УДК 004.054 DOI:10.31854/1813-324X-2021-7-1-94-104

Модель аудита защищенности объекта критической информационной инфраструктуры тестовыми информационно-техническими воздействиями

С.И. Макаренко[1, 2*], **Г.Е. Смирнов**[2, 3]

[1]Санкт-Петербургский федеральный исследовательский центр Российской академии наук,
Санкт-Петербург, 199178, Российская Федерация
[2]Санкт-Петербургский государственный электротехнический университет "ЛЭТИ" им. В.И. Ульянова (Ленина),
Санкт-Петербург, 197376, Российская Федерация
[3]ООО «Корпорация «Интел групп»,
Санкт-Петербург, 197372, Российская Федерация
*Адрес для переписки: mak-serg@yandex.ru

Информация о статье
Поступила в редакцию 29.01.2021
Принята к публикации 12.02.2021

Ссылка для цитирования: Макаренко С.И., Смирнов Г.Е. Модель аудита защищенности объекта критической информационной инфраструктуры тестовыми информационно-техническими воздействиями // Труды учебных заведений связи. 2021. Т. 7. № 1. С. 94–104. DOI:10.31854/1813-324X-2021-7-1-94-104

Аннотация: *В статье представлена модель аудита защищенности объекта критической информационной инфраструктуры тестовыми информационно-техническими воздействиями. Данная модель формализует процесс аудита объекта в виде многоуровневой топологической модели, отдельные уровни которой соответствуют: затратам ресурса на проведение воздействий, тестовым информационно-техническими воздействиям, уязвимостям, элементам объекта и уровням ущерба. Использование этой модели в практике аудита позволит обосновать наиболее эффективные воздействия по критерию «эффективность/стоимость», а также сформировать тестовые наборы, которые обеспечат рациональную полноту аудита объекта критической инфраструктуры.*

Ключевые слова: *критическая информационная инфраструктура, тестирование на проникновение, аудит информационной безопасности, информационно-техническое воздействие.*

1. ВВЕДЕНИЕ. ПОСТАНОВКА ЗАДАЧИ НА РАЗРАБОТКУ МОДЕЛИ

В 2017 г. в России был принят федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», который устанавливает перечень объектов и субъектов, относящихся к критической информационной инфраструктуре (КИИ) РФ, а также обязует разработать комплекс мер, направленных на аудит состояния информационной безопасности (ИБ) объектов КИИ и обеспечения ее защищенности.

В подавляющем числе случаев аудит объектов КИИ проводится на основе сравнительного анализа с нормативно-правовой документацией, регламентирующей обеспечение ИБ, или на основе анализа рисков. Вместе с тем, в предыдущих работах авторов [1, 2] указывается на необходимость формирования еще одного типа практического подхода к аудиту, а именно – аудита на основе экспериментальных исследований системы или ее прототипа. Данный тип аудита проводится с применением против системы средств или способов информационных воздействий с целью практической проверки эффективности технических или организационных мер защиты, а также выявления новых уязвимостей системы. При этом для обеспечения достоверности аудита используемые воздействия должны быть аналогичны реально применяемым непрофессиональными и профессиональными нарушителями [3, 4]. В некоторых работах, например, таких как [5–11], для обозначения такого подхода используется термин «тестирование на проникновение» (в англоязычной литературе – «penetration testing», «pen-testing»), а также другие термины: «активный аудит», «инструментальный аудит» и др., но при этом суть подхода к аудиту не меняется.

Таким образом, можно говорить о том, что одним из перспективных направлений практического аудита ИБ объектов КИИ является реализация в отношении них тестов на проникновение – воздействие на объект тестовых информационно-технических воздействий (ИТВ), которые с высокой степенью вероятности могут использоваться нарушителями. Несмотря на то, что такое тестирование представляет собой достаточно адекватный и в высокой степени достоверный подход к оценке защищенности, он не получил широкого распространения. Основными причинами этого, на взгляд авторов, является отсутствие единой общепризнанной научно-методической базы для проведения аудита такого типа.

В международной практике, как правило, проведение аудита защищенности объекта путем использования тестов на проникновение регламентируется стандартами: OSSTMM; ISSAF; OWASP; PTES; NIST SP 800-115; BSI; PETA и др. Достаточно полный содержательный анализ этих стандартов представлен в предыдущей работе авторов [13]. При этом, как показал проведенный анализ, в основу этих стандартов не положены какие-либо системные или хотя бы общетеоретические подходы.

Практическим вопросам оценки состояния ИБ объектов путем их тестирования посвящены отечественные работы Маркова А.С. и др. [4], Скабцова Н. [5], Климова С.М. [13, 14], Петренко А.А., Петренко С.А. [15], Бойко А.А. [16–18], Храмова В.Ю. [17, 18], Щеглова А.В. [18], Дьяковой А.В. [16, 17], Макаренко С.И. [1, 2]. В работах Барановой Е.К. [19, 20], Бегаева А.Н. и др. [21], Богораза А.Г., Песковой О.Ю. [22], Дорофеева А. [23], Умницына М.Ю. [24], Бородина М.К., Бородиной П.Ю. [25], Полтавцевой М.А., Печенкина А.И. [26], Кадана А.М., Доронина А.К. [27], Еременко Н.Н., Кокоулина А.Н. [28], Туманова С.А. [29], Кравчука А.В. [30], Горбатова В.С., Мещерякова А.А. [31], рассматриваются именно такие практические способы аудита защищенности информационных систем, как тестирование на проникновение или «penetration testing». В некоторых работах такой тип тестирования указан под наименованием «инструментальный аудит».

Анализ вышеуказанных трудов показал следующее. Работы, посвященные вопросам экспериментального тестирования реальных информационных систем, рассматривают такие способы и сценарии исключительно как «тестирование на проникновение» или как «инструментальный аудит», при этом проведение такого типа аудита в отечественной практике не регламентируется какими-либо общепринятыми руководящими документами или методиками тестирования. В некоторых отечественных работах по тестированию на проникновение рекомендуется делать акцент на необходимости выявления наиболее «зрелищных» уязвимостей или тех уязвимостей, устранение которых принесет максимальные экономические выгоды компании, выполняющий аудит.

Таким образом, можно сделать вывод, что перспективным направлением развития отечественной теории и практики тестирования на проникновение должны опираться на уже известные методики и стандарты проведения подобного типа тестирования, которые уже разработаны, преимущественно, за рубежом.

К работам, в которых сделана попытка подвести научную основу под тестирование специальными ИТВ, относятся работы: Pfleeger C.P., et al. [32], McDermott J.P. [33], Макаренко С.И. [2], Pfleeger C.P., et al. [34], Ami P., Hasan A. [35], Holik F., et al. [36], Herzog P. [37]. В статье McDermott J.P. [33] представлена модель тестирования в формализме теории сетей Петри. В работе Макаренко С.И. [2] сделана попытка систематизировать и подвести научную базу под возможности использования тестовых ИТВ для оценки защищенности объектов КИИ. В статьях Pfleeger C. P., et al. [32], Alisherov F., Sattarova F. [34], Ami P., et al. [36], Herzog P. [37] представлены различные варианты методик тестирования. Однако во всех этих работах вопросы формирования базовой модели аудита защищенности объекта КИИ, на основе которой можно было бы обосновывать наборы тестовых ИТВ под различные задачи аудита – не рассматривались.

Целью статьи является разработка модели аудита защищенности объекта КИИ тестовыми ИТВ, которая может использоваться для научно-обоснованного формирования тестовых наборов под различные задачи аудита.

Для достижения цели статьи необходимо сформировать формальное описание процесса тестирования объекта КИИ в виде многоуровневой топологической модели, которая взаимосвязано учитывает: эффективность отдельных ИТВ i, в части выявленного и потенциально предотвращенного ущерба $\{z\}$; ориентированности их на проверку конкретного множества уязвимостей $\{u\}$ элементов $\{e\}$ объекта КИИ; расход в процессе тестирования определенного количества ресурса r_i (в данном случае под абстрактным ресурсом может пониматься расход времени аудитора, оплата его труда, стоимость машинного времени, затраты на специализированное оборудование и т. д.).

2. ФОРМАЛИЗАЦИЯ МОДЕЛИ

Для формализации модели введем следующие обозначения:

$\pi/\pi_{отн}$ – абсолютное/относительное значение полноты выявленного и потенциально предотвращенного ущерба;

$E = \{e\}$ – множество элементов, составляющих объект КИИ;

e_j – j-ый элемент объекта КИИ;

$g(e_j, e_m, \sigma_n)$ – вес ребра, соединяющего e_j и e_m элементы объекта КИИ, характеризующий дестабилизирующее влияние со стороны элемента e_j на элемент e_m при нарушении у элемента e_j свойства ИБ σ_n;

$I = \{i\}$ – множество тестовых ИТВ;

i_j – j-ое тестовое ИТВ;

j, l, m, n – переменная-счетчик;

N_I – количество тестовых ИТВ, которое соответствует количеству элементов множества I;

N_U – количество уязвимостей, которое соответствует количеству элементов множества U;

R – количество ресурса аудитора;

r_j – количество ресурса аудитора, расходуемое на организацию и проведение j-го тестового ИТВ;

r_n – затраты ресурса аудитора на проведение n-го тестового ИТВ;

$s(x)$ – степень вершины x, равная количеству инцидентных ей ребер, которые соответствуют тем или иным условиям;

u – уязвимость объекта КИИ;

$U = \{u\}$ – множество уязвимостей объекта КИИ;

$v(x_1, x_2)$ – вес ребра, соединяющего x_1 и x_2 элементы модели;

$z(e_j, \sigma_n)$ – ущерб от нарушения свойства ИБ σ_n у элемента e_j;

$Z = \{z\}$ – суммарный показатель ущерба, который может быть причинен объекту КИИ;

σ_n – свойство ИБ: $n = 1$ – доступность; $n = 2$ – целостность; $n = 3$ – конфиденциальность.

Модель тестирования защищенности объекта КИИ представлена в формализме теории графов и теории множеств и имеет иерархическую уровневую структуру (рисунок 1): ресурсы, тестовые ИТВ; уязвимости, элементы объекта КИИ, ущерб объекту КИИ.

Уровень ресурсов

На первом уровне модели формализуются ресурсы, необходимые для реализации соответствующих тестовых ИТВ, упорядоченные по возрастанию «стоимости». Связь уровня ресурсов с уровнем тестовых ИТВ осуществляется путем постановки в соответствие каждому ИТВ i_j определенного элемента r_j.

Это соответствие формализуется ребром $v(r_j, i_j)$, вес которого пропорционален нормированным затратам ресурсов на проведение i_j ИТВ:

$$v(r_j, i_j) = \frac{r_j}{\sum_{n=1}^{N_I} r_n} \qquad (1)$$

Выбор выражения (1) обусловлен следующими соображениями. Во-первых, множество весов ребер, ведущих с уровня ресурсов на уровень тестовых ИТВ, должно быть нормировано к единице, т. е. $\sum_{j=1}^{N_I} v(r_j, i_j) = 1$. Во-вторых, так как в дальнейшем на данной модели планируется поиск рациональных тестовых ИТВ, которые будут основаны на алгоритмах поиска кратчайших путей, то более лучшему ребру, которое соответствует использованию ИТВ с меньшими затратами ресурсов, должно соответствовать меньшее значение веса ребра. Выражение (1) удовлетворяет данным условиям.

Уровень тестовых ИТВ

На втором уровне модели формализуются множество тестовых ИТВ $I = \{i\}$, которые могут быть использованы для оценки защищенности объекта КИИ.

Связь уровня тестовых ИТВ с уровнем уязвимостей осуществляется путем постановки в соответствие каждому ИТВ i_j подмножества элементов $\{u_m\}$ уровня уязвимостей, т. е. тех уязвимостей $\{u_m\}$, которые могут быть использованы j-ым ИТВ для нанесения того или иного ущерба объекту КИИ. Это соответствие i_j и $\{u_m\}$ формализуется множествами ребер $\{(i_j, u_m)\}$, где $m = 1 \ldots M_j$ – счетчик ребер, инцидентных вершине i_j. Вес каждого ребра $v(i_j, u_m)$ пропорционален нормированной степени вершины i_j относительно числа инцидентных ребер, ведущих к элементам $\{u_m\}$ на уровне уязвимостей:

$$v(i_j, u_m) = \frac{1}{N_I \cdot s(i_j | i_j \to \{u\})}, \qquad (2)$$

где $s(i_j | i_j \to \{u\})$ – степень вершины i_j, равная количеству инцидентных ей ребер, ведущих к элементам $\{u\}$, например, для схемы модели на рисунке 1: $s(i_1) = 2$, $s(i_2) = 3$, $s(i_3) = 1$.

Выбор выражения (2) обусловлен следующими теми же соображениями, что и для выражения (1). Во-первых, множество весов ребер, ведущих с уровня тестовых ИТВ на уровень уязвимостей, должно быть нормировано к единице т. е. $\sum_{j,m} v(i_j, u_m) = 1$. Во-вторых, ребру от более лучшего узла i, в смысле, ИТВ тестирующему большее число уязвимостей $\{u_m\}$, должно соответствовать меньшее значение веса ребра.

Уровень уязвимостей

На третьем уровне модели формализуются множество уязвимостей $U = \{u\}$, которые потенциально присутствуют в элементах объекта КИИ и могут быть использованы нарушителем для дестабилизирующего воздействия на элементы объекта КИИ и причинения ущерба.

Связь уровня уязвимостей с уровнем элементов объекта КИИ осуществляется путем постановки в соответствие каждой уязвимости u_j подмножества вершин $\{e_l\}$ уровня элементов, т. е. тех элементов $\{e_l\}$, которым может быть нанесен ущерб путем эксплуатации j-ой уязвимости. Это соответствие u_j и $\{e_l\}$ формализуется множествами ребер $\{(u_j, e_l)\}$, где $l = 1 \ldots L_j$ – счетчик ребер инцидентных вершине u_j.

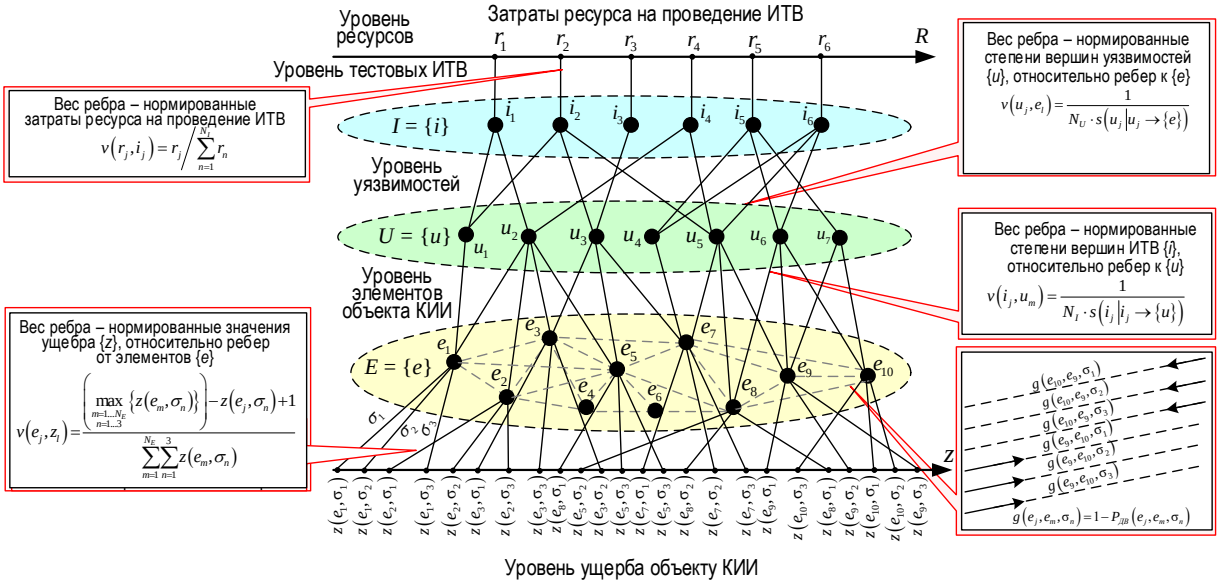

Рис. 1. Схема модели аудита защищенности объекта КИИ тестовыми ИТВ

Fig. 1. An Audit Model for Estimation Security of Critical Infrastructure Objects with Test Cyber Attacks

Вес каждого ребра $v(u_j, e_l)$ обратно пропорционален нормированной степени вершины u_j относительно числа инцидентных ребер, ведущих к вершинам $\{e_l\}$ на уровне элементов:

$$v(u_j, e_l) = \frac{1}{N_U \cdot s(u_j | u_j \to \{e\})}, \quad (3)$$

где $s(u_j | u_j \to \{e\})$ – степень вершины u_j, равная количеству инцидентных ей ребер, ведущих к элементам $\{e\}$, например для схемы модели (см. рисунок 1) $s(u_1) = 2$, $s(u_3) = 3$, $s(u_4) = 1$.

Выбор выражения (3) обусловлен теми же соображениями, что и для выражения (2). Во-первых, множество весов ребер, ведущих с уровня тестовых ИТВ на уровень уязвимостей, должно быть нормировано к единице, т. е. $\sum_{j,l} v(u_j, e_l) = 1$. Во-вторых, ребру от более лучшего узла u, в смысле, уязвимости u, которая соответствует большему числу тестируемых элементов $\{e_l\}$, должно соответствовать меньшее значение веса ребра.

Уровень элементов объектов КИИ

На четвертом уровне модели формализуются множество элементов объекта КИИ $E = \{e\}$, дестабилизирующее воздействие на которые через эксплуатацию тех или иных уязвимостей приведет к причинению ущерба.

На данном уровне существует два типа связей:

– связь элементов между собой, которая определяется вероятностью $P_{ДВ}(e_j, e_m, \sigma_n)$ дестабилизирующего влияния элемента e_j на элемент e_m при нарушении у элемента e_j свойства ИБ σ_n;

– связь вершин $\{e_j\}$ уровня элементов с вершинами $\{z_l\}$ уровня ущерба.

Связь элементов $\{e_j\}$ между собой в рамках одного уровня задается ребрами вида (e_j, e_m). Вес каждого ребра $g(e_j, e_m, \sigma_n)$ определяется обратной величиной вероятности дестабилизирующего влияния $P_{ДВ}(e_j, e_m, \sigma_n)$:

$$g(e_j, e_m, \sigma_n) = 1 - P_{ДВ}(e_j, e_m, \sigma_n). \quad (4)$$

Выбор выражения (4) обусловлен тем, что ребру с большей величиной вероятности дестабилизирующего влияния $P_{ДВ}(e_j, e_m, \sigma_n)$, что соответствует более полному охвату тестируемых элементов $\{e_m\}$, должно соответствовать меньшее значение веса ребра. Если дестабилизирующее влияние отсутствует, то $g(e_j, e_m, \sigma_n) = 1$, т. е. становится «непроходимым» в топологическом смысле относительно весов ребер $v(u_j, e_l)$ и $v(e_j, z_l)$, значение которых много меньше 1, в связи с чем $g(e_j, e_m, \sigma_n) = 1$ можно не учитывать.

Связь вершин $\{e_j\}$ уровня элементов с вершинами $\{z_l\}$ уровня ущерба осуществляется путем постановки в соответствие каждому элементу e_j по свойству ИБ σ_n вершины $z_l(e_j, \sigma_n)$ уровня ущерба. Это соответствие e_j и $\{z_l\}$ формализуется множествами ребер $\{(e_j, z_l)\}$. Вес каждого ребра $v(e_j, z_l)$ обратно пропорционален нормированной степени ущерба z_l:

$$v(e_j, z_l) = \frac{\left(\max\limits_{\substack{m=1\ldots N_E \\ n=1\ldots 3}} \{z(e_m, \sigma_n)\} \right) - z(e_j, \sigma_n) + 1}{\sum\limits_{m=1}^{N_E} \sum\limits_{n=1}^{3} z(e_m, \sigma_n)}, \quad (5)$$

где N_E – количество элементов объекта КИИ, которое соответствует количеству элементов множества E; $\sum_{m=1}^{N_E} \sum_{n=1}^{3} z(e_m, \sigma_n)$ – сумма ущерба по всем элементам объекта КИИ и свойствам ИБ; $n = 1 \ldots 3$ –

счетчик свойств ИБ σ_n; $\max\limits_{\dots}\{\dots\}$ – значение максимального ущерба среди всех комбинаций элементов и свойств ИБ.

Выбор выражения (5) обусловлен следующими соображениями. Во-первых, множество весов ребер, ведущих с уровня элементов объекта КИИ на уровень ущерба, должно стремиться к единице, т. е. $\sum_{j,l} v(e_j, z_l) \to 1$. Во-вторых, более лучшему ребру, в смысле, большего значения ущерба, должно соответствовать меньшее значение веса ребра. Суммирование единицы в числителе необходимо для исключения обнуления числителя в весе ребра, соответствующего значению максимального ущерба.

На пятом уровне модели формализуются значения ущербов объекту КИИ, упорядоченные по возрастанию «стоимости». Каждое конкретное значение $z(e_j, \sigma_n)$ численно равно «стоимости» ущерба, который наносится объекту КИИ при нарушении σ_n-го свойства ИБ на его элементе e_j.

В общем виде модель тестирования защищенности объекта КИИ представлена на рисунке 1.

3. ОБСУЖДЕНИЕ МОДЕЛИ

Особенностями данной модели является то, что максимальная длина пути от произвольного узла уровня ресурсов $\{r_i\}$ до произвольного узла уровня ущерба $\{z(e_j, \sigma_n)\}$ равна 4, т. к. максимальное значение ребра между каждым уровнем равно 1. Это значение соответствует худшему варианту выбора тестового ИТВ. Наилучший вариант пути «затраты ресурсов – ИТВ – уязвимость – элементы объекта – ущерб» стремится к 0. Таким образом, «оптимальность» выбранного набора тестовых ИТВ относительно пути «затраты ресурсов – ИТВ – уязвимость – элементы объекта – ущерб» может быть оценена по степени приближения суммарного веса пути к нулю. Разница в суммарных весах различных путей, может выступать численной оценкой степени преимущества одного пути, по сравнению с другим.

4. ПРЕОБРАЗОВАНИЕ МОДЕЛИ ДЛЯ ПРИМЕНЕНИЯ К НЕЙ ТЕОРИИ ГРАФОВ

Представленная модель тестирования объекта КИИ (см. рисунок 1), в большей степени соответствует логике проведения тестирования, но не в полной мере подходит для применения к ней подходов исследования из теории графов, прежде всего – методов и алгоритмов поиска кратчайших путей.

В работах [38–40] обосновывается метод и алгоритмы одновременного поиска как кратчайших, так и дополнительных путей в графе, упорядоченных по убыванию расстояния. В работах [41, 42] рассматриваются прикладные вопросы кластеризации объектов, соответствующих определенному заранее заданному критерию. Предлагается, приняв за основу подходы, изложенные в работах [38–45], сформировать методики выбора тестовых ИТВ, обеспечивающих рациональную полноту тестирования объекта КИИ. Вместе с тем, для применения подходов [38–42] к модели тестирования объекта КИИ необходимо ее преобразовать таким образом, чтобы к ней было возможно применение алгоритмов поиска кратчайших и дополнительных путей в графе [38–40].

Основу преобразования иерархической модели составит объединение в единый кластер-вершину R всех вершин на уровне ресурсов и такое же объединение всех вершин в кластер-вершину Z на уровне ущерба [41, 42]. При этом значение весов ребер не изменяется, а переходные выражения, позволяющие из значения веса ребра определить соответствующие значение параметра модели, будут получены из выражений (1) и (5):

а) для пересчета значения веса ребра $v(R, i_j)$ в значение ресурса r_j, необходимое для проведения ИТВ i_j:

$$r_j = v(R, i_j) \cdot \sum_{n=1}^{N_I} r_n ; \qquad (6)$$

б) для пересчета значения веса ребра $v(e_j, Z)$ в значение ущерба z_l:

$$z(e_j, \sigma_n) = \left(\max_{\substack{m=1\dots N_E \\ n=1\dots 3}} \{z(e_m, \sigma_n)\} \right) - \left(v(e_j, Z) \cdot \sum_{m=1}^{N_E} \sum_{n=1}^{3} z(e_m, \sigma_n) \right) + 1. \qquad (7)$$

Пример преобразования модели для абстрактного прототипа объекта КИИ представлен на рисунке 2.

5. ПРИМЕР ФОРМИРОВАНИЯ МОДЕЛИ

Составим модель тестирования абстрактного объекта КИИ, взяв за основу схему на рисунке 1. При этом, в соответствии с рамками исследования, в качестве прототипа объекта КИИ рассмотрим некоторый абстрактный центр связи, имеющий в своем составе 10 элементов (под ними может пониматься, например, 10 одновременно функционирующих комплектов телекоммуникационного оборудования), которым свойственны 7 уязвимостей.

Рассмотрим вариант тестирования, в котором 6 тестовых ИТВ, 7 уязвимостей, 10 элементов объекта КИИ, которые, при нарушении конкретных свойств ИБ, соответствуют определенной стоимости ущерба, которая приведена в таблице 1. Причем каждое ИТВ для своей реализации требует такого же количества условных единиц ресурса, что и его номер, т. е. 1-е ИТВ требует 1-й единицы ресурса, 2-е ИТВ – 2-й единицы ресурса и т. д. По формуле (1) рассчитаем значение весов ребер $v(r_j, i_j)$, которые связывают каждое ИТВ i_j и соответствующее значение затрат ресурса r_j (колонка A таблицы 2).

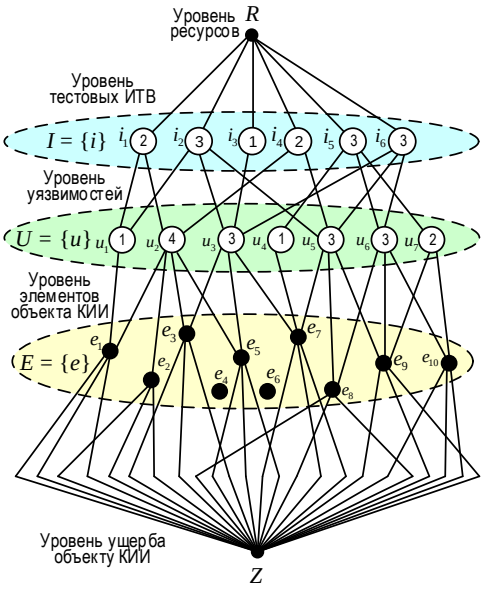

Рис. 2. Схема преобразования модели

Fig. 2. Scheme of Transformation the Model

ТАБЛИЦА 1. Исходные данные для моделирования ущерба в условных единицах

TABLE 1. Initial Data for Damage Modeling in Conventional Units

Свойства ИБ	Элементы объекта КИИ							
	e_1	e_2	e_3	e_5	e_7	e_8	e_9	e_{10}
σ_1	1	3	6	10	13	9	18	19
σ_2	2	5	8	12	16	15	21	22
σ_3	4	7	11	14	17	20	24	23

Определим степени вершин на уровне ИТВ $s(i_j|i_j \to \{u\})$ по количеству инцидентных им ребер, ведущих к элементам $\{u\}$. Затем по формуле (2) определим значения весов ребер $v(i_j, u_m)$, исходящих из вершин $\{i_j\}$ уровня ИТВ в вершины $\{u_m\}$ уровня уязвимостей (колонка *B* таблицы 2).

Определим степени вершин на уровне уязвимостей $s(u_j|u_j \to \{e\})$ по количеству инцидентных им ребер, ведущих к элементам $\{e\}$. Затем по формуле (3) определим значения весов ребер $v(u_j, e_l)$, исходящих из вершин $\{u_j\}$ уровня уязвимостей в вершины $\{e_l\}$ уровня элементов объекта (колонка *C* таблицы 2).

ТАБЛИЦА 2. Расчетные значения степеней вершин и весов ребер

TABLE 2. Calculated Values of Vertexes Degrees and Edges Weights

Уровни / № узла, j	*A.* Расчетные значения весов ребер $v(r_j, i_j)$, связывающих уровень ресурсов и уровень тестовых ИТВ	*B.* Расчетные значения степеней вершин $s(i_j\|i_j \to \{u\})$ на уровне тестовых ИТВ и значения весов ребер $v(i_j, u_m)$, связывающих уровень тестовых ИТВ и уровень уязвимостей		*C.* Расчетные значения степеней вершин $s(u_j\|u_j \to \{e\})$ на уровне уязвимостей и значения весов ребер $v(u_j, e_l)$, связывающих уровень уязвимостей и уровень элементов объекта КИИ	
	Вес ребра $v(r_j, i_j)$	Степень вершины $s(i_j\|i_j \to \{u\})$	Вес ребра $v(i_j, u_m)$	Степень вершины $s(u_j\|u_j \to \{e\})$	Вес ребра $v(u_j, e_l)$
1	0,048	2	0,083	1	0,143
2	0,095	3	0,056	4	0,036
3	0,143	1	0,167	3	0,048
4	0,19	2	0,083	1	0,143
4	0,238	3	0,056	3	0,048
5	0,286	3	0,056	3	0,048
6	0,048	2	0,083	2	0,071
7	–	–	–	1	0,143

При рассмотрении уровня элементов объекта КИИ введем допущение, что дестабилизирующее влияние одного элемента на другой отсутствует и все элементы рассматриваются независимо – $\forall P_{ДВ}(e_j, e_m, \sigma_n) = 0$, поэтому $\forall g(e_j, e_m, \sigma_n) = 1$. С учетом того, что значения $\forall v(u_j, e_l)$ и $\forall v(e_j, z_l)$ много меньше 1, то можно считать такое значение $\forall g(e_j, e_m, \sigma_n)$ «топологически непроходимым» и в дальнейших расчетах не учитывать.

В соответствии с выражением (5) определим значения весов ребер $v(e_j, z_l)$, исходящих из вершин $\{e_j\}$ уровня элементов в вершины $\{z_l\}$ уровня ущербов на основании исходных данных (см. таблицу 1). Значения весов ребер $v(e_j, z_l)$ представлены в таблице 3. В общем виде модель аудита защищенности объекта КИИ с рассчитанными значениями степеней вершин и весами ребер представлена на рисунке 3. Иерархическая модель позволяет вести анализ применимости тех или иных ИТВ методами теории графов – путем поиска кратчайших путей т. к. выбор весов ребер сформирован таким образом, чтобы меньшему значению веса ребра соответствовал «лучший вариант перехода» с одного уровня модели на другой.

ТАБЛИЦА 3. Значения весов ребер $v(e_j, z_l)$ по свойствам σ_n

TABLE 3. The Values of the Edge Weights $v(e_j, z_l)$ by the Properties σ_n

Свойства ИБ	Элементы объекта КИИ							
	e_1	e_2	e_3	e_5	e_7	e_8	e_9	e_{10}
σ_1	0,08	0,073	0,063	0,05	0,04	0,053	0,023	0,02
σ_2	0,077	0,067	0,057	0,043	0,030	0,033	0,013	0,01
σ_3	0,07	0,06	0,047	0,037	0,027	0,017	0,003	0,007

Например, применяя на топологической модели алгоритм поиска кратчайшего пути Дейкстры между множеством узлов на уровне ресурсов $\{r\}$ и узлов на уровне ущерба $\{z\}$, можно установить, что кратчайший путь между верхним и нижним уровнями лежит по узлам (r_2, i_2, u_5, e_9, z_{24}), а его длина равна 0,201. На основании этого можно сделать вывод о предпочтительности использования ИТВ i_2 для тестирования объекта КИИ (обозначен на рисунке 3 черной жирной линией). Дальнейший анализ возможностей использования этого ИТВ показывает, что оно может быть использовано для тестирования: уязвимостей $\{u_1, u_3, u_5\}$, элементов $\{e_1, e_3, e_5, e_7, e_8, e_9\}$ – пути тестирования обозначены на рисунке 3 серыми жирными линиями. При этом расходы условного ресурса для проведения тестирования составят $r = 2$. Суммарный выявленный и потенциально предотвращенный ущерб для всех свойств ИБ вышеуказанных элементов составит $\pi = 221$ условных единиц. Это значение, с учетом того, что суммарный ущерб по всем уязвимостям и элементам объекта КИИ равен 300 условным единицам, составляет относительное значение выявленного и потенциально предотвращенного ущерба $\pi_{отн} = 73$ %.

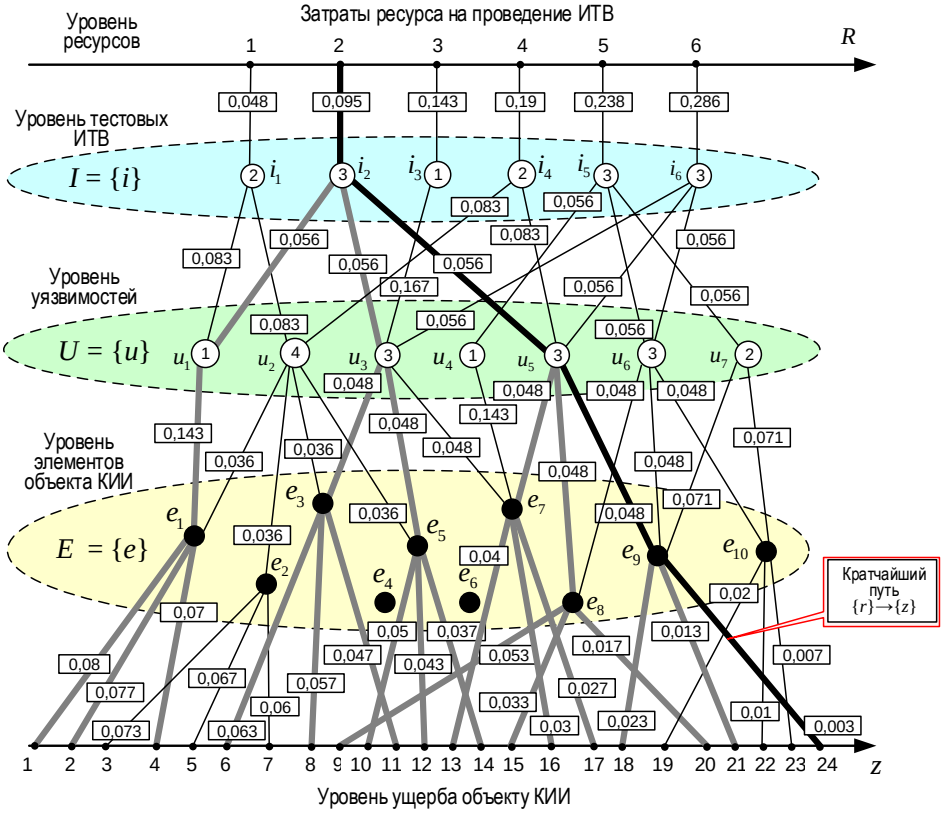

Рис. 3. Пример модель аудита защищенности объекта КИИ

Fig. 3. An Example of the Model of Security Audit of a Critical Information Infrastructure Object

ВЫВОДЫ

Данная модель формализует процесс тестирования объекта КИИ в виде многоуровневой топологической модели, отдельные уровни которой соответствуют: затратам ресурса на проведение ИТВ, тестовым ИТВ, уязвимостям, элементам объекта КИИ и уровням ущерба. Применение к данной модели методов поиска кратчайших путей позволяет определить «более лучшие» ИТВ по критерию «эффективность/стоимость», а также сформировать тестовые наборы ИТВ, которые обеспечат рациональную полноту аудита объекта КИИ. В дальнейшей работе данная модель используется в составе методики, для обоснования набора тестовых ИТВ для рациональной полноты оценки защищенности объекта КИИ в условиях ограниченных ресурсов.

Новизной представленной в данном подразделе модели тестирования защищенности объекта КИИ, отличающей ее от формальных подходов, представленных в работах [2, 32–37, 43, 44], является то, что модель в формальном виде взаимоувязано учитывает:

– эффективность отдельных тестовых ИТВ, в части выявленного и потенциально предотвращенного ущерба;

– ориентированность отдельных ИТВ на проверку конкретного множества уязвимостей определенных элементов объекта КИИ;

– расход в процессе тестирования определенного количества ресурса аудитора.

Исследование модели подходами из теории графов позволит обосновать тестовые наборы ИТВ обеспечивающих рациональную полноту аудита защищенности объекта КИИ.

Список используемых источников

1. Макаренко С.И. Аудит информационной безопасности: основные этапы, концептуальные основы, классификация мероприятий // Системы управления, связи и безопасности. 2018. № 1. С. 1–29. DOI:10.24411/2410-9916-2018-10101
2. Макаренко С.И. Аудит безопасности критической инфраструктуры специальными информационными воздействиями. Монография. СПб.: Наукоемкие технологии, 2018. 122 с.
3. Кашаев Т.Р. Алгоритмы активного аудита информационной системы на основе технологий искусственных иммунных систем. Автореф. дис. … канд. техн. наук. Уфа: УГАТУ, 2008. 19 с.
4. Марков А.С., Цирлов В.Л., Барабанов А.В. Методы оценки несоответствия средств защиты информации. М.: Радио и связь, 2012. 192 с.
5. Скабцов Н. Аудит безопасности информационных систем. СПб.: Питер, 2018. 272 с.
6. Penetration Testing. Procedures & Methodologies. EC-Council Press, 2011. 237 p.
7. Kennedy D., O'Gorman J., Kearns D., Aharoni M. Metasploit. The Penetration Tester's Guide. San Francisco: No Starch Press, 2011. 299 p.
8. Makan K. Penetration Testing with the Bash shell. Birmingham: Pact Publishing, 2014. 133 p.
9. Cardwell K. Building Virtual Pentesting Labs for Advanced Penetration Testing. Birmingham: Pact Publishing, 2016. 518 p.
10. Макаренко С.И. Информационное оружие в технической сфере: терминология, классификация, примеры // Системы управления, связи и безопасности. 2016. № 3. С. 292–376. DOI:10.24411/2410-9916-2016-10311
11. Макаренко С.И. Проблемы и перспективы применения кибернетического оружия в современной сетецентрической войне // Спецтехника и связь. 2011. № 3. С. 41–47.
12. Макаренко С.И., Смирнов Г.Е. Анализ стандартов и методик тестирования на проникновение // Системы управления, связи и безопасности. 2020. № 4. С. 44–72. DOI:10.24411/2410-9916-2020-10402
13. Климов С. М. Имитационные модели испытаний критически важных информационных объектов в условиях компьютерных атак // Известия ЮФУ. Технические науки. 2016. № 8(181). С. 27–36.
14. Климов С.М., Сычёв М.П. Стендовый полигон учебно-тренировочных и испытательных средств в области обеспечения информационной безопасности // Информационное противодействие угрозам терроризма. 2015. № 24. С. 206–213.
15. Петренко А.А., Петренко С.А. Киберучения: методические рекомендации ENISA // Вопросы кибербезопасности. 2015. № 3(11). С. 2–14.
16. Бойко А.А., Дьякова А.В. Способ разработки тестовых удаленных информационно-технических воздействий на пространственно распределенные системы информационно-технических средств // Информационно-управляющие системы. 2014. № 3(70). С. 84–92.
17. Бойко А.А., Дьякова А.В., Храмов В.Ю. Методический подход к разработке тестовых способов удаленного информационно-технического воздействия на пространственно распределенные системы информационно-технических средств // Кибернетика и высокие технологии XXI века XV Международная научно-техническая конференция. Воронеж: НПФ «САКВОЕЕ», 2014. С. 386–395.
18. Бойко А.А., Обущенко Е.Ю., Щеглов А.В. Особенности синтеза полного множества тестовых способов удаленного информационно-технического воздействия на пространственно распределенные системы информационно-технических средств // Вестник Воронежского государственного университета. Серия: Системный анализ и информационные технологии. 2017. № 2. С. 33–45.
19. Баранова Е.К., Худышкин А.А. Особенности анализа безопасности информационных систем методом тестирования на проникновение // Моделирование и анализ безопасности и риска в сложных системах. Труды международной научной школы МАБР. 2015. С. 200–205.
20. Баранова Е.К., Чернова М.В. Сравнительный анализ программного инструментария для анализа и оценки рисков информационной безопасности // Проблемы информационной безопасности. Компьютерные системы. 2014. № 4. С. 160–168.
21. Бегаев А.Н., Бегаев С.Н., Федотов В.А. Тестирование на проникновение. СПб: Университет ИТМО, 2018. 45 с.
22. Богораз А.Г., Пескова О.Ю. Методика тестирования и оценки межсетевых экранов // Известия ЮФУ. Технические науки. 2013. № 12(149). С. 148–156.
23. Дорофеев А. Тестирование на проникновение: демонстрация одной уязвимости или объективная оценка защищенности? // Защита информации. Инсайд. 2010. № 6(36). С. 72–73.
24. Умницын М.Ю. Подход к полунатурному анализу защищенности информационной системы // Известия Волгоградского государственного технического университета. 2018. № 8(218). С. 112–116.
25. Бородин М.К., Бородина П.Ю. Тестирование на проникновение средства защиты информации VGATE R2 // Региональная информатика и информационная безопасность. СПб., 2017. С. 264–268.

26. Полтавцева М.А., Печенкин А.И. Интеллектуальный анализ данных в системах поддержки принятия решений при тестировании на проникновение // Проблемы информационной безопасности. Компьютерные системы. 2017. № 3. С. 62–69.
27. Кадан А.М., Доронин А.К. Инфраструктурные облачные решения для задач тестирования на проникновение // Ученые записки ИСГЗ. 2016. Т. 14. № 1. С. 296–302.
28. Еременко Н.Н., Кокоулин А.Н. Исследование методов тестирования на проникновение в информационных системах // Master's Journal. 2016. № 2. С. 181–186.
29. Туманов С.А. Средства тестирования информационной системы на проникновение // Доклады Томского государственного университета систем управления и радиоэлектроники. 2015. № 2 (36). С. 73–79.
30. Кравчук А.В. Модель процесса удаленного анализа защищенности информационных систем и методы повышения его результативности // Труды СПИИРАН. 2015. № 1(38). С. 75–93.
31. Горбатов В.С., Мещеряков А.А. Сравнительный анализ средств контроля защищенности вычислительной сети // Безопасность информационных технологий. 2013. Т. 20. № 1. С. 43–48.
32. Pfleeger C.P., Pfleeger S.L., Theofanos M.F. A methodology for penetration testing // Computers & Security. 1989. Т. 8. № 7. С. 613–620.
33. McDermott J. P. Attack net penetration testing // NSPW. 2000. С. 15–21.
34. Alisherov F., Sattarova F. Methodology for penetration testing // International Journal of Grid and Distributed Computing. 2009. С. 43–50.
35. Ami P., Hasan A. Seven phrase penetration testing model // International Journal of Computer Applications. 2012. Т. 59. № 5. С. 16–20.
36. Holik F., Horalek J., Marik O., Neradova S., Zitta S. Effective penetration testing with Metasploit framework and methodologies // Proceedings of the 15th International Symposium on Computational Intelligence and Informatics (CINTI). IEEE, 2014. PP. 237–242. DOI:10.1109/CINTI.2014.7028682
37. Herzog P. Open-source security testing methodology manual // Institute for Security and Open Methodologies (ISECOM). 2003. URL: https://untrustednetwork.net/files/osstmm.en.2.1.pdf (дата обращения 12.02.2021)
38. Макаренко С.И. Метод обеспечения устойчивости телекоммуникационной сети за счет использования ее топологической избыточности // Системы управления, связи и безопасности. 2018. № 3. С. 14–30. DOI: 10.24411/2410-9916-2018-10302
39. Цветков К.Ю., Макаренко С.И., Михайлов Р.Л. Формирование резервных путей на основе алгоритма Дейкстры в целях повышения устойчивости информационно-телекоммуникационных сетей // Информационно-управляющие системы. 2014. № 2(69). С. 71–78.
40. Макаренко С.И., Квасов М.Н. Модифицированный алгоритм Беллмана-Форда с формированием кратчайших и резервных путей и его применение для повышения устойчивости телекоммуникационных систем // Инфокоммуникационные технологии. 2016. Т. 14. № 3. С. 264–274.
41. Макаренко С. И. Обеспечение устойчивости телекоммуникационной сети за счет ее иерархической кластеризации на области маршрутизации // Труды учебных заведений связи. 2018. Т. 4. № 4. С. 54–67. DOI:10.31854/1813-324X-2018-4-4-54-67
42. Макаренко С.И. Локализация областей воздействия дестабилизирующих факторов в сети связи на основе алгоритма иерархической кластеризации Ланса-Вильямса // Радиотехнические и телекоммуникационные системы. 2014. № 4(16). С. 70–77.
43. Аветисян А.И., Белеванцев А.А., Чукляев И.И. Технологии статического и динамического анализа уязвимостей программного обеспечения // Вопросы кибербезопасности. 2014. № 3(4). С. 20–28.
44. Мясников А.В. Построение модели информационной системы для автоматизации тестирования на проникновение // Проблемы информационной безопасности. Компьютерные системы. 2020. № 3. С. 32–39.

* * *

Model of Security Audit of a Critical Information Infrastructure Object with Use the Test Cyber Attacks

S. Makarenko[1, 2], **G. Smirnov**[2, 3]

[1]Saint-Petersburg Federal Research Center of the Russian Academy of Sciences,
St. Petersburg, 199178, Russian Federation
[2]Saint-Petersburg Electrotechnical University "LETI",
St. Petersburg, 197376, Russian Federation
[3]Intel Group ltd,
St. Petersburg, 197372, Russian Federation

Article info
DOI:10.31854/1813-324X-2021-7-1-94-104
Received 29th January 2021
Accepted 12th February 2021

For citation: Makarenko S., Smirnov G. Model of Security Audit of a Critical Information Infrastructure Object with Use the Test Cyber Attacks. *Proc. of Telecom. Universities.* 2021;7(1):94–104. (in Russ.) DOI:10.31854/1813-324X-2021-7-1-94-104

Abstract: *The article presents a model for auditing the security of a critical information infrastructure object by test information and technical influences. This model formalizes an object in the form audit process of a multilevel topological model, the individual levels of which correspond to: resource costs for impacts, test information and technical impacts, vulnerabilities, object elements and damage levels. The use of this model in audit practice will make it possible to substantiate the most effective impacts on the basis of the "efficiency / cost" criterion, as well as form test suites that will ensure the rational completeness of the audit of a critical infrastructure facility.*

Keywords: *critical information infrastructure, penetration testing, security audit, cyber attack.*

References

1. Makarenko S.I. Audit of Information Security - the Main Stages, Conceptual Framework, Classification of Types. *Systems of Control, Communication and Security*. 2018;1:1-29 (in Russ.) DOI:10.24411/2410-9916-2018-10101
2. Makarenko S.I. *Security audit of critical infrastructure with special information impacts. Monograph*. Saint Petersburg: Naukoemkie tehnologii Publ.; 2018. 122 p. (in Russ.)
3. Kashaev T.R. Algorithms for Active Audit of the Information System Based on Artificial Immune System Technologies. PhD Thesis. Ufa: Ufa State Aviation Technical University Publ.; 2008. 19 p. (in Russ.)
4. Markov A.S., Tsirlov V.L., Barabanov A.V. *Methods of Compliance of Information Security*. Moscow: Radio i Sviaz Publ.; 2012. 192 p. (in Russ.)
5. Skabtsov N. *Security Audit of Information Systems*. Saint Petersburg: Piter Publ.; 2018. 272 p. (in Russ.)
6. *Penetration Testing. Procedures & Methodologies*. EC-Council Press; 2011. 237 p.
7. Kennedy D., O'Gorman J., Kearns D., Aharoni M. *Metasploit. The Penetration Tester's Guide*. San Francisco: No Starch Press; 2011. 299 p.
8. Makan K. *Penetration Testing with the Bash shell*. Birmingham: Pact Publishing; 2014. 133 p.
9. Cardwell K. *Building Virtual Pentesting Labs for Advanced Penetration Testing*. Birmingham: Pact Publishing; 2016. 518 p.
10. Makarenko S.I. Information Weapon in Technical Area – Terminology, Classification and Examples. *Systems of Control, Communication and Security*. 2016;3:292-376. (in Russ.) DOI:10.24411/2410-9916-2016-10311
11. Makarenko S.I. Problems and Prospects for the Use of Cyber Weapons in Today's Network-Centric Warfare. *Specialized Machinery and Communication*. 2011;3:41–47. (in Russ.)
12. Makarenko S.I., Smirnov G.E. Analysis of Penetration Testing Standards and Methodologies. *Systems of Control, Communication and Security*. 2020;4:44–72. (in Russ.) DOI:10.24411/2410-9916-2020-10402
13. Klimov S.M. Imitating Models of Testing the Critically Important Information Objects in the Conditions of Computer Attacks. *Izvestiya SFedU. Engineering Sciences*. 2016;181(8):27–36. (in Russ.)
14. Klimov S.M., Sychev M.P. Poster polygon for training and testing facilities in the field of information security. *Information counteraction to the terrorism threats*. 2015;24:206–213. (in Russ.)
15. Petrenko A.A., Petrenko S.A. Cyber education: methodical recommendations ENISA. *Voprosy kiberbezopasnosti*. 2015;11(3):2–14. (in Russ.)
16. Boyko A.A., Djakova A.V. Method of Developing Test Remote Information-Technical Impacts on Spatially Distributed Systems of Information-Technical Tools. *Informatsionno-upravliaiushchie sistemy*. 2014;70(3):84–92. (in Russ.)
17. Boyko A.A., Djakova A.V. Hramov V.Ju. Methodological Approach to the Development of Test Methods for Remote Information Technology Impact on Spatially Distributed Systems of Information Technology Tools. *Cybernetics and high technologies of the XXI century XV international scientific and technical conference*. Voronezh: SAKVOEE Publ.; 2014. p.386–395 (in Russ.)
18. Boyko A.A., Obushenko E.Y., Shcheglov A.V. About synthesis of a full set of test methods of remote information-technical impacts on spatially distributed systems of information-technical tools. *Proceedings of Voronezh State University. Series: Systems analysis and information technologies*. 2017;2:33–45. (in Russ.)
19. Baranova E.K., Hudyshkin A.A. Features of Information System Security Analysis by Penetration Testing. *Proceedings of the international scientific school on Modeling and analysis of security and risk in complex systems, MABR-2015*]. 2015. p.200–205 (in Russ.)
20. Baranova E.K., Chernova M.V. Comparative analysis of programming tools for cybersecurity risk assessment. *Information Security Problems. Computer Systems*. 2014;4:160–168 (in Russ.)
21. Begaev A.N., Begaev S.N., Fedotov V.A. *Penetration testing*. Saint Petersburg: Saint Petersburg National Research University of Information Technologies Mechanics and Optics Publ.; 2018. 45 p. (in Russ.)
22. Bogoras A.G., Peskova O.Y. Methodology for testing and assessment of firewalls. *Izvestiya SFedU. Engineering Sciences*. 2013;149(12):148–156. (in Russ.)

23. Dorofeev A. Penetration Testing: Demonstration of One Vulnerability or an Objective Security Assessment? *Zaŝita informacii. Inside*. 2010;36(6):72–73. (in Russ.)
24. Umnitsyn M.Y. Approach to semi-natural security evaluation of information system. *Izvestia VSTU*. 2018;218(8): 112–116 (in Russ.)
25. Borodin M. K., Borodina P. Ju. VGATE R2 Information Security Penetration Testing. *Regional'naja informatika i informacionnaja bezopasnost* [*Regional Informatics and information security*]. Saint Petersburg, 2017. p.264–268 (in Russ.)
26. Poltavtseva M.A., Pechenkin A.I. Data mining methods in penetration tests decision support system. *Information Security Problems. Computer Systems*. 2017;3:62–69. (in Russ.)
27. Kadan A.M., Doronin A.K. Cloud infrastructure solutions for penetration testing. *Uchenye zapiski ISGZ*. 2016;14(1): 296–302. (in Russ.)
28. Eremenko N.N., Kokoulin A.N. Research of methods of penetration testing in information systems. *Master's Journal*. 2016;2:181–186 (in Russ.)
29. Tumanov S.A. Penetration testing tools for information systems. *Proceedings of Tomsk State University of Control Systems and Radioelectronics*. 2015;36(2):73–79. (in Russ.)
30. Kravchuk A. V. The model of process of remote security analysis of information systems and methods of improving it's performance. *SPIIRAS Proceedings*. 2015;38(1):75–93. (in Russ.)
31. Gorbatov V.S., Meshcheryakov A.A. Comparative analysis of computer network security scanners. *IT Security*. 2013;20(1):43–48. (in Russ.)
32. Pfleeger C.P., Pfleeger S.L., Theofanos M.F. A methodology for penetration testing. *Computers & Security*. 1989;8(7): 613–620.
33. McDermott J. P. Attack net penetration testing. *NSPW*. 2000:15–21.
34. Alisherov F., Sattarova F. Methodology for penetration testing. *International Journal of Grid and Distributed Computing*. 2009:43–50.
35. Ami P., Hasan A. Seven phrase penetration testing model. International Journal of Computer Applications. 2012;59(5):16–20.
36. Holik F., Horalek J., Marik O., Neradova S., Zitta S. Effective penetration testing with Metasploit framework and methodologies. *2014 IEEE 15th International Symposium on Computational Intelligence and Informatics (CINTI)*. IEEE; 2014. p.237–242. DOI:10.1109/CINTI.2014.7028682
37. Herzog P. Open-source security testing methodology manual. *Institute for Security and Open Methodologies (ISECOM)*. 2003. Available from: https://untrustednetwork.net/files/osstmm.en.2.1.pdf [Accessed 12th February 2021]
38. Makarenko S.I. Stability method of telecommunication network with using topological redundancy. *Systems of Control, Communication and Security*. 2018;3:14–30. (in Russ.) DOI:10.24411/2410-9916-2018-10302
39. Tsvetcov K.U., Makarenko S.I., Mikhailov R.L. Forming of Reserve Paths Based on Dijkstra's Algorithm in the Aim of the Enhancement of the Stability of Telecommunication Networks. *Informatsionno-upravliaiushchie sistemy.* 2014:69(2):71–78. (in Russ.)
40. Makarenko S.I., Kvasov M.N. Modified Bellman-Ford Algorithm with Finding the Shortest and Fallback Paths and its Application for Network Stability Improvement. *Infocommunikacionnye tehnologii.* 2016;14(3):264–274. (in Russ.) DOI:10.18469/ikt.2016.14.3.06
41. Makarenko S.I. Hierarchical Clustering of Telecommunication Network to the Independent Routing Areas for the Purposes to Ensure Stability. *Proceedings of Telecommunication Universities*. 2018;4(4):54-67. (in Russ.) DOI:10.31854/1813-324X-2018-4-4-54-67
42. Makarenko S.I. Area localization of destabilizing factors influence in communication network on the basis of Lance-Williams algorithm of hierarchical clustering. *Radio and telecommunication systems.* 2014;4:70–77. (in Russ.)
43. Avetisyan A.I., Belevantsev A.A., Chucklyaev I.I. The technologies of static and dynamic analyses detecting vulnerabilities of software. *Voprosy kiberbezopasnosti*. 2014;4(3):20–28 (in Russ.).
44. Myasnikov A.V. Building information system model for application in penetration testing automation problem. *Information Security Problems. Computer Systems*. 2020;3:32–39 (in Russ.).

Сведения об авторах:

МАКАРЕНКО Сергей Иванович — доктор технических наук, доцент, ведущий научный сотрудник лаборатории информационных технологий в системном анализе и моделировании Санкт-Петербургского федерального исследовательского центра РАН, профессор кафедры информационной безопасности Санкт-Петербургского государственного электротехнического университета «ЛЭТИ» им. В.И. Ульянова (Ленина), mak-serg@yandex.ru
https://orcid.org/0000-0001-9385-2074

СМИРНОВ Глеб Евгеньевич — преподаватель кафедры информационной безопасности Санкт-Петербургского государственного электротехнического университета «ЛЭТИ» им. В.И. Ульянова (Ленина), научный сотрудник ООО «Корпорация «Интел групп» science.cybersec@yandex.ru