УДК 004.056

Модель анализа защищенности объекта информатизации железнодорожного транспорта и методика обоснования набора тестовых информационно-технических воздействий для этого

Смирнов Г. Е.

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 модели анализа защищенности объекта информатизации железнодорожного транспорта и методики обоснования набора тестовых информационно-технических воздействий для этого, 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 модель анализа защищенности объекта информатизации железнодорожного транспорта и методика обоснования набора тестовых информационно-технических воздействий для этого. Методика основана на модели и 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.*

Библиографическая ссылка на статью:
Смирнов Г. Е. Модель анализа защищенности объекта информатизации железнодорожного транспорта и методика обоснования набора тестовых информационно-технических воздействий для этого // Системы управления, связи и безопасности. 2022. № 4. С. 137-189. DOI: 10.24412/2410-9916-2022-4-137-189

Reference for citation:
Smirnov G. E. Model for analyzing the security of an informatization object of railway transport and method for justifying a set of test cyber attacks for this. *Systems of Control, Communication and Security*, 2022, no. 4, pp. 137-189 (in Russian). DOI: 10.24412/2410-9916-2022-4-137-189

Введение

В 2017 г. в России был принят федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». Данный закон устанавливает перечень объектов, относящихся к критической информационной инфраструктуре (КИИ) РФ, а также обязует владельцев объектов КИИ разработать комплекс мер, направленных на обеспечение их информационной безопасности (ИБ). При этом к КИИ отнесен и железнодорожный транспорт (ЖТ), в связи с чем актуальным является формирование новых предложений по повышению полноты аудита ИБ объектов информатизации (ОИ) ЖТ как объекта КИИ.

В подавляющем числе случаев аудит ИБ объектов КИИ проводиться на основе сравнительного анализа с нормативно-правовой документацией, регламентирующей обеспечение ИБ, или на основе анализа рисков. Вместе с тем, в работах Макаренко С.И. [1, 2] указывается на необходимость формирования еще одного типа практического подхода к аудиту ИБ, 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. В некоторых работах, например, таких как [3-9], для такого подхода используется термин «тестирование на проникновение» (в англоязычной литературе – «penetration testing»), а также другие термины «активный аудит», «инструментальный аудит» и др., но при этом суть подобного практического подхода к аудиту не меняется.

Практическим вопросам оценки состояния ИБ ОИ и информационных систем (ИС) путем их тестирования посвящены отечественные работы Климова С. М. [11, 12], Петренко А. А., Петренко С. А. [13], Маркова А. С., Цирлова В. Л., Барабанова А. В. [4], Скабцова Н. [5], Бойко А. А. [14-16], Храмова В. Ю. [15-17], Щеглова А. В. [16, 17], Дьяковой А. В. [14, 15], Макаренко С.И. [1, 2]. Теоретическим вопросам развития тестирования, как средства контроля состояния ИБ объектов посвящены работы Пакулина Н. В., Шнитман В. З., Никешина А. В. [18], Аветисяна А. И., Белеванцева А. А., Чукляева И. И. [10] и Макаренко С.И. [1, 2, 43-49].

В работах Барановой Е.К. [19, 20], Бегаева А.Н., Бегаева С.Н., Федотова В.А. [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 оценивания защищённости информационных систем, как тестирование на проникновение или «penetration testing». В некоторых работах, такой тип тестирования указан под наименованием «инструментальный аудит».

Вопросам повышения защищённости ИО и ИС КИИ в условиях деструктивных информационных воздействий, в том числе и преднамеренно-тестирующего характера, посвящены работы Е.Б. Дроботуна [62-65].

Вопросам состава, структуры и функционирования ИС и ОИ ЖТ посвящены работы Г.В. Санькова, Т.А. Одуденко [32], О.А. Исакова [33], Г.В. Самме [34].

Вопросам оценки ИБ ОИ и ИС ЖТ посвящены работы: А.А. Корниенко [36-38], А.П. Глухова [35-37], В.В. Василенко [35, 36], А.А. Сидака [35, 36], С.Е. Ададурова [35, 37, 38], Е.И. Беловой [35, 37], Д.Н. Бирюкова [36], С.В. Диасамидзе [38], И.В. Котенко [39-42], И.Б. Саенко [40-42], А.А. Чечулина [39], Д.С. Левшуна [39], А.В. Чернова [42, 50], М.А. Бутаковой [42, 50].

Вместе с тем, анализ вышеперечисленных работ показывает, что вопросы оценки защищенности ОИ ЖТ именно за счет использования тестовых информационно-технических воздействий (ИТВ) исследованы в недостаточной степени.

Целью статьи является разработка модели анализа защищенности ОИ ЖТ и методики обоснования набора тестовых ИТВ для этого. Такое тестирование, по замыслу автора, дополнит стандартные мероприятия анализа защищенности ОИ ЖТ и повысит полноту оценки их ИБ.

Данная работа продолжает и развивает направление исследований, проводимое научной школой С.И. Макаренко, посвященное развитию теории и практики тестирования на проникновения специальными ИТВ в интересах аудита ИБ ИС, представленное в работах [1, 2, 43-49]. В частности, в основу данной работы положена интеграция научных результатов, полученных с участием автора, ранее представленных в работах [45, 46, 48].

1. Анализ объектов информатизации и информационных систем железнодорожного транспорта

Анализ работ Г.В. Санькова, Т.А. Одуденко [32], О.А. Исакова [33], Г.В. Самме [34] показал, что ИС ЖТ относится к классу больших корпоративных систем, содержащих большое количество ОИ и предназначена для решения как информационных задач, так и задач управления ЖТ. Главная цель применения ИС ЖТ состоит в информационном обеспечении технологических процессов и автоматизации принятия решений в сфере ЖТ, в интересах достижения максимальной эффективности его работы в условиях рыночной экономики.

ИС ЖТ представляется в виде двухуровневой структуры. Первый уровень – обеспечивающий, представлен информационной средой и инфраструктурой информатизации, второй уровень – прикладной, реализуется путем использования ОИ и информационных технологий (ИТ), объединённых в ИТ-комплексы, решающих конкретные задачи управления и автоматизации функций ЖТ.

Информационная среда – информация, реализованная в системе баз данных (БД), которая обеспечивает функционирование ОИ, органов управления и отдельных пользователей ЖТ. Информационная среда формирует единое информационное пространство (ЕИП), в котором все абоненты и пользователи ЖТ обеспечены необходимой им информацией.

Инфраструктура информатизации ЖТ включает в себя:

1) главный вычислительный центр (ГВЦ) ЖТ, объединяющий и поддерживающий БД для проведения общесетевой маркетинговой, финансовой и экономической деятельности и управления перевозочным процессом;
2) информационно-вычислительные центры (ИВЦ) ЖТ на дорогах, реализующие комплексы информационных услуг для управлений и отделений дорог;
3) сети связи и телекоммуникаций, устройства автоматического съема информации с подвижного состава, вычислительное оборудование, обеспечивающее выполнение операций формирования, сбора, передачи, хранения, обработки и представления информации.

Отдельные ИТ, обеспечивают автоматизацию основных функций ЖТ, составляют ИТ-комплексы:

1) управление перевозочным процессом;
2) управление маркетингом, экономикой и финансами;
3) управление инфраструктурой ЖТ;
4) управление непроизводственной сферой.

Рассмотрим эти комплексы более подробно.

1. ИТ-комплекс управления перевозочным процессом обеспечивает информационное сопровождение в области грузовых и пассажирских перевозок. Основными функциями по управлению грузовыми перевозками являются организация поездо- и грузопотоков на сети, диспетчерское управление поездной работой, управление локомотивными и вагонными парками, грузовой и коммерческой работой, обслуживание грузовой клиентуры, разработка графика движения поездов, норм эксплуатационной работы, планирование перевозок и прочее. Основными функциями по управлению пассажирскими перевозками являются организация обслуживания пассажиров и информационно-справочный сервис, планирование пассажирских перевозок в международном и внутридорожном сообщении, управление нормативами, тарифами внутренних и международных перевозок, организацию эксплуатации и ремонта парка пассажирских вагонов, управление багажными и почтовыми перевозками, организацию билетно-кассовых операций и др. В рамках этого ИТ-комплекса функционируют:

– автоматизированная система оперативного управления перевозками (АСОУП) – основной элемент ИТ-комплекса управления перевозочным процессом;
– система резервирования и продажи билетов («Экспресс-2»);
– единые центры диспетчерского управления (ЕЦДУ);
– система учета, контроля дислокации, анализа использования и регулирования вагонного парка (ДИСПАРК);
– автоматизированная система контроля за использованием и продвижением контейнеров (ДИСКОН);
– автоматизированная система фирменного транспортного обслуживания (АКС ФТО);

– автоматизированные системы управления сортировочными (АСУ СС), грузовыми (АСУ ГС) станциями и контейнерными пунктами (АСУ КП);
– автоматизированная система централизованной подготовки и оформления перевозочных документов (ЭТРАН);
– сетевая интегрированная Российская информационно-управляющая система (СИРИУС) и др.

2. ИТ-комплекс управления маркетингом, экономикой и финансами охватывает финансовую деятельность, бухгалтерский учет, маркетинговую деятельность и тарифную политику, управление развитием отрасли ЖТ, технической политикой и научно-исследовательскими и опытно-конструкторскими работами, нормативно-правовую работу, управление эксплуатационными расходами и др. ИТ этого комплекса ориентированы на формирование заказов, увеличение доходов, укрепление конъюнктурного положения за счет сохранения и увеличения доли ЖТ на транспортном рынке страны, на стабильное обеспечение денежных и платежных ресурсов, минимизацию затрат, на совершенствование экономической работы и инвестиционной политики. В рамках комплекса функционируют и внедряются ИТ управления финансовой деятельностью, ресурсами, способы расчетов за грузовые перевозки, взаиморасчетов за пользование вагонами и др. Основу этого ИТ-комплекса составляет единый комплекс автоматизированной системы управления финансовой деятельностью (ЕК АСУФР).

3. ИТ-комплекс управления инфраструктурой ЖТ представлен базовыми информационными технологиями, охватывающими управление эксплуатационной работой пассажирского хозяйства, хозяйств пути и сооружений, информатизации и связи, хозяйства энергоснабжения, локомотивного и вагонного хозяйств, управление проектированием и капитальным строительством объектов инфраструктуры, управление ремонтно-восстановительными работами и работами в чрезвычайных условиях, управление промышленностью ЖТ, материально-техническим снабжением и т.д. В составе этого ИТ-комплекса функционируют различные автоматизированные системы управления технологическими процессами (АСУ ТП): управления путевым хозяйством, устройствами энергоснабжения, сигнализации, средствами информатизации и связи.

4. ИТ-комплекс информационных технологий управления непроизводственной сферой железнодорожного транспорта представляет собой совокупность функций, обеспечивающих управление персоналом, учебными заведениями, жилищно-коммунальным хозяйством, рабочим снабжением, здравоохранением.

Основными факторами, актуализирующими значимость вопросов обеспечения ИБ, применительно к ИС ЖД, являются следующие [50]:

– интеграция в единые ИТ-комплексы подавляющего числа критических функций, связанных с управлением движением поездов и жизнедеятельности ЖТ;
– постоянное усложнение программного обеспечения (ПО) и оборудования, используемых в ИТ-комплексах управления ЖТ;

– существующая практика удаленной настройки и технического обслуживания элементов ИС ЖТ, осуществления разработчиками и поставщиками оборудования, входящего в состав элементов информационной инфраструктуры железнодорожного транспорта;
– интенсивное совершенствование потенциальными злоумышленниками средств и способов ИТВ, методов социальной инженерии для нанесения ущерба, а также участившиеся попытки их применения в противоправных целях и конкурентной борьбе;
– риск сокрытия попыток или фактов нарушения штатного функционирования ИС ЖТ со стороны эксплуатирующих подразделений;
– временное вынужденное привлечение к созданию элементов ИТ-комплексов ЖТ, в том числе АСО УП и различных АСУ ТП, производителей и поставщиков программно-аппаратных средств обработки, хранения и передачи информации и применение неконтролируемых программно-аппаратных решений.

Помимо вышеуказанных факторов, нужно отметить следующее. ЖТ является одним из ключевых элементов транспортной инфраструктуры РФ, обеспечивая до 88% грузооборота страны (для сравнения: доля автомобильного транспорта составляет 4%, а водного – 8%) [40]. В связи с этим ЖТ является одной из основных целей для злоумышленников и профессиональных нарушителей – сил информационных операций недружественных стран, при ведении информационного противоборства [1, 2]. В связи с этим, при обострении геополитической обстановки в мире информационная инфраструктура и ИС ЖТ РФ, могут оказаться объектом воздействия не только злоумышленников, но и профессиональных нарушителей, в связи с чем оценка реальной защищенности ОИ и ИС ЖТ является важной задачей, имеющий государственное значение.

2 Модель анализа защищенности объекта информатизации на основе использования тестовых информационно-технических воздействий

2.1 Постановка задачи на моделирование

Задача разработки модели соответствует формированию формального описания процесса тестирования ОИ 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; 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.).

Для формализации модели введем следующие обозначения:

π – абсолютное значение полноты выявленного и потенциально предотвращенного ущерба;

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

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

e_j – j-ый элемент ОИ;

$g(e_j, e_m, \sigma_n)$ – вес ребра соединяющего e_j и e_m элементы ОИ, 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 – переменная-счетчик;

l – переменная-счетчик;

m – переменная-счетчик;

n – переменная-счетчик;

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 ОИ;

$U=\{u\}$ – множество уязвимостей ОИ;

$v(x_1, x_2)$ – 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 ОИ;

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

2.2 Формализация модели на основе графоаналитического представления

Модель анализа защищенности ОИ на основе использования тестовых ИТВ представлена в формализме теории графов и теории множеств и имеет иерархическую структуру (рис. 1):

1) уровень ресурсов;

2) уровень тестовых ИТВ;

3) уровень уязвимостей;

4) уровень элементов ОИ;

5) уровень ущерба ОИ.

Рассмотрим структуру и формальные связи между этими уровнями подробно.

1. На 1-м 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:

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

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.

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. $\sum_{j=1}^{N_I} v\left(r_j, i_j\right) = 1$. 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.

2. На 2-м уровне модели формализуются множество тестовых ИТВ $I=\{i\}$, которые могут быть использованы для оценки защищенности ОИ.

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-м ИТВ для нанесения того или иного ущерба ОИ. Это соответствие i_j и $\{u_m\}$ формализуется множествами ребер $\{(i_j, u_m)\}$, где $m=1...M_j$ – 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:

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

где: $s\left(i_j \middle| i_j \to \{u\}\right)$ – степень вершины i_j, равная количеству инцидентных ей ребер, ведущих к элементам $\{u\}$, например, для схемы модели на рис. 1 $s(i_1)=2$, $s(i_2)=3$, $s(i_3)=1$; N_I – количество тестовых ИТВ, которое соответствует количеству элементов множества I.

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. $\sum_{j,m} v\left(i_j, u_m\right) = 1$. Во-вторых, ребру от более лучшего узла i, в смысле, ИТВ, те-

стирующему большее число уязвимостей $\{u_m\}$, должно соответствовать меньшее значение веса ребра.

3. На 3-м уровне модели формализуются множество уязвимостей $U=\{u\}$, которые потенциально присутствуют в элементах ОИ и могут быть использованы нарушителем для дестабилизирующего воздействия на элементы объекта и причинения ущерба.

Связь уровня уязвимостей с уровнем элементов ОИ 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-й уязвимости. Это соответствие u_j и $\{e_l\}$ формализуется множествами ребер $\{(u_j, e_l)\}$, где $l=1...L_j$ – счетчик ребер инцидентных вершине u_j. 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:

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

где: $s\left(u_j \middle| u_j \to \{e\}\right)$ – степень вершины u_j, равная количеству инцидентных ей ребер, ведущих к элементам $\{e\}$, например для схемы модели на рис. 1 $s(u_1)=2$, $s(u_3)=3$, $s(u_4)=1$; N_U – количество уязвимостей, которое соответствует количеству элементов множества U.

Выбор выражения (3) обусловлен следующими 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. $\sum_{j,l} v\left(u_j, e_l\right) = 1$. 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.

4. На 4-м уровне модели формализуются множество элементов ОИ $E=\{e\}$, дестабилизирующее воздействие на которые, через эксплуатацию тех или иных уязвимостей приведет к причинению ущерба.

На данном уровне существует два типа связей:

- связь элементов ОИ 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, при этом σ_1 – соответствует свойству доступности, σ_2 – целостности; σ_3 – конфиденциальности;
- связь вершин $\{e_j\}$ уровня элементов с вершинами $\{z_l\}$ уровня ущерба.

Связь элементов ОИ $\{e_j\}$ 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 $P_{ДВ}(e_j, e_m, \sigma_n)$:

$$g(e_j, e_m, \sigma_n) = 1\text{-}P_{ДВ}(e_j, e_m, \sigma_n). \tag{5}$$

Выбор выражения (5) обусловлен следующими соображениями. 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. становиться «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 ОИ с вершинами $\{z_l\}$ уровня ущерба осуществляется путем постановки в соответствие каждому элементу e_j по свойству ИБ σ_n (n=1 – доступность; n=2 – целостность; n=3 – конфиденциальность) 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:

$$v\left(e_j, z_l\right)=\frac{\left(\max\limits_{\substack{m=1\ldots N_E \\ n=1\ldots 3}}\left\{z\left(e_m,\sigma_n\right)\right\}\right)-z\left(e_j,\sigma_n\right)+1}{\sum\limits_{m=1}^{N_E}\sum\limits_{n=1}^{3} z\left(e_m,\sigma_n\right)}, \qquad (6)$$

где: $z(e_j, \sigma_n)$ – «стоимость» ущерба, который наносится ОИ при нарушение σ_n-го свойства ИБ на его элементе e_j; N_E – количество элементов ОИ, которое соответствует количеству элементов множества N; n=1...3 – счетчик свойств ИБ σ_n; $\sum\limits_{m=1}^{N_E}\sum\limits_{n=1}^{3} z\left(e_m,\sigma_n\right)$ – сумма ущерба по всем элементам ОИ и свойствам ИБ; $\max\limits_{\substack{m=1\ldots N_E \\ n=1\ldots 3}}\left\{z\left(e_m,\sigma_n\right)\right\}$ – значение максимального ущерба среди всех комбинаций элементов и свойств ИБ.

Выбор выражения (6) обусловлен следующими соображениями. Во-первых, множество весов ребер, ведущих с уровня элементов ОИ на уровень ущерба, должно стремиться к единице т.е. $\sum\limits_{j,l} v\left(e_j, z_l\right)\to 1$. 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.

5. На 5-м уровне модели формализуются значения ущербов ОИ, упорядоченные по возрастанию «стоимости». Каждое конкретное значение $z(e_j, \sigma_n)$ численно равно «стоимости» ущерба, который наносится ОИ при нарушении σ_n-го свойства ИБ на его элементе e_j.

В общем виде модель анализа защищенности ОИ на основе использования тестовых ИТВ представлена на рис. 1.

Особенностями данной модели является следующее.

Максимальная длина пути от произвольного узла уровня ресурсов $\{z_i\}$ 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 ОИ – ущерб» стремиться к 0.

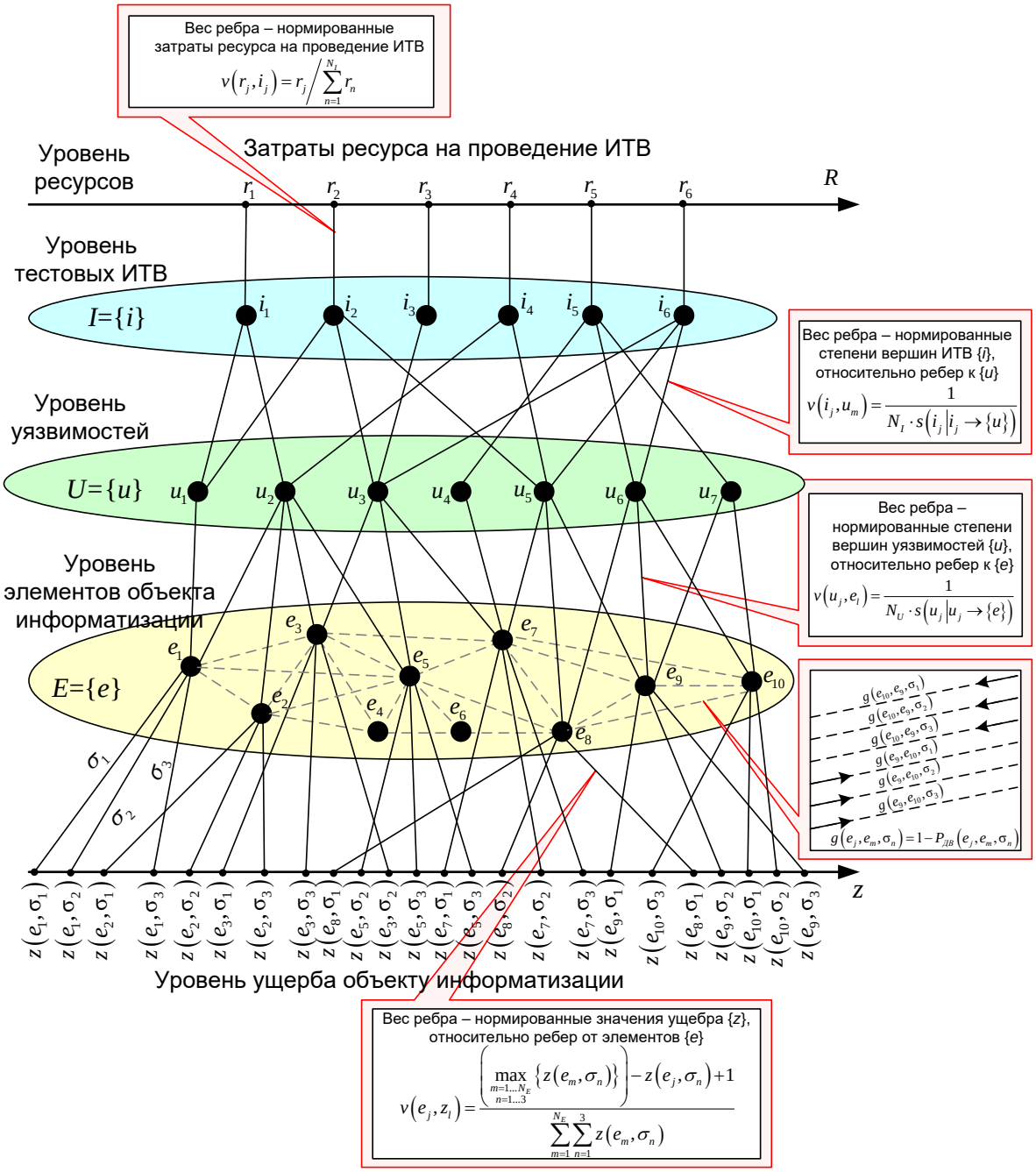


Рис. 1. Схема модели анализа защищенности ОИ
на основе использования тестовых ИТВ

Таким образом, «оптимальность» выбранного набора тестовых ИТВ относительно пути «затраты ресурсов – ИТВ – уязвимость – элементы ОИ – ущерб» могут быть оценены 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. Абсолютным значением полноты π выявленного и потенциально предотвращенного ущерба для ОИ, при выборе конкретного набора $\{i\}$ тестовых ИТВ, может служить значение суммы ущерба $z(e_j, \sigma_n)$, которое соответствует путям «ИТВ – уязвимость – элементы ОИ – ущерб», включенных в набор ИТВ $\{i\}$:

$$\sum_{\{i\}} z(e,u,i,\sigma)=\pi\,. \qquad (7)$$

Относительной полнотой $\pi_{\text{отн}}$ можно считать величину выявленного и потенциально предотвращенного ущерба отношение выявленного и предотвращенного ущерба при выборе конкретного набора $\{i\}$ тестовых ИТВ к суммарной стоимости ущерба для всех возможных комбинаций уязвимостей, элементов ОИ и их свойств ИБ:

$$\frac{\sum\limits_{\{i\}} z(e,u,i,\sigma)}{\sum\limits_{\forall\{u\},\{e\},\{\sigma\}} z(e,u,i,\sigma)} = \pi_{\text{отн}}. \qquad (8)$$

Пример формирования модели, для абстрактного прототипа ОИ, представлен в подразделе 2.3.

2.3 Пример формализации модели

Составим модель тестирования абстрактного ОИ взяв за основу схему на рис. 1. При этом, в соответствии с рамками исследования, в качестве прототипа ОИ рассмотрим абстрактный узел системы связи ИИ ЖТ, имеющий в своем составе 10 элементов, которым свойственны 7 уязвимостей.

Рассмотрим вариант тестирования, в котором 6 тестовых ИТВ, 7 уязвимостей, 10 элементов ОИ, 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-е единицы ресурса и т.д.

Таблица 1 – Исходные данные для моделирования ущерба в условных единицах

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

Рассчитаем значение весов ребер $v(r_j, i_j)$, которые связывают каждое ИТВ i_j и соответствующее значение затрат ресурса r_j по формуле (1). Расчетные значения весов ребер $v(r_j, i_j)$ представлены в таблице 2.

Таблица 2 – Расчетные значения весов ребер $v(r_j, i_j)$, связывающих уровень ресурсов и уровень тестовых ИТВ

№ узла, j	Вес ребра $v(r_j, i_j)$
1	0,048
2	0,095
3	0,143
4	0,19
4	0,238
5	0,286
6	0,048

Определим степени вершин на уровне ИТВ $s\left(i_j \middle| i_j \to \{u\}\right)$ 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. Значение степеней вершин $s\left(i_j \middle| i_j \to \{u\}\right)$ и значения весов ребер $v(i_j, u_m)$ представлены в таблице 3.

Таблица 3 – Расчетные значения степеней вершин $s\left(i_j \middle| i_j \to \{u\}\right)$ на уровне тестовых ИТВ и значения весов ребер $v(i_j, u_m)$, связывающих уровень тестовых ИТВ и уровень уязвимостей

№ узла, j	Степень вершины $s\left(i_j \middle| i_j \to \{u\}\right)$	Вес ребра $v(r_j, i_j)$
1	2	0,083
2	3	0,056
3	1	0,167
4	2	0,083
4	3	0,056
5	3	0,056
6	2	0,083

Определим степени вершин на уровне уязвимостей $s\left(u_j \middle| u_j \to \{e\}\right)$ 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. Значение степеней вершин $s\left(u_j \middle| u_j \to \{e\}\right)$ и значения весов ребер $v(u_j, e_l)$ представлены в таблице 4.

Таблица 4 – Расчетные значения степеней вершин $s\left(u_j \middle| u_j \to \{e\}\right)$ на уровне уязвимостей и значения весов ребер $v(u_j, e_l)$, связывающих уровень уязвимостей и уровень элементов ОИ

№ узла, j	Степень вершины $s\left(u_j \middle| u_j \to \{e\}\right)$	Вес ребра $v(r_j, i_j)$
1	1	0,143
2	4	0,036
3	3	0,048
4	1	0,143
4	3	0,048
5	3	0,048
6	2	0,071
7	1	0,143

При рассмотрении уровня элементов ОИ 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 (6) 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 в таблице 1. Значения весов ребер $v(e_j, z_l)$ представлены в таблице 5.

Таблица 5 – Значения весов ребер $v(e_j, z_l)$ по свойствам σ_n

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

В общем виде модель тестирования защищенности ОИ с рассчитанными значениями степеней вершин и весами ребер представлена на рис. 2.

Представленная на рис. 2 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.

Например, по результатам рассчитанной модели на рис. 2, применяя алгоритм поиска кратчайшего пути 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 ОИ. Дальнейший анализ возможностей использования этого ИТВ показывает, что оно может быть использовано для тестирования: уязвимостей $\{u_1, u_3, u_5\}$, элементов $\{e_1, e_3, e_5, e_7, e_8, e_9\}$, при этом расходы условного ресурса для проведения тестирования составят r=2. Суммарный выявленный и потенциально предотвращенный ущерб для всех свойств ИБ вышеуказанных элементов составит π=221 условных единиц. Это значение, с учетом того, что суммарный ущерб по всем уязвимостям и элементам ОИ равен 300 условным единицам, составляет относительное значение выявленного и потенциально предотвращенного ущерба $\pi_{отн}$=73%. Иллюстрация предпочтительности использования ИТВ i_2 для тестирования ОИ представлена рис. 3.

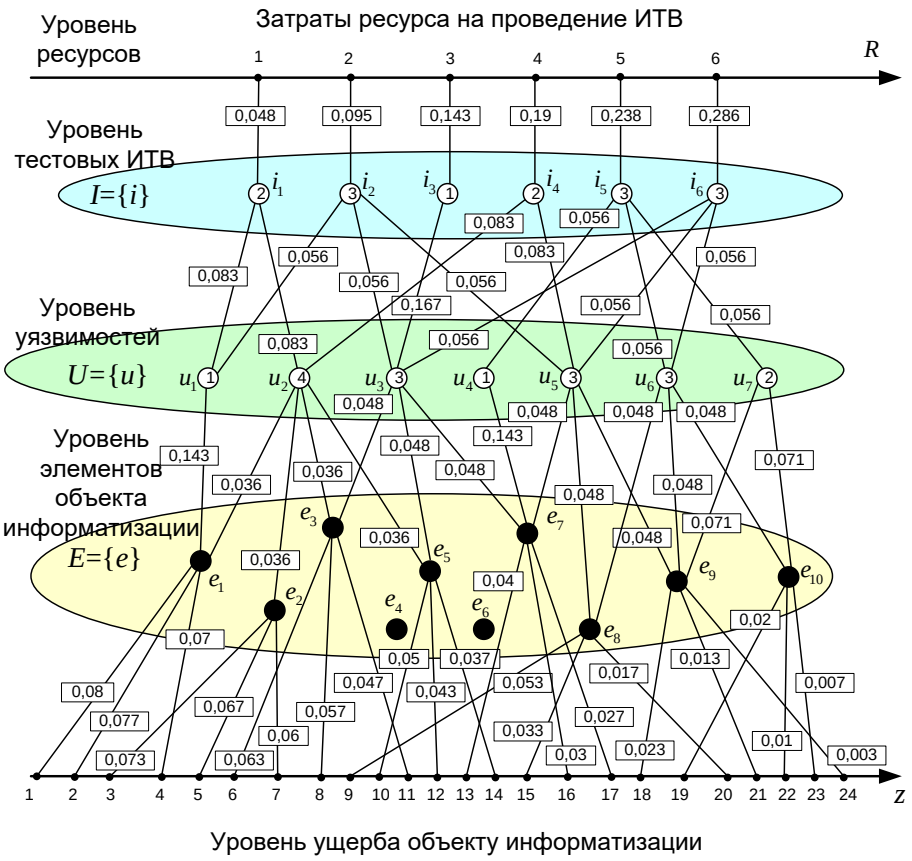


Рис. 2. Пример расчёта значений степеней вершин и весов ребер в модели анализа защищенности ОИ на основе использования тестовых ИТВ

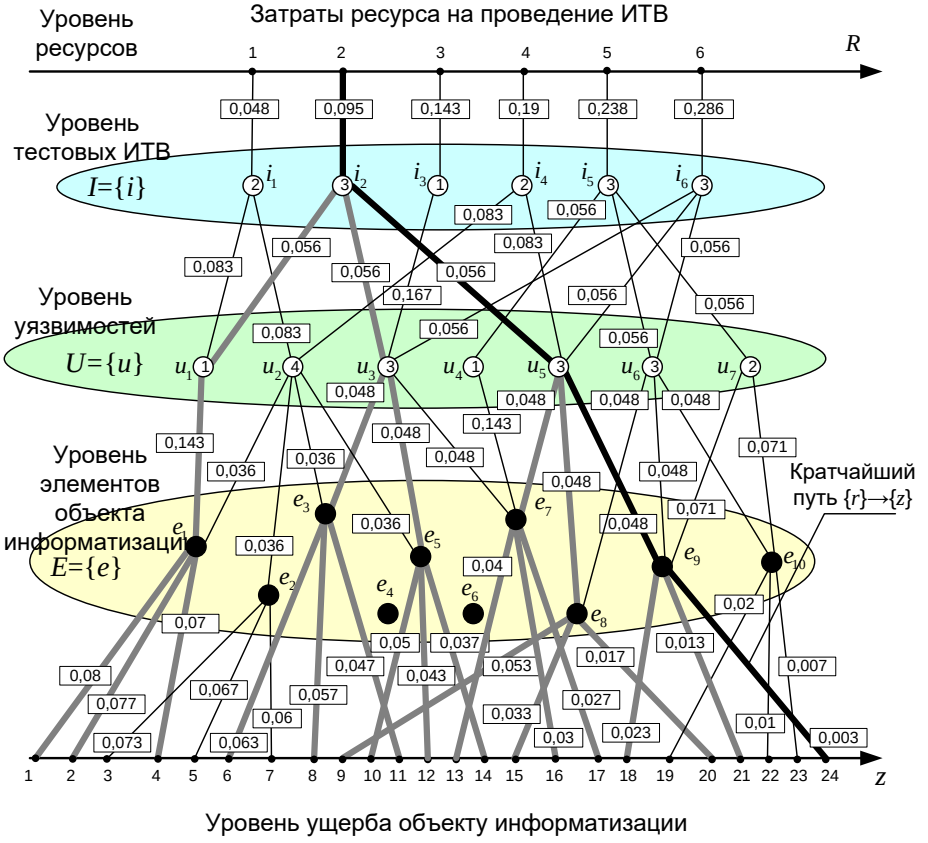


Рис. 3. Иллюстрация предпочтительности использования ИТВ i_2 для тестирования ОИ

2.4 Преобразование модели для применения к ней графоаналитических методов исследования

Представленная на рис. 1 модель анализа защищенности объекта информатизации на основе использования тестовых ИТВ, в большей степени соответствует логике проведения тестирования, но не в полной мере подходит для применения к ней графоаналитических методов исследования из теории графов, прежде всего – методов и алгоритмов поиска кратчайших путей.

В работах [51-55] обосновывается метод одновременного поиска как кратчайших, так и дополнительных путей, упорядоченных по убыванию в графе. В работах [56-58] рассматриваются прикладные вопросы кластеризации объектов, соответствующих определенному заранее заданному критерию. Предлагается, приняв подходы, изложенные в работах [51-58], за основу сформировать методику обоснования набора тестовых ИТВ для обеспечения рациональной полноты оценки уязвимостей объекта информатизации при ограничениях на стоимость ресурсов. Вместе с тем для применения подходов [51-58] к модели анализа защищенности объекта информатизации на основе использования тестовых ИТВ, необходимо ее преобразовать таким образом, чтобы к ней было возможно применение алгоритмов поиска кратчайших и дополнительных путей в графе [52, 53].

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 [56-58]. При этом значение весов ребер не изменяться, а переходные выражения, позволяющие из значения веса ребра определить соответствующие значение параметра модели будут получены из выражений (1) и (6):

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

$$r_j = v\left(R, i_j\right) \cdot \sum_{n=1}^{N_I} r_n ; \tag{9}$$

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;

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

$$z\left(e_j, \sigma_n\right) = \left(\max_{\substack{m=1...N_E \\ n=1...3}} \left\{ z\left(e_m, \sigma_n\right) \right\} \right) - \left(v\left(e_j, Z\right) \cdot \sum_{m=1}^{N_E} \sum_{n=1}^{3} z\left(e_m, \sigma_n\right) \right) + 1, \tag{10}$$

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

Вариант преобразования модели на рис. 3, в соответствии с вышеуказанными подходами, представлен на рис. 4.

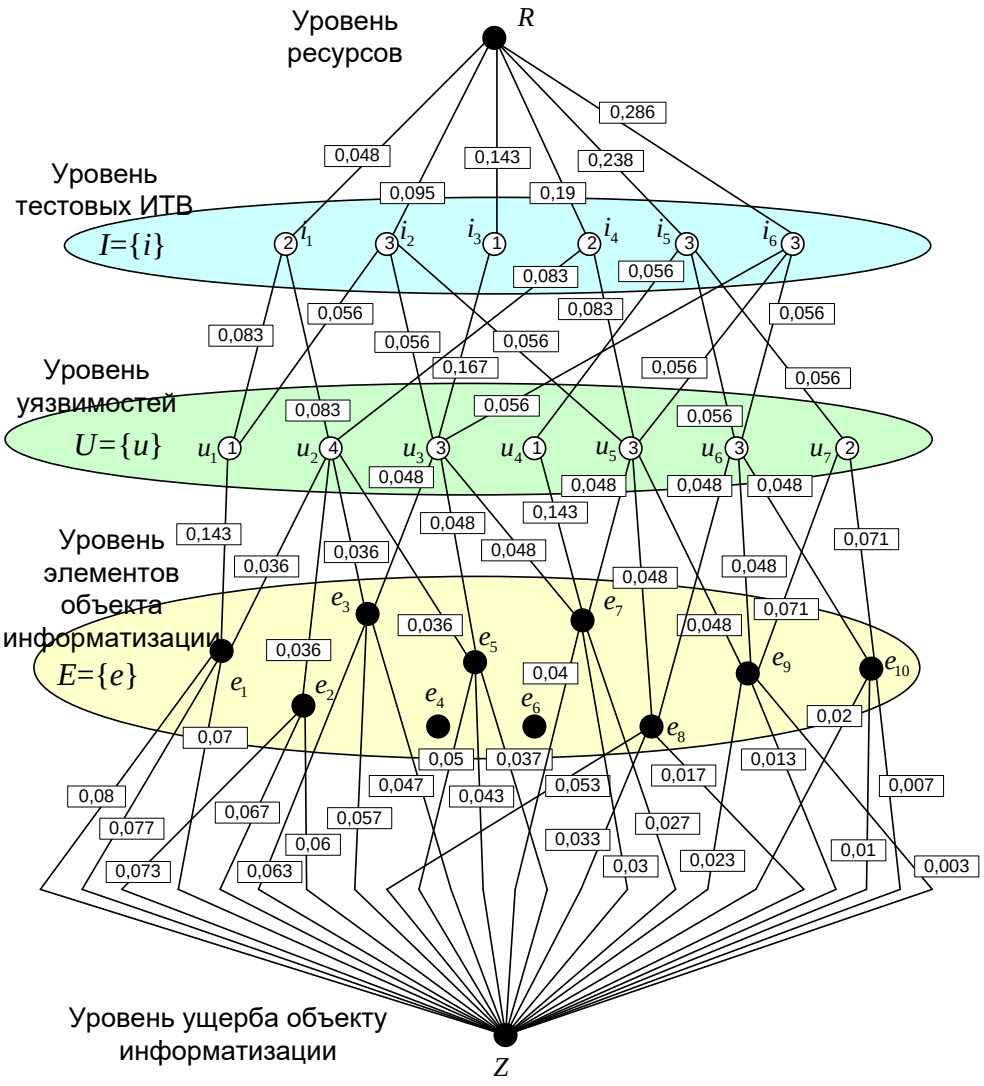


Рис. 4 Вариант преобразования модели анализа защищенности ОИ на основе использования тестовых ИТВ

2.5 Выводы по модели

Применение к процессу анализа защищенности ОИ путем использования тестовых ИТВ метода синтеза структуры графов позволило сформировать соответствующую модель. Данная модель формализует процесс анализа защищенности ОИ в виде многоуровневой топологической модели, отдельные уровни которой соответствует: затратам ресурса на проведение ИТВ, тестовым ИТВ, уязвимостям, элементам ОИ и уровням ущерба. Применение к данной модели графоаналитических методов, а именно – методов и алгоритмов поиска кратчайших путей позволяет определить «более лучшие» ИТВ по критерию «эффективность/стоимость», а также сформировать тестовые наборы ИТВ, которые обеспечат рациональную полноту аудита ОИ. В дальнейшей работе данная модель используется в составе методики обоснования набора тестовых ИТВ для

обеспечения рациональной полноты оценки уязвимостей ОИ при ограничениях на стоимость ресурсов.

Новизной, представленной в данном подразделе, модели тестирования защищенности ОИ, отличающей ее от формальных подходов, представленных в работах С.А. Петренко, И.В. Котенко, И.Б. Саенко, А.С. Маркова, В.Л. Цирлова, А.Н. Бегаева, С.М. Климова, А.А. Бойко и др., является то, что:

- на основе известного метода синтеза структуры графов сформирована оригинальная структура 4-х уровневого графа, увязывающего между собой: отдельные тестовые ИТВ; расход ресурса на их проведение; проверяемые уязвимости; тестируемые элементы и подсистемы объекта информатизации; показатели выявленного и потенциально предотвращенного ущерба;
- на основе известного аналитического метода математической индукции для графа модели обоснованы и введены функциональные зависимости для определения весов межуровневых ребер, с учетом: количества ИТВ; имеющегося ресурса аудитора; количества проверяемых уязвимостей, определяемых каждым ИТВ в каждом элементе объекта информатизации; показателем выявленного и потенциально предотвращенного ущерба соответствующей выявлению каждой уязвимости.

Исследование модели подходами из теории графов, позволяет обосновать тестовые наборы ИТВ, обеспечивающие рациональную полноту аудита и тестирования защищенности ОИ.

3 Методика обоснования набора тестовых ИТВ для обеспечения рациональной полноты оценки уязвимостей объекта информатизации при ограничениях на стоимость ресурсов

3.1 Постановка задачи на разработку методики

Задача разработки методики *m* обоснования набора тестовых ИТВ для рациональной полноты оценки уязвимостей ОИ в условиях ограниченных ресурсов может быть представлена как научно-обоснованное формирование такого набора 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 ОИ e сопоставляются уровни ущерба $z(e, u, i, \sigma)$, наносимого ОИ 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» $z(e,u,i,\sigma)$ при использовании тестового набора $\{i\}$ для тестирования уязвимостей $\{u\}$, относительно тестируемых элементов объекта $\{e\}$ и свойств ИБ $\{\sigma\}$:

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

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 $\{\sigma\}$:

$$\pi_{\text{отн}} = \frac{\pi}{\Pi}.$$

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

Для формализации методики введем следующие обозначения:

π – абсолютное значение полноты выявленного и потенциально предотвращенного ущерба;

π_m – абсолютное значение полноты выявленного и потенциально предотвращенного ущерба m-м ИТВ в тестовом наборе;

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

$\pi_{\text{отн}\,m}$ – относительное значение полноты выявленного и потенциально предотвращенного ущерба m-м ИТВ в тестовом наборе;

B – множество узлов потенциальных дополнительных путей тестирования;

C – множество весов ребер потенциальных дополнительных путей тестирования;

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

e_j – j-й элемент ОИ;

$G(W, V)$ – граф модели тестирования защищенности ОИ;

$I=\{i\}$ – множество тестовых ИТВ;

i_j – j-е тестовое ИТВ;

j – переменная-счетчик;

k – переменная-счетчик;

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

l – переменная-счетчик;

m – переменная-счетчик;

N – количество узлов в графе G;

n – переменная-счетчик;

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 ОИ;

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

$R_{\text{гр}}$ – ограничения на ресурс, расходуемый в процессе тестирования защищенности ОИ;

$R_{\text{тест}}$ – затраты ресурса, необходимые для тестирования защищенности ОИ тестовым набором T;

S – множество весов дополнительных путей к узлам графа G;

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

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

u – уязвимость ОИ;

$U=\{u\}$ – множество уязвимостей ОИ;

V – множество весов ребер в графе G модели тестирования защищенности ОИ.

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

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

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

z – ущерб;

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

$z(i, u, e, \sigma)$ – ущерб, от воздействия ИТВ i, через уязвимость u на элемент e по свойству ИБ σ;

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 ОИ $\{e\}$ и свойств ИБ $\{\sigma\}$.

3.2 Исходные положения и посылки

Разработка методики обоснования набора тестовых ИТВ предполагается вести на основе приложения подходов к исследованию теории графов к модели анализа защищенности объекта информатизации на основе использования тестовых ИТВ. Введем понятие «путь тестирования».

Путь тестирования – путь на графе модели тестирования защищенности ОИ, проходящий через узлы и ребра, которые соответствуют единственной оригинальной комбинации ресурса r_i, тестового ИТВ i, уязвимости u элемента объекта e и уровня ущерба $z(i, u, e, \sigma)$, наносимого объекту 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 анализа защищенности объекта информатизации на основе использования тестовых ИТВ.

В качестве графа, на котором будет весить поиск путей тестирования, а также соответствующих им ИТВ, будем использовать преобразованную модель анализа защищенности объекта информатизации на основе использования тестовых ИТВ, вариант которой представлен на рис. 3. 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 тестового ИТВ, для решения поставленной задачи, подразумевает наличие направленного графа. В связи с этим преобразуем ненаправленный граф модели оценки защищенности ОИ (рис. 3) в направленный граф, в котором направления ребер заданы сверху – вниз (рис. 5).

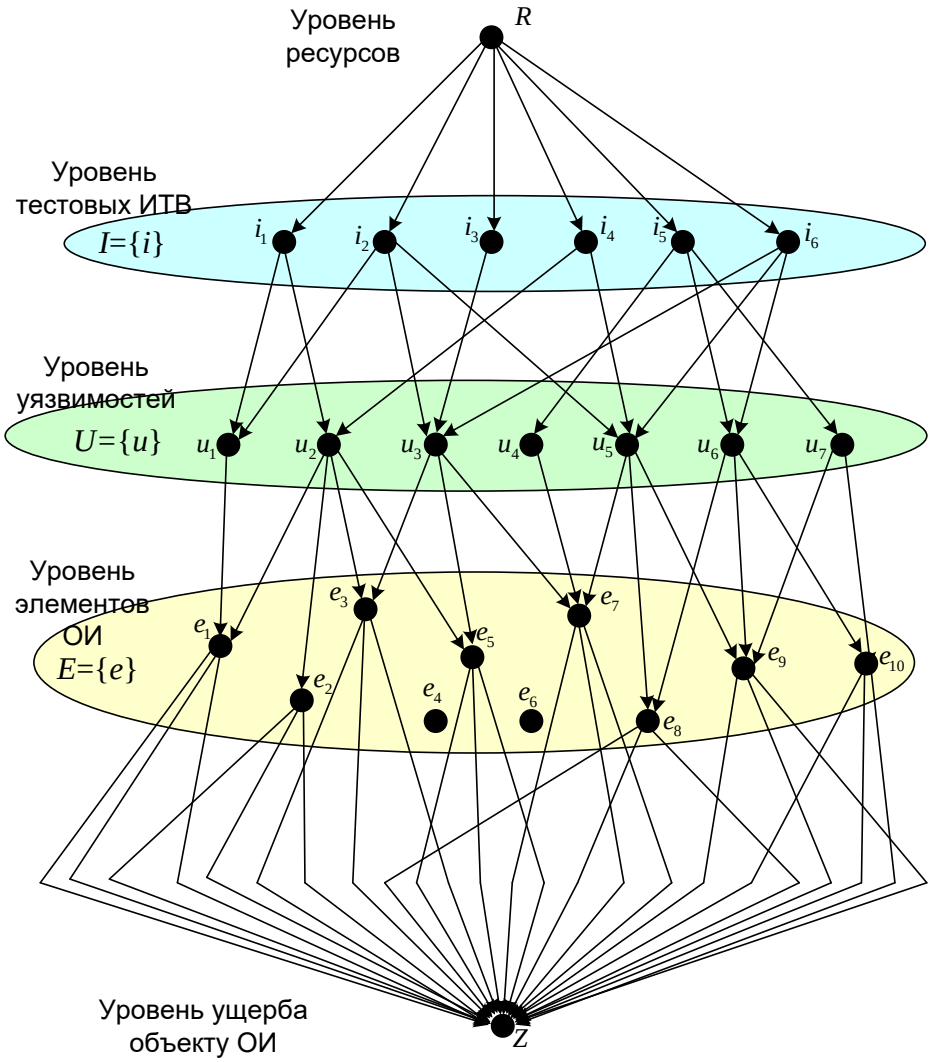


Рис. 5. Преобразования графа модели анализа защищенности ОИ на основе использования тестовых ИТВ

Анализ фундаментальных работ в области теории графов [59, 60] показал, что для решения задачи поиска путей в графах применяются математические алгоритмы поиска кратчайших путей. При этом наиболее широко используемым таким алгоритмом является алгоритм Дейкстры [61]. Однако особенностью этого алгоритма является то, что он является «поглощающим» и формирует из каждого узла графа к другому узлу только один путь, являющейся кратчайшим по сумме весов ребер в сети. Таком образом, можно обосновать единственный оптимальный вариант одиночного ИТВ, однако 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

№4. 2022
ISSN 2410-9916

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 рассматривалось в работах [51-55], однако эти работы не имеют отношения к вопросам ИБ, а посвящены вопросам обоснования маршрутов передачи данных в компьютерных сетях. Предлагается, приняв работы [51-55] за теоретический базис, разработать методику обоснования набора тестовых ИТВ путем нахождения комбинаций путей тестирования в графе модели, представленной на рис. 5, при этом в основу методики положить доработку известного алгоритма поиска кратчайших путей Дейкстры [52].

3.3 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.

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 (рис. 6).

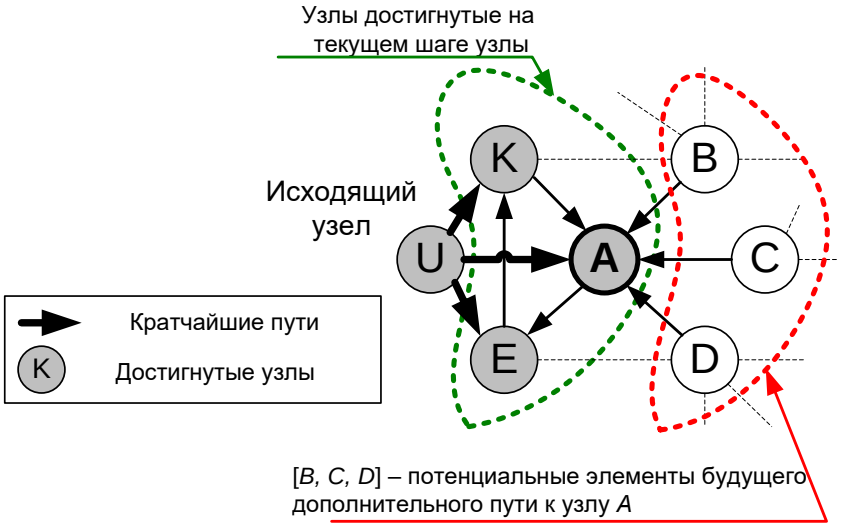


Рис. 6. Запоминание потенциальных элементов будущих дополнительных путей к узлу A

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

DOI: 10.24412/2410-9916-2022-4-137-189
URL: https://sccs.intelgr.com/archive/2022-04/06-Smirnov.pdf

потенциальным элементом дополнительного пути, формируется дополнительный путь к ранее достигнутому узлу, через только что достигнутый узел.

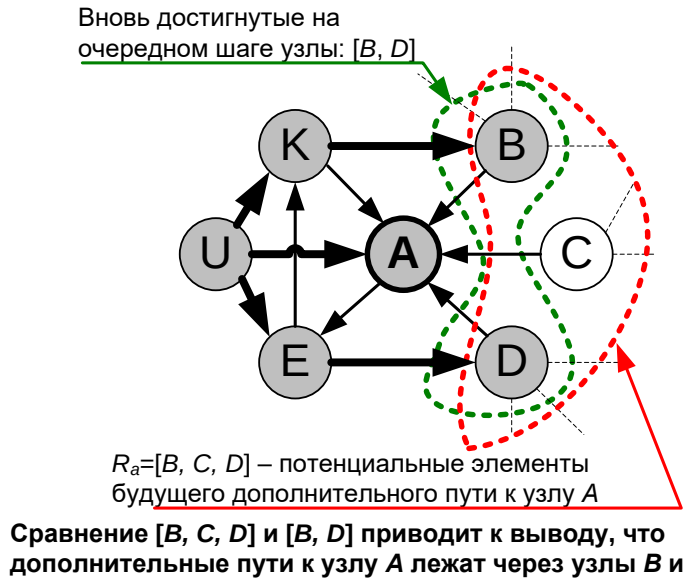


Рис. 7. Формирование дополнительного пути к вершине *A*

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.

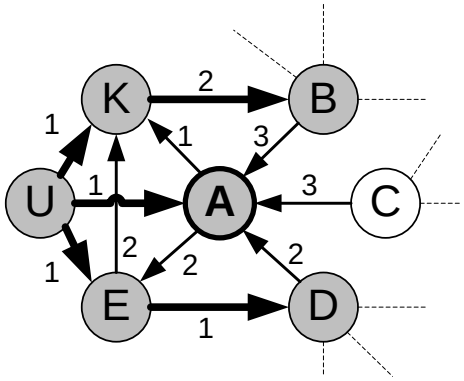


Рис. 8. Пример построения дополнительных путей к вершине *A*

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 (рис. 9).

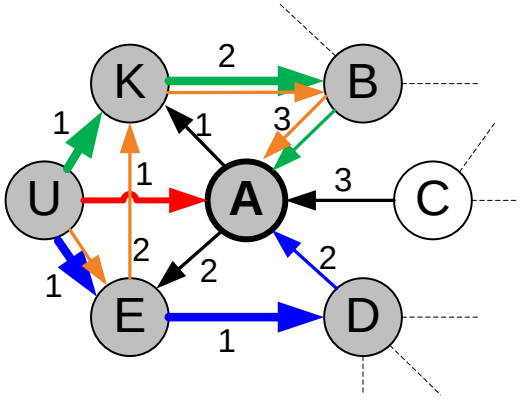
Схема формирования упорядоченного множества путей тестирования на основе модифицированного алгоритма Дейкстры приведена на рис. 10.

Входными параметрами методики являются:

- граф модели тестирования защищенности ОИ – $G(W, V)$, где: W – множество узлов графа G модели тестирования защищенности ОИ, на ос-

нове которого формируются пути тестирования; V – множество весов ребер в графе G модели тестирования защищенности ОИ.

- количество узлов в графе G – N;
- вес ребер, соединяющих произвольные n-й и j-й узлы $V(W_n, W_j)$ графа G.



Кратчайший путь	Вес	Дополнительные пути	Вес
UA	1	*U E D A*	4
		U K B A	6
		U E K B A	8

Рис. 9. Пример ранжирования дополнительных путей к узлу *A*

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.

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

2. 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.

3. 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.

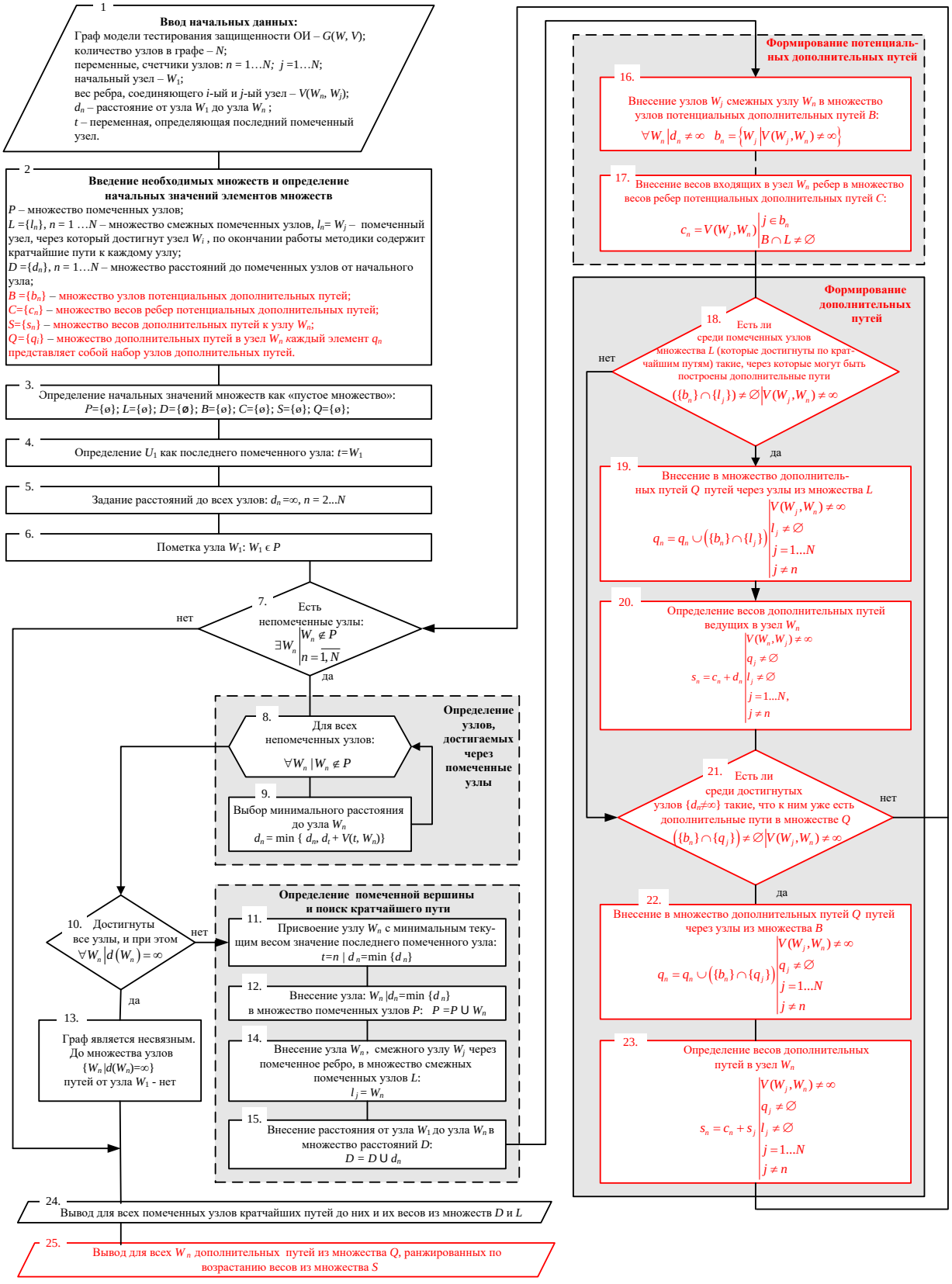


Рис. 10. Схема этапа формирования упорядоченного множества путей тестирования на основе модифицированного алгоритма Дейкстры

4. *S* – множество весов дополнительных путей к узлам. Это множество содержит веса путей из множества *Q* и используется для ранжирования допол-

нительных 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.10. 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 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.

3.4 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 $\pi \to \max$ (относительного значения $\pi_{отн} \to 100\%$), 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 ОИ 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,

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. 4) 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 $R_{\text{тест}}$ и r_j, меньше ограничения на затраты ресурса $R_{\text{гр}}$, 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 $R_{\text{тест}}+r_j > R_{\text{гр}}$, 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-м 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 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:

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

При этом значения ущерба $z(e_k, \sigma_n)$ для отдельных ребер графа G (рис. 4) пересчитываются из весов ребер $v(e_k, Z)$ в соответствии с выражением:

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

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

Б. Производится оценка относительного суммарного ущерба $\pi_{\text{отн } m}$, который может быть выявлен m-м ИТВ в тестовом наборе:

$$\pi_{\text{отн}\,m} = \frac{\pi_m}{\Pi},$$

а также оценка нарастающего итога по показателю $\pi_{\text{отн}} = \sum_m \pi_{\text{отн}\,m}$.

Шаг 5. Проверяем условия: если значение суммарного выявленного и потенциально предотвращенного ущерба π достаточно для заказчика тестирования, либо относительное значение выявленного и потенциально предотвращенного ущерба $\pi_{\text{отн}} \rightarrow 100\%$ 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 $\{i, u, e, \sigma\}$), 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 объекта информатизации при ограничениях на стоимость ресурсов, представлена на рис. 11.

3.5 Пример применения методики

Рассмотрим применение методики, взяв за основу модель на рис. 2 и 3. Преобразуем модель на рис. 2 в направленный граф, в котором для всех путей тестирования узел R является исходным, а узел Z – конечным. Полученный граф представлен на рис. 4.

На первом этапе методики к данной модели применяется модифицированный алгоритм Дейкстры для поиска кратчайших и дополнительных путей тестирования в заданном графе. Результаты применения первого этапа методики к заданному графу приведены в приложении к статье в таблице П.1.

В результате первого этапа методики, алгоритмом поиска кратчайшего и дополнительных путей между узлами R и Z установлено, что кратчайший путь лежит по узлам (r_2, i_2, u_5, e_9, z_{24}), а его вес равен 0,201. Кроме того, сформировано упорядоченное множество дополнительных путей тестирования между узлами R и Z. Подробно использование модифицированного алгоритма Дейкстры для формирования кратчайшего и дополнительных путей рассмотрено в работе [52].

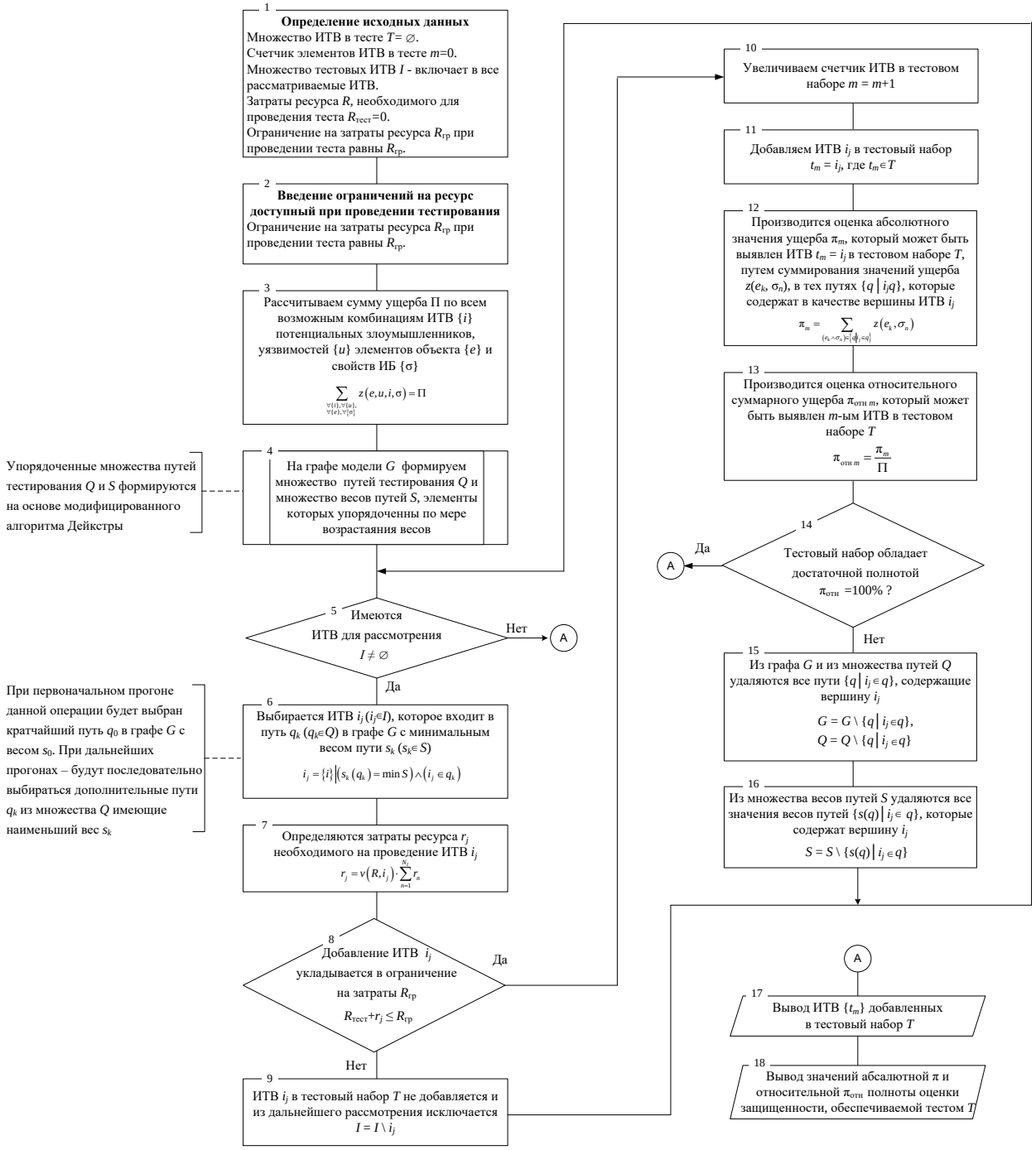


Рис. 11. Схема методики с конкретизацией этапа выбора путей тестирования, обеспечивающих рациональную полноту оценки уязвимостей ОИ при ограничениях на стоимость ресурсов

Рассмотрим более подробно применение именно второго этапа методики.

На шаге 0 зададим исходные данные. Определим множество тестовых ИТВ как пустое множество: $T=\varnothing$. Счетчик m элементов ИТВ в множестве T приравняем нулю: m=0. В множество I тестовых ИТВ включим все рассматриваемые ИТВ: I = U i_j. Затраты ресурса, необходимого для тестирования защищенности ОИ приравняем к нулю: $R_{тест}$=0.

Ограничение на затраты ресурса $R_{гр}$ при проведении тестирования пока вводить не будем, для того чтобы показать, как соотносится полнота тестирования и условная стоимость тестового набора.

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

$$\Pi = \sum_{\substack{\forall\{i\},\forall\{u\},\\ \forall\{e\},\forall\{\sigma\}}} z(e,u,i,\sigma) = 300.$$

Первый прогон.

Шаг 1. Из кратчайшего пути $q_0=(R, i_2, u_5, e_9, \sigma_3, Z)$ с минимальным весом s_0=0,201 выбирается ИТВ i_2.

Шаг 2. Определяем затраты ресурса необходимого на проведение ИТВ i_2. Значение ресурса r_2, расходуемого для проведения ИТВ i_2, пересчитывается из весов ребер $v(R, i_2)$ в соответствии с выражением:

$$r_2 = v(R, i_2) \cdot \sum_{n=1}^{N_I} r_n \approx 2;$$

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

Шаг 3. Проверяем условие на ограничение $R_{гр}$ по сумме текущих затрат ресурса на проведение теста $R_{тест}$. Так как ранее ограничение по $R_{гр}$ не было задано, то это условие можно пропустить.

Увеличиваем счетчик ИТВ в тестовом наборе на 1 ($m = m$+1=1) и добавляем ИТВ i_2 в тестовый набор ($t_1 = i_2$, где t_1 – первый элемент тестового набора T).

Условная стоимость теста $R_{тест} = R_{тест} + r_2 = 2$.

Шаг 4. В связи с принятием решения решение о добавлении ИТВ i_2 в тестовый набор T в качестве элемента t_1, выполняются следующие операции.

А. Производится оценка абсолютного значения ущерба π_1, который может быть выявлен первым ИТВ в тестовом наборе $t_1 = i_2$ (рис. 12):

$$\pi_1 = \sum_{i_2 \in \{q\}} q = 221.$$

Нарастающий итог по показателю абсолютного значения ущерба:

$$\pi = \sum_m \pi_m = 221.$$

Б. Производится оценка относительного суммарного ущерба $\pi_{отн\,1}$, который выявлен первым ИТВ в тестовом наборе $t_1 = i_2$:

$$\pi_{отн\,1} = \frac{\pi_1}{\Pi} = \frac{221}{300} \approx 73\%,$$

а также оценка нарастающего итога по показателю относительного суммарного ущерба:

$$\pi_{отн} = \sum_m \pi_{отн\,m} = 73\%.$$

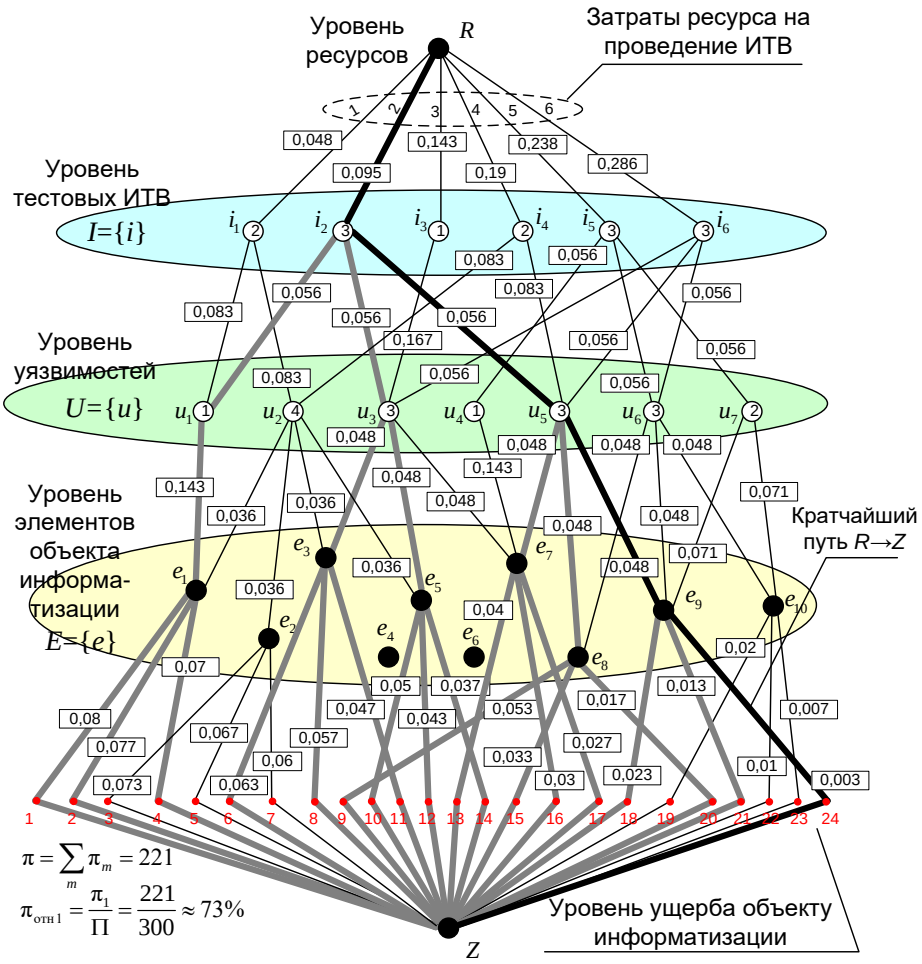


Рис. 12. Оценка ущерба, выявляемого ИТВ i_2

Шаг 5. Проверяем условие достаточности значение суммарного выявленного и потенциально предотвращенного ущерба π и $\pi_{отн}$. Так как в данном примере эти значения достаточности на задавались то продолжаем выполнение операций до достижения $\pi_{отн} \rightarrow 100\%$.

Шаг 6. Производим операции удаления тех путей тестирования (комбинаций $\{i_2, u, e, \sigma\}$), которые охвачены ИТВ i_2 (рис. 13):

А. Из графа G и из множества путей Q удаляются все пути $\{q \mid i_2 \in q\}$, содержащие вершину i_j:

$$G = G \setminus \{q \mid i_2 \in q\},$$
$$Q = Q \setminus \{q \mid i_2 \in q\}.$$

Б. Из множества весов путей S удаляются все значения весов путей $\{s(q) \mid i_2 \in q\}$, которые содержат вершину i_j:

$$S = S \setminus \{s(q) \mid i_2 \in q\}.$$

Полученный в результате удаления граф G представлен на рис. 14, а состав множеств Q и S – в таблице П.2 в приложении к статье.

Шаг 7. Переходим к шагу 1 – начинаем второй прогон этапа.

Проводя аналогичные действия на 2-м погоне в качестве минимального будет выбран путь (R, i_1, u_2, e_2, σ_3, Z) (рис. 15). На 3-м прогоне – путь (R, i_5, u_2, e_2, σ_3, Z) (рис. 16).

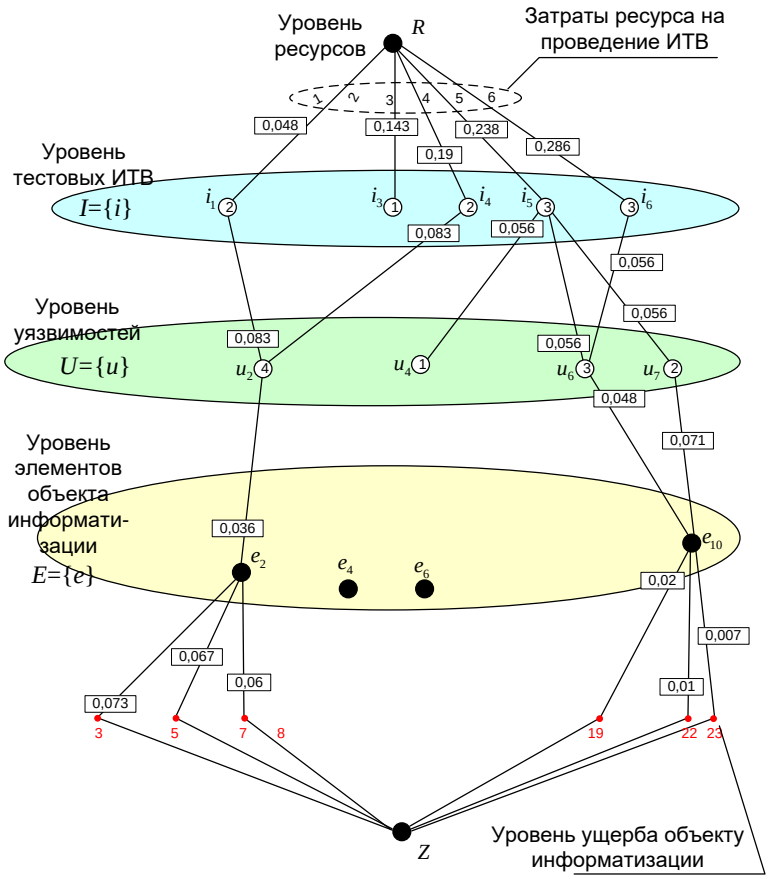


Рис. 14. Результаты удаления тех путей тестирования (комбинаций $\{i_2, u, e, \sigma\}$), которые уже охвачены ИТВ i_2

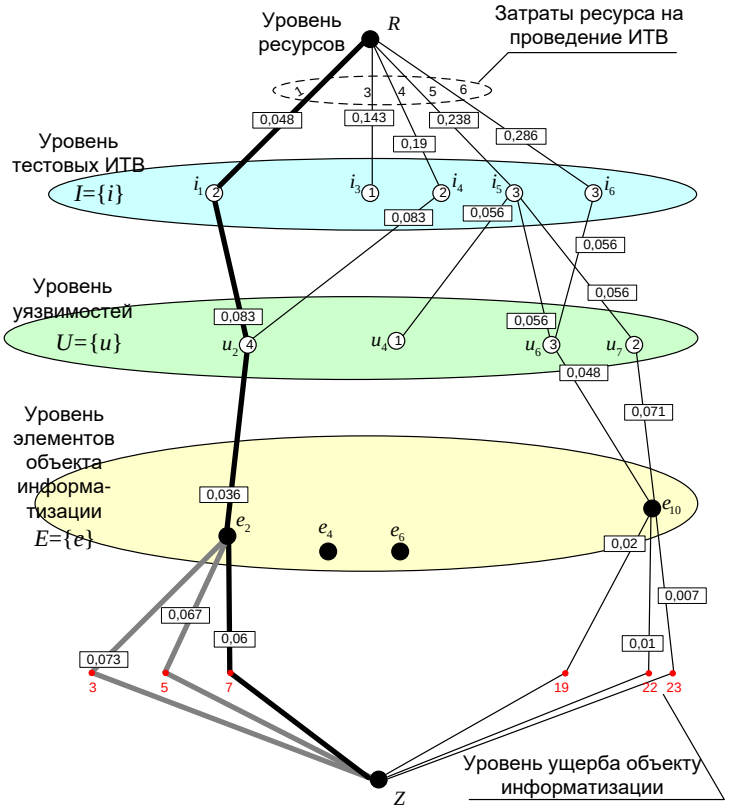


Рис. 15. Результаты выбора ИТВ i_1 и комбинаций $\{i_1, u, e, \sigma\}$, на втором прогоне второго этапа методики

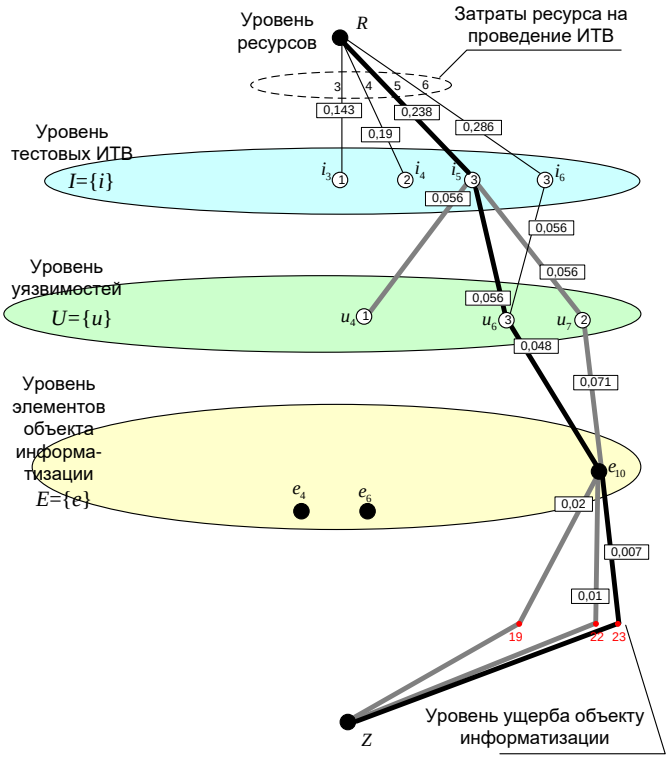


Рис. 16. Результаты выбора ИТВ i_5 и комбинаций $\{i_5, u, e, \sigma\}$, на третьем прогоне второго этапа методики

Результаты выбора, на различных прогонах, достигаемые значения полноты тестирования и затраты на это представлены в таблице 6.

Таким образом, важным преимуществом представленной методики является возможность формирования рациональных зависимостей «полнота тестирования / стоимость тестирования» в соответствии с которыми научно-обоснованно выбирать состав тестового набора и последовательность применения отдельных тестовых ИТВ.

Таблица 6 – Результаты выбора, на различных прогонах 2-го этапа методики, достигаемые значения полноты тестирования и затраты

№ прогона, m	1	2	3
Выбранный путь тестирования	$(R, i_2, u_5, e_9, \sigma_3, Z)$	$(R, i_1, u_2, e_2, \sigma_3, Z)$	$(R, i_5, u_2, e_2, \sigma_3, Z)$
Длина пути	0,201	0,226	0,347
Выбранный ИТВ, i_m	i_2	i_1	i_5
Состав теста T	(i_2)	(i_2, i_1)	(i_2, i_1, i_5)
Полнота тестирования:			
абсолютная:			
π_m	221	15	64
π	221	236	300
относительная:			
$\pi_{отн\ m}$	73%	5%	22%
$\pi_{отн}$	73%	78%	100%
Условные затраты:			
на выбранный ИТВ	2	1	5
всего на тест	2	3	8

3.6 Выводы по методике

Представленная методика на первом этапе позволяет на основе модели тестирования защищенности ОИ 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 e и уровня ущерба $z(i, u, e, \sigma)$, наносимого объекту 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», так и от известных стандартов, методик и руководств по тестированию на проникновение, является то, что:

- методика основана на *модели анализа защищенности объекта информатизации на основе использования тестовых ИТВ*, которая впервые разработана в данном исследовании, и представляет оригинальный 2-х этапный процесс нахождения рационального множества тестовых ИТВ, причем использование каждого ИТВ соответствует пути тестирования: «стоимость ресурса – тестовое ИТВ – проверяемые уязвимости – элементы объекта информатизации – выявленный и потенциально предотвращенный ущерб» на 4-х уровневом графе модели;
- в состав 1-го этапа методики введены оригинальные операции, основанные на модификации известного алгоритма поиска кратчайших путей Дейкстры из теории графов, которые обеспечивают формирование не одного (как в алгоритме Дейкстры), а упорядоченного множества путей тестирования, ранжированных по показателю «эффективность/стоимость»;
- в состав 2-го этапа методики введены оригинальные операции, основанные на известных аналитических методах теории множеств, которые из упорядоченного множества путей тестирования выбирают «лучшие» пути, таким образом, чтобы тестовый набор ИТВ максимизировал полноту тестирования по показателю суммарных значений выявленного и потенциально предотвращенного ущерба при ограничениях на стоимость ресурса тестирования.

4 Сравнительный анализ эффективности предлагаемой методики с другими стратегиями выбора информационно-технических воздействий для тестирования

Как было показано выше, в настоящее время, в подавляющем числе работ по «активному аудиту», «инструментальному аудиту», «тестированию на проникновение», «penetration testing», фактически никак не обосновывается выбор

тестовых ИТВ, особенно по критерию «эффективность / стоимость». Исследователи этого типа тестирования отмечают, что выбор конкретных тестовых ИТВ в составе теста остается за экспертом, и в основном, формирование тестового набора осуществляется эвристическим способом. В большинстве случаев, ИТВ, включаемые в тест, направлены на выявление тех уязвимостей, на которые обращает внимание заказчик и исправление которых в максимальной степени выгодны эксперту (особенно, если по итогам тестирования ожидается принятие решения о заказе определенной системы защиты). Таким образом, тестированию характерна субъективность как в отношении ожидаемых результатов со стороны заказчика, так и в отношении заинтересованности эксперта в обнаружении наиболее «зрелищных» уязвимостей с целью склонения заказчика к организации определенной конфигурации защиты.

С учетом вышесказанного, для оценки предлагаемой методики с точки зрения ее эффективности проведем ее сравнительный анализ с другими стратегиями тестирования.

При проведении сравнения будем использовать следующие допущения:

- тестовый набор формируется из 50% доступных ИТВ;
- оцениваемые показатели:
    - относительная суммарная полнота выявленного и потенциально предотвращенного ущерба $\pi_{отн}$;
    - суммарные затраты ресурса на проведение тестирования;
- альтернативные стратегии выбора ИТВ для тестового набора, с которыми производится сравнение предлагаемой методики:
    - рандомизированная стратегия выбора тестов;
    - стратегия максимизации стоимости тестирования;
    - стратегия минимизации стоимости тестирования.

Первая стратегия фактически соответствует варианту эвристического определения тестовых ИТВ, исходя из некоторых субъективных предпочтений эксперта-аудитора или заказчика.

Вторая стратегия соответствует достаточно часто встречающейся ситуации, когда специалисты, проводящее тестирование, намеренно используют наиболее дорогостоящие ИТВ с целью извлечь максимальную экономическую выгоду.

Третья стратегия характерна для заказчиков или аудиторов, которые стремятся сэкономить на проведении тестирования и проводят наименее затратные ИТВ.

Обобщенные итоговые выводы сравнительного анализа предлагаемой методики, и рассматриваемых стратегий тестирования ОИ, применительно к графу на рис. 4, представлены на рис. 17.

Анализ результатов на рис. 17 позволяет сделать следующие обобщенные выводы.

1. Представленная методика обоснования набора тестовых ИТВ для рациональной полноты оценки уязвимостей ОИ в условиях ограниченных ресурсов, обеспечивает на 22% большее значение полноты оценки защищенности

№4. 2022
ISSN 2410-9916

ОИ, чем при оценке защищенности объекта в соответствии со стратегией минимизации стоимости тестирования.

Рис. 17. Итоговые результаты сравнительного анализа предлагаемой методики и рассматриваемых стратегий тестирования ОИ

2. Представленная методика, при равной полноте оценки защищенности ОИ (достигаемая полнота – 100%), обеспечивает на 20% меньший расход ресурсов, чем при оценке защищенности объекта в соответствии с рандомизированной стратегией тестирования.

3. Представленная методика, при равной полноте оценки защищенности ОИ (достигаемая полнота – 100%), обеспечивает на 46% меньший расход ресурсов, чем при оценке защищенности объекта в соответствии со стратегией максимизации стоимости тестирования.

4. Таким образом, так как в результате моделирования теоретических положений научных результатов диссертации доказан положительный эффект, заключающийся в повышении полноты оценки защищенности и снижения расхода ресурсов, требуемых на тестирование, то можно сделать вывод, что цель диссертационного исследования, сформулированная как повышение показателя «полнота / стоимость» оценки защищенности ОИ путем обоснованного выбора тестовых ИТВ при проведении его анализа – является достигнутой.

Выводы

Для формализации процесса аудита ОИ тестовыми ИТВ разработана *модель анализа защищенности ОИ на основе использования тестовых ИТВ* в виде многоуровневой топологической структуры, отдельные уровни которой соответствует: затратам ресурса на проведение ИТВ, тестовым ИТВ, уязвимостям, элементам ОИ и уровням ущерба.

DOI: 10.24412/2410-9916-2022-4-137-189
URL: https://sccs.intelgr.com/archive/2022-04/06-Smirnov.pdf

Новизной, представленной в данном подразделе, модели тестирования защищенности ОИ, отличающей ее от формальных подходов, представленных в работах С.А. Петренко, И.В. Котенко, И.Б. Саенко, А.С. Маркова, В.Л. Цирлова, А.Н. Бегаева, С.М. Климова, А.А. Бойко, Е.Б. Дроботуна и др., является то, что:

- на основе известного метода синтеза структуры графов сформирована оригинальная структура 4-х уровневого графа, увязывающего между собой: отдельные тестовые ИТВ; расход ресурса на их проведение; проверяемые уязвимости; тестируемые элементы и подсистемы объекта информатизации; показатели выявленного и потенциально предотвращенного ущерба;
- на основе известного аналитического метода математической индукции для графа модели обоснованы и введены функциональные зависимости для определения весов межуровневых ребер, с учетом: количества ИТВ; имеющегося ресурса аудитора; количества проверяемых уязвимостей, определяемых каждым ИТВ в каждом элементе объекта информатизации; показателем выявленного и потенциально предотвращенного ущерба соответствующей выявлению каждой уязвимости.

Исследование модели подходами из теории графов, позволяет обосновать тестовые наборы ИТВ, обеспечивающие рациональную полноту аудита и тестирования защищенности ОИ.

Исследование модели аналитическими методами из теории графов, позволяет определить «более лучшие» ИТВ по критерию «эффективность/стоимость», а в дальнейшем, на их основе сформировать тестовые наборы ИТВ, которые обеспечат рациональную полноту аудита ОИ.

На основе разработанной модели, сформирована *методика обоснования набора тестовых ИТВ для рациональной полноты оценки уязвимостей ОИ при ограниченных на стоимость ресурсов*. Методика состоит из двух этапов. На первом этапе на основе ранее разработанной модели формируется 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 ОИ e и уровня ущерба $z(i, u, e, \sigma)$, наносимого ОИ S по свойству ИБ σ. На втором этапе методики производится выбор из кратчайшего пути и множества дополнительных путей, упорядоченных по возрастанию весов, 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 сформированной методики, которые отличают ее как от известных научных работ в области «инструментального аудита» и «тестирования на проникновение», так и от известных руководств по тестированию на проникновение, является то, что:

- методика основана на *модели анализа защищенности объекта информатизации на основе использования тестовых ИТВ*, которая впервые разработана в данном исследовании, и представляет оригинальный

2-х этапный процесс нахождения рационального множества тестовых ИТВ, причем использование каждого ИТВ соответствует пути тестирования: «стоимость ресурса – тестовое ИТВ – проверяемые уязвимости – элементы объекта информатизации – выявленный и потенциально предотвращенный ущерб» на 4-х уровневом графе модели;

- в состав 1-го этапа методики введены оригинальные операции, основанные на модификации известного алгоритма поиска кратчайших путей Дейкстры из теории графов, которые обеспечивают формирование не одного (как в алгоритме Дейкстры), а упорядоченного множества путей тестирования, ранжированных по показателю «эффективность/стоимость»;
- в состав 2-го этапа методики введены оригинальные операции, основанные на известных аналитических методах теории множеств, которые из упорядоченного множества путей тестирования выбирают «лучшие» пути, таким образом, чтобы тестовый набор ИТВ максимизировал полноту тестирования по показателю суммарных значений выявленного и потенциально предотвращенного ущерба при ограничениях на стоимость ресурса тестирования.

На основе разработанной методики в третьем разделе диссертации формируются научно-обоснованные рекомендации по архитектуре автоматизированного комплекса анализа защищенности ОИ с использованием тестовых ИТВ.

Приложения

Таблица П.1 – Результаты применения первого этапа методики к графу на рис. 4

Индекс элементов множеств Q и S	Элементы множества Q (пути тестирования)	Элементы множества S (вес пути тестирования)	Примечание
0	(R, i_2, u_5, e_9, σ_3, Z)	0,201	кратчайший путь
1	(R, i_1, u_2, e_5, σ_3, Z)	0,203	
2	(R, i_1, u_2, e_5, σ_2, Z)	0,21	
3	(R, i_2, u_5, e_9, σ_2, Z)	0,211	
4	(R, i_1, u_2, e_3, σ_3, Z)	0,213	
5	(R, i_2, u_5, e_8, σ_3, Z)	0,215	
6	(R, i_1, u_2, e_5, σ_1, Z)	0,216	
7	(R, i_2, u_5, e_9, σ_1, Z)	0,221	
8	(R, i_1, u_2, e_3, σ_2, Z)	0,223	
9	(R, i_2, u_3, e_7, σ_3, Z)	0,225	
10	(R, i_2, u_5, e_7, σ_3, Z)	0,225	
11	(R, i_1, u_2, e_2, σ_3, Z)	0,226	
12	(R, i_2, u_3, e_7, σ_2, Z)	0,228	
13	(R, i_2, u_5, e_7, σ_2, Z)	0,228	
14	(R, i_1, u_2, e_3, σ_1, Z)	0,23	
15	(R, i_2, u_5, e_8, σ_2, Z)	0,231	
16	(R, i_1, u_2, e_2, σ_2, Z)	0,233	

Индекс элементов множеств Q и S	Элементы множества Q (пути тестирования)	Элементы множества S (вес пути тестирования)	Примечание
17	$(R, i_2, u_3, e_5, \sigma_3, Z)$	0,235	
18	$(R, i_1, u_2, e_1, \sigma_3, Z)$	0,236	
19	$(R, i_2, u_3, e_7, \sigma_1, Z)$	0,238	
20	$(R, i_2, u_5, e_7, \sigma_1, Z)$	0,238	
21	$(R, i_1, u_2, e_2, \sigma_1, Z)$	0,24	
22	$(R, i_2, u_3, e_5, \sigma_2, Z)$	0,241	
23	$(R, i_1, u_2, e_1, \sigma_2, Z)$	0,243	
24	$(R, i_2, u_3, e_3, \sigma_3, Z)$	0,245	
25	$(R, i_1, u_2, e_1, \sigma_1, Z)$	0,246	
26	$(R, i_2, u_3, e_5, \sigma_1, Z)$	0,248	
27	$(R, i_2, u_5, e_8, \sigma_1, Z)$	0,251	
28	$(R, i_2, u_3, e_3, \sigma_2, Z)$	0,255	
29	$(R, i_2, u_3, e_3, \sigma_1, Z)$	0,261	
30	$(R, i_4, u_5, e_9, \sigma_3, Z)$	0,324	
31	$(R, i_4, u_5, e_9, \sigma_2, Z)$	0,334	
32	$(R, i_4, u_5, e_8, \sigma_3, Z)$	0,338	
33	$(R, i_1, u_1, e_1, \sigma_3, Z)$	0,343	
34	$(R, i_5, u_6, e_9, \sigma_3, Z)$	0,3446	
35	$(R, i_4, u_5, e_9, \sigma_1, Z)$	0,3447	
36	$(R, i_4, u_2, e_5, \sigma_3, Z)$	0,346	
37	$(R, i_5, u_6, e_{10}, \sigma_3, Z)$	0,347	
38	$(R, i_4, u_5, e_7, \sigma_3, Z)$	0,348	
39	$(R, i_1, u_1, e_1, \sigma_2, Z)$	0,35	
40	$(R, i_5, u_6, e_{10}, \sigma_2, Z)$	0,3512	
41	$(R, i_4, u_5, e_7, \sigma_2, Z)$	0,3514	
42	$(R, i_4, u_2, e_5, \sigma_2, Z)$	0,352	
43	$(R, i_1, u_1, e_1, \sigma_1, Z)$	0,353	
44	$(R, i_5, u_6, e_9, \sigma_2, Z)$	0,3546	
45	$(R, i_4, u_5, e_8, \sigma_2, Z)$	0,3547	
46	$(R, i_4, u_2, e_3, \sigma_3, Z)$	0,356	
47	$(R, i_5, u_6, e_8, \sigma_3, Z)$	0,357	
48	$(R, i_4, u_2, e_5, \sigma_1, Z)$	0,359	
49	$(R, i_5, u_6, e_{10}, \sigma_1, Z)$	0,3612	
50	$(R, i_4, u_5, e_7, \sigma_1, Z)$	0,3614	
51	$(R, i_2, u_1, e_1, \sigma_3, Z)$	0,363	
52	$(R, i_5, u_6, e_9, \sigma_1, Z)$	0,364	
53	$(R, i_4, u_2, e_3, \sigma_2, Z)$	0,366	
54	$(R, i_5, u_7, e_9, \sigma_3, Z)$	0,368	
55	$(R, i_4, u_2, e_2, \sigma_3, Z)$	0,369	
56	$(R, i_2, u_1, e_1, \sigma_2, Z)$	0,37	
57	$(R, i_5, u_7, e_{10}, \sigma_3, Z)$	0,371	
58	$(R, i_4, u_2, e_3, \sigma_1, Z)$	0,372	
59	$(R, i_2, u_1, e_1, \sigma_1, Z)$	0,373	
60	$(R, i_5, u_6, e_8, \sigma_2, Z)$	0,3746	
61	$(R, i_4, u_5, e_8, \sigma_1, Z)$	0,3747	
62	$(R, i_5, u_7, e_{10}, \sigma_2, Z)$	0,375	
63	$(R, i_4, u_2, e_2, \sigma_2, Z)$	0,376	
64	$(R, i_5, u_7, e_9, \sigma_2, Z)$	0,378	

Индекс элементов множеств Q и S	Элементы множества Q (пути тестирования)	Элементы множества S (вес пути тестирования)	Примечание
65	(R, i_4, u_2, e_1, σ_3, Z)	0,379	
66	(R, i_4, u_2, e_2, σ_1, Z)	0,382	
67	(R, i_3, u_3, e_7, σ_3, Z)	0,383	
68	(R, i_5, u_7, e_{10}, σ_1, Z)	0,385	
69	(R, i_4, u_2, e_1, σ_2, Z)	0,386	
70	(R, i_3, u_3, e_7, σ_2, Z)	0,387	
71	(R, i_5, u_7, e_9, σ_1, Z)	0,388	
72	(R, i_4, u_2, e_1, σ_1, Z)	0,389	
73	(R, i_6, u_5, e_9, σ_3, Z)	0,392	
74	(R, i_6, u_6, e_9, σ_3, Z)	0,392	
75	(R, i_3, u_3, e_5, σ_3, Z)	0,393	
76	(R, i_5, u_6, e_8, σ_1, Z)	0,394	
77	(R, i_6, u_6, e_{10}, σ_3, Z)	0,395	
78	(R, i_3, u_3, e_7, σ_1, Z)	0,397	
79	(R, i_6, u_6, e_{10}, σ_2, Z)	0,398	
80	(R, i_3, u_3, e_5, σ_2, Z)	0,4	
81	(R, i_6, u_5, e_9, σ_2, Z)	0,402	
82	(R, i_6, u_6, e_9, σ_2, Z)	0,402	
83	(R, i_3, u_3, e_3, σ_3, Z)	0,403	
84	(R, i_6, u_5, e_8, σ_3, Z)	0,405	
85	(R, i_6, u_6, e_3, σ_3, Z)	0,405	
86	(R, i_3, u_3, e_5, σ_1, Z)	0,407	
87	(R, i_6, u_6, e_{10}, σ_1, Z)	0,408	
88	(R, i_6, u_5, e_9, σ_1, Z)	0,412	
89	(R, i_6, u_6, e_9, σ_1, Z)	0,412	
90	(R, i_3, u_3, e_3, σ_2, Z)	0,413	
91	(R, i_6, u_3, e_7, σ_3, Z)	0,415	
92	(R, i_6, u_5, e_7, σ_3, Z)	0,415	
93	(R, i_6, u_3, e_7, σ_2, Z)	0,418	
94	(R, i_6, u_5, e_7, σ_2, Z)	0,418	
95	(R, i_3, u_3, e_3, σ_1, Z)	0,42	
96	(R, i_6, u_5, e_8, σ_2, Z)	0,422	
97	(R, i_6, u_6, e_8, σ_2, Z)	0,422	
98	(R, i_6, u_3, e_5, σ_3, Z)	0,425	
99	(R, i_6, u_3, e_7, σ_1, Z)	0,428	
100	(R, i_6, u_5, e_7, σ_1, Z)	0,428	
101	(R, i_6, u_3, e_5, σ_2, Z)	0,432	
102	(R, i_6, u_3, e_3, σ_3, Z)	0,435	
103	(R, i_6, u_3, e_5, σ_1, Z)	0,438	
104	(R, i_6, u_5, e_8, σ_1, Z)	0,442	
105	(R, i_6, u_6, e_8, σ_1, Z)	0,442	
106	(R, i_6, u_3, e_3, σ_2, Z)	0,445	
107	(R, i_6, u_3, e_3, σ_1, Z)	0,452	
108	(R, i_5, u_4, e_7, σ_3, Z)	0,463	
109	(R, i_5, u_4, e_7, σ_2, Z)	0,466	
110	(R, i_5, u_4, e_7, σ_1, Z)	0,476	

Таблица П.2 – Результаты удаления тех путей тестирования (комбинаций $\{i_2, u, e, \sigma\}$), которые охвачены ИТВ i_2

Индекс элементов множеств Q и S	Элементы множества Q (пути тестирования)	Элементы множества S (вес пути тестирования)	Примечание
1	$(R, i_1, u_2, e_5, \sigma_3, Z)$	0,203	
2	$(R, i_1, u_2, e_5, \sigma_2, Z)$	0,21	
4	$(R, i_1, u_2, e_3, \sigma_3, Z)$	0,213	
6	$(R, i_1, u_2, e_5, \sigma_1, Z)$	0,216	
8	$(R, i_1, u_2, e_3, \sigma_2, Z)$	0,223	
11	$(R, i_1, u_2, e_2, \sigma_3, Z)$	0,226	
14	$(R, i_1, u_2, e_3, \sigma_1, Z)$	0,23	
16	$(R, i_1, u_2, e_2, \sigma_2, Z)$	0,233	
18	$(R, i_1, u_2, e_1, \sigma_3, Z)$	0,236	
21	$(R, i_1, u_2, e_2, \sigma_1, Z)$	0,24	
23	$(R, i_1, u_2, e_1, \sigma_2, Z)$	0,243	
25	$(R, i_1, u_2, e_1, \sigma_1, Z)$	0,246	
30	$(R, i_4, u_5, e_9, \sigma_3, Z)$	0,324	
31	$(R, i_4, u_5, e_9, \sigma_2, Z)$	0,334	
32	$(R, i_4, u_5, e_8, \sigma_3, Z)$	0,338	
33	$(R, i_1, u_1, e_1, \sigma_3, Z)$	0,343	
34	$(R, i_5, u_6, e_9, \sigma_3, Z)$	0,3446	
35	$(R, i_4, u_5, e_9, \sigma_1, Z)$	0,3447	
36	$(R, i_4, u_2, e_5, \sigma_3, Z)$	0,346	
37	$(R, i_5, u_6, e_{10}, \sigma_3, Z)$	0,347	
38	$(R, i_4, u_5, e_7, \sigma_3, Z)$	0,348	
39	$(R, i_1, u_1, e_1, \sigma_2, Z)$	0,35	
40	$(R, i_5, u_6, e_{10}, \sigma_2, Z)$	0,3512	
41	$(R, i_4, u_5, e_7, \sigma_2, Z)$	0,3514	
42	$(R, i_4, u_2, e_5, \sigma_2, Z)$	0,352	
43	$(R, i_1, u_1, e_1, \sigma_1, Z)$	0,353	
44	$(R, i_5, u_6, e_9, \sigma_2, Z)$	0,3546	
45	$(R, i_4, u_5, e_8, \sigma_2, Z)$	0,3547	
46	$(R, i_4, u_2, e_3, \sigma_3, Z)$	0,356	
47	$(R, i_5, u_6, e_8, \sigma_3, Z)$	0,357	
48	$(R, i_4, u_2, e_5, \sigma_1, Z)$	0,359	
49	$(R, i_5, u_6, e_{10}, \sigma_1, Z)$	0,3612	
50	$(R, i_4, u_5, e_7, \sigma_1, Z)$	0,3614	
52	$(R, i_5, u_6, e_9, \sigma_1, Z)$	0,364	
53	$(R, i_4, u_2, e_3, \sigma_2, Z)$	0,366	
54	$(R, i_5, u_7, e_9, \sigma_3, Z)$	0,368	
55	$(R, i_4, u_2, e_2, \sigma_3, Z)$	0,369	
57	$(R, i_5, u_7, e_{10}, \sigma_3, Z)$	0,371	
58	$(R, i_4, u_2, e_3, \sigma_1, Z)$	0,372	
60	$(R, i_5, u_6, e_8, \sigma_2, Z)$	0,3746	
61	$(R, i_4, u_5, e_8, \sigma_1, Z)$	0,3747	
62	$(R, i_5, u_7, e_{10}, \sigma_2, Z)$	0,375	
63	$(R, i_4, u_2, e_2, \sigma_2, Z)$	0,376	
64	$(R, i_5, u_7, e_9, \sigma_2, Z)$	0,378	
65	$(R, i_4, u_2, e_1, \sigma_3, Z)$	0,379	
66	$(R, i_4, u_2, e_2, \sigma_1, Z)$	0,382	

67	(R, i_3, u_3, e_7, σ_3, Z)	0,383	
68	(R, i_5, u_7, e_{10}, σ_1, Z)	0,385	
69	(R, i_4, u_2, e_1, σ_2, Z)	0,386	
70	(R, i_3, u_3, e_7, σ_2, Z)	0,387	
71	(R, i_5, u_7, e_9, σ_1, Z)	0,388	
72	(R, i_4, u_2, e_1, σ_1, Z)	0,389	
73	(R, i_6, u_5, e_9, σ_3, Z)	0,392	
74	(R, i_6, u_6, e_9, σ_3, Z)	0,392	
75	(R, i_3, u_3, e_5, σ_3, Z)	0,393	
76	(R, i_5, u_6, e_8, σ_1, Z)	0,394	
77	(R, i_6, u_6, e_{10}, σ_3, Z)	0,395	
78	(R, i_3, u_3, e_7, σ_1, Z)	0,397	
79	(R, i_6, u_6, e_{10}, σ_2, Z)	0,398	
80	(R, i_3, u_3, e_5, σ_2, Z)	0,4	
81	(R, i_6, u_5, e_9, σ_2, Z)	0,402	
82	(R, i_6, u_6, e_9, σ_2, Z)	0,402	
83	(R, i_3, u_3, e_3, σ_3, Z)	0,403	
84	(R, i_6, u_5, e_8, σ_3, Z)	0,405	
85	(R, i_6, u_6, e_3, σ_3, Z)	0,405	
86	(R, i_3, u_3, e_5, σ_1, Z)	0,407	
87	(R, i_6, u_6, e_{10}, σ_1, Z)	0,408	
88	(R, i_6, u_5, e_9, σ_1, Z)	0,412	
89	(R, i_6, u_6, e_9, σ_1, Z)	0,412	
90	(R, i_3, u_3, e_3, σ_2, Z)	0,413	
91	(R, i_6, u_3, e_7, σ_3, Z)	0,415	
92	(R, i_6, u_5, e_7, σ_3, Z)	0,415	
93	(R, i_6, u_3, e_7, σ_2, Z)	0,418	
94	(R, i_6, u_5, e_7, σ_2, Z)	0,418	
95	(R, i_3, u_3, e_3, σ_1, Z)	0,42	
96	(R, i_6, u_5, e_8, σ_2, Z)	0,422	
97	(R, i_6, u_6, e_8, σ_2, Z)	0,422	
98	(R, i_6, u_3, e_5, σ_3, Z)	0,425	
99	(R, i_6, u_3, e_7, σ_1, Z)	0,428	
100	(R, i_6, u_5, e_7, σ_1, Z)	0,428	
101	(R, i_6, u_3, e_5, σ_2, Z)	0,432	
102	(R, i_6, u_3, e_3, σ_3, Z)	0,435	
103	(R, i_6, u_3, e_5, σ_1, Z)	0,438	
104	(R, i_6, u_5, e_8, σ_1, Z)	0,442	
105	(R, i_6, u_6, e_8, σ_1, Z)	0,442	
106	(R, i_6, u_3, e_3, σ_2, Z)	0,445	
107	(R, i_6, u_3, e_3, σ_1, Z)	0,452	
108	(R, i_5, u_4, e_7, σ_3, Z)	0,463	
109	(R, i_5, u_4, e_7, σ_2, Z)	0,466	
110	(R, i_5, u_4, e_7, σ_1, Z)	0,476	

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: 05.13.19. – М., 2008. – 19 с.

4. Марков А. С., Цирлов В. Л., Барабанов А. В. Методы оценки несоответствия средств защиты информации / под ред. А.С. Маркова. – 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. 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.

11. Климов С. М. Имитационные модели испытаний критически важных информационных объектов в условиях компьютерных атак // Известия ЮФУ. Технические науки. 2016. № 8 (181). С. 27-36.

12. 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.

13. Петренко А. А., Петренко С. А. Кибероружения: методические рекомендации ENISA // Вопросы кибербезопасности. 2015. № 3 (11). С. 2-14.

14. 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.

15. 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.

16. 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.

17. Щеглов А. В., Храмов В. Ю. Способ разработки тестовых удаленных информационно-технических воздействий на пространственно-распределенные системы информационно-технических средств // Сборник студенческих научных работ факультета компьютерных наук ВГУ ФГБОУ ВО «Воронежский государственный университет». – Воронеж, 2016. – С. 203-210.

18. Пакулин Н. В., Шнитман В. З., Никешин А. В. Автоматизация тестирования соответствия для телекоммуникационных протоколов // Труды Института системного программирования РАН. 2014. Т. 26. № 1. С. 109-148.

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. Санькова Г. В., Одуденко Т. А. Информационные технологии в перевозочном процессе. – Хабаровск: ДВГУПС, 2012. – 111 с.

33. Исаков О. А. Вопросы совершенствования АСУ железнодорожного транспорта. – Саарбрюкен: LAP LAMBERT Academic Publishing, 2011. – 218 с.

34. Самме Г. В. Информационные системы железнодорожного транспорта. – М.: РГОПТУПС, 2008. – 30 с.

35. Глухов А. П., Василенко В. В., Сидак А. А., Ададуров С. Е., Белова Е. И. Определение уровня безопасности значимых объектов критической информационной инфраструктуры железнодорожного транспорта // Двойные технологии. 2020. № 1 (90). С. 84-88.

36. Глухов А. П., Бирюков Д. Н., Василенко В. В., Корниенко А. А., Сидак А. А. Методологические аспекты упреждающего управления информационной безопасностью железнодорожного транспорта / А.П. Глухов, // Двойные технологии. 2019. № 3 (88). С. 86-92.

37. Ададуров С. Е., Глухов А. П., Корниенко А. А., Белова Е. И. О безопасности критической информационной инфраструктуры // Автоматика, связь, информатика. 2020. № 4. С. 2-4.

38. Ададуров С. Е., Диасамидзе С. В., Корниенко А. А., Сидак А. А Международная кибербезопасность на железнодорожном транспорте: методологические подходы и нормативная методическая база // Вестник научно-исследовательского института железнодорожного транспорта. 2015. № 6. С. 9-15.

39. Котенко И. В., Чечулин А. А., Левшун Д. С. Анализ защищенности инфраструктуры железнодорожного транспорта на основе аналитического моделирования // Защита информации. Инсайд. 2017. № 6 (78). С. 48-57.

40 Котенко И. В., Саенко И. Б. Об архитектуре многоуровневой интеллектуальной системы обеспечения информационной безопасности автоматизированных систем на железнодорожном транспорте // Методы и технические средства обеспечения безопасности информации. 2014. № 23. С. 97-98.

41. Котенко И. В., Саенко И. Б. Предложения по созданию многоуровневой интеллектуальной системы обеспечения информационной безопасности автоматизированных систем на железнодорожном транспорте // Вестник Ростовского государственного университета путей сообщения. 2013. № 3 (51). С. 69-79.

42. Котенко И. В., Саенко И. Б., Чернов А. В., Бутакова М. А. Построение многоуровневой интеллектуальной системы обеспечения информационной безопасности для автоматизированных систем железнодорожного транспорта // Труды СПИИРАН. 2013. № 7 (30). С. 7-25.

43. 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

44. 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

45. 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

46. Макаренко С. И., Смирнов Г. Е. Методика обоснования тестовых информационно-технических воздействий, обеспечивающих рациональную полноту аудита защищенности объекта критической информационной инфраструктуры // Вопросы кибербезопасности. 2021. № 6 (46). С. 12-25. DOI: 10.21681/2311-3456-2021-6-12-25

47. Макаренко С. И. Тестирование на проникновение на основе стандарта NIST SP 800-115 // Вопросы кибербезопасности. 2022. № 3 (49). С. 44-57. DOI: 10.21681/2311-3456-2022-3-44-57

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.

50. Бутакова М. А., Чернов А. В., Шевчук П. С., Ковалев С. М. Управление безопасностью киберфизических систем на основе оперативного ситуационного информирования об инцидентах // Труды Ростовского государственного университета путей сообщения. 2016. № 5. С. 14-16.

51. 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.

52. 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.

53. 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. DOI: 10.18469/ikt.2016.14.3.06

54. Макаренко С. И. Усовершенствованный протокол маршрутизации OSPF, обеспечивающий повышенную устойчивость сетей связи // Труды учебных заведений связи. 2018. Т. 4. № 2. С. 82-90.

55. 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

56. 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.

57. Ушанев К. В., Макаренко С. И. Классификация информационных потоков в сети связи для обоснования целесообразности применения к ним способов обеспечения качества обслуживания // Инфокоммуникационные технологии. 2016. Т. 14. № 2. С. 142-152.

58. 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.

59. Татт У. Теория графов. – М.: Мир, 1988. – 424 с.

60. Свами М., Тхуласираман К. Графы, сети и алгоритмы. – М.: Мир, 1984. – 454 с.

61. Кормен Т., Лейзерсон Ч., Ривест Р. Алгоритмы: построение и анализ – М.: МЦНМО, 2000. – 960 с.

62. Дроботун Е. Б. Теоретические основы построения систем защиты от компьютерных атак для автоматизированных систем управления. Монография. – СПб.: Наукоемкие технологии, 2017. – 120 с.

63. Дроботун Е. Б. Синтез систем защиты автоматизированных систем управления от разрушающих программных воздействий // Программные продукты и системы. 2016. № 3. С. 51-59. DOI: 10.15827/0236-235X.115.051-059

64. Дроботун Е. Б., Бердышев В. П. Защита автоматизированных систем управления военного назначения от разрушающих программных воздействий // Военная мысль. 2016. № 10. С. 15-19.

65. Дроботун Е. Б., Козлов Д. В., Марковский А. С. Программный комплекс расследования инцидентов информационной безопасности // Программные продукты, системы и алгоритмы. 2016. № 2. С. 8.

References

1. Makarenko S. I. Audit of Information Security - the Main Stages, Conceptual Framework, Classification of Types. *Systems of Control, Communication and Security*, 2018, no. 1, pp. 1-29 (in Russian). 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, 2018. 122 p. (in Russian).

3. Kashaev T. R. *Algoritmy aktivnogo audita informatsionnoi sistemy na osnove tekhnologii iskusstvennykh immunnykh sistem. Avtoreferat dis.* [Algorithms for active audit of information system based on artificial immune systems. Abstract D.Ph. thesis]. Moscow, 2008. 19 p. (in Russian).

4. Markov A. S., Tsirlov V. L., Barabanov A. V. *Metody otsenki nesootvetstviia sredstv zashchity informatsii* [Methods of compliance of information security]. Moscow, Radio i Sviaz Publ., 2012. 192 p. (in Russian).

5. Skabtsov N. *Audit bezopasnosti informatsionnykh system* [Security audit of information systems]. Saint Petersburg, Piter Publ., 2018. 272 p. (in Russian).

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. Avetisyan A. I., Belevantsev A. A., Chucklyaev I. I. The technologies of static and dynamic analyses detecting vulnerabilities of software. *Voprosy kiberbezopasnosti*, 2014, vol. 4, no. 3, pp. 20-28 (in Russian).

11. Klimov S. M. Imitating models of testing the critically important information objects in the conditions of computer attacks. *Izvestiya SFedU. Engineering Sciences*, 2016, vol. 181, no. 8, pp. 27-36 (in Russian).

12. 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, no. 24, pp. 206-213 (in Russian).

13. Petrenko A. A., Petrenko S. A. Cyber education: methodical recommendations ENISA. *Voprosy kiberbezopasnosti*, 2015, vol. 11, no. 3, pp. 2-14 (in Russian).

14. 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, vol. 70, no. 3, pp. 84-92 (in Russian).

15. Boyko A. A., Djakova A. V. Hramov V. Ju. Metodicheskij podhod k razrabotke testovyh sposobov udalennogo informacionno-tehnicheskogo vozdejstvija na prostranstvenno raspredelennye sistemy informacionno-tehnicheskih sredstv [Methodological approach to the development of test methods for remote information technology impact on spatially distributed systems of information technology tools]. *Kibernetika i vysokie tehnologii XXI veka XV Mezhdunarodnaja nauchno-tehnicheskaja konferencija* [*Cybernetics and high technologies of the XXI century XV international scientific and technical conference*]. Voronezh, SAKVOEE, 2014. pp. 386-395 (in Russian).

16. 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, no. 2, pp. 33-45 (in Russian).

17. Shcheglov A. V., Hramov V. Ju. Sposob razrabotki testovyh udalennyh informacionno-tehnicheskih vozdejstvij na prostranstvenno-raspredelennye sistemy informacionno-tehnicheskih sredstv [Method for developing test remote information technology impacts on spatially distributed information technology systems]. *Sbornik studencheskih nauchnyh rabot fakul'teta komp'juternyh nauk «Voronezhskij gosudarstvennyj universitet»* [*Collection of student research papers of the faculty of computer science of Voronezh state University*]. Voronezh, 2016, pp. 203-210 (in Russian).

18. Pakulin N. V., Shnitman V. Z., Nikeshin A. V. Avtomatizatsiia testirovaniia sootvetstviia dlia telekommunikatsionnykh protokolov [Automation of compliance testing for telecommunication protocols]. *Proceedings of the Institute for System Programming of the RAS*, 2014, vol. 26, no. 1, pp. 109-148 (in Russian).

19. Baranova E. K., Hudyshkin A. A. Osobennosti analiza bezopasnosti informacionnyh sistem metodom testirovanija na proniknovenie [Features of information system security analysis by penetration testing]. *Modelirovanie i analiz bezopasnosti i riska v slozhnyh sistemah. Trudy mezhdunarodnoj nauchnoj shkoly MABR – 2015* [*Modeling and analysis of security and risk in complex systems. Proceedings of the international scientific school MABR - 2015*], 2015, pp. 200-205 (in Russian).

20. Baranova E. K., Chernova M. V. Comparative analysis of programming tools for cybersecurity risk assessment. *Information Security Problems. Computer Systems*, 2014, no. 4, pp. 160-168 (in Russian).

21. Begaev A. N., Begaev S. N., Fedotov V. A. *Testirovanie na proniknovenie* [*Penetration testing*]. Saint Petersburg, Saint Petersburg National Research University of Information Technologies, Mechanics and Optics Publ., 2018. 45 p. (in Russian).

22. Bogoras A. G., Peskova O. Y. Methodology for testing and assessment of firewalls. *Izvestiya SFedU. Engineering Sciences*, 2013, vol. 149, no. 12, pp. 148-156 (in Russian).

23. Dorofeev A. Testirovanie na proniknovenie: demonstracija odnoj ujazvimosti ili obektivnaja ocenka zashhishhennosti? *Zasita informacii. Inside*, 2010, vol. 36, no. 6, pp. 72-73 (in Russian).

24. Umnitsyn M. Y. Approach to semi-natural security evaluation of information system. *Izvestia VSTU*, 2018, vol. 218, no. 8, pp. 112-116 (in Russian).

25. Borodin M. K., Borodina P. Ju. Testirovanie na proniknovenie sredstva zashhity informacii VGATE R2 [VGATE R2 information security penetration testing]. *Regional'naja informatika i informacionnaja bezopasnost* [*Regional Informatics and information security*], Saint Petersburg, 2017, pp. 264-268 (in Russian).

26. Poltavtseva M. A., Pechenkin A. I. Data mining methods in penetration tests decision support system. *Information Security Problems. Computer Systems*, 2017, no. 3, pp. 62-69 (in Russian).

27. Kadan A. M., Doronin A. K. Cloud infrastructure solutions for penetration testing. *Uchenye zapiski ISGZ*, 2016, vol. 14, no. 1, pp. 296-302 (in Russian).

28. Eremenko N. N., Kokoulin A. N. Research of methods of penetration testing in information systems. *Master's Journal*, 2016, no. 2, pp. 181-186 (in Russian).

29. Tumanov S. A. Penetration testing tools for information systems. *Proceedings of Tomsk State University of Control Systems and Radioelectronics*, 2015, vol. 36, no. 2, pp. 73-79 (in Russian).

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, vol. 38, no. 1, pp. 75-93 (in Russian).

31. Gorbatov V. S., Meshcheryakov A. A. Comparative analysis of computer network security scanners. *IT Security*, 2013, vol. 20, no. 1, pp. 43-48 (in Russian).

32. Sankova G. V., Odudenko T. A. *Informatsionnye tekhnologii v perevozochnom protsesse* [*Information technologies in the transportation process*]. Khabarovsk, Far Eastern State University of Railway Engineering Publ., 2012. 111 p. (in Russian).

33. Isakov O. A. *Voprosy sovershenstvovaniya ASU zheleznodorozhnogo transporta* [*Issues of improving the automated control system of railway transport*]. – Saarbryuken, LAP LAMBERT Academic Publishing, 2011. 218 p. (in Russian).

34. Samme G. V. *Informatsionnye sistemy zheleznodorozhnogo transporta* [*Railway transport information systems*]. Moscow, Russian State Open Technical University of Railways Publ., 2008. 30 p. (in Russian).

35. Gluhov A. P., Vasilenko V. V., Sidak A. A., Adadurov S. E., Belova E. I. Determination of the security level of significative objects of critical information infrastructure of railway transport. *Dual technology*, 2020, no. 1 (90), pp. 84-88 (in Russian).

36. Glukhov A. P., Biryukov D. N., Vasilenko V. V., Kornienko A. A., Sidak A. A. Methodological aspects of proactive management of railroad transport information security. *Dual technology*, 2019, no. 3 (88), pp. 86-92 (in Russian).

37. Adadurov S. E., Glukhov A. P., Kornienko A. A., Belova E. I. Principles of railway transport critical information infrastructure security supporting. *Automation, Communications, Informatics*, 2020, no. 4, pp. 2-4 (in Russian).

38. Adadurov S. E., Diasamidze S. V., Kornienko A. A., Sidak A. A. International cybersecurity on railway transport: methodological approaches and normal procedural framework. *Russian railway science journal*, 2015, no. 6, pp. 9-15 (in Russian).

39. Kotenko I. V., Chechulin A. A., Levshun D. S. Security analysis of railway transport infrastructure on the base of analytical modeling. *Zasita informacii. Inside*, 2017, no. 6 (78), pp. 48-57 (in Russian).

40. Kotenko I. V., Saenko I. B. Ob arkhitekture mnogourovnevoy intellektual'noy sistemy obespecheniya informatsionnoy bezopasnosti avtomatizirovannykh sistem na zheleznodorozhnom transporte [About the architecture of a multi-level intelligent information security system for automated systems in railway transport]. *Metody i tekhnicheskie sredstva obespecheniya*

bezopasnosti informatsii [*Methods and technical means of ensuring information security*], 2014, no. 23, pp. 97-98 (in Russian).

41. Kotenko I. V., Saenko I. B. Proposals on creation of a multi-level intelligent information security system of automated systems on railway transport. *Vestnik RGUPS*, 2013, no. 3 (51), pp. 69-79 (in Russian).

42. Kotenko I. V., Saenko I. B., Chernov A. V., Butakova M. A. The construction of a multi-level intelligent information security system for automated systems of railway transport. *SPIIRAS Proceedings*, 2013, no. 7 (30), pp. 7-25 (in Russian).

43. Makarenko S. I., Smirnov G. E. Analysis of penetration testing standards and methodologies. *Systems of Control, Communication and Security*, 2020, no. 4, pp. 44-72 (in Russian). DOI: 10.24411/2410-9916-2020-10402

44. Makarenko S. I. Criteria and parameters for estimating quality of penetration testing. *Voprosy kiberbezopasnosti*, 2021, vol. 43, no. 3, pp. 43-57 (in Russian). DOI: 10.21681/2311-3456-2021-3-43-57

45. Makarenko S. I., Smirnov G. E. Model of Security Audit of a Critical Information Infrastructure Object with Use the Test Cyber Attacks. *Proceedings of Telecommunication Universities*, 2021, vol. 7, no. 1, pp. 94-104 (in Russian). DOI: 10.31854/1813-324X-2021-7-1-94-104

46. Makarenko S. I., Smirnov G. E. Selection method of test cyber attacks that ensure the rational completeness of the penetration testing of a critical information infrastructure object. *Voprosy kiberbezopasnosti*, 2021, vol. 46, no. 6, pp. 12-25 (in Russian). DOI: 10.21681/2311-3456-2021-6-12-25

47. Makarenko S. I. Penetration testing in accordance with NIST SP 800-115 standard. *Voprosy kiberbezopasnosti*, 2022, vol. 49, no. 3, pp. 44-57 (in Russian). DOI: 10.21681/2311-3456-2022-3-44-57

48. Smirnov G. E., Makarenko S. I. The Use of Test Information and Technical Impacts for Security Audit of Information Systems of Railway Transport. *Intellectual Technologies on Transpor*t, 2020, vol. 23, no. 3, pp. 20-29 (in Russian).

49. Smirnov G. E., Makarenko S. I. Use of test information and technical impacts for preventive security audit of information and telecommunication networks. *Ekonomika i kachestvo sistem svyazi*, 2020, vol. 17, no. 3, pp. 43-59 (in Russian).

50. Butakova M. A., Chernov A. V., Shevchuk P. S., Kovalev S. M. Cyber-physical systems security management based on operational situational incidents information. *Trudy Rostovskogo gosudarstvennogo universiteta putey soobshcheniya*, 2016, no. 5, pp. 14-16 (in Russian).

51. Makarenko S. I. Stability method of telecommunication network with using topological redundancy. *Systems of Control, Communication and Security*, 2018, no. 3, pp. 14-30 (in Russian). DOI: 10.24411/2410-9916-2018-10302.

52. 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*, vol. 69, no. 2, 2014, pp. 71-78 (in Russian).

53. Makarenko S. I., Kvasov M. N. Modified Bellman-Ford Algorithm with Finding the Shortest and Fallback Paths and its Application for Network Stability Improvement. *Infokommunikacionnye tehnologii*, 2016, vol. 14, no. 3, pp. 264-274 (in Russian). DOI: 10.18469/ikt.2016.14.3.06

54. Makarenko S. I. The Improved OSPF Protocol for High Network Stability. *Proceedings of Telecommunication Universities*, 2018, vol. 4, no. 2, pp. 82-90 (in Russian).

55. Makarenko S. I Improved Routing and Signaling Functions of PNNI Protocol for High Network Stability. *Proceedings of Telecommunication Universities*, 2020, vol. 6, no. 2, pp. 45-59 (in Russian). DOI: 10.31854/1813-324X-2020-6-2-45-59

56. Makarenko S. I. Hierarchical Clustering of Telecommunication Network to the Independent Routing Areas for the Purposes to Ensure Stability. *Proceedings of Telecommunication Universities*, 2018, vol. 4, no. 4, pp. 54-67. DOI: 10.31854/1813-324X-2018-4-4-54-67 (in Russian).

57. Ushanev K. V., Makarenko S. I. Classification of telecommunication network information flows to rationale for application of methods for improving quality of service. *Infokommunikacionnye tehnologii*, 2016, vol. 14, no. 2, pp. 142-152. DOI: 10.18469/ikt.2016.14.2.05 (in Russian).

58. 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, no. 4, pp. 70-77 (in Russian).

59. Tatt W. *Teoriya grafov* [*Graph theory*]. Moscow, Mir Publ., 1988. 424 p.

60. Svami M. Tkhulasiraman K. *Grafy, seti i algoritmy* [*Graphs, networks and algorithms*]. Moscow, Mir Publ., 1984. 454 p.

61. Kormen T., Leyzerson Ch., Rivest R. *Algoritmy: postroenie i analiz* [*Algorithms: construction and analysis*]. Moscow, Moscow Center for Continuing Mathematical Education Publ., 2000. 960 p.

62. Drobotun E. B. *Teoreticheskie osnovy postroeniya sistem zashchity ot komp'yuternykh atak dlya avtomatizirovannykh sistem upravleniya. Monografiya* [*Theoretical foundations of building protection systems against computer attacks for automated control systems. Monograph*]. Saint Petersburg, Naukoemkie Tekhnologii Publ., 2017. 120 p. (in Russian).

63. Drobotun E. B. Synthesis of protection systems of automated control systems against destroying program influence. *Software & Systems*, 2016, no. 3, pp. 51-59 (in Russian). DOI: 10.15827/0236-235X.115.051-059

64. Drobotun E. B., Berdyshev V. P. Zashchita avtomatizirovannykh sistem upravleniya voennogo naznacheniya ot razrushayushchikh programmnykh vozdeystviy [Protection of automated control systems for military purposes from destructive software influences]. *Military Thought*, 2016, no. 10, pp. 15-19 (in Russian).

65. Drobotun E. B., Kozlov D. V., Markovskiy A. S. Programmnyy kompleks rassledovaniya intsidentov informatsionnoy bezopasnosti [Information Security

Incident Investigation Software Package]. *Software Journal: Theory and Applications*, 2016, no. 2, pp. 8 (in Russian).

Статья поступила 20.11.2022 г.

Информация об авторе

Смирнов Глеб Евгеньевич – соискатель ученой степени кандидата технических наук. Преподаватель кафедры информационной безопасности. Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» имени В.И. Ульянова (Ленина). Область научных интересов: информационная безопасность, тестирование на проникновение. E-mail: science.cybersec@yandex.ru

Адрес: Россия, 197022, Санкт-Петербург, ул. Профессора Попова, 5.

Model for analyzing the security of an informatization object of railway transport and method for justifying a set of test cyber attacks for this

G. E. Smirnov

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 model for analyzing the security of an informatization object of railway transport and method for justifying a set of test cyber attacks for this, 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.*** *Model for analyzing the security of an informatization object of railway transport and method for justifying a set of test cyber attacks for this is presented in the paper. The method is based on the model. 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 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.*

Information about Author

Gleb Evgenievich Smirnov – Doctorate Student. Lecturer of the Department of Information Security. Saint Petersburg Electrotechnical University 'LETI'. Field of research: information security, penetration testing. E-mail: science.cybersec@yandex.ru

Address: Russia, 197022, St. Petersburg, Professor Popov str., 5.