DOI: 10.24412/2413-2527-2022-331-5-18

Методика обоснования тестовых информационно-технических воздействий при анализе защищенности объектов информатизации железнодорожного транспорта

Г. Е. Смирнов
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина)
Санкт-Петербург, Россия
science.cybersec@yandex.ru

Аннотация. **В статье рассмотрены основные информационные системы и объекты информатизации железнодорожного транспорта. Показано, что они являются ключевыми объектами критической информационной инфраструктуры Российской Федерации, а анализ состояния их реальной защищенности — важной государственной задачей. Предложено проводить анализ защищенности за счет использования тестовых информационно-технических воздействий, аналогичных воздействиям, которые прогнозируются к применению злоумышленниками. Разработана методика обоснования тестовых воздействий при анализе защищенности объектов информатизации железнодорожного транспорта на основе алгоритма Дейкстры, позволяющая формировать множество путей, ранжированных по суммарной метрике пути, и состоящая из двух этапов: формирования упорядоченного множества путей тестирования и выбора путей тестирования, обеспечивающих рациональную полноту оценки уязвимостей, при ограничениях на ресурсы.**

Ключевые слова: **информационная безопасность, аудит, тестирование, алгоритм Дейкстры, информационно-техническое воздействие, критическая информационная инфраструктура, объект информатизации, железнодорожный транспорт.**

Введение

В 2017 году в России 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.

Вопросы обеспечения ИБ и оценки защищенности различных ОИ исследованы в работах [1–9]. Вопросам состава, структуры и функционирования информационных систем (ИС) и ОИ ЖТ посвящены работы [10–12]. Работы [13–21] посвящены вопросам оценки ИБ ОИ и ИС ЖТ. Вместе с тем вопросы оценки защищенности ОИ ЖТ, именно за счет использования тестовых информационно-технических воздействий (ИТВ), исследованы в недостаточной степени.

Целью статьи является разработка методики обоснования тестовых ИТВ при анализе защищенности ОИ ЖТ. 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 в рамках аудита ИБ, представленное работами [22–28].

Анализ объектов информатизации и задач обеспечения ее защищенности

Анализ работ [10–12] показал, что ИС ЖТ относится к классу больших корпоративных систем, содержит 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), объединенных 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.

Обеспечение автоматизации основных функций ЖТ выполняют ИТ-комплексы:

- управления перевозочным процессом;
- управления маркетингом, экономикой и финансами;
- управления инфраструктурой ЖТ;
- управления непроизводственной сферой.

Рассмотрим эти комплексы более подробно.

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, организация эксплуатации и ремонта парка пассажирских вагонов, управление багажными и почтовыми перевозками, организация 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.

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).

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.

ИТ-комплекс 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 [19]:

– 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, осуществляемая 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 АСОУП 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%) [16]. В связи с этим ЖТ выступает одной из основных целей для злоумышленников и профессиональных нарушителей — сил информационных операций недружественных стран при ведении информационного противоборства. При обострении геополитической обстановки в мире информационная инфраструктура и ИС ЖТ РФ могут оказаться объектом воздействия не только злоумышленников, но и профессиональных нарушителей, поэтому оценка реальной защищенности ОИ и ИС ЖТ является важной задачей, имеющей государственное значение.

Постановка задачи на разработку методики

В предыдущей статье по этой тематике [25] автором была сформирована модель процесса тестирования ОИ ЖТ в виде многоуровневой топологической модели, которая взаимосвязанно учитывает: эффективность отдельных ИТВ i в части выявленного и потенциально предотвращенного ущерба $\{z\}$; ориентированность их на проверку конкретного множества уязвимостей $\{u\}$ элементов $\{e\}$ объекта информатизации; расход в процессе тестирования определенного количества ресурса r_i (в данном случае под абстрактным ресурсом может пониматься расход времени аудитора, оплата его труда, стоимость машинного времени, затраты на специализированное оборудование и т. д.). В данной работе будет показано, как с использованием модели [25] сформировать набор тестовых ИТВ, обеспечивающий рациональную полноту аудита защищенности ОИ ЖТ.

Задача на разработку методики m обоснования набора тестовых ИТВ для рациональной полноты оценки уязвимостей ОИ ЖТ формулируется следующим образом. Сформировать такой набор тестовых ИТВ $I = \{i\}$, который бы в условиях ограниченности ресурсов аудитора R максимизировал важность выявляемых уязвимостей $\{u\}$, с учетом того, что отдельным уязвимостям u и элементам ОИ ЖТ e сопоставляются уровни ущерба $z(e, u, i, \sigma)$, наносимого ОИ S по определенному свойству ИБ σ (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 ОИ $\{e\}$ 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 $\{\sigma\}$:

$$\pi_{отн} = \frac{\pi}{\Pi}.$$

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

Введение системы обозначений

Для формализации методики введем следующие обозначения:

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

$\pi_m/\pi_{отн\ m}$ — абсолютное/относительное значение полноты выявленного и потенциально предотвращенного ущерба m-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, l, m, n — переменные-счетчики;

L — множество смежных помеченных вершин графа G, то есть множество расстояний до помеченных вершин от начальной вершины;

N — количество узлов в графе G;

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

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

P — множество помеченных вершин в графе G;

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

R — исходный узел ресурсов в графе G модели тестирования защищенности ОИ;

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

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

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

S — множество весов дополнительных путей к узлам графа G;

$T = \{t\}$ — множество тестовых ИТВ, выбранных для проведения тестирования защищенности 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 ($W = R \vee I \vee U \vee E \vee Z$);

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;

$Z = \{z\}$ — суммарный показатель ущерба, который может быть причинен ОИ;

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

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

Исходные положения и посылки

Разработку методики обоснования набора тестовых ИТВ предполагается вести на основе приложения подходов к исследованию теории графов к модели тестирования защищенности объекта информатизации [17]. Введем понятие пути тестирования.

Путь тестирования — путь на графе модели тестирования защищенности объекта информатизации, проходящий через узлы и ребра, которые соответствуют единственной оригинальной комбинации ресурса r_i, тестового ИТВ i, уязвимости u элемента ОИ e и уровня ущерба $z(i, u, e, \sigma)$, наносимого ОИ по свойству ИБ σ.

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

В качестве графа, на котором будет вестись поиск путей тестирования, а также соответствующих им ИТВ, будем использовать преобразованную модель модели оценки защищенности ОИ, вариант которой представлен в работе [17] (рис. 1).

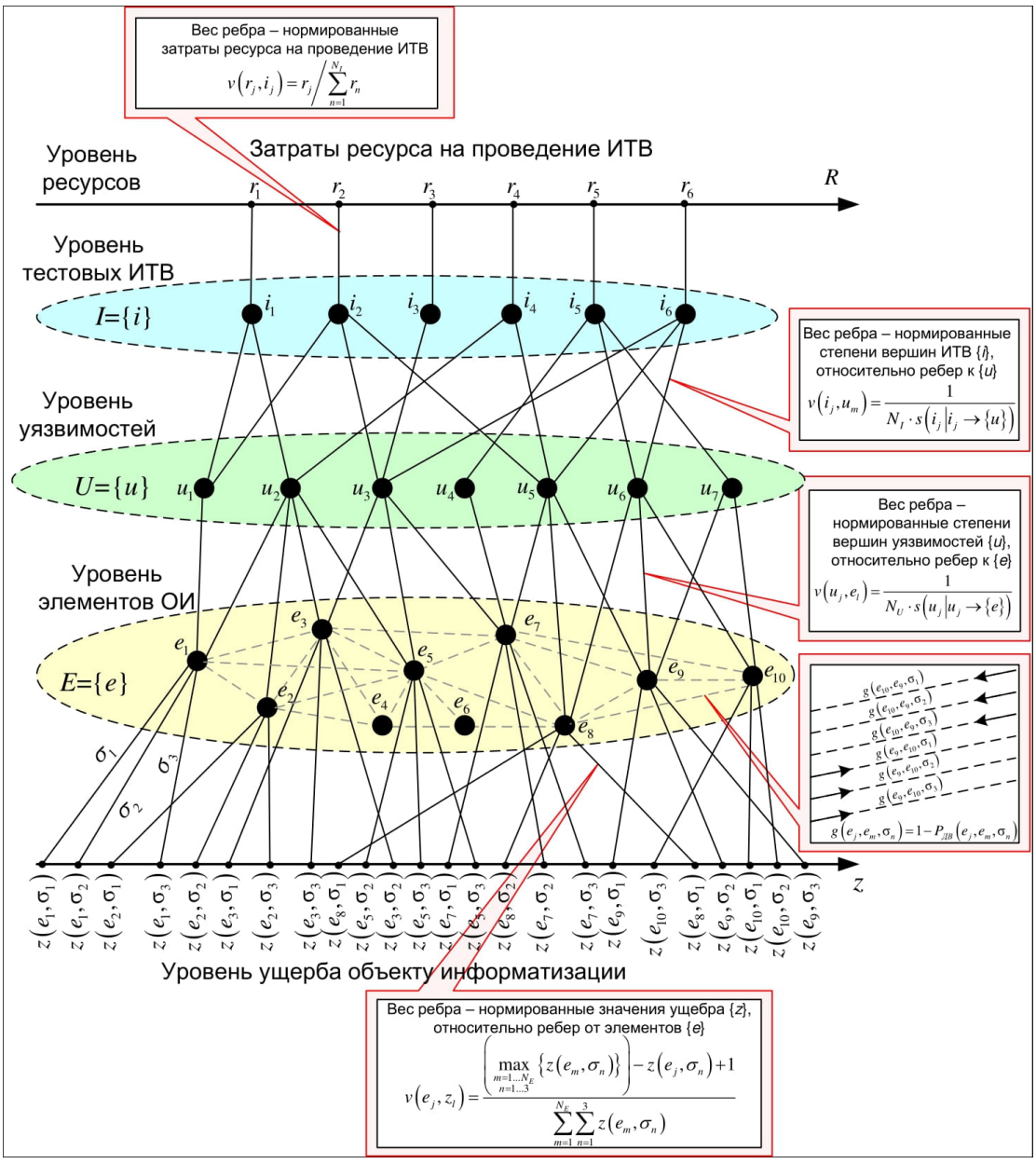

Рис. 1. Схема модели оценки защищенности ОИ тестовыми ИТВ

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» к «худшим» путям тестирования. Логика формирования набора тестовых ИТВ подразумевает наличие направленного графа. В связи с этим преобразуем ненаправленный граф модели оценки защищенности ОИ (рис. 1) в направленный граф, в котором направления ребер заданы сверху вниз (рис. 2).

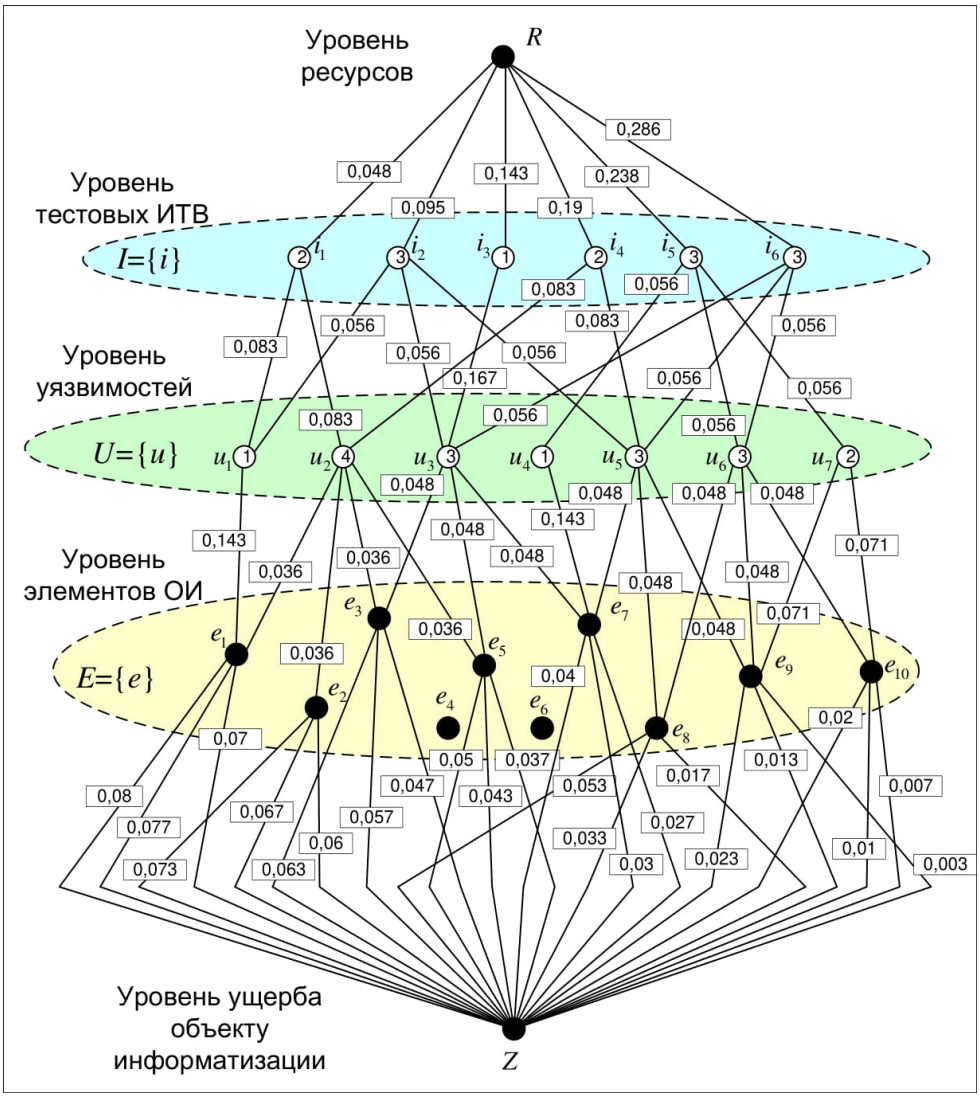

Рис. 2. Вариант модели оценки защищенности ОИ

Анализ фундаментальных работ в области теории графов [29, 30] показал, что для решения задачи вычисления кратчайших путей в графах применяются соответствующие математические алгоритмы поиска кратчайших путей. При этом наиболее широко используемым таким алгоритмом является алгоритм Дейкстры [31]. Однако особенностью этого алгоритма является то, что он является «поглощающим» и формирует из каждого узла графа к другому узлу только один путь, являющийся кратчайшим по сумме весов ребер в сети. Таком образом, можно обосновать только единственный оптимальный вариант одиночного ИТВ. Вместе с тем для обоснования набора нескольких ИТВ необходимо вычислять не только кратчайшие пути тестирования, но и другие комбинации путей, соответствующих другим ИТВ, после чего группировать их степени увеличения стоимости тестирования. Это требует формирования набора путей тестирования, которые были бы ранжированы, с одной стороны, по уровню вскрываемого ущерба, а с другой — по степени затрат ресурсов на тестирование. Решение этой задачи потребует создания нового математического алгоритма на основе алгоритма Дейкстры с целью разработки новой функциональности — способности формировать множество путей, ранжированных по суммарной метрике пути, из начального узла графа (R) в конечных узел (Z). Решение подобной задачи уже рассматривалось в работах [32–36], однако эти работы не имеют отношения к вопросам ИБ, а посвящены исключительно вопросам обоснования маршрутов передачи данных в компьютерных сетях. Предлагается, приняв работы [32–36] за теоретический базис, разработать методику обоснования набора тестовых ИТВ путем нахождения комбинаций путей тестирования в графе модели, представленной на рисунке 2, при этом в основу методики положить математический алгоритм, основанный на алгоритме поиска кратчайших путей Дейкстры [33].

ПЕРВЫЙ ЭТАП МЕТОДИКИ — ФОРМИРОВАНИЕ 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. Основой предлагаемой модификации алгоритма Дейкстры являются следующие положения, ранее обоснованные в работе [33].

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

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

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

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

Схема формирования упорядоченного множества путей тестирования на основе модифицированного алгоритма Дейкстры, ранее разработанного автором и представленного в работе [26], приведена на рисунке 3.

Входными параметрами этого этапа методики являются:

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

б) количество узлов в графе G — N;

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

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

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

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

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

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

К блокам, отличающим данный этап методики от известного алгоритма Дейкстры, относятся блоки 16–23, 25 на рисунке 3. 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.

ВТОРОЙ ЭТАП МЕТОДИКИ — ВЫБОР 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 $R_{гр}$.

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 ($T = \emptyset$). 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 $\{\sigma\}$:

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

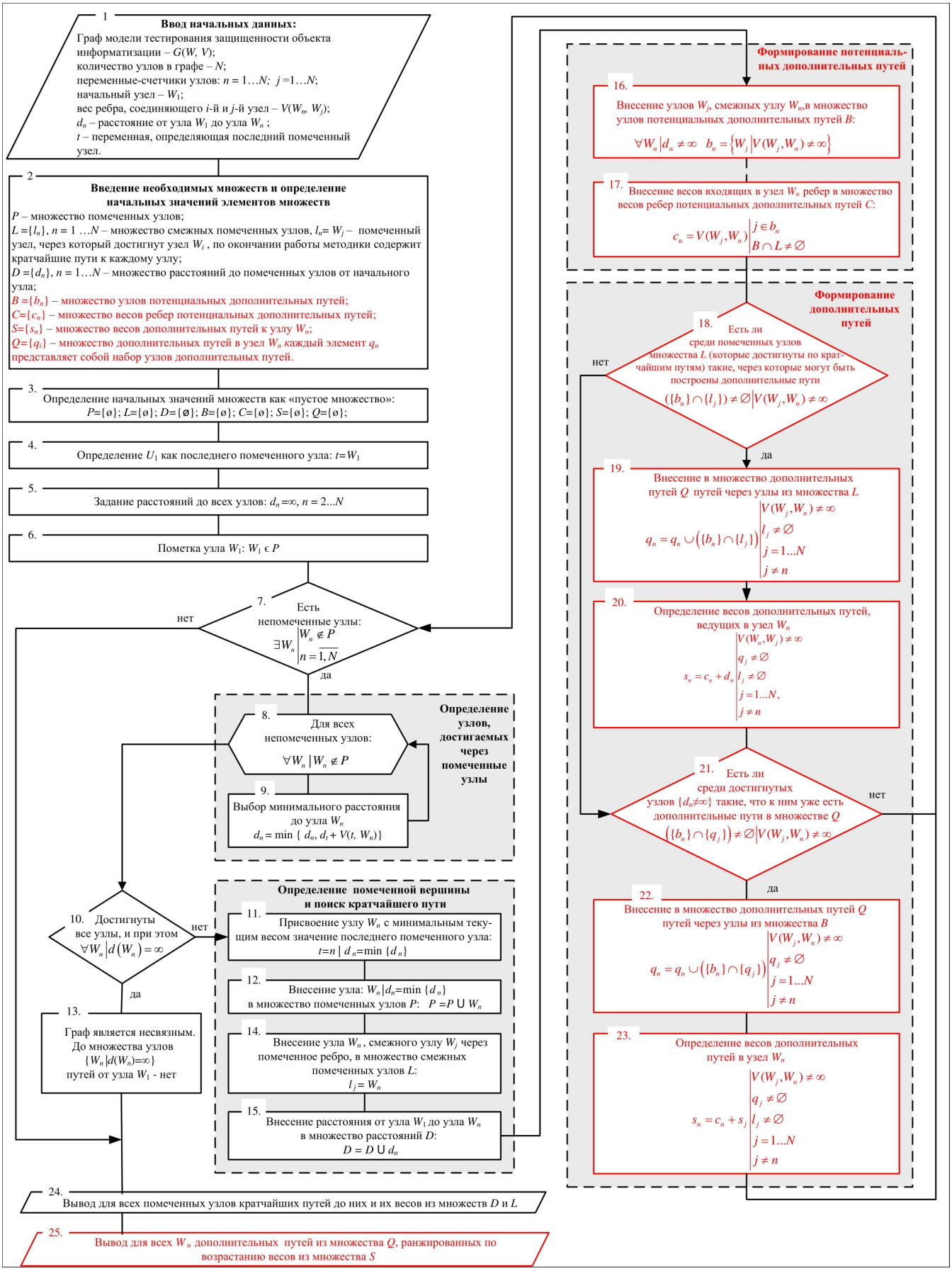

Рис. 3. Схема этапа формирования упорядоченного множества путей тестирования на основе модифицированного алгоритма Дейкстры

Шаг 1. Если множество рассматриваемых ИТВ не пустое ($I \neq \emptyset$), 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 ($s_k \in S$):

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

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. 2) пересчитываются из весов ребер $v(R, i_j)$ в соответствии с выражением:

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

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:

1. 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 ОИ при использовании ИТВ i_j, путем суммирования значений ущерба $z(e_k, \sigma_n)$, в тех путях $\{q \mid i_j \in q\}$, которые содержат в качестве вершины ИТВ i_j:

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

При этом значения ущерба $z(e_k, \sigma_n)$ для отдельных ребер графа G (рис. 2) пересчитываются из весов ребер $v(e_k, Z)$ в соответствии с выражением:

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

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

2. 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. Проверяются условия: если значение суммарного выявленного и потенциально предотвращенного ущерба π достаточно для заказчика тестирования либо относительное значение выявленного и потенциально предотвращенного ущерба $\pi_{\text{отн}} \to 100$ %, то процесс формирования тестового набора останавливается. Если вышеуказанные условия не выполняются, то выполняются дальнейшие операции.

Шаг 6. Производятся операции удаления тех путей тестирования (комбинаций $\{i, u, e, \sigma\}$), которые уже охвачены ИТВ, включенными в тестовый набор T.

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

$$G = G \setminus \{q | i_j \in q\} ,$$

$$Q = Q \setminus \{q | i_j \in q\} .$$

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

$$S = S \setminus \{s(q) | i_j \in q\} .$$

Шаг 7. Переход к шагу 1.

Общая схема методики с конкретизацией этапа выбора путей тестирования, обеспечивающих рациональную полноту оценки уязвимостей, при ограничениях на ресурсы представлена на рисунке 4.

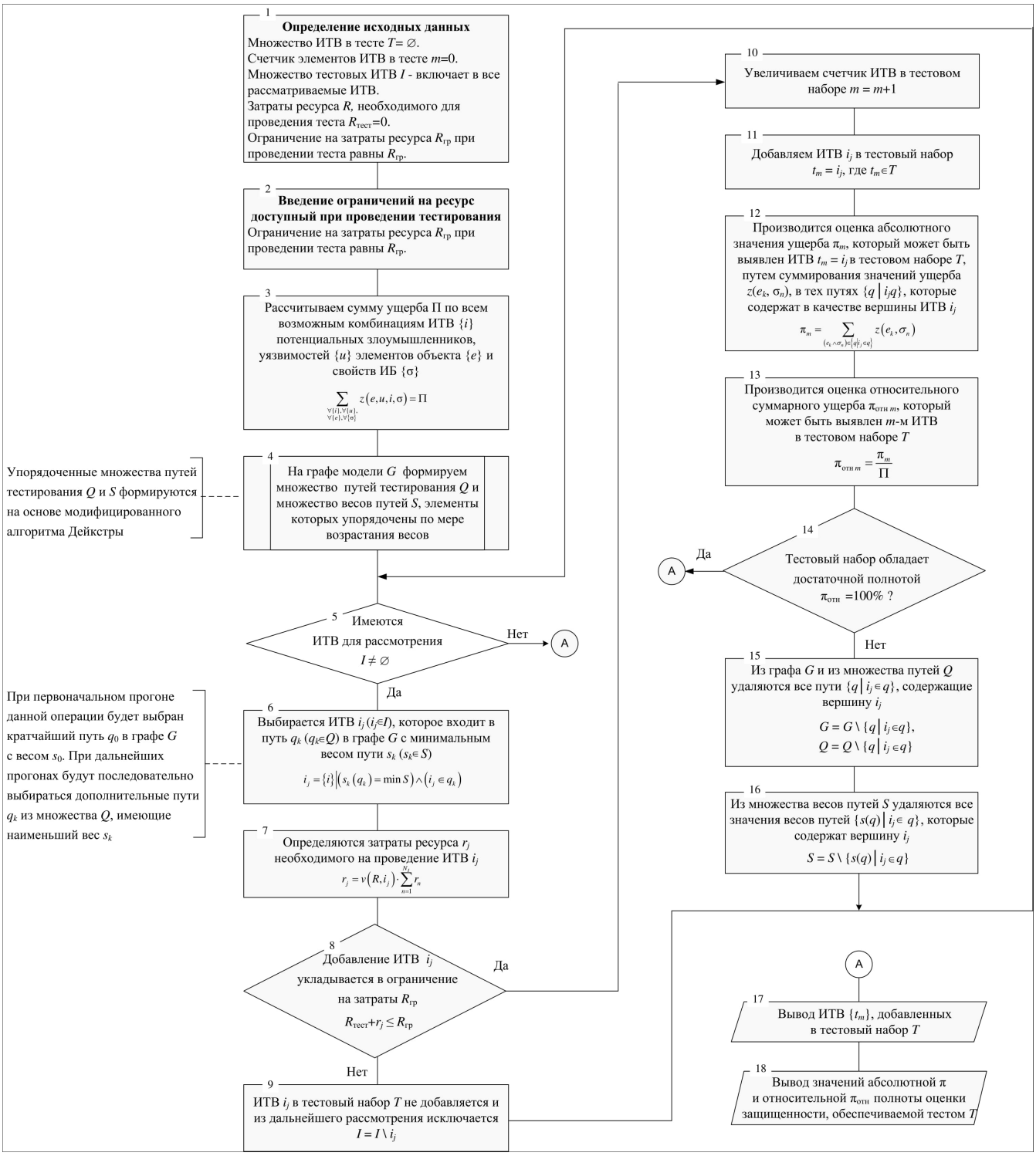

Рис. 4. Схема методики с конкретизацией этапа выбора путей тестирования, обеспечивающих рациональную полноту оценки уязвимостей, при ограничениях на ресурсы

Выводы

Представленная методика на первом этапе позволяет на основе модели тестирования защищенности ОИ ЖТ 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 ОИ ЖТ 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 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 $R_{гр}$.

Элементами новизны данной методики, которые отличают ее от известных руководств по тестированию на проникновение [28], является то, что, во-первых, методика основана на модели тестирования защищенности ОИ, которая впервые разработана в данном исследовании, во-вторых, в состав методики введены оригинальные операции, которые на первом этапе методики за счет использования модификации известного алгоритма Дейкстры формируют упорядоченное множество путей тестирования, ранжированных по показателю «эффективность/стоимость», а на втором этапе — осуществляют формирование тестового набора из тех ИТВ, которые являются элементами «лучших» путей тестирования, таким образом, чтобы тестовый набор максимизировал абсолютную суммарную стоимость обнаруженного ущерба в рамках заданных ограничений на расход ресурса тестирования.

Данная методика предполагается к внедрению в автоматизированные комплексы тестирования защищенности ОИ ЖТ, архитектура и функциональность которых была изложена в работах [37, 38].

Литература

1. Рябцев, С. С. Метод выявления вредоносных роботов на основе данных процесса коллективного принятия решений в роевых робототехнических системах // Системы управления, связи и безопасности. 2022. № 3. С. 105–137. DOI: 10.24412/2410-9916-2022-3-105-137.

2. Будко, Н. П. Обзор графо-аналитических подходов к мониторингу информационно-телекоммуникационных сетей и их применение для выявления аномальных состояний / Н. П. Будко, Н. В. Васильев // Системы управления, связи и безопасности. 2021. № 6. С. 53–75.
DOI: 10.24412/2410-9916-2021-6-53-75.

3. Построение профиля атакующего на основе анализа сетевого трафика в критических инфраструктурах / Е. В. Федорченко, Е. С. Новикова, Д. А. Гайфулина, И. В. Котенко // Системы управления, связи и безопасности. 2021. № 6. С. 76–89. DOI: 10.24412/2410-9916-2021-6-76-89.

4. Обеспечение информационной безопасности киберфизических объектов на основе прогнозирования и обнаружения аномалий их состояния / В. И. Васильев, А. М. Вульфин, В. Е. Гвоздев, [и др.] // Системы управления, связи и безопасности. 2021. № 6. С. 90–119.
DOI: 10.24412/2410-9916-2021-6-90-119.

5. Израилов, К. Е. Модель классификации уязвимостей интерфейсов транспортной инфраструктуры «умного города» / К. Е. Израилов, Д. С. Левшун, А. А. Чечулин // Системы управления, связи и безопасности. 2021. № 5. С. 199–223. DOI: 10.24412/2410-9916-2021-5-199-223.

6. Горбачев, А. А. Модель функционирования и алгоритм проактивной защиты сервиса электронной почты от сетевой разведки / А. А. Горбачев, С. П. Соколовский, С. В. Усатиков // Системы управления, связи и безопасности. 2021. № 3. С. 60–109.
DOI: 10.24412/2410-9916-2021-3-60-109.

7. Методика оценки актуальных угроз и уязвимостей на основе технологий когнитивного моделирования и Text Mining / В. И. Васильев, А. М. Вульфин, А. Д. Кириллова, Н. В. Кучкарова // Системы управления, связи и безопасности. 2021. № 3. С. 110–134.
DOI: 10.24412/2410-9916-2021-3-110-134.

8. Методика разработки программы аудита информационной безопасности с учетом весовых коэффициентов значимости свидетельств аудита на основе метода анализа иерархий / В. А. Воеводин, П. В. Маркин, М. С. Маркина, Д. С. Буренок // Системы управления, связи и безопасности. 2021. № 2. С. 96–129.
DOI: 10.24412/2410-9916-2021-2-96-129.

9. Заколдаев, Д. А. Формальная модель обеспечения информационной безопасности при управлении ресурсами на производствах / Д. А. Заколдаев, А. Ю. Гришенцев // Системы управления, связи и безопасности. 2021. № 1. С. 33–61. DOI: 10.24411/2410-9916-2021-10102.

10. Санькова, Г. В. Информационные технологии в перевозочном процессе: Учебное пособие / Г. В. Санькова, Т. А. Одуденко. — Хабаровск: ДВГУПС, 2012. — 111 с.

11. Исаков, О. А. Вопросы совершенствования АСУ железнодорожного транспорта. — Саарбрюккен: Lambert Academic Publishing, 2011. — 224 с.

12. Методологические аспекты обеспечения информационной безопасности перевозочного процесса / С. Е. Ададуров, А. П. Глухов, А. А. Корниенко, Е. И. Белова // Управление товарными потоками и перевозочным процессом на железнодорожном транспорте на основе клиентоориентированности и логистических технологий: Коллективная монография членов и научных партнеров Объединенного ученого совета ОАО «РЖД» / под ред. Б. М. Лапидуса и А. Т. Осьминина. — Санкт-Петербург: ЛЕМА, 2019. — С. 251–263. — (Бюллетень Объединенного ученого совета ОАО «РЖД» № 4–6, 2019).

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

14. Определение уровня безопасности значимых объектов критической информационной инфраструктуры железнодорожного транспорта / А. П. Глухов, В. В. Василенко, А. А. Сидак, [и др.] // Двойные технологии. 2020. № 1 (90). С. 84–88.

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

16. Котенко, И. В. Об архитектуре многоуровневой интеллектуальной системы обеспечения информационной безопасности автоматизированных систем на железнодорожном транспорте / И. В. Котенко, И. Б. Саенко // Методы и технические средства обеспечения безопасности информации (МиТСОБИ): Сборник материалов 23-й научно-технической конференции (Санкт-Петербург, Россия, 30 июня–03 июля 2014 г). — Санкт-Петербург: Изд-во Политехнического ун-та, 2014. — С. 97–98.

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

18. Построение многоуровневой интеллектуальной системы обеспечения информационной безопасности для автоматизированных систем железнодорожного транспорта / И. В. Котенко, И. Б. Саенко, А. В. Чернов, М. А. Бутакова // Труды СПИИРАН. 2013. Вып. 7 (30). С. 7–25.

19. Управление безопасностью кибер-физических систем на основе оперативного ситуационного информирования об инцидентах / М. А. Бутакова, А. В. Чернов, П. С. Шевчук, С. М. Ковалев // Труды Ростовского государственного университета путей сообщения (Труды РГУПС). 2016. № 5. С. 14–16.

20. Методологические аспекты упреждающего управления информационной безопасностью железнодорожного транспорта / А. П. Глухов, Д. Н. Бирюков, В. В. Василенко, [и др.] // Двойные технологии. 2019. № 3 (88). С. 86–92.

21. О безопасности критической информационной инфраструктуры / С. Е. Ададуров, А. П. Глухов, А. А. Корниенко, Е. И. Белова // Автоматика, связь, информатика. 2020. № 4. С. 2–4. DOI: 10.34649/AT.2020.4.4.001.

22. 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.

23. Макаренко, С. И. Аудит безопасности критической инфраструктуры специальными информационными воздействиями: Монография. — Санкт-Петербург: Наукоемкие технологии, 2018. — 122 с.

24. 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.

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

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

27. 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.

28. Макаренко, С. И. Анализ стандартов и методик тестирования на проникновение / С. И. Макаренко, Г. Е. Смирнов // Системы управления, связи и безопасности. 2020. № 4. С. 44–72. DOI: 10.24411/2410-9916-2020-10402.

29. Татт, У. Т. Теория графов = Graph Theory / У. Т. Татт; пер. с англ. Г. П. Гаврилова. — Москва: Мир. Редакция литературы по математическим наукам, 1988. — 424 с.

30. Свами, М. Графы, сети и алгоритмы = Graphs, Networks, and Algorithms / М. Свами, К. Тхуласираман; пер. с англ. М. В. Горбатовой, [и др.]; под ред. В. А. Горбатова. — Москва: Мир. Редакция литературы по новой технике, 1984. — 455 с.

31. Кормен, Т. Алгоритмы: построение и анализ = Introduction to Algorithms / Т. Кормен, Ч. Лейзерсон, Р. Ривест; пер. с англ. К. Белова, [и др.]. — Москва: МЦНМО, 2000. — 960 с. — (Классические учебники: Computer science).

32. 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.

33. Цветков, К. Ю. Формирование резервных путей на основе алгоритма Дейкстры в целях повышения устойчивости информационно-телекоммуникационных сетей / К. Ю. Цветков, С. И. Макаренко, Р. Л. Михайлов // Информационно-управляющие системы. 2014. № 2 (69). С. 71–78.

34. Макаренко, С. И. Модифицированный алгоритм Беллмана-Форда с формированием кратчайших и резервных путей и его применение для повышения устойчивости телекоммуникационных систем / С. И. Макаренко, М. Н. Квасов // Инфокоммуникационные технологии. 2016. Т. 14, № 3. С. 264–274. DOI: 10.18469/ikt.2016.14.3.06.

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

36. 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.

37. Смирнов, Г. Е. Использование тестовых информационно-технических воздействий для аудита защищенности информационных систем железнодорожного транспорта / Г. Е. Смирнов, С. И. Макаренко // Интеллектуальные технологии на транспорте. 2020. № 3 (23). С. 20–29.

38. Смирнов, Г. Е. Использование тестовых информационно-технических воздействий для превентивного аудита защищенности информационно-телекоммуникационных сетей / Г. Е. Смирнов, С. И. Макаренко // Экономика и качество систем связи. 2020. № 3 (17). С. 43–58.

DOI: 10.24412/2413-2527-2022-331-5-18

Justification Method of Test Information-Technical Impacts for Security Analysis of Informatization Objects of Railway Transport

G. E. Smirnov
Saint Petersburg Electrotechnical University
Saint Petersburg, Russia
science.cybersec@yandex.ru

Abstract. **The article discusses the main information objects and automated systems of railway transport. It is shown that these systems are objects of a critical information infrastructure. In accordance with the legislation of the Russian Federation and the analysis of their real security is an important task. In the article is proposed to analyze the security of the objects and systems through using test information-technology impacts, which are predicted to be used by hackers. The justification method of information-technology impacts based on the Dijkstra's algorithm, which makes it possible to form a set of paths ranked by the total path metric is consisting of two stages: the stage of forming an ordered set of testing paths and the stage of choosing testing paths that ensure the rational completeness of vulnerability assessment with restrictions on resources.**

Keywords: **information security, audit, testing, Dijkstra's algorithm, information and technical impact, critical information infrastructure, informatization facility, railway transport.**

REFERENCES

1. Ryabtsev S. S. A Method for Detecting Byzantine Robots Based on Data from the Collective Decision-Making Process in Swarm Robotic Systems [Metod vyyavleniya vredonosnykh robotov na osnove dannykh protsessa kollektivnogo prinyatiya resheniy v roevykh robototekhnicheskikh sistemakh], *Systems of Control, Communication and Security [Sistemy upravleniya, svyazi i bezopasnosti]*, 2022, No. 3, Pp. 105–137.
DOI: 10.24412/2410-9916-2022-3-105-137.

2. Budko N. P., Vasiliev N. V. Review of Graph-Analytical Approaches to Monitoring of Information and Telecommunication Networks and Their Application to Identify Abnormal States [Obzor grafo-analiticheskikh podkhodov k monitoringu informatsionno-telekommunikatsionnykh setey i ikh primenenie dlya vyyavleniya anomalnykh sostoyaniy], *Systems of Control, Communication and Security [Sistemy upravleniya, svyazi i bezopasnosti]*, 2021, No. 6, Pp. 53–75.
DOI: 10.24412/2410-9916-2021-6-53-75.

3. Fedorchenko E. V., Novikova E. S., Gaifulina D. A., Kotenko I. V. Attacker Profiling Based on the Network Traffic Analysis [Postroenie profilya atakuyushchego na osnove analiza setevogo trafika v kriticheskikh infrastrukturakh], *Systems of Control, Communication and Security [Sistemy upravleniya, svyazi i bezopasnosti]*, 2021, No. 6, Pp. 76–89.
DOI: 10.24412/2410-9916-2021-6-76-89.

4. Vasilyev V. I., Vulfin A. M., Gvozdev V. E., et al. Ensuring Information Security of Cyber-Physical Objects Based on Predicting and Detecting Anomalies in Their State [Obespechenie informatsionnoy bezopasnosti kiberfizicheskikh obektov na osnove prognozirovaniya i obnaruzheniya anomaliy ikh sostoyaniya], *Systems of Control, Communication and Security [Sistemy upravleniya, svyazi i bezopasnosti]*, 2021, No. 6, Pp. 90–119. DOI: 10.24412/2410-9916-2021-6-90-119.

5. Izrailov K. E., Levshun D. S., Chechulin A. A. Vulnerability Classification Model for Smart City Transport Infrastructure Interfaces [Model klassifikatsii uyazvimostey interfeysov transportnoy infrastruktury «umnogo goroda»], *Systems of Control, Communication and Security [Sistemy upravleniya, svyazi i bezopasnosti]*, 2021, No. 5, Pp. 199–223.
DOI: 10.24412/2410-9916-2021-5-199-223.

6. Gorbachev A. A., Sokolovsky S. P., Usatikov S. V. Functioning Model and Algorithm of Email Service Proactive Protection from Network Intelligence [Model funktsionirovaniya i algoritm proaktivnoy zashchity servisa elektronnoy pochty ot setevoy razvedki], *Systems of Control, Communication and Security [Sistemy upravleniya, svyazi i bezopasnosti]*, 2021, No. 3, Pp. 60–109. DOI: 10.24412/2410-9916-2021-3-60-109.

7. Vasilyev V. I., Vulfin A. M., Kirillova A. D., Kuchkarova N. V. Methodology for Assessing Current Threats and Vulnerabilities Based on Cognitive Modeling Technologies and Text Mining [Metodika otsenki aktualnykh ugroz i uyazvimostey na osnove tekhnologiy kognitivnogo modelirovaniya i Text Mining], *Systems of Control, Communication and Security [Sistemy upravleniya, svyazi i bezopasnosti]*, 2021, No. 3, Pp. 110–134.
DOI: 10.24412/2410-9916-2021-3-110-134.

8. Voevodin V. A., Markin P. V., Markina M. S., Burenok D. S. Technique for Developing an Information Security Audit Program Taking into Account the Weight Coefficients of Certificates Audit Based on the Hierarchy Analysis Method [Metodika razrabotki programmy audita informatsionnoy bezopasnosti s uchetom vesovykh koeffitsientov znachimosti svidetelstv audita na osnove metoda analiza ierarkhiy], *Systems of Control, Communication and Security [Sistemy upravleniya, svyazi i bezopasnosti]*, 2021, No. 2, Pp. 96–129.
DOI: 10.24412/2410-9916-2021-2-96-129.

9. Zakoldaev D. A., Grishentsev A. Y. Formal Model of Information Security in the Management of Resources in Production [Formalnaya model obespecheniya informatsionnoy bezopasnosti pri upravlenii resursami na proizvodstvakh], *Systems of Control, Communication and Security [Sistemy upravleniya, svyazi i bezopasnosti]*, 2021, No. 1, Pp. 33–61.
DOI: 10.24411/2410-9916-2021-10102.

10. Sankova G. V., Odudenko T. A. Information technologies in the transportation process: Study guide [Informatsionnye tekhnologii v perevozochnom protsesse: Uchebnoe

posobie]. Khabarovsk, Far Eastern State Transport University, 2012, 111 p.

11. Isakov O. A. Questions of improving the automated control system of railway transport [Voprosy sovershenstvovaniya ASU zheleznodorozhnogo transporta]. Saarbrücken, LAP Lambert Academic Publishing, 2011, 224 p.

12. Adadurov S. E., Glukhov A. P., Kornienko A. A., Belova E. I. Methodological Aspects of Ensuring Information Security of the Transportation Process [Metodologicheskie aspekty obespecheniya informatsionnoy bezopasnosti perevozochnogo protsessa]. *In: Lapidus B. M., Osminin A. T. (eds) Management of goods flows and the transportation process on railway transport based on customer orientation and logistics technologies: A collective monograph of members and scientific partners of the Joint Scientific Council of Russian Railways JSC [Upravlenie tovarnymi potokami i perevozochnym protsessom na zheleznodorozhnom transporte na osnove klientoorientirovannosti i logisticheskikh tekhnologiy: kollektivnaya monografiya chlenov i nauchnykh partnerov Obedinennogo uchenogo soveta OAO «RZhD»]*. Saint Petersburg, LEMA Publishing House, 2019, Pp. 251–263.

13. Kotenko I. V., Chechulin A. A., Levshun D. S. Security Analysis of Railway Transport Infrastructure on the Base of Analytical Modeling [Analiz zashchishchennosti infrastruktury zheleznodorozhnogo transporta na osnove analiticheskogo modelirovaniya], *Zaŝita Informacii. Inside [Zashchita informatsii. Insayd]*, 2017, No. 6 (78), Pp. 48–57.

14. Gluhov A. P., Vasilenko V. V., Sidak A. A., et al. Determination of the Security Level of Significative Objects of Critical Information Infrastructure of Railway Transport [Opredelenie urovnya bezopasnosti znachimykh obektov kriticheskoy informatsionnoy infrastruktury zheleznodorozhnogo transporta], *Dual Technologies [Dvoynye tekhnologii]*, 2020, No. 1 (90), Pp. 84–88.

15. Adadurov S. E., Diasamidze S. V., Kornienko A. A., Sidak A. A. International Cybersecurity on Railway Transport: Methodological Approaches and Normal Procedural Framework [Mezhdunarodnaya kiberbezopasnost na zheleznodorozhnom transporte: metodologicheskie podkhody i normativnaya metodicheskaya baza], *Russian Railway Science Journal [Vestnik Nauchno-issledovatelskogo instituta zheleznodorozhnogo transporta]*, 2015, No. 6, Pp. 9–15.

16. Kotenko I. V., Saenko I. B. On the Architecture of a Multi-Level Intelligent Information Security System of Automated Systems in Railway Transport [Ob arkhitekture mnogourovnevoy intellektualnoy sistemy obespecheniya informatsionnoy bezopasnosti avtomatizirovannykh sistem na zheleznodorozhnom transporte], *Methods and Technical Means of Information Security(MiTSOBI): Collection of Materials of the 23rd Scientific and Technical Conference [Metody i tekhnicheskie sredstva obespecheniya bezopasnosti informatsii (MiTSOBI): Sbornik materialov 23-y nauchno-tekhnicheskoy konferentsii], Saint Petersburg, Russia, June 30–July 03, 2014*. Saint Peterburg, St. Petersburg State Polytechnic University, 2014, Pp. 97–98.

17. Kotenko I. V., Saenko I. B. Proposals on Creation of a Multi-Level Intelligent Information Security System of Automated Systems on Railway Transport [Predlozheniya po sozdaniyu mnogourovnevoy intellektualnoy sistemy obespecheniya informatsionnoy bezopasnosti avtomatizirovannykh sistem na zheleznodorozhnom transporte], *Vestnik Rostovskogo Gosudarstvennogo Universiteta Putey Soobshcheniya (Vestnik RGUPS),* 2013, No. 3 (51), Pp. 69–79.

18. 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 [Postroenie mnogourovnevoy intellektualnoy sistemy obespecheniya informatsionnoy bezopasnosti dlya avtomatizirovannykh sistem zheleznodorozhnogo transporta], *SPIIRAS Proceedings [Trudy SPIIRAN]*, 2013, Is. 7 (30), Pp. 7–25.

19. Butakova M. A., Chernov A. V., Shevchuk P. S., Kovalev S. M. Cyber-Physical Systems Security Management Based on Operational Situational Incidents Information [Upravlenie bezopasnostyu kiber-fizicheskikh sistem na osnove operativnogo situatsionnogo informirovaniya ob intsidentakh], *Trudy Rostovskogo gosudarstvennogo universiteta putej soobshcheniya (Trudy RGUPS)*, 2016, No. 5, Pp. 14–16.

20. Glukhov A. P., Biryukov D. N., Vasilenko V. V., et al. Methodological Aspects of Proactive Management of Railroad Transport Information Security [Metodologicheskie aspekty uprezhdayushchego upravleniya informatsionnoy bezopasnostyu zheleznodorozhnogo transporta], *Dual Technologies [Dvoynye tekhnologii]*, 2019, No. 3 (88), Pp. 86–92.

21. Adadurov S. E., Glukhov A. P., Kornienko A. A., Belova E. I. Principles of Railway Transport Critical Information Infrastructure Security Supporting [O bezopasnosti kriticheskoy informatsionnoy infrastruktury], *Automation, Communications, Informatics [Avtomatika, svyaz, informatika]*, 2020, No. 4, Pp. 2–4. DOI: 10.34649/AT.2020.4.4.001.

22. Makarenko S. I. Audit of Information Security — The Main Stages, Conceptual Framework, Classification of Types [Audit informatsionnoy bezopasnosti: osnovnye etapy, kontseptualnye osnovy, klassifikatsiya meropriyatiy], *Systems of Control, Communication and Security [Sistemy upravleniya, svyazi i bezopasnosti]*, 2018, No. 1, Pp. 1–29.
DOI: 10.24411/2410-9916-2018-10101.

23. Makarenko S. I. Security audit of critical infrastructure with special information impacts: Monograph [Audit bezopasnosti kriticheskoy infrastruktury spetsialnymi informatsionnymi vozdeystviyami: Monografiya]. Saint Petersburg, Naukoemkie tekhnologii Publishing House, 2018, 122 p.

24. Makarenko S. I. Penetration Testing in Accordance with NIST SP 800-115 Standard [Testirovanie na proniknovenie na osnove standarta NIST SP 800-115], *Cybersecurity Issues [Voprosy kiberbezopasnosti]*, 2022, No. 3 (49), Pp. 44–57.
DOI: 10.21681/2311-3456-2022-3-44-57.

25. Makarenko S. I., Smirnov G. E. Model of Security Audit of a Critical Information Infrastructure Object with Use the Test Cyber Attacks [Model audita zashchishchennosti obekta kriticheskoy informatsionnoy infrastruktury testovymi informatsionno-tekhnicheskimi vozdeystviyami], *Proceedings of Telecommunication Universities [Trudy uchebnykh zavedeniy svyazi]*, 2021, Vol. 7, No. 1, Pp. 94–104.
DOI: 10.31854/1813-324X-2021-7-1-94-104.

26. 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 [Metodika obosnovaniya testovykh informatsionno-tekhnicheskikh vozdeystviy, obespechivayushchikh ratsionalnuyu polnotu audita zashchishchennosti obekta kriticheskoy informatsionnoy infrastruktury], *Cybersecurity Issues [Voprosy kiberbezopasnosti]*, 2021, No. 6 (46), Pp. 12–25.

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

27. Makarenko S. I. Criteria and Parameters for Estimating Quality of Penetration Testing [Kriterii i pokazateli otsenki kachestva testirovaniya na proniknovenie], *Cybersecurity Issues [Voprosy kiberbezopasnosti]*, 2021, No. 3 (43), Pp. 43–57. DOI: 10.21681/2311-3456-2021-3-43-57.

28. Makarenko S. I., Smirnov G. E. Analysis of Penetration Testing Standards and Methodologies [Analiz standartov i metodik testirovaniya na proniknovenie], *Systems of Control, Communication and Security [Sistemy upravleniya, svyazi i bezopasnosti]*, 2020, No. 4, Pp. 44–72.
DOI: 10.24411/2410-9916-2020-10402.

29. Tutte W. T. Graph Theory [Teoriya grafov]. Moscow, Mir Publishers, 1988, 424 p.

30. Swamy M. N. S., Thulasiraman K. Graphs, Networks, and Algorithms [Grafy, seti i algoritmy]. Moscow, Mir Publishers, 1984, 455 p.

31. Cormen T. H., Leiserson C. E., Rivest R. L. Introduction to Algorithms [Algoritmy: postroenie i analiz]. Moscow, Moscow Center for Continuous Mathematical Education, 2000, 960 p.

32. Makarenko S. I. Stability Method of Telecommunication Network with Using Topological Redundancy [Metod obespecheniya ustoychivosti telekommunikatsionnoy seti za schet ispolzovaniya ee topologicheskoy izbytochnosti], *Systems of Control, Communication and Security [Sistemy upravleniya, svyazi i bezopasnosti]*, 2018, No. 3, Pp. 14–30.
DOI: 10.24411/2410-9916-2018-10302.

33. Tsvetcov K. U., Makarenko S. I., Mikhailov R. L. Forming Reserve Paths Based on Dijkstra Algorithm in Order to Enhance Stability of Telecommunication Networks [Formirovanie rezervnykh putey na osnove algoritma Deykstry v tselyakh povysheniya ustoychivosti informatsionno-telekommunikatsionnykh setey], *Information and Control Systems [Informatsionno-upravlyayushchie sistemy]*, 2014, No. 2 (69), Pp. 71–78.

34. Makarenko S. I., Kvasov M. N. Modified Bellman-Ford Algorithm with Forming the Shortest and Fallback Paths and Its Application for Telecommunication Network Stability Improvement [Modifitsirovannyy algoritm Bellmana-Forda s formirovaniem kratchayshikh i rezervnykh putey i ego primenenie dlya povysheniya ustoychivosti telekommunikatsionnykh sistem], *Infocommunication Technologies [Infokommunikatsionnye tekhnologii]*, 2016, Vol.14, No. 3, Pp. 264–274.
DOI: 10.18469/ikt.2016.14.3.06.

35. Makarenko S. I. The Improved OSPF Protocol for High Network Stability [Usovershenstvovannyy protokol marshrutizatsii OSPF, obespechivayushchiy povyshennuyu ustoychivost setey svyazi], *Proceedings of Telecommunication Universities [Trudy uchebnykh zavedeniy svyazi]*, 2018, Vol. 4, No. 2, Pp. 82–90.

36. Makarenko S. I. Improved Routing and Signaling Functions of PNNI Protocol for High Network Stability [Usovershenstvovanie funktsiy marshrutizatsii i signalizatsii protokola PNNI s tselyu povysheniya ustoychivosti seti svyazi], *Proceedings of Telecommunication Universities [Trudy uchebnykh zavedeniy svyazi]*, 2020, Vol. 6, No. 2, Pp. 45–59. DOI: 10.31854/1813-324X-2020-6-2-45-59.

37. Smirnov G. E., Makarenko S. I. The Use of Test Information and Technical Impacts for Security Audit of Information Systems of Railway Transport [Ispolzovanie testovykh informatsionno-tekhnicheskikh vozdeystviy dlya audita zashchishchennosti informatsionnykh sistem zheleznodorozhnogo transporta], *Intellectual Technologies on Transport [Intellektualnye tekhnologii na transporte]*, 2020, No. 3 (23), Pp. 20–29.

38. Smirnov G. E., Makarenko S. I. The use of test information and technical impacts for preventive audit security audit of information and telecommunication networks [Ispolzovanie testovykh informatsionno-tekhnicheskikh vozdeystviy dlya preventivnogo audita zashchishchennosti informatsionno-telekommunikatsionnykh setey], *Economics and quality of communication systems [Ekonomika i kachestvo sistem svyazi]*, 2020, No. 3 (17), Pp. 43–58.