МЕТОДИКА ОБОСНОВАНИЯ ТЕСТОВЫХ ИНФОРМАЦИОННО-ТЕХНИЧЕСКИХ ВОЗДЕЙСТВИЙ, ОБЕСПЕЧИВАЮЩИХ РАЦИОНАЛЬНУЮ ПОЛНОТУ АУДИТА ЗАЩИЩЕННОСТИ ОБЪЕКТА КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Макаренко С. И.[1], Смирнов Г. Е.[2]

Актуальность. *В настоящее время вопросы безопасности информационных систем объектов критической инфраструктуры приобретают важное значение. Вместе с тем текущие задачи аудита информационной безопасности (ИБ) объектов критической инфраструктуры, как правило, ограничиваются проверкой их на соответствие требованиям по ИБ со стороны руководящих документов. Однако при таком подходе к аудиту зачастую остается неясным защищенность этих объектов от реальных атак злоумышленников. Для объективной проверки такой защищенности объекты подвергают процедуре тестирования, а именно – тестированию на проникновение. Анализ отечественных и зарубежных публикаций в этой области показывает, что в настоящее время отсутствует какой-либо формальный подход к выбору тестовых информационно-технических воздействий при проведении такого тестирования.*

Целью работы *является формирование методики обоснования тестовых информационно-технических воздействий, обеспечивающих рациональную полноту аудита защищенности объекта критической информационной инфраструктуры.*

Методы исследования. *Для достижения цели исследования в работе использованы методы теории вероятностей и математической статистики, методы теории графов и теории множеств.*

Результаты. *В статье представлена методика обоснования тестовых информационно-технических воздействий. Данная методика формализует процесс выбора тестов в виде двухэтапной процедуры. На первом этапе на основе топологической модели тестирования объекта формируется множество путей тестирования, причем эти пути упорядочиваются по степени повышения веса. При этом, под весом пути понимается показатель «эффективность/стоимость» отдельной комбинации ресурса тестового воздействия, уязвимости элемента объекта и уровня ущерба, наносимого объекту по определенному свойству информационной безопасности. На втором этапе методики из упорядоченного множества путей тестирования производится выбор такого множества тестовых информационно-технических воздействий и формирование из них тестового набора, который бы обеспечивал максимизацию абсолютной суммарной стоимости обнаруженного ущерба, в рамках заданных ограничений на расход ресурса при тестировании. Использование представленной методики 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.*

DOI:10.21681/2311-3456-2021-6-12-25

Введение

В 2017 г. в России был принят федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», который устанавливает перечень информационных систем 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 реального тестирования объекта информационно-техническими воздействиями (ИТВ), аналогичными

1 Макаренко Сергей Иванович, доктор технических наук, доцент, ведущий научный сотрудник Санкт-Петербургского Федерального исследовательского центра Российской академии наук, г. Санкт-Петербург, Россия. E-mail: mak-serg@yandex.ru, ORCID: 0000-0001-9385-2074

2 Смирнов Глеб Евгеньевич, преподаватель кафедры информационной безопасности Санкт-Петербургского государственного электротехнического университета «ЛЭТИ» им. В.И. Ульянова (Ленина), г. Санкт-Петербург, Россия. E mail: science.cybersec@yandex.ru

тем, которые применяют злоумышленники и нарушители [3, 4]. Такой аудит позволяет на практике оценить эффективность технических и организационных мер защиты, а также выявить новые уязвимости объекта КИИ. В некоторых работах, например, таких как [5–11], для обозначения такого практического подхода к аудиту используется термин «тестирование на проникновение» (в англоязычной литературе – «penetration testing» или «pen-testing»), а также термины «активный аудит», «инструментальный аудит» и др. Несмотря на то, что такой аудит представляет собой достаточно адекватный и в высокой степени достоверный подход к оценке защищенности объектов КИИ, он не получил широкого распространения. Основными причинами этого, на взгляд авторов, является отсутствие единой общепризнанной научно-методической базы для проведения аудита такого типа.

На международном уровне проведение аудита защищенности какого-либо объекта информатизации путем использования тестов на проникновение регламентируется стандартами: OSSTMM; ISSAF; OWASP; PTES; NIST SP 800-115; BSI; PETA и др. Достаточно подробный содержательный анализ этих стандартов представлен в предыдущей работе авторов [13]. Однако, при этом в основу этих стандартов не положены какие-либо математические 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 («penetration testing») и «инструментальный аудит». Анализ вышеуказанных работ показал, что проведение «тестирования на проникновение» и «инструментального аудита» в отечественной практике не регламентируется какими-либо 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, выполняющей аудит.

Таким образом, можно сделать вывод, что перспективные направления 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., Pfleeger S.L., Theofanos M.F. [32], McDermott J.P. [33], Макаренко С.И. [2], Alisherov F., Sattarova F. [34], Ami P., Hasan A. [35], Но-

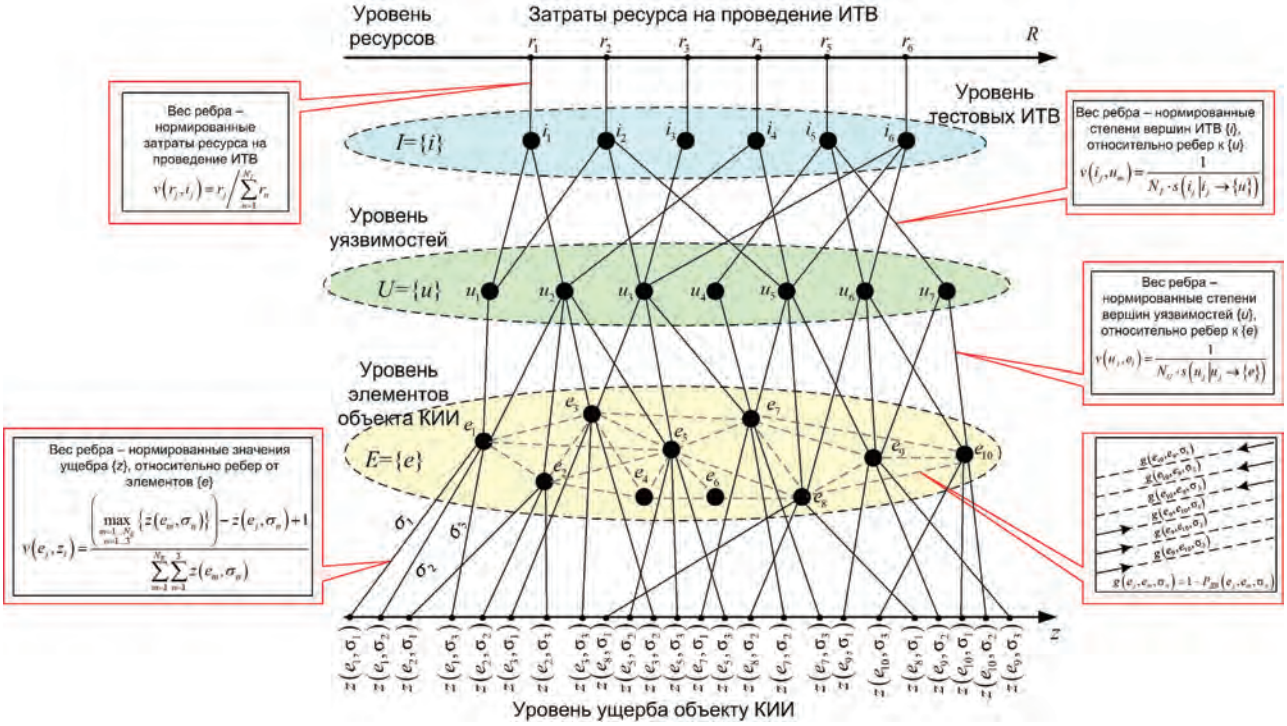

Рис. 1. Схема модели аудита защищенности объекта КИИ тестовыми ИТВ [39]

lik F., Horalek J., Marik O., Neradova S., Zitta S. [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., Pfleeger S.L., Theofanos M.F. [32], Alisherov F., Sattarova F. [34], Holik F., Horalek J., Marik O., Neradova S., Zitta S. [36], Herzog P. [37] представлены различные варианты методик тестирования. Однако в этих работах вопросы формирования методики обоснования наборов тестовых ИТВ для аудита защищенности объекта КИИ – не рассматривались. Как показано в работе [38], при обосновании набора тестовых ИТВ целесообразно руководствоваться критерием «эффективность / стоимость», выбирая те ИТВ, которые обеспечивают максимизацию полноты, оперативности и достоверности тестирования при минимизации стоимости разработки и проведения тестов. Именно этот подход принят за основу в данной работе.

Целью статьи является разработка методики обоснования тестовых ИТВ, обеспечивающих рациональную полноту аудита защищенности объекта КИИ.

В предыдущей статье по этой тематике [39] авторами была сформирована модель процесса тестирования объекта КИИ в виде многоуровневой топологической модели (рис. 1), 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.). В данной работе будет показано, как с использованием модели [39] сформировать набор тестовых ИТВ, обеспечивающий рациональную полноту аудита защищенности объекта КИИ.

Научная задача на разработку методики *m* обоснования набора тестовых ИТВ для рациональной полноты оценки уязвимостей объекта КИИ формулируется следующим образом. Сформировать такой набор тестовых ИТВ *I*={*i*}, который бы в условиях ограниченности ресурсов аудитора *R* максимизировал бы важность выявляемых уязвимостей {*u*}, с учетом того, что отдельным уязвимостям *u* и элементам объекта КИИ *e* сопоставляются уровни ущерба *z*(*e*, *u*, *i*, σ), наносимого объекту КИИ *S* по свойству ИБ σ (имеется ввиду: конфиденциальность целостность, доступность) при потенциальной эксплуатации уязвимости *u* элемента *e* злоумышленником путем применения *i*-го ИТВ. При этом абсолютным показателем рациональной полноты *π* является сумма «стоимости выявленного и потенциально предотвращенного ущерба» *z*(*e*, *u*, *i*, σ) при использовании тестового набора {*i*} для тестирования уязвимостей {*u*}, относительно тестируемых элементов объекта {*e*} и свойств ИБ {*σ*}:

$$\sum_{\{i\},\{u\},\{e\}} z(e,u,i,\sigma) = \pi. \quad (1)$$

Относительным значением рациональной полноты $\pi_{отн}$ является абсолютный показатель рациональной полноты *π*, отнесенный к сумме ущерба П по всем возможным комбинациям ИТВ {*i*} потенциальных злоумышленников, уязвимостей {*u*} элементов объекта {*e*} и свойств ИБ {*σ*}:

$$\pi_{отн} = \frac{\pi}{\Pi}. \quad (2)$$

Фактически требуется найти такие тестовые ИТВ, которые при ограниченных затратах ресурса *R* максимизировали бы стоимость выявленного и предотвращенного ущерба *π*.

Используемая система обозначений

Для формализации методики введем следующие обозначения:

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

$\pi_m/\pi_{отн\ m}$ – абсолютное/относительное значение полноты выявленного и потенциально предотвращенного ущерба *m*-ым ИТВ в тестовом наборе;

B – множество узлов потенциальных дополнительных путей тестирования;

C – множество весов ребер потенциальных дополнительных путей тестирования;

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

e_j – *j*-ый элемент объекта КИИ;

G(*W, V*) – граф модели тестирования защищенности объекта КИИ;

I = {*i*} – множество тестовых ИТВ;

i_j – *j*-ое тестовое ИТВ;

j, *l*, *m*, *n* – переменные-счетчики;

L – множество смежных помеченных вершин графа *G*, т.е. множество расстояний до помеченных вершин от начальной вершины;

N – количество узлов в графе *G;*

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

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

P – множество помеченных вершин в графе *G*;

Q – множество дополнительных путей в узлы, которое содержит дополнительные пути в рассматриваемый узел, сформированные в результате проведения логических операций над входящими в него элементами и элементами множеств *B* и *L*;

R – исходный узел ресурсов в графе *G* модели тестирования защищенности объекта КИИ;

$R_{гр}$ – ограничения на ресурс, расходуемый в процессе тестирования защищенности объекта КИИ;

$R_{тест}$ – затраты ресурса, необходимые для тестирования защищенности объекта КИИ тестовым набором *T*;

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

S – множество весов дополнительных путей к узлам графа G;

$T=\{t\}$ – множество тестовых ИТВ, выбранных для проведения тестирования защищенности объекта КИИ в результате применения методики;

t – тестовое ИТВ включенное в тестовый набор T для проведения тестирования защищенности объекта КИИ;

u – уязвимость объекта КИИ;

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

V – множество весов ребер в графе G модели тестирования защищенности объекта КИИ;

$V(W_n, W_j)$ – вес ребра, соединяющего произвольные n-ый и j-ый узлы графа G;

W – множество узлов графа G модели тестирования защищенности объекта КИИ, независимо от уровней расположения ($W = R \cup I \cup U \cup E \cup Z$);

Z – конечный узел ущерба в графе G модели тестирования защищенности объекта КИИ;

z – ущерб;

$z(e_j, \sigma_n)$ – 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;

$П$ – сумма ущерба по всем возможным комбинациям ИТВ $\{i\}$ потенциальных злоумышленников, уязвимостей $\{u\}$ элементов объекта $\{e\}$ и свойств ИБ $\{\sigma\}$.

Исходные положения и посылки

Разработка методики обоснования набора тестовых ИТВ предполагается вести на основе приложения подходов к исследованию теории графов к модели тестирования защищенности объекта КИИ [39]. Введем понятие «путь тестирования».

Путь тестирования – путь на графе модели тестирования защищенности объекта КИИ, проходящий через узлы и ребра, которые соответствуют единственной

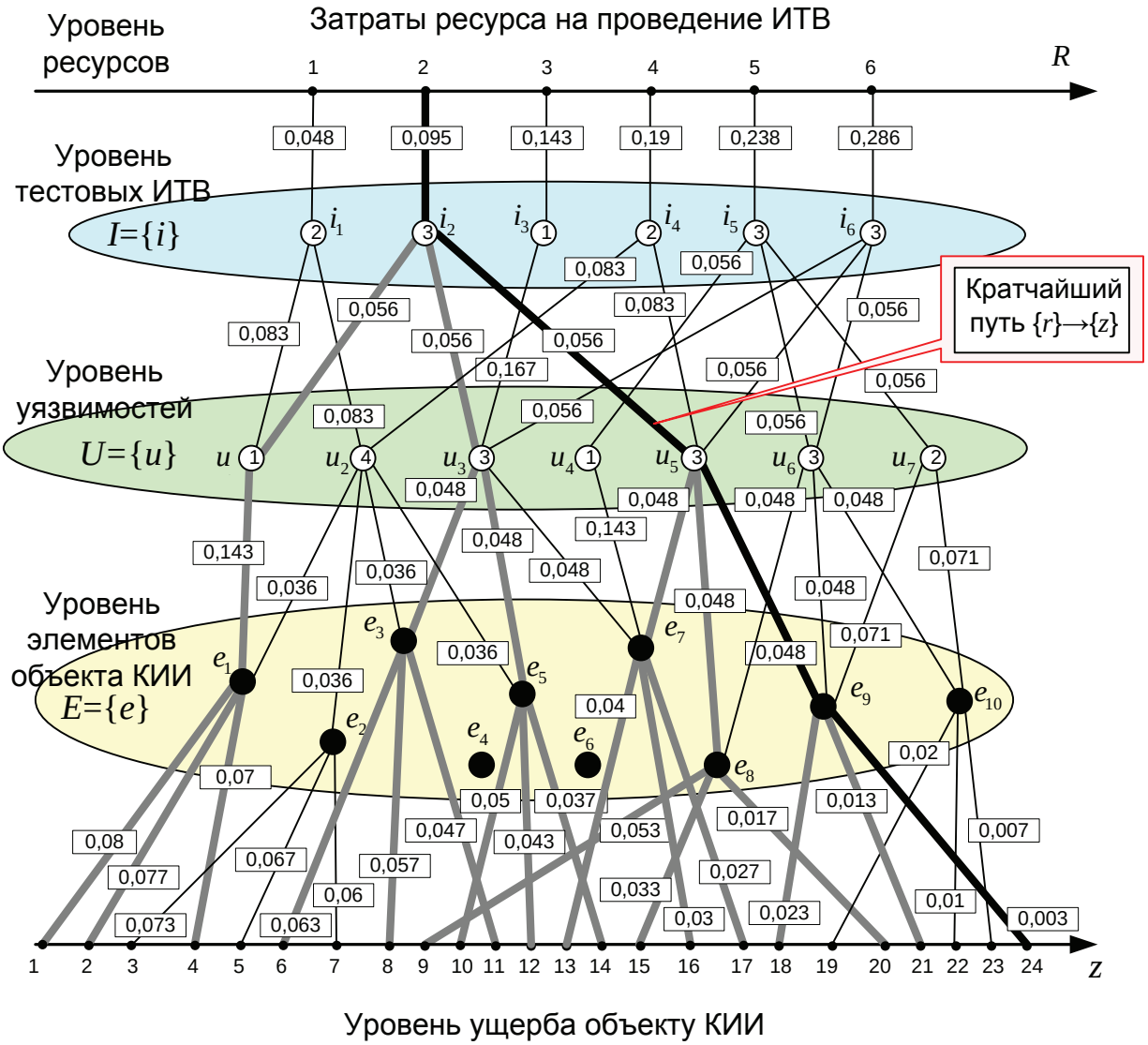

Рис. 2. Вариант модели аудита защищенности объекта КИИ [39]

оригинальной комбинации ресурса r_i, тестового ИТВ *i*, уязвимости *u* элемента объекта КИИ *e* и уровня ущерба *z*(*i*, *u*, *e*, *σ*), наносимого объекту КИИ S по свойству ИБ σ.

В результате введения такого понятия задача обоснования набора тестовых ИТВ может быть сведена к задаче поиска множества кратчайших путей тестирования на графе модели тестирования защищенности объекта КИИ.

В качестве графа, на котором будет вестись поиск путей тестирования, а также соответствующих им ИТВ, будем использовать преобразованную модель модели оценки защищенности объекта КИИ, вариант которой был представлен в работе [39] (рис. 2). Особенностью этого графа является то, что «наилучшие ребра», с точки зрения полноты и стоимости тестирования, обладают минимальным весом, а в целом, веса ребер упорядочены по мере возрастания весов, при переходе от «лучших», в смысле тестирования, к «худшим» путям тестирования.

Логика формирования набора тестовых ИТВ, подразумевает наличие направленного графа. В связи с этим преобразуем ненаправленный граф модели оценки защищенности объекта КИИ (рис. 2) в направленный граф, в котором направления ребер заданы сверху вниз (рис. 3).

Анализ фундаментальных работ в области теории графов [40, 41] показал, что для решения задачи вычис-

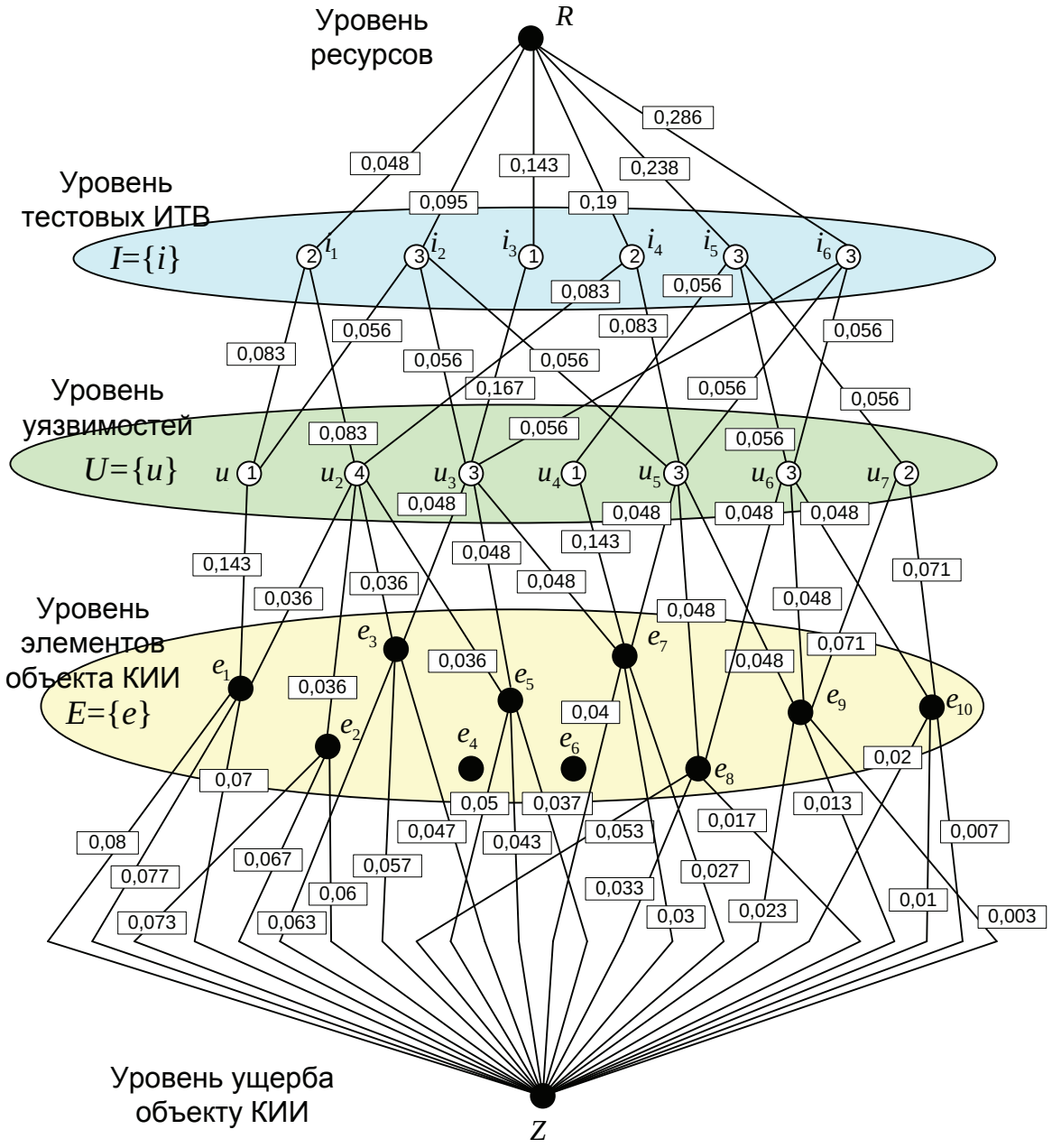

Рис. 3. Схема преобразования модели

ления кратчайших путей в графах применяются соответствующие математические алгоритмы поиска кратчайших путей. При этом наиболее широко используемым таким алгоритмом является алгоритм Дейкстры [42]. Однако особенностью этого алгоритма является то, что он является «поглощающим» и формирует из каждого узла графа к другому узлу только один путь, являющийся кратчайшим по сумме весов ребер в сети. Таким образом, можно обосновать только единственный оптимальный вариант одиночного ИТВ. Вместе с тем для обоснования набора нескольких ИТВ необходимо вычислять не только кратчайшие пути тестирования, но и другие комбинации путей, соответствующих другим ИТВ, после чего группировать их степени увеличения стоимости тестирования. Это требует формирования набора путей тестирования, которые были бы ранжированы, с одной стороны, по уровню вскрываемого ущерба, а с другой стороны, по степени затрат ресурсов на тестирование. Решение этой задачи потребует доработки математического алгоритма Дейкстры с целью добавления в него новой функциональности – способности формировать множество путей, ранжированных по суммарной метрике пути, из начального узла графа (*R*) в конечных узел (*Z*). Решение подобной задачи уже рассматривалось в работах авторов [43-47], однако эти работы не имеют отношения к вопросам ИБ, а посвящены исключительно вопросам обоснования маршрутов передачи данных в компьютерных сетях. Предлагается, приняв работы [43-47] за теоретический базис, разработать методику обоснования набора тестовых ИТВ путем нахождения комбинаций путей тестирования в графе модели, представленной на рис. 1, при этом в основу методики положить доработку известного алгоритма поиска кратчайших путей Дейкстры [42].

Этап формирования упорядоченного множества путей тестирования

В ходе модификации алгоритма Дейкстры в него дополнительно вносятся изменения, направленные на расширение его функциональности, связанной с возможностью формирования нескольких путей, ранжированных по степени повышения метрики. В основу предлагаемой модификации алгоритма Дейкстры являются следующие положения, ранее обоснованные в работе одного из авторов [43].

1) При достижении очередного узла в графе, запоминаются исходящие узлы входящих в этот узел ребер, как потенциальные элементы будущих дополнительных путей тестирования к этому узлу.

2) При очередном шаге функционирования методики, достигнутый очередной узел графа модели проверяется как потенциальный элемент дополнительного пути тестирования для всех уже достигнутых узлов. Если он является потенциальным элементом дополнительного пути, формируется дополнительный путь к ранее достигнутому узлу, через только что достигнутый узел.

3) Если к ранее достигнутому узлу графа модели уже были сформированы дополнительные пути, и он участвует в создании нового дополнительного пути к очередному узлу, то к очередному узлу формируется множество дополнительных путей с включением в них всех возможных вариантов дополнительных путей, сформированных ранее. Причем если в дополнительный путь входит сам очередной узел модели, то такой путь, во избежание циклов, в дополнительные не включается.

4) Все дополнительные пути к узлам модели упорядочиваются в соответствии с минимизацией суммы весов, входящих в них ребер, и вносятся в таблицу путей тестирования, одновременно с кратчайшим путем.

Схема формирования упорядоченного множества путей тестирования на основе модифицированного алгоритма Дейкстры, ранее разработанного авторами и представленного в работе [44], приведена на рис. 4.

Входными параметрами этого этапа методики являются:

а) граф модели тестирования защищенности объекта КИИ – $G(W, V)$, где: W – множество узлов графа G модели тестирования защищенности объекта КИИ, на основе которого формируются пути тестирования; V – множество весов ребер в графе G модели тестирования защищенности объекта КИИ.

б) количество узлов в графе G – N;

в) вес ребер, соединяющих произвольные n-ый и j-ый узлы $V(W_n, W_j)$ графа G.

Для обеспечения поиска не только кратчайшего, но и других дополнительных путей тестирования, помимо имеющихся множеств, предусмотренных логикой функционирования алгоритма Дейкстры (P – множество помеченных вершин, L – множество смежных помеченных вершин, множество расстояний до помеченных и вершин от начальной вершины) вводятся следующие дополнительные множества.

а) B – множество узлов потенциальных дополнительных путей. В это множество вносятся достигнутые узлы, смежные рассматриваемому. В дальнейшем, элементы множества используются при нахождении дополнительных путей.

б) C – множество весов ребер потенциальных дополнительных путей. В это множество вносятся веса ребер, исходящих из узлов, вносимых в множество B и входящих в рассматриваемый узел.

в) Q – множество дополнительных путей в узлы, содержит дополнительные пути в рассматриваемый узел, сформированные в результате проведения логических операций над входящими в него элементами и элементами множеств B и L.

г) S – множество весов дополнительных путей к узлам. Это множество содержит веса путей из множества Q и используется для ранжирования дополнительных путей при выводе результатов функционирования данного этапа методики.

К блокам, отличающим данный этап методики от известного алгоритма Дейкстры, относятся блоки 16-23, 25 на рис. 4. В блоках 16-17 реализуется формирование элементов множества узлов B к текущему рассматриваемому узлу за счет использования положения № 1 по модификации алгоритма Дейкстры. Далее, в блоках 18-23, путем пересечения элементов множества B и L, а также Q, осуществляется формирование элементов множества Q с учетом положения № 2 по модификации

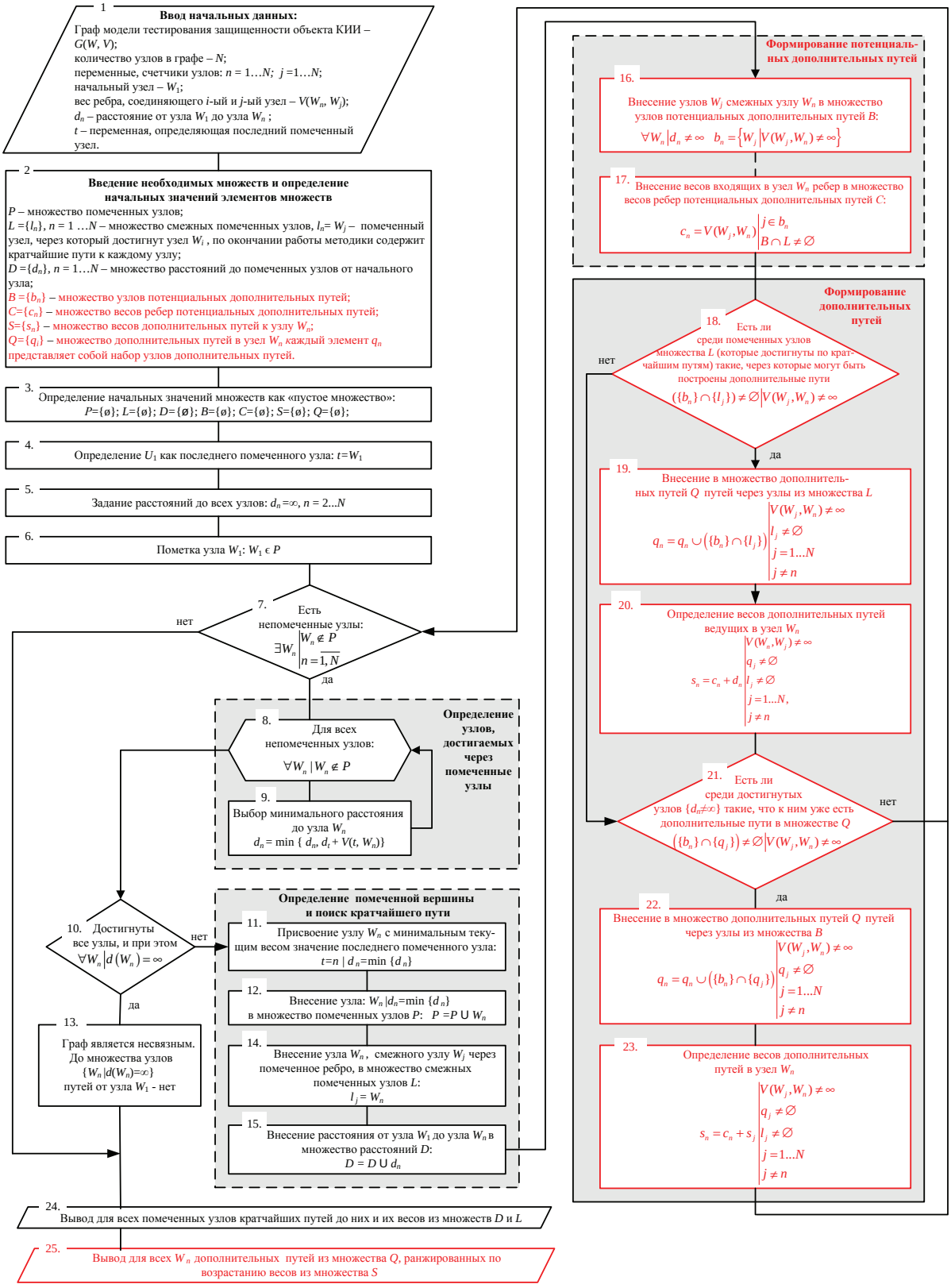

Рис. 4. Схема этапа формирования упорядоченного множества путей тестирования на основе модифицированного алгоритма Дейкстры

алгоритма Дейкстры. В блоке 25 осуществляется ранжировка дополнительных маршрутов по сумме весов, входящих в их состав ребер. Блоки 3-15, 24 соответствуют стандартному алгоритму Дейкстры. По итогам работы нулевому элементу множества Q присваивается значение кратчайшего пути из множества L.

Этап выбора путей тестирования, обеспечивающих рациональную полноту оценки уязвимостей, при ограничениях на ресурсы

Содержание данного этапа состоит в выборе из кратчайшего пути и упорядоченного по возрастанию весов множества путей Q (с весами сформированными в множестве S) на графе модели G такого ранжированного множества ИТВ и формирование из них тестового набора T, который бы обеспечивал максимизацию абсолютной суммарной стоимости обнаруженного ущерба $\pi \rightarrow \max$ (относительного значения $\pi_{отн} \rightarrow 100\%$), в рамках заданных ограничений на расход ресурса тестирования $R_{огр}$.

В целом этап выбора путей тестирования, обеспечивающих рациональную полноту оценки уязвимостей, при ограничениях на ресурсы, состоит из следующей последовательности шагов.

Шаг 0. Определение исходных данных. Множество тестовых ИТВ – пустое ($T=\varnothing$). Счетчик m элементов ИТВ в множестве T равен нулю ($m=0$). Множество тестовых ИТВ I включает в себя все рассматриваемые ИТВ. Затраты ресурса, необходимого для тестирования защищенности объекта КИИ равны нулю ($R_{тест}=0$). Вводим ограничение на затраты ресурса $R_{гр}$ при проведении тестирования.

Рассчитываем сумму ущерба П по всем возможным комбинациям ИТВ $\{i\}$ потенциальных злоумышленников, уязвимостей $\{u\}$ элементов объекта $\{e\}$ и свойств ИБ $\{\sigma\}$:

$$\sum_{\substack{\forall\{i\},\forall\{u\},\\ \forall\{e\},\forall\{\sigma\}}} z(e,u,i,\sigma) = \Pi.$$

Шаг 1. Если множество рассматриваемых ИТВ не пустое $I \neq \varnothing$ то из него выбирается ИТВ i_j, которое входит в путь q_k ($q_k \in Q$) в графе G с минимальным весом пути s_k ($s_k \in S$):

$$i_j = \{i\} \left| \left(s_k(q_k) = \min S\right) \wedge \left(i_j \in q_k\right). \right.$$

При первоначальном прогоне данного шага множество I будет содержать все возможные ИТВ $\{i\}$ и будет выбран кратчайший путь q_0 в графе G с весом s_0. При дальнейших прогонах – множество I будет убывать, за счет исключения ИТВ, а из множества Q будут последовательно выбираться дополнительные пути q_k из множества Q имеющие наименьший вес s_k.

Шаг 2. Определяются затраты ресурса необходимого на проведение ИТВ i_j. Значение ресурса r_j, расходуемого для проведения j-го ИТВ, для отдельных ребер графа G (рис. 3) пересчитываются из весов ребер $v(R, i_j)$ в соответствии с выражением:

$$r_j = v\left(R, i_j\right) \cdot \sum_{n=1}^{N_I} r_n,$$

где: r_j – затраты ресурса аудитора на проведение j-го тестового ИТВ; r_n – затраты ресурса аудитора на проведение n-го тестового ИТВ; N_I – количество тестовых ИТВ; n – переменная-счетчик.

Шаг 3. Проверяется условие: если при добавлении в тестовый набор j-го ИТВ i_j сумма текущих затрат ресурса на проведение теста $R_{тест}$ и r_j меньше ограничения на затраты ресурса $R_{гр}$, то увеличиваем счетчик ИТВ в тестовом наборе на 1 ($m = m+1$) и добавляем ИТВ i_j в тестовый набор ($t_m = i_j$, где $t_m \in T$), и продолжаем выполнение дальнейших операций. Если $R_{тест}+r_j > R_{гр}$, то ИТВ i_j в тестовый набор T не добавляется и из дальнейшего рассмотрения исключается ($I = I \setminus i_j$). В последнем случае возвращаемся к шагу 1.

Шаг 4. При принятии решения о добавлении ИТВ i_j в тестовый набор T в качестве элемента t_m, выполняются следующие операции:

а) Производится оценка абсолютного значения ущерба π_m, который может быть выявлен m-ым ИТВ в тестовом наборе, а также нарастающего итога по показателю $\pi = \sum_m \pi_m$. Для этого производится суммирование значений «стоимости» ущерба, который наносится объекту КИИ при использовании ИТВ i_j, путем суммирования значений ущерба $z(e_k, \sigma_n)$ в тех путях $\{q \mid i_j \in q\}$, которые содержат в качестве вершины ИТВ i_j:

$$\pi_m = \sum_{(e_k \wedge \sigma_n) \in \{q | i_j \in q\}} z\left(e_k, \sigma_n\right)$$

При этом значения ущерба $z(e_k, \sigma_n)$ для отдельных ребер графа G (рис. 3) пересчитываются из весов ребер $v(e_k, Z)$ в соответствии с выражением:

$$z\left(e_k, \sigma_n\right) = \left(\max_{\substack{l=1\ldots N_E \\ n=1\ldots 3}} \left\{z\left(e_l, \sigma_n\right)\right\}\right) - \left(v\left(e_k, Z\right) \cdot \sum_{l=1}^{N_E} \sum_{n=1}^{3} z\left(e_l, \sigma_n\right)\right) + 1,$$

где: $z(e_k, \sigma_n)$ – «стоимость» ущерба, который наносится объекту КИИ при нарушение σ_n-го свойства ИБ на его элементе e_k; N_E – количество элементов объекта КИИ, которое соответствует количеству элементов множества E; $n=1\ldots3$ – счетчик свойств ИБ σ_n; $\sum_{l=1}^{N_E} \sum_{n=1}^{3} z\left(e_l, \sigma_n\right)$ – сумма ущерба по всем элементам объекта КИИ и свойствам ИБ; $\max_{\substack{l=1\ldots N_E \\ n=1\ldots 3}} \left\{z\left(e_l, \sigma_n\right)\right\}$ – значение максимального ущерба среди всех комбинаций элементов и свойств ИБ.

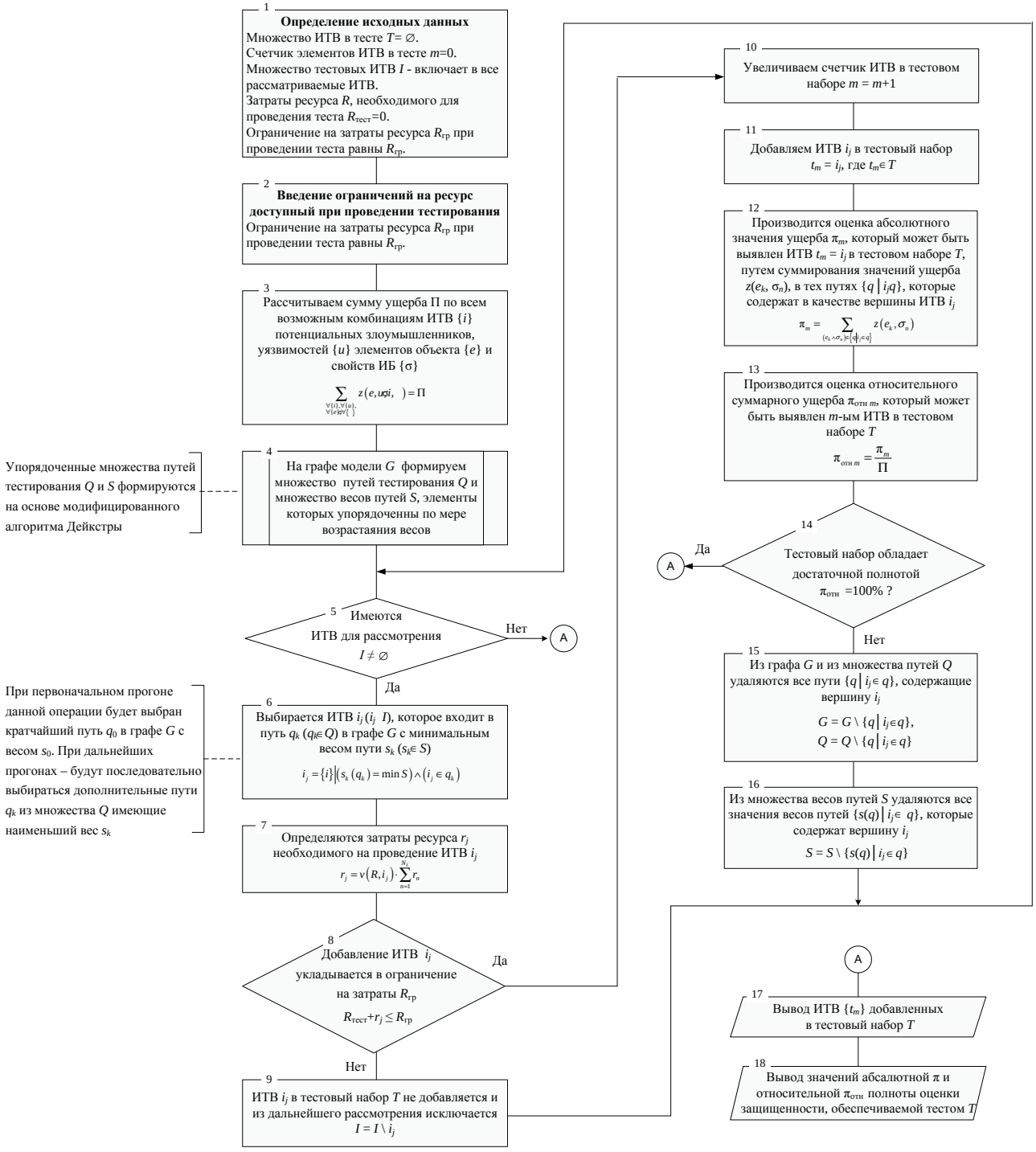

Рис. 5. Схема методики с конкретизацией этапа выбора путей тестирования, обеспечивающих рациональную полноту оценки уязвимостей при ограничениях на ресурсы

б) Производится оценка относительного суммарного ущерба $\pi_{отн\,m}$, который может быть выявлен m-ым ИТВ в тестовом наборе:

$$\pi_{отн\,m} = \frac{\pi_m}{\Pi},$$

а также оценка нарастающего итога по показателю:

$$\pi_{отн} = \sum_m \pi_{отн\,m}.$$

Шаг 5. Проверяем условия: если значение суммарного выявленного и потенциально предотвращенного ущерба р достаточно для заказчика тестирования, либо относительное значение выявленного и потенциально предотвращенного ущерба $\pi_{отн} \rightarrow 100\%$, то останавливаем процесс формирования тестового набора. Если вышеуказанные условия не выполняются, то продолжаем выполнение дальнейших операций.

Шаг 6. Производим операции удаления тех путей тестирования (комбинаций {i, u, e, σ}), которые уже охвачены ИТВ, включенными в тестовый набор T:

а) Из графа G и из множества путей Q удаляются все пути $\{q \mid i_j \in q\}$, содержащие вершину i_j:
$G = G \setminus \{q \mid i_j \in q\}$,
$Q = Q \setminus \{q \mid i_j \in q\}$.

б) Из множества весов путей S удаляются все значения весов путей $\{s(q) \mid i_j \in q\}$, которые содержат вершину i_j:
$S = S \setminus \{s(q) \mid i_j \in q\}$.

Шаг 7. Переходим к шагу 1.

Общая схема методики с конкретизацией этапа выбора путей тестирования, обеспечивающих рациональную полноту оценки уязвимостей, при ограничениях на ресурсы, представлена на рис. 5.

Выводы

Представленная методика на первом этапе позволяет на основе модели тестирования защищенности объекта КИИ формировать множество путей тестирования с их ранжированием по степени повышения веса. При этом под весом пути понимается показатель «эффективность/стоимость» отдельной комбинации ресурса r_i, тестового ИТВ i, уязвимости u элемента объекта КИИ e и уровня ущерба $z(i, u, e, \sigma)$, наносимого объекту КИИ S по свойству ИБ σ. На втором этапе методики производится выбор из кратчайшего пути и упорядоченного по возрастанию весов множества дополнительных путей такого ранжированного множества ИТВ $\{i\}$ и формирование из них тестового набора T, который бы обеспечивал максимизацию абсолютной суммарной стоимости обнаруженного ущерба $\pi \rightarrow \max$ (относительного значения $\pi_{отн} \rightarrow 100\%$), в рамках заданных ограничений на расход ресурса тестирования $R_{огр}$.

Элементами новизны данной методики, которые отличают ее как от известных научных работ в области «инструментального аудита» и «тестирования на проникновение» [1-11, 13-37], так и от известных руководств по тестированию на проникновение [12], является то, что, во-первых, методика основана на модели тестирования защищенности объекта КИИ, которая впервые разработана в данном исследовании, во-вторых, в состав методики введены оригинальные операции, которые на первом этапе методики за счет использования модификации известного алгоритма Дейкстры формируют упорядоченное множество путей тестирования, ранжированных по показателю «эффективность/стоимость», а на втором этапе методики – осуществляют формирование тестового набора, из тех ИТВ, которые являются элементами «лучших» путей тестирования, таким образом, чтобы тестовый набор максимизировал абсолютную суммарную стоимость обнаруженного ущерба в рамках заданных ограничений на расход ресурса тестирования.

Данная методика предполагается к внедрению в автоматизированные комплексы тестирования защищенности объекта КИИ, архитектура и функциональность которых изложена в работах [48, 49].

Рецензент: ***Марков Алексей Сергеевич***, доктор технических наук, профессор кафедры «Информационная безопасность» Финансового университета при Правительстве Российской Федерации, старший научный сотрудник. E-mail: a.markov@npo-echelon.ru

Исследование выполнено в рамках госбюджетной темы НИР СПИИРАН № 0073-2019-0004.

Литература

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. Критерии и показатели оценки качества тестирования на проникновение // Вопросы кибербезопасности. 2021. № 3 (43). С. 43-57. DOI: 10.21681/2311-3456-2021-3-43-57
39. 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
40. Татт У. Теория графов. М.: Мир, 1988. 424 с.
41. Свами М., Тхуласираман К. Графы, сети и алгоритмы. М.: Мир, 1984. 454 с.
42. Кормен Т., Лейзерсон Ч., Ривест Р. Алгоритмы: построение и анализ. М.: МЦНМО, 2000. 960 с.
43. 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
44. 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.
45. 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.
46. Макаренко С.И. Усовершенствованный протокол маршрутизации OSPF, обеспечивающий повышенную устойчивость сетей связи // Труды учебных заведений связи. 2018. Т. 4. № 2. С. 82–90.
47. Макаренко С.И. Усовершенствование функций маршрутизации и сигнализации протокола PNNI с целью повышения устойчивости сети связи // Труды учебных заведений связи. 2020. Т. 6. № 2. С. 45–59. DOI: 10.31854/1813-324X-2020-6-2-45-59
48. Смирнов Г. Е., Макаренко С. И. Использование тестовых информационно-технических воздействий для аудита защищенности информационных систем железнодорожного транспорта // Интеллектуальные технологии на транспорте. 2020. № 3 (23). С. 20–29.
49. Смирнов Г. Е., Макаренко С. И. Использование тестовых информационно-технических воздействий для превентивного аудита защищенности информационно-телекоммуникационных сетей // Экономика и качество систем связи. 2020. № 3 (17). С. 43–59.

SELECTION METHOD OF TEST CYBER ATTACKS THAT ENSURE THE RATIONAL COMPLETENESS OF THE PENETRATION TESTING OF A CRITICAL INFORMATION INFRASTRUCTURE OBJECT

Makarenko S. I.[3], Smirnov G. E.[4]

Relevance. *Security issues of information systems in critical infrastructure objects become important now. However, current tasks of information security audit of critical infrastructure objects are mainly limited to checking them for compliance with requirements of standards and documents. With this approach to the audit, security of these objects from real attacks by hackers remains unclear. Therefore, objects are subjected to a testing procedure, namely, penetration testing, in order to objectively verify their security. An analysis of publications in this area shows that there is not mathematical approaches to selection of test cyber attacks for penetration testing set.*

The goals of the paper *is to form the selection method of test cyber attacks that ensure the rational completeness of the security audit of a critical information infrastructure object.*

Research methods. *Methods of probability theory and mathematical statistics, methods of graph theory and set theory are used in the paper to achieve the research goals.*

Results. *The Select Method of test cyber attacks for security audit of a critical information infrastructure object with rational completeness is presented in the paper. This method formalizes the selection process in the form of a two-stage procedure. At the first stage, based on the topological model of the object testing, a set of testing paths is formed, and these paths are ordered by the degree of weight increase. The path weight is the efficiency/cost indicator*

3 Sergey I. Makarenko, Dr.Sc., Docent, Leading Researcher. St. Petersburg Federal Research Center of the Russian Academy of Sciences, Saint Petersburg Russia. E mail: mak-serg@yandex.ru. ORCID: 0000-0001-9385-2074

4 Gleb E. Smirnov, doctoral candidate. Lecturer at the Department of Information Security, Saint Petersburg Electrotechnical University «LETI», Saint Petersburg, Russia. E mail: science.cybersec@yandex.ru

that takes in account the test resource for realized of a test cyber attack, the vulnerability of an object element, and the level of damage caused to the element by this test cyber attack. At the second stage of the method, from an ordered set of test paths are selected of such, which would ensure the maximization of the whole absolute cost of the detected damage, within the limits on the resource making of test cyber attacks. It is using of this method in audit practice will allow us to justify the most effective test cyber attacks according to the "efficiency/cost" criterion, as well as to form test sets that will ensure the rational completeness of the audit of the critical infrastructure object.

Keywords: *critical information infrastructure, penetration testing, information security audit, information technology impact.*

References

1. Makarenko S. I. Audit informatcionnoi` bezopasnosti: osnovny`e e`tapy`, kontceptual`ny`e osnovy`, classifikatciia meropriiatii` // Sistemy` upravleniia, sviazi i bezopasnosti. 2018. № 1. S. 1-29. DOI: 10.24411/2410-9916-2018-10101
2. Makarenko S. I. Audit bezopasnosti kriticheskoi` infrastruktury` spetcial`ny`mi informatcionny`mi vozdei`stviiami. Monografiia. – SPb.: Naukoemkie tekhnologii, 2018. – 122 s.
3. Kashaev T. R. Algoritmy` aktivnogo audita informatcionnoi` sistemy` na osnove tekhnologii` iskusstvenny`kh immunny`kh sistem. Avtoref. dis. ... kand. tekhn. nauk. – Ufa: UGATU, 2008. – 19 s.
4. Markov A. S., Tcirlov V. L., Barabanov A. V. Metody` ocenki nesootvetstviia sredstv zashchity` informatcii. – M.: Radio i sviaz`, 2012. – 192 s.
5. Skabtcov N. Audit bezopasnosti informatcionny`kh sistem. – SPb.: Peter, 2018. – 272 s.
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. Informatcionnoe oruzhie v tekhnicheskoi` sfere: terminologiia, classifikatciia, primery` // Sistemy` upravleniia, sviazi i bezopasnosti. 2016. № 3. S. 292-376. DOI: 10.24411/2410-9916-2016-10311
11. Makarenko S. I. Problemy` i perspektivy` primeneniia kiberneticheskogo oruzhiia v sovremennoi` setecentricheskoi` voi`ne // Spetctekhnika i sviaz`. 2011. № 3. S. 41-47.
12. Makarenko S. I., Smirnov G. E. Analiz standartov i metodik testirovaniia na proniknovenie // Sistemy` upravleniia, sviazi i bezopasnosti. 2020. № 4. S. 44–72. DOI: 10.24411/2410-9916-2020-10402
13. Climov S. M. Imitatcionny`e modeli ispy`tanii` kriticheski vazhny`kh informatcionny`kh ob``ektov v usloviiakh komp`iuterny`kh atak // Izvestiia IUFU. Tekhnicheskie nauki. 2016. № 8 (181). S. 27-36.
14. Climov S. M., Sy`chyov M. P. Stendovy`i` poligon uchebno-trenirovochny`kh i ispy`tatel`ny`kh sredstv v oblasti obespecheniia informatcionnoi` bezopasnosti // Informatcionnoe protivodei`stvie ugrozam terrorizma. 2015. № 24. S. 206–213.
15. Petrenko A. A., Petrenko S. A. Kiberucheniia: metodicheskie rekomendatcii ENISA // Voprosy` kiberbezopasnosti. 2015. № 3(11). S. 2-14.
16. Boi`ko A. A., D`iakova A. V. Sposob razrabotki testovy`kh udalenny`kh informatcionno-tekhnicheskikh vozdei`stvii` na prostranstvenno raspredelenny`e sistemy` informatcionno-tekhnicheskikh sredstv // Informatcionno-upravliaiushchie sistemy`. 2014. № 3 (70). S. 84–92.
17. Boi`ko A. A., D`iakova A. V., KHramov V. Iu. Metodicheskii` podhod k razrabotke testovy`kh sposobov udalennogo informatcionno-tekhnicheskogo vozdei`stviia na prostranstvenno raspredelenny`e sistemy` informatcionno-tekhnicheskikh sredstv // Kibernetika i vy`sokie tekhnologii XXI veka XV Mezhdunarodnaia nauchno-tekhnicheskaia konferentciia. – Voronezh: NPF «SAKVOEE», 2014. – S. 386–395.
18. Boi`ko A. A., Obushchenko E. Iu., Shcheglov A. V. Osobennosti sinteza polnogo mnozhestva testovy`kh sposobov udalennogo informatcionno-tekhnicheskogo vozdei`stviia na prostranstvenno raspredelenny`e sistemy` informatcionno-tekhnicheskikh sredstv // Vestneyk Voronezhskogo gosudarstvennogo universiteta. Seriia: Sistemny`i` analiz i informatcionny`e tekhnologii. 2017. № 2. S. 33–45.
19. Baranova E. K., Hudy`shkin A. A. Osobennosti analiza bezopasnosti informatcionny`kh sistem metodom testirovaniia na proniknovenie // Modelirovanie i analiz bezopasnosti i riska v slozhny`kh sistemakh. Trudy` mezhdunarodnoi` nauchnoi` shkoly` MABR. 2015. S. 200–205.
20. Baranova E. K., Chernova M. V. Sravnitel`ny`i` analiz programmnogo instrumentariia dlia analiza i ocenki riskov informatcionnoi` bezopasnosti // Problemy` informatcionnoi` bezopasnosti. Komp`iuterny`e sistemy`. 2014. № 4. S. 160–168.
21. Begaev A. N., Begaev S. N., Fedotov V. A. Testirovanie na proniknovenie. – SPb: Universitet ITMO, 2018. – 45 s.
22. Bogoraz A. G., Peskova O. Iu. Metodika testirovaniia i ocenki mezhsetevy`kh e`kranov // Izvestiia IUFU. Tekhnicheskie nauki. 2013. № 12 (149). S. 148–156.
23. Dorofeev A. Testirovanie na proniknovenie: demonstratciia odnoi` uiazvimosti ili ob``ektivnaia ocenka zashchishchennosti? // Zashchita informatcii. Insai`d. 2010. № 6 (36). S. 72–73.
24. Umnitcy`n M. Iu. Podhod k polunaturnomu analizu zashchishchennosti informatcionnoi` sistemy` // Izvestiia Volgogradskogo gosudarstvennogo tekhnicheskogo universiteta. 2018. № 8(218). S. 112–116.
25. Borodin M. K., Borodina P. Iu. Testirovanie na proniknovenie sredstva zashchity` informatcii VGATE R2 // Regional`naia informatika i informatcionnaia bezopasnost`. – SPb., 2017. – S. 264–268.

26. Poltavtceva M. A., Pechenkin A. I. Intellektual`ny`i` analiz danny`kh v sistemakh podderzhki priniatiia reshenii` pri testirovanii na proniknovenie // Problemy` informatcionnoi` bezopasnosti. Komp`iuterny`e sistemy`. 2017. № 3. S. 62–69.
27. Kadan A. M., Doronin A. K. Infrastrukturny`e oblachny`e resheniia dlia zadach testirovaniia na proniknovenie // Ucheny`e zapiski ISGZ. 2016. T. 14. № 1. S. 296–302.
28. Eremenko N. N., Kokoulin A. N. Issledovanie metodov testirovaniia na proniknovenie v informatcionny`kh sistemakh // Master's Journal. 2016. № 2. S. 181–186.
29. Tumanov S. A. Sredstva testirovaniia informatcionnoi` sistemy` na proniknovenie // Doclady` Tomskogo gosudarstvennogo universiteta sistem upravleniia i radioe`lektroniki. 2015. № 2 (36). S. 73–79.
30. Kravchuk A. V. Model` protcessa udalennogo analiza zashchishchennosti informatcionny`kh sistem i metody` povy`sheniia ego rezul`tativnosti // Trudy` SPIIRAN. 2015. № 1 (38). S. 75–93.
31. Gorbatov V.S., Meshcheriakov A.A. Sravnitel`ny`i` analiz sredstv kontrolia zashchishchennosti vy`chislitel`noi` seti // Bezopasnost` informatcionny`kh tekhnologii`. 2013. T. 20. № 1. S. 43–48.
32. Pfleeger C. P., Pfleeger S. L., Theofanos M. F. A methodology for penetration testing // Computers & Security. 1989. T. 8. № 7. S. 613–620.
33. McDermott J. P. Attack net penetration testing // NSPW. 2000. S. 15–21.
34. Alisherov F., Sattarova F. Methodology for penetration testing // International Journal of Grid and Distributed Computing. 2009. S. 43–50.
35. Ami P., Hasan A. Seven phrase penetration testing model // International Journal of Computer Applications. 2012. T. 59. № 5. S. 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 (data obrashcheniia 12.02.2021)
38. Makarenko S. I. Kriterii i pokazateli ocenki kachestva testirovaniia na proniknovenie // Voprosy` kiberbezopasnosti. 2021. № 3 (43). S. 43-57. DOI: 10.21681/2311-3456-2021-3-43-57
39. Makarenko S. I., Smirnov G. E. Model` audita zashchishchennosti ob``ekta kriticheskoi` informatcionnoi` infrastruktury` testovy`mi informatcionno-tekhnicheskimi vozdei`stviiami // Trudy` uchebny`kh zavedenii` sviazi. 2021. T. 7. № 1. S. 94–104. DOI: 10.31854/1813-324X-2021-7-1-94-104
40. Tatt U. Teoriia grafov. – M.: Mir, 1988. – 424 s.
41. Svami M., Thulasiraman K. Grafy`, seti i algoritmy`. – M.: Mir, 1984. – 454 s.
42. Kormen T., Lei`zerson Ch., Rivest R. Algoritmy`: postroenie i analiz. – M.: MTCNMO, 2000. – 960 s.
43. Makarenko S. I. Metod obespecheniia ustoi`chivosti telekommunikatcionnoi` seti za schet ispol`zovaniia ee topologicheskoi` izby`tochnosti // Sistemy` upravleniia, sviazi i bezopasnosti. 2018. № 3. S. 14–30. DOI: 10.24411/2410-9916-2018-10302
44. TCvetkov K. Iu., Makarenko S. I., Mihai`lov R. L. Formirovanie rezervny`kh putei` na osnove algoritma Dei`kstry` v tceliakh povy`sheniia ustoi`chivosti informatcionno-telekommunikatcionny`kh setei` // Informatcionno-upravliaiushchie sistemy`. 2014. № 2 (69). S. 71–78.
45. Makarenko S. I., Kvasov M. N. Modifitcirovanny`i` algoritm Bellmana-Forda s formirovaniem kratchai`shikh i rezervny`kh putei` i ego primenenie dlia povy`sheniia ustoi`chivosti telekommunikatcionny`kh sistem // Infokommunikatcionny`e tekhnologii. 2016. T. 14. № 3. S. 264–274.
46. Makarenko S.I. Usovershenstvovanny`i` protokol marshrutizatcii OSPF, obespechivaiushchii` povy`shennuiu ustoi`chivost` setei` sviazi // Trudy` uchebny`kh zavedenii` sviazi. 2018. T. 4. № 2. S. 82–90.
47. Makarenko S.I. Usovershenstvovanie funktcii` marshrutizatcii i signalizatcii protokola PNNI s tcel`iu povy`sheniia ustoi`chivosti seti sviazi // Trudy` uchebny`kh zavedenii` sviazi. 2020. T. 6. № 2. S. 45–59. DOI: 10.31854/1813-324X-2020-6-2-45-59
48. Smirnov G. E., Makarenko S. I. Ispol`zovanie testovy`kh informatcionno-tekhnicheskikh vozdei`stvii` dlia audita zashchishchennosti informatcionny`kh sistem zheleznodorozhnogo transporta // Intellektual`ny`e tekhnologii na transporte. 2020. № 3 (23). S. 20–29.
49. Smirnov G. E., Makarenko S. I. Ispol`zovanie testovy`kh informatcionno-tekhnicheskikh vozdei`stvii` dlia preventivnogo audita zashchishchennosti informatcionno-telekommunikatcionny`kh setei` // E`konomika i kachestvo sistem sviazi. 2020. № 3 (17). S. 43–59.