает, частичное, полное
	Целостность (I)	не оказывает, частичное, полное
	Доступность (A)	не оказывает, частичное, полное
Временная метрика (Temp)		
Возможность использования		Не определено, теоретически, есть концепция, есть сценарий, высокая.
Уровень исправления		Не определено, временно, рекомендовано, недоступно.
Степень достоверности источника		Не определено, не подтверждена, не доказана, подтверждена
Контекстная метрика (Env)		
Вероятность нанесения ущерба		Не определено, низкая, средняя, высокая.
Плотность ущерба		Не определена, низкая, средняя, высокая.
Требования к конфиденциальности		Не определены, низкие, средние, высокие.
Требования к целостности		Не определены, низкие, средние, высокие.
Требования к доступности		Не определены, низкие, средние, высокие.

Граф возможных траекторий

Нарушители обычно проникают в компьютерные сети с помощью цепочки эксплойтов, каждый элемент которое создает основу для следующего элемента. Сочетание таких эксплойтов составляет цепочку, называемую траекторией атаки, совокупность которых образуют граф возможных траекторий (ГВТ) заканчивающийся в состоянии, где нарушитель может успешно достичь своей цели. Существует достаточно алгоритмов, которые были разработаны для построения ГВТ атак [4] [5]. Однако очень трудно анализировать сеть с помощью ГВТ, когда количество узлов и сложность сети увеличиваются, поскольку сложность построения и вычислительные затраты возрастают экспоненциально.

Использование Марковских цепей

Для построения формальной модели доступа к узлу предлагается использовать Марковские цепи, отражающие реальное поведение атакующего.

Марковскую цепь можно определить как дискретный стохастический процесс [6], определенный на конечном наборе состояний. Тогда Марковскую цепь можно представить как последовательность случайных переменных $x_0, x_1, \ldots, x_n \in S$, удовлетворяющая "свойству Марковиана", то есть:

$$P[X_{n+1} = y | X_0 = x_0,\ X_1 = x_1, \ldots, X_n = x_n] = P[X_{n+1} = y | X_n = x_n]$$

Марковские свойства означают, что: 1) переходы между состояниями лишены памяти; 2) переход к следующему шагу зависит только от текущего состояния и ни от одного из предыдущих состояний. Можно соотнести эти свойства с поведением нарушителя в том смысле, что нарушитель может использовать разные траектории (последовательность узлов) до достижения цели-узла.

Предполагается: 1) выбор наилучшего промежуточного узла зависит от трех факторов, а именно: эксплойтности, характеризующей уязвимости подсистемы доступа; влияния уязвимостей на нарушения конфиденциальности, целостности и доступности, а также индивидуального навыка атакующего; 2) переходные состояния не зависят от времени; 3) может быть определена некоторая матрица вероятностей перехода P(x, y) и начальное распределение вероятностей

$$R = \{r_1, r_2, \ldots, r_n\}.$$

Тогда, имея матрицу P(x, y), вектор начальных рисков R, используя основные свойства Марковского процесса можно определить риски узлов и риск всей сети.

Построение модели

Основным компонентом предлагаемой модели является ГВТ, который строится путем изучения топологии сети, служб, запущенных на каждом узле, правил, определенных на брандмауэрах, и уязвимостей, связанные с каждым узлом, на котором запущены различные службы.

Схема предлагаемого моделирования представлена на Рисунке 1.

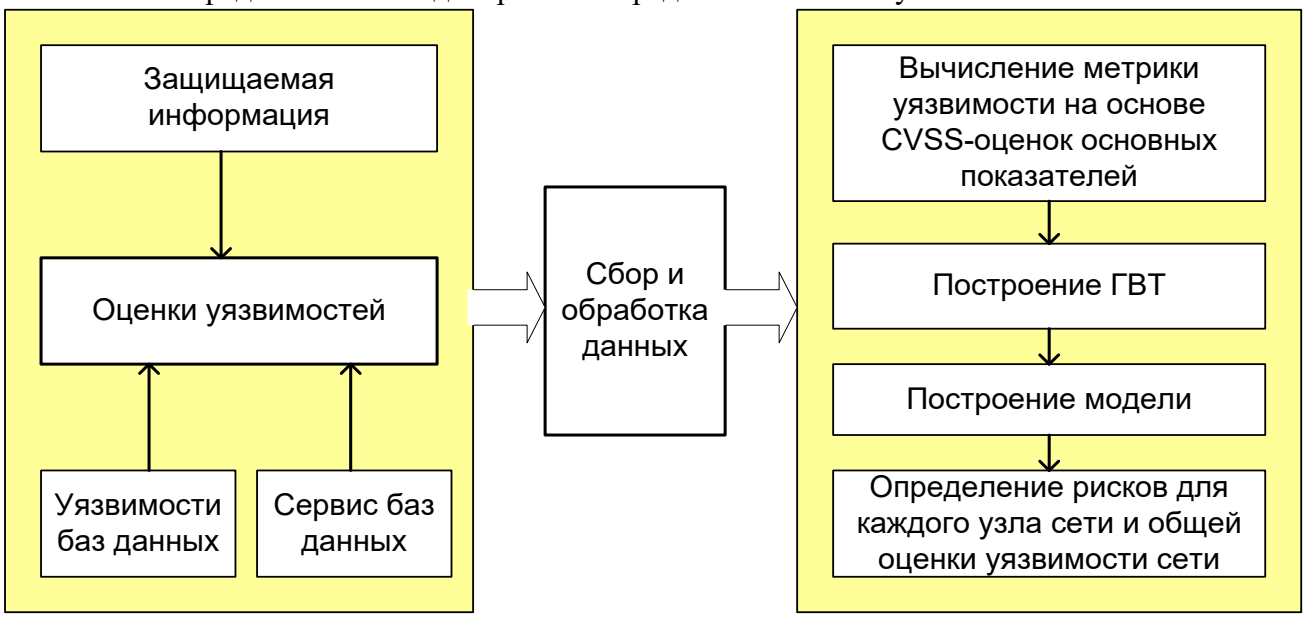


Рисунок 1 – Схема моделирования
Figure 1 – Scheme of simulation

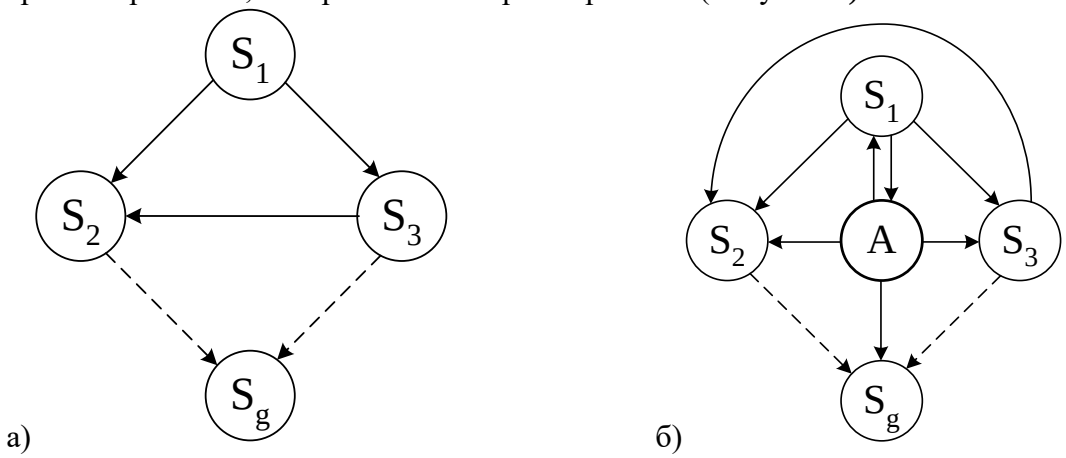
Предполагается, что:

1) в рассматриваемой сети присутствует ограниченное число узлов, и каждый узел представляет собой узел, каждый из которых запускает различные виды услуг и там же могут существовать различные уязвимости, для которых определены CVSS - системой соответствующие баллы Exp и Imp, которыми можно пометить ребра ГВТ, используемого для определения вероятности возможности использования нарушителем i-й уязвимости;

2) нарушитель выберет уязвимость, которая максимизирует шансы успеха в компрометации состояния узла-цели;

3) если нарушитель, по какой-либо причине, завершает атаку, то он перейдет в исходное состояние.

Центральная составляющая предлагаемой модели - ГВТ доступа к узлу. Для примера рассмотрен ГВТ, построенный на трех вершинах (Рисунок 2).



а) б)

Рисунок 2 – Примеры ГВТ: а) без нарушителя, б) с нарушителем

Figure 2 – Examples of GPT: a) without the intruder, b) with the intruder

На Рисунке 2(а) Si, - узлы, Sg – целевой узел. Число узлов равно количеству станций в сети. Направленные ребра между двумя узлами представляют собой отношения между соответствующими двумя станциями в сети: в исходном ГВТ нет множественных ребер. Пунктирные линии ребер означают, что между узлами могут присутствовать другие промежуточные узлы.

На Рисунке 2(б) в ГВТ добавлен дополнительный узел А для представления нарушителя.

Нарушитель может атаковать узел, к которому имеет непосредственный доступ, и, преодолев защиту этого узла, развивает атаки, пока не достигнет целевого узла Sg. При этом перед ним возникает задача выбора следующего узла для атаки, с целью достижения узла Sg. Это выбор, скорее всего, зависит от двух обозначенных выше параметров: Exp, характеризующий сложность преодоления защиты узла, и Imp, характеризующий уязвимости узла. При этом, каждый узел оценивается в CVSS-баллах в шкале (0,10), где 0 означает наиболее защищенный узел и 10 означает наименее защищенный.

То есть, для решения задачи выбора очередного узла для атаки нарушитель может использовать значение базовой метрики (1).

Принимая окончательное решение о переходе с одного узла на другой, атакующий опирается также и на собственные навыки и опыт. Это субъективный фактор, который может оказать существенное влияние на выбор нарушителя очередного узла для атаки: способен сместить решение в ту или иную сторону. Этот фактор можно учесть в модели

как фактор смещения β. В результате функцию выбора можно представить следующим выражением:

$$\alpha_{jk} = \beta \cdot Exp(v_k) + (1-\beta) \cdot \mathrm{Imp}(v_k), \quad 0 < \beta < 1, \tag{2}$$

где a_{jk} - это "выгода" от перемещения от узла j до узла k, v_k - функция уязвимости, значение которой характеризует возможность преодоления защиты k-го узла нарушителем; β - коэффициент смещения, принимающий значение от 0 до 1.

Если значения a_{jk} определить для каждой пары узлов сети, то ее защищенность от атак, с точки зрения нарушителя, можно охарактеризовать матрицей смежности:

$$A = \begin{bmatrix} 0 & a_{01} & \dots & a_{0g} & \dots & a_{0n} \\ a_{10} & 0 & \dots & a_{1g} & \dots & a_{1n} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots \\ a_{n0} & a_{n1} & \dots & a_{ng} & \dots & 0 \end{bmatrix}$$

Диагональные значения матрицы A равны нулю, т.к. нет препятствий для нарушителя перемещениям от j-го узла к самому j-му узлу. Нормализация значений a_{jk} матрицы A позволяет получить значения фикции принадлежности нечеткому множеству «Узел S_k доступен для атаки из узла S_j»:

$$\mu_{jk} = \frac{a_{jk}}{\sum_i a_{ji}} \tag{3}$$

Тогда характеристика сети в матричном виде:

$$M = DA \tag{4}$$

где M - матрица переходов, определяющая возможность перехода нарушителя из одного узла в другой, D-диагональная матрица, вычисленная с помощью правила нормализации

$$d_{jk} = \begin{cases} 1 \Big/ \sum_i a_{ji} \ if \ \ j = k \\ 0 \qquad otherwise \end{cases} \tag{5}$$

Пусть нарушитель начинает атаковать от начального узла к целевому узлу. Узлы ГВТ могут быть использованы нарушителем, если любой из дочерних узлов является истинным. Анализ риска основан на относительном значении ранга для каждого узла ГВТ. Начальное значение вектора риска $R = \{r_1, r_2, ..., r_n\}$ вычисляется на основе количества узлов, присутствующих в ГВТ. Если в ГВТ существует n узлов, то можно установить все ранги узлов равные $1/n$ и этот начальный риск становится стартовым узлом атакующего.

Величина риска r_k для узла k вычисляется с помощью итерационной процедуры до получения устойчивого значения. Предполагая, что $r_k(t-1)$ - это предыдущее значение риска узла k, его следующее значение $r_k(t)$ вычисляется по выражению

$$r_k(t) = \sum_j r_k(t-1)\mu_{jk} \tag{6}$$

В матричной форме выражение (6) примет вид

$$R_t = R_{t-1}M\,. \tag{7}$$

Значения риска нормализуются: $0 \le r_k \le 1$, $\sum_j r_k = 1$. Значение R вычисляется рекурсивно до сходимости $\left(\left|R_t - R_{t-1}\right|\right)^{\mathrm{T}}\left(\left|R_t - R_{t-1}\right|\right) \le \varepsilon$, где ε - заданное малое положительное число.

Эта итерация сходится к устойчивому значению вектора R*, как собственному вектору матрицы M.

Алгоритм оценивания рисков включает следующие шаги.

Шаг 1. Инициализация. Каждому значению вектора рисков присваивается начальное значение 1/*n*.

Шаг 2. Итерационная процедура коррекции значений рисков до наступления условия сходимости для каждой вершины ГВТ.

Шаг 3. Определение приоритетов защиты узлов сети по полученным значениям рисков.

Шаг 4.Определение суммы рисков как общего показателя информационной безопасности сети.

Результаты

В качестве результата предлагается рассмотреть следующий пример. Для проверки предложенной модели было использована сеть (Рисунок 3).

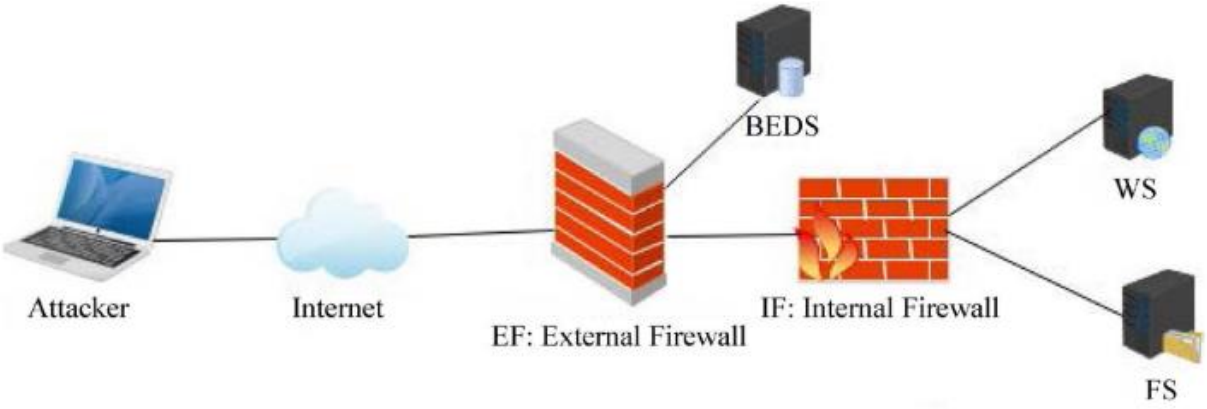


Рисунок 3 – Пример топологии сети
Figure 3 – Example of network topology

В этой сети есть три целевых узла: общедоступный веб-сервер (WS), общедоступный файловый сервер (FS) и сервер бэкэнд базы данных (BEDS). Предполагается, что нарушитель находится за пределами сети. Передача пакетов на целевой узел управляется с помощью двух брандмауэров: внешний брандмауэр (EF) и внутренний (IF). EF позволяет передачу любого пакета серверам WS и FS из-за пределов сети и запрещает доступ к ресурсам BEDS непосредственно из-за пределов сети. IF управляет передачей пакетов внутри сети. Краткое описание правил брандмауэра и сетевого сценария приведено в Таблице 2.

Таблица 2 – Правила брандмауэра
Table 2 – Firewall rules

Источник	Приемник	Служба	Действие
All	WS	http	Allow
All	WS	ftp	Allow
All	FS	ftp	Allow
WS	BEDS	oracle	Allow
FS	BEDS	ftp	Allow
All	All	All	Denoy

Пусть каждый из целевых узлов содержит одну уязвимость. Нарушитель использует оценку уязвимости, чтобы скомпрометировать узел. Это показано ниже в Таблице 3 вместе с баллами уязвимостей Exp и Imp, которые взяты из [3].

Таблица 3 – Уязвимости узлов
Table 3 – Nodes vulnerabilities

Узел	Уязвимость	CVE-ID	Base	Imp	Exp
WS	Apache Chunked Code	CVE-2002-0392	7,5	6,4	10
FS	Wuftpd Sockprintf	CVE-2003-1327	9,3	10	8,6
BEDS	Oracle Tns listener	CVE-2002-1675	7,5	6,4	10

На основе топологии сети (Рисунок 3), с учетом правил брандмауэров и баллов уязвимостей, связанных с соответствующим узлом, сгенерирован ГВТ доступа к узлу (Рисунок 4).

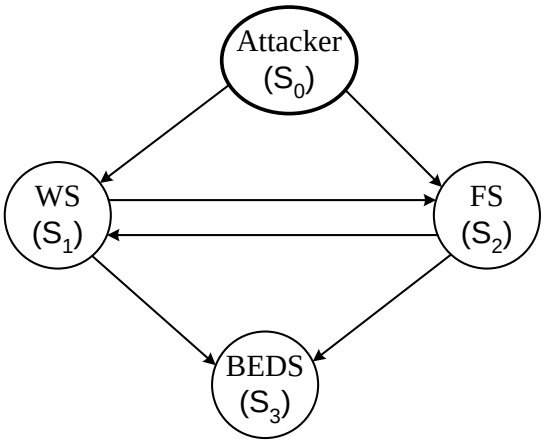


Рисунок 4 – ГВТ для рассматриваемого примера
Figure 4 – GPT for the example under consideration

В ГВТ обозначены узлы нарушителя (attacker), Web Server, File Server и Backend Database Server (BEDS) как S_0, S_1, S_2, и S_3, соответственно. Ребра от всех узлов до узла S_0 опущены.

Пусть $\beta = 0{,}5$, тогда, используя выражение (2), в соответствии с ГВТ (Рисунок 4), можно рассчитать матрицу смежности *A*. Поскольку принято, что если нарушитель прекращает атаку, то он возвращается к первоначальному узлу, элементы первого столбца матрицы A равны 1, а остальные все элементы определены в соответствии с выражением (2). Например, $a_{12} = 0.5 \cdot 10 + 0.5 \cdot 6.4 = 8.2$. Это и есть значение α_{12}, на которое нарушитель ориентируется при выборе перемещения с узла S_0 на узел S_1. Также определены остальные элементы матрицы A:

$$A = \begin{bmatrix} 0 & 8,2 & 9,3 & 0 \\ 1 & 0 & 9,3 & 8,2 \\ 1 & 8,2 & 0 & 8,2 \\ 1 & 0 & 0 & 0 \end{bmatrix}$$

Далее матрица A преобразуется в матрицу M с помощью выражения (4), в котором матрица D:

$$D = \begin{bmatrix} 0,05714 & 0 & 0 & 0 \\ 0 & 0,05405 & 0 & 0 \\ 0 & 0 & 0,05747 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Матрица переходов M:

$$M = \begin{bmatrix} 0 & 0,47 & 0,53 & 0 \\ 0,054 & 0 & 0,50 & 0,44 \\ 0,057 & 0,47 & 0 & 0,47 \\ 1 & 0 & 0 & 0 \end{bmatrix}$$

Основываясь на предложенном алгоритме ранжирования рисков определен начальный вектор риска R = (0.25, 0.25, 0.25, 0.25). После запуска итерационной процедуры (7) и обнаружения ее сходимости получены следующие значения (Таблица 4).

Таблица 4 – Риски узлов
Table 4 – Risks of nodes

Узел	**Риск**
S_0	0,260
S_1	0,245
S_2	0,262
S_3	0,231

Из полученных значений ri можно сделать вывод, что узел S2 является менее защищенным, чем S1 и S3. Поэтому иммунные детекторы должны быть установлены в первую очередь на узел S2. Общая сумма рисков, связанных с узлом S1, S2 , и S3 равна 0,74. Это значение можно использовать в качестве показателя безопасности, указывающего, что эта сеть не очень безопасна по отношению к данным уязвимостям и

существующим отношениям доступа между серверами. Следовательно, доступ к защищаемым ресурсам требует более совершенной защиты.

Заключение

Предложена формальная модель оценивания риска информационной безопасности с использованием ГВТ доступа к ресурсам сети. Модель, использующая Марковские цепи в сочетании с балльными CVSS-оценками позволяет проанализировать уязвимости, связанные со структурой сети. Модель позволяет определить критические узлы, существующие в ГВТ доступа к узлу. Основываясь на этой информации, администратор сети может принять соответствующее решение, в частности, об установке иммунных детекторов с учетом приоритетов.

Предложенный алгоритм ранжирования рисков достаточно гибок в том смысле, что позволяет спрогнозировать действия нарушителя с учетом его навыков и опыта, задавая смещение β в вычислениях значений функции «выгоды». Алгоритм был рассмотрен относительно базовой метрики (Base), но он, с таким же успехом, может быть использован для оценивания риска путем использования временной метрики (Temp) или контекстной метрики (Env).

Предложенная модель может быть встроена в систему защиты информации существующих автоматизированных систем или использована при построении автоматизированных систем в защищенном исполнении.

БЛАГОДАРНОСТИ

Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта №19-07-01107\19.

ЛИТЕРАТУРА

1. Токарев В.Л., Сычугов А.А. Обнаружение вредоносного программного обеспечения с использованием иммунных детекторов. *Известия Тульского государственного университета. Технические науки*. 2017;10:216-230.
2. Tokarev V.L., Sychugov A.A. Multi-agent system for network attack detection. *International Journal of Civil Engineering and Technology (IJCIET)*. 2018;9(6):279-286.
3. Банк данных угроз безопасности информации. Калькулятор CVSS v2. Доступно по адресу: https://bdu.fstec.ru/calc
4. Токарев В.Л. Распознавание стратегии противодействующей стороны по текущим наблюдениям. *Доклады Томского государственного университета систем управления и радиоэлектроники*. 2014;(6):184-187.
5. Jha, S., Sheyner, O. and Wing, J. (2002) Two Formal Analyses of Attack Graphs. *Proceedings of 15th IEEE Computer Security Foundations Workshop*. 2002;6:49-63.
6. Mehta V., Bartzis C., Zhu H., Clarke E. and Wing J. Ranking Attack Graphs. *International Workshop on Recent Advances in Intrusion Detection*. 2006;1:127-124.
7. Дынкин Е. Б. Основания теории марковских процессов. Физматлит. 2006.

REFERENCES

1. Tokarev V.L., Sychugov A.A. Detection of malware using immune detectors. *Bulletin of the Tula State University. Technical science*. 2017;10:216-230.

2. Tokarev V.L., Sychugov A.A. Multi-agent system for network attack detection. *International Journal of Civil Engineering and Technology (IJCIET).* 2018;9(6):279-286.
3. Databank of information security threats. CVSS Calculator v2. Available at: https://bdu.fstec.ru/calc
4. Tokarev V.L. Recognition of the opposing side's strategy based on current observations. *Reports of the Tomsk State University of Control Systems and Radioelectronics.* 2014;(6):184-187.
5. Jha, S., Sheyner, O. and Wing, J. (2002) Two Formal Analyzes of Attack Graphs. *Proceedings of 15th IEEE Computer Security Foundations Workshop*. 2002;6:49-63.
6. Mehta V., Bartzis C., Zhu H., Clarke E. and Wing J. Ranking Attack Graphs. *International Workshop on Recent Advances in Intrusion Detection*. 2006;1:127-124.
7. Dynkin E.B. *Foundations of the theory of Markov processes*. Fizmatlit. 2006.

ИНФОРМАЦИЯ ОБ АВТОРАХ / INFORMATION ABOUT THE AUTHORS

Токарев Вячеслав Леонидович, доктор техн. наук, профессор, кафедра информационной безопасности, ФГБОУ ВО «Тульский государственный университет» Институт прикладной математики и компьютерных наук, Тула, Российская Федерация.
e-mail: unwaiter@mail.ru

Vyacheslav L. Tokarev, Dr. Sci. (Tech), information Security Department, Federal State Budgetary Educational Institution of Higher Education “Tula StateUniversity”, Tula, Russian Federation

Сычугов Алексей Алексеевич, канд. техн. наук, доцент, информационной безопасности, ФГБОУ ВО «Тульский государственный университет» Институт прикладной математики и компьютерных наук, Тула, Российская Федерация.
e-mail: xru2003@yandex.ru

Aleksey A. Sychugov, Phd (Tech), information Security Department, Federal State Budgetary Educational Institution of Higher Education “Tula StateUniversity”, Tula, Russian Federation