БЕЗОПАСНОСТЬ ЦИФРОВЫХ ТЕХНОЛОГИЙ. – 2025. – № 4 (119). – 9–22

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 004 DOI: 10.17212/2782-2230-2025-4-9-22

ФОРМИРОВАНИЕ СВЯЗЕЙ ВНУТРЕННИХ ТРЕБОВАНИЙ БИЗНЕС-ПРОЦЕССА С ТРЕБОВАНИЯМИ К ИНФОРМАЦИОННЫМ СИСТЕМАМ ОРГАНИЗАЦИИ*

Е.Ю. ГОРОДЕЦКАЯ[1], А.Ф. НЕБ[2]

[1] *РФ, 630008, г. Новосибирск, ул. Кирова, 86, Сибирский государственный университет телекоммуникаций и информатики, преподаватель кафедры безопасности информации и технологий. E-mail: elena.shmanina-97@yandex.ru*

[2] *РФ, 660037, г. Красноярск, пр. имени газеты «Красноярский рабочий», 31, Сибирский государственный университет науки и технологий имени академика М.Ф. Решетнева, лаборант кафедры безопасности информационных технологий. E-mail: angelinaneb@mail.ru*

Применение методов управления информационной безопасностью в настоящее время базируется на частичной автоматизации и экспертных оценках, что в общем случае приводит к неточностям и неполноте данных, используемых для принятия решений. В статье рассмотрен вариант автоматизированного формирования связей внутренних требований бизнес-процесса на основе моделирования архитектуры информационной системы и предъявления требований к ее компонентам с использованием ресурсно-сервисной модели. Предлагается вариант реализации ресурсно-сервисной модели с учетом формирования динамического атрибутированного гиперграфа, представляющего собой модель связей трех уровней требований к информационным системам: включение в бизнес-процесс (соответствия регламенту бизнес-процесса), управление уязвимостями, управление конфигурациями. Предложенный подход реализован в виде практической задачи и может быть применен в реальных информационных системах.

Ключевые слова: моделирование, гиперграф, конфигурация, активы, управление информационной безопасностью

ВВЕДЕНИЕ

В 2023 году агентством Gartner был предложен метод CTEM (Continuous Threat Exposure Management), суть которого заключается в проактивном и интерактивном подходе к выявлению и анализу источников угроз безопас-

* Статья получена 10 ноября 2025 г.

ности информации, к снижению их уровня. Эта цель достигается в пять этапов (рис. 1) [1].

1. Идентификация поверхности атаки – определение процессов, входящих в цикл оценки защищенности.

2. Обнаружение уязвимостей – определение риск-профилей в рамках цикла оценки защищенности и площади атаки.

3. Приоритизация уязвимостей – определение срочности и важности устранения уязвимостей.

4. Валидация – оценка вероятности успеха атаки, анализ негативных последствий и проверка реакции команды по обеспечению информационной безопасности на возникающие угрозы.

5. Подготовка плана реагирования на случай инцидента – назначение задач и распределение ресурсов для реализации плана устранения уязвимостей.

Рис. 1. Этапы цикла CTEM

Основополагающими положениями модели являются проведение глубокой аналитики и цикличность осуществления шагов. При оценке рисков определена необходимость соотнесения технической уязвимости с бизнес-приоритетами. Преимуществом данного метода является его непрерывное проактивное воздействие и наличие программной реализации.

При этом остаются открытыми некоторые вопросы:

– порядок определения уязвимостей и последствий от реализации этих уязвимостей для сценария обеспечения непрерывности бизнес-процесса;

– проведение оценки возможности реализации бизнес-процесса с учетом требований к конфигурации элементов информационных систем организации.

Кроме того, на этапе идентификации поверхности атаки проводится определение площади применения метода и приоритизация активов. Однако не указано, по каким критериям может определяться сфера охвата действия метода. Правильная сегментация системы позволит сократить количество переменных в оценке защищенности системы, а также упростит процесс классификации технических активов организации по принадлежности к процессам передачи информации.

Таким образом, актуальна задача определения границ применения метода и возможности его доработки с точки зрения формирования внутренних связей между требованиями к бизнес-процессу и требованиями к информационной системе организации.

Цель работы – повышение эффективности управления информационной безопасностью путем реализации модели оценки выполнения установленных требований информационной безопасности в ИТ-инфраструктуре в рамках бизнес-процесса на основе динамического атрибутированного гиперграфа.

Практическая значимость работы заключается в том, что разрабатываемая модель может быть применена для создания специализированного программного модуля в составе систем управления ИБ. Это решение позволит в автоматизированном режиме оценивать риски прохождения конфиденциальной информации по маршруту бизнес-процесса, визуализировать «узкие места» и оперативно блокировать небезопасные операции, тем самым повышая общий уровень защищенности ИТ-инфраструктуры.

Описание инфраструктуры и в целом подход к формированию связей в этой статье использует гиперграфы как формальные средства оценки и моделирования, ранее неоднократно применявшиеся в сходных задачах [2–5]. При этом задействованный в работе динамический атрибутированный гиперграф и модель на его основе предложена Е.Ю. Городецкой в рамках предыдущих исследований и ранее не применялась.

1. ВНУТРЕННИЕ ТРЕБОВАНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1.1. ОПИСАНИЕ ВНУТРЕННИХ ТРЕБОВАНИЙ

Информационная безопасность в современной организации рассматривается не только как совокупность мер по защите данных, но и как механизм

обеспечения устойчивой и непрерывной работы бизнес-процессов. В зрелой ИТ-инфраструктуре требования к безопасности формируются на нескольких уровнях, которые отличаются назначением, источниками появления и характером контроля.

Нормативные требования – это законодательные и отраслевые обязательства, выполнение которых является базовым условием функционирования организации. Эти требования определяют минимально необходимый уровень безопасности и должны быть выполнены независимо от того, какие процессы, сервисы и модели используются внутри компании.

В этой работе нормативные требования не рассматриваются, так как предполагается, что организация уже обеспечивает их реализацию. Модель, разрабатываемая в рамках исследования, предназначена для обработки нормативной базы с обеспечением более детального анализа выполнения внутренних требований, вытекающих из бизнес-логики предприятия.

Ключевым источником внутренних требований являются бизнес-процессы.

Бизнес-процесс – это набор взаимосвязанных действий, направленных на достижение результата, значимого для организации. Важнейшими свойствами бизнес-процесса являются непрерывность (процесс не должен останавливаться без веской причины) и устойчивость (процесс должен сохранять работоспособность при воздействии различных угроз и изменений).

На каждом этапе бизнес-процесса предъявляются свои требования:

- к данным, которые обрабатываются;
- к используемым сервисам;
- к ПО и конфигурации;
- к активам инфраструктуры;
- к условиям безопасности.

Таким образом, истинный смысл требований ИБ проявляется именно через способность инфраструктуры обеспечить нужные параметры функционирования бизнес-процессов.

1.2. РЕСУРСНО-СЕРВИСНАЯ МОДЕЛЬ

ИТ-инфраструктура – экосистема, в которой постоянно что-то меняется: изнашивается и обновляется оборудование, добавляются новые элементы, запускаются новые сервисы и процессы. Современное предприятие нуждается в мощном инструменте, позволяющем полноценно видеть всю инфраструктуру и строить стратегию управления ресурсами и сервисами на основе данных

о взаимодействии компонентов инфраструктуры. Таким мощным инструментом является ресурсно-сервисная модель (РСМ).

Ресурсно-сервисная модель (РСМ) – это схема, которая описывает все элементы ИТ-инфраструктуры компании и показывает взаимосвязи между ними. Обычно на РСМ отображается, какие компоненты инфраструктуры участвуют в формировании конкретной услуги или сервиса [6].

Ресурсно-сервисная модель состоит из трех ключевых элементов:

1) ресурсы предоставляют физический и виртуальный потенциал, необходимый для оказания соответствующих сервисов: серверы, рабочие станции, коммуникационные линии и другое оборудование для осуществления операций предприятия;

2) сервисы, являющиеся функциональными единицами, которые реализуют заданные функции и предоставляют требуемые услуги пользователям. Каждому сервису соответствуют конкретные ресурсы, обеспечивающие его функционирование. Следовательно, между ресурсами и сервисами возникают тесные взаимосвязи, которые формируют уникальную структуру каждой конкретной ИТ-инфраструктуры;

3) зависимости, показывающие, как различные ресурсы и сервисы влияют друг на друга, образуя единый механизм, который функционирует в интересах компании.

Таким образом, использование ресурсно-сервисной модели для анализа инфраструктурных зависимостей может быть следующим. Предположим, что в компании существует определенный сервис электронной почты, зависящий от почтового сервера, DNS-серверов и каналов связи. Используя РСМ, можно проследить, как изменение состояния одного ресурса (например, отказ DNS-сервера) повлияет на работу самого сервиса электронной почты и других связанных сервисов.

2. ФОРМИРОВАНИЕ СВЯЗЕЙ ВНУТРЕННИХ ТРЕБОВАНИЙ

2.1. ФОРМИРОВАНИЕ СВЯЗЕЙ

Предложенная реализация формирования связей основана на модели динамического атрибутированного гиперграфа [7] и предназначена для динамической оценки соответствия процесса передачи информации в рамках бизнес-процесса внутренним требованиям информационной безопасности (ИБ).

Она работает по следующему принципу: определяет, существует ли в данный момент безопасный путь для передачи конфиденциальной инфор-

мации через информационную систему, который удовлетворяет трем ключевым требованиям ИБ:

- соответствие регламенту бизнес-процесса;
- приемлемый уровень уязвимостей используемого программного обеспечения;
- соответствие конфигурации узлов (устройств) требуемым профилям настройки.

Модель представляет собой динамический ориентированный атрибутированный гиперграф, который позволяет объединять узлы системы в группы (гиперребра) не только по прямым связям, но и по общим атрибутам (требованиям ИБ). Это отличает его от обычного графа.

В рамках реализации модели будет затрагиваться оценка выполнения внутренних требований предприятия, поскольку требования законодательства должны быть выполнены в любом случае, т. е. независимо от внутренних требований.

Каждому узлу (устройству) присваиваются три бинарных атрибута (1/0), отражающих выполнение одного из трех требований ИБ в реальном времени.

Модель динамически обновляется, отражая текущее состояние системы. Это позволяет оценивать безопасность не статично, а в каждый момент времени t.

Архитектура модели состоит из трех логических плоскостей, каждая из которых проверяет свое требование.

1. Плоскость бизнес-процесса: проверяет, задействован ли узел в текущем этапе бизнес-процесса и передается ли информация по защищенному каналу. Атрибут $a_1 = 1$, если узел активен в процессе.

2. Плоскость уязвимостей: проверяет, не превышает ли уровень критичности уязвимостей программного обеспечения на узле заданного порога, который отображает переменная k (например, $k = 7$ по БДУ ФСТЭК [8]). Атрибут $a_2 = 1$, если узел безопасен.

3. Плоскость конфигураций: проверяет, соответствует ли профиль настройки узла (ОС, ПО, параметры) эталонному профилю, требуемому для данного бизнес-процесса. Атрибут $a_3 = 1$, если конфигурация корректна.

Процесс принятия решения: гиперребро (связь, объединяющая узлы по всем трем атрибутам) может быть построено, если для всех узлов на этом пути $a_1 = a_2 = a_3 = 1$. Матрица инцидентности рассчитывается для каждого временного среза t. Если в момент времени t существует непрерывный путь от начальной до конечной вершины, состоящий из таких безопасных гиперребер, передача информации разрешена. Если какой-либо атрибут на критич-

ном узле становится равен нулю, путь разрывается и на основе моделирования либо находится альтернативный путь, либо блокируется реализация бизнес-процесса.

2.2. РАБОТА С ТРЕБОВАНИЯМИ НА УРОВНЕ ИНФОРМАЦИОННЫХ СИСТЕМ

Модель можно рассматривать как систему, которая интегрирует и делает оперативные выводы из данных, собираемых системами ITAM и SMDB.

Атрибут a_1 (задействованность в бизнес-процессе) напрямую зависит от данных ITAM.

Интерпретация: ITAM-система содержит реестр всех активов и их взаимосвязей. Модель использует эти данные, чтобы знать, какие узлы физически существуют и должны участвовать в процессе. Атрибут $a_1 = 1$ означает, что актив не только числится в реестре ITAM, но и логически назначен на текущий этап бизнес-процесса.

CMDB (конфигурационная база данных) содержит интерфейс ответа на вопросы «В каком они состоянии?» и «Соответствуют ли они политикам?».

Атрибут a_2 (уровень уязвимостей) напрямую зависит от данных CMDB и интеграции с системами управления уязвимостями.

Интерпретация: CMDB хранит информацию об установленном на активе программном обеспечении (версия ОС, пакеты, приложения). Модель получает актуальный список ПО для каждого узла. Затем она сверяет этот список с базой уязвимостей (например, БДУ ФСТЭК). Следовательно, $a_2 = 1$ – это результат проверки, что ни у одного ПО на данном активе нет неустраненных уязвимостей с критичностью выше порога. По сути, это автоматизированная проверка на основе данных CMDB и средства сканирования уязвимостей.

Атрибут a_3 (соответствие профилю настройки) полностью базируется на данных CMDB.

Интерпретация: это ядро управления конфигурацией. CMDB хранит эталонные конфигурации (золотые образцы) для разных ролей устройств. Модель в реальном времени сравнивает фактическую конфигурацию узла с эталонным профилем из CMDB. Следовательно, $a_3 = 1$ означает, что конфигурация узла строго соответствует эталону, предписанному для его роли в текущем бизнес-процессе. Любое отклонение (несанкционированно открытый порт, измененная политика паролей) приводит к $a_3 = 0$.

2.3. АПРОБАЦИЯ ФОРМИРОВАНИЯ ВНУТРЕННИХ ТРЕБОВАНИЙ НА РЕСУРСНО-СЕРВИСНОЙ МОДЕЛИ

Для реализации модели оценки выполнения требований ИБ в ИТ-инфраструктуре будет взят бизнес-процесс проведения киберучений на учебно-тренировочной платформе (киберполигоне) AMPIRE [9]. В рамках киберучений будут использоваться 2 аудитории: 502 (8 компьютеров на ОС РедОС) и 501 (9 компьютеров, 5 на ОС РедОС и 4 на ОС Windows). В 501-й аудитории один коммутатор, который имеет выход в интернет, в 502-й аудитории 2 коммутатора, которые соединены последовательно и имеют выход в интернет и к VPN-серверу на ampire. Для проведения киберучений необходимо, чтобы на каждом компьютере был установлен OpenVPN и был доступ к интернету. Поскольку аудитории входят в состав информационной системы университета, необходимо предъявить самостоятельно требования к компьютерам и коммутаторам.

Для упрощения представления модели далее рассмотрим практическую реализацию ее в виде ресурсно-сервисной модели в рамках управления активами на базе Security Vision AM.

Пример построенной модели приведен на рис. 2, 3.

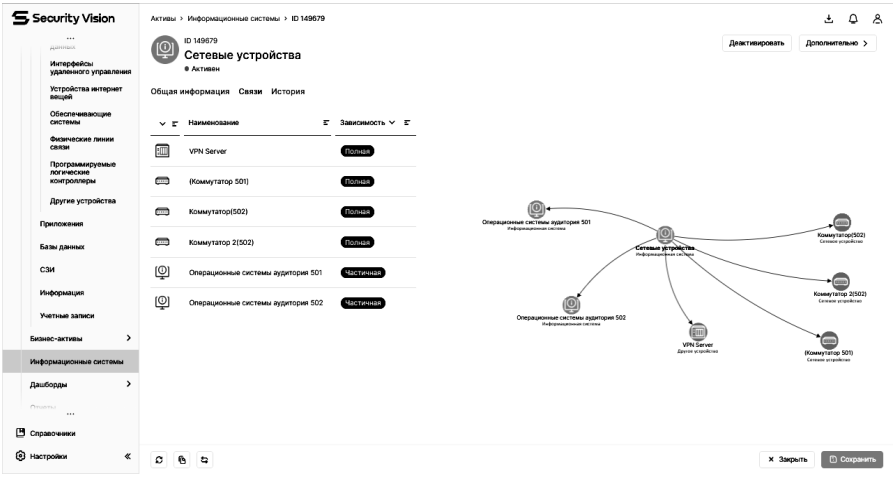

Рис. 2. Реализация внутренних связей

Связи указываются для всех типов активов в соответствии с расчетом модельной архитектуры и далее преобразуются в полную ресурсно-сервисную модель.

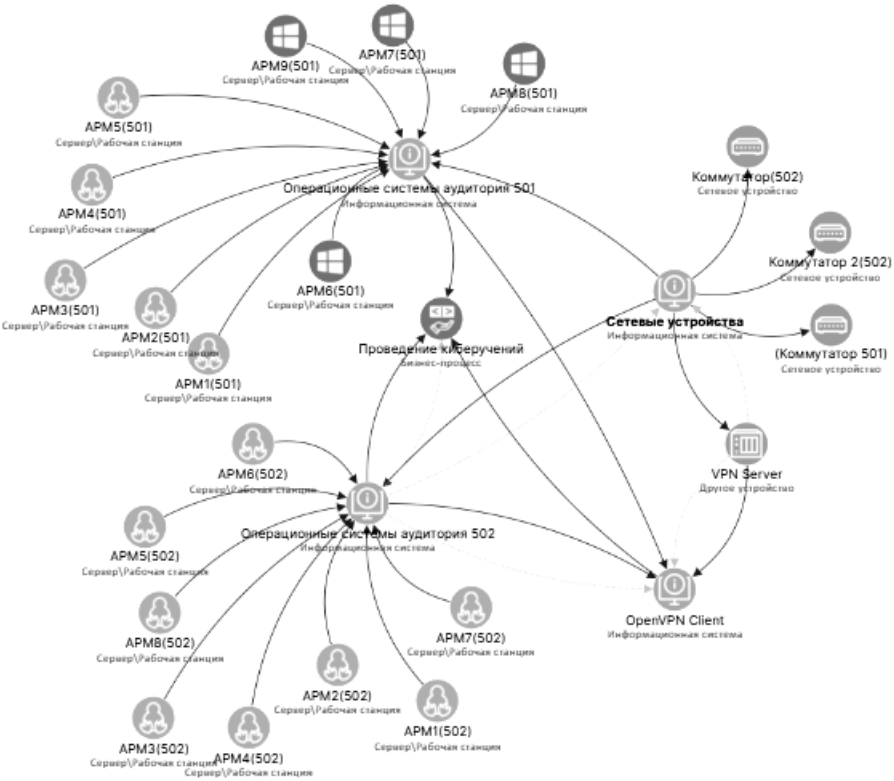

Рис. 3. Ресурсно-сервисная модель

Построение ресурсно-сервисной модели позволяет добиться следующих результатов:

- реализовать модельную архитектуру в виде звездчатого графа;
- сформировать связи между требованиями бизнес-процесса и требованиями к информационным системам;
- проанализировать зависимости;
- оценить возможность реализации бизнес-процесса.

ЗАКЛЮЧЕНИЕ

При реализации ресурсно-сервисной модели с использованием описанного подхода и с учетом формирования модельной архитектуры бизнес-процесса как управляемого объекта в виде гиперграфа [10] достигается возможность управления характеристиками информационных систем методом СТЕМ. При этом появляется возможность формальной оценки выполнения внутренних требований бизнес-процесса в автоматизированном режиме, что ранее представляло сложность.

Показано, как можно упростить представление гиперграфа и реализовать его в виде ресурсно-сервисной модели и связанных плоскостей, что позволяет ускорить практическую реализацию подхода в реальных системах.

В целом реализация подхода служит цели формирования модели безопасности автоматизированной системы [11] и может применяться на практике и в исследовательских задачах.

СПИСОК ЛИТЕРАТУРЫ

1. Continuous Threat Exposure Management. – URL: https://xmcyber.com/ctem/ (accessed: 01.12.2025).

2. *Соловейчик К.А., Светлов Р.В., Аркин П.А.* Байесовские сети принятия решений в задачах управления рисками информационной подсистемы организации // Известия СПбГЭУ. – 2021. – № 2 (128). – С. 88–99.

3. *Kulikov I., Zhukova N.* Practical aspects of using knowledge graphs for telecommunication networks modelling // Informatics and automation. – 2020. – P. 1–5.

4. *Касьянов В.Н.* Методы и средства визуализации информации на основе атрибутированных иерархических графов с портами // Сибирский аэрокосмический журнал. – 2023. – Т. 24, № 1. – С. 8–17.

5. *Chodrow P., Mellor A.* Annotated hypergraphs: models and applications // Applied Network Science. – 2020. – Vol. 5 (1). – P. 9. – DOI: 10.1007/s41109-020-0252-y.

6. Ресурсно-сервисная модель: что это такое и какие задачи решает в управлении ИТ-ландшафтом. – URL: https://www.naumen.ru/products/bsm/articles/rsm/ (дата обращения: 01.12.2025).

7. *Zolotarev V., Gorodetskaya E., Kuznetsov A.* Evaluation of approaches to modeling information risk of telecommunication systems based on hypergraphs // Lecture Notes in Networks and Systems. – 2025. – Vol. 1456: AISMA-2025: Inter-

national Workshop on Advanced Information Security Management and Applications. – P. 510–521. – DOI: 10.1007/978-3-032-07275-7_46.

8. ФСТЭК России. Банк данных угроз безопасности информации. – URL: https://bdu.fstec.ru/ (дата обращения: 01.12.2025).

9. Моделирование вектора сетевых атак на локальную сеть с применением базы MITRE ATT&CK / А.Р. Касимова, В.В. Золотарев, Л.Х. Сафиуллина, Д.И. Сабирова // Прикаспийский журнал: управление и высокие технологии. – 2023. – № 4 (64). – С. 88–96. – DOI: 10.54398/20741707_2023_4_88. – EDN MPSCDH.

10. *Золотарев В.В.* Формирование модели управляемого объекта на основе гиперграфа в цикле непрерывного детектирования и реагирования на инциденты информационной безопасности // Прикаспийский журнал: управление и высокие технологии. – 2024. – № 1 (65). – С. 37–44.

11. Методика построения модели безопасности автоматизированных систем / В.Г. Жуков, М.Н. Жукова, В.В. Золотарев, И.В. Ковалев // Программные продукты и системы. – 2012. – № 2. – С. 70–74. – EDN OZYEVV.

Городецкая Елена Юрьевна, преподаватель кафедры безопасности и управления телекоммуникациями Сибирского государственного университета телекоммуникаций и информатики. Основное направление научных исследований – управление информационной безопасностью. E-mail: elena.shmanina-97@yandex.ru

Неб Ангелина Федоровна, лаборант кафедры безопасности информационных технологий Сибирского государственного университета науки и технологий имени академика М.Ф. Решетнёва. Область научных интересов – разработка автоматизированных сценариев управления информационной безопасностью. E-mail: angelinaneb@mail.ru

DOI: 10.17212/2782-2230-2025-4-9-22

Links formation between the internal requirements of the business process and information systems of the organization*

E.Yu. Gorodetskaya[1], A.F. Neb[2]

[1] *Siberian State University of Telecommunications and Informatics, 86 Kirova Street, Novosibirsk, 630008, Russian Federation, Lecturer at the Department of Security Technologies. E-mail: elena.shmanina-97@yandex.ru*

[2] *Siberian State University of Science and Technology named after Academician M.F. Reshetnyova, 31 Avenue named after the newspaper "Krasnoyarsk Worker", Krasnoyarsk, 660037, Russian Federation, laboratory assistant of Department of Information Technology Security. E-mail: h1ppyfox1@gmail.com*

The application of information security management methods is currently based on partial automation and expert assessments, which generally leads to inaccuracies and incompleteness in the data used for decision-making. The article considers a variant of the automated formation of links between the internal requirements of a business process based on modeling the architecture of an information system and making requirements for its components using a resource-service model. A variant of the implementation of the resource-service model is proposed, taking into account the formation of a dynamic attributed hypergraph, which is a model of connections between three levels of information system requirements: inclusion in the business process (compliance with business process regulations), vulnerability management, and configuration management. The proposed approach is implemented as a practical task and can be applied in real information systems.

Keywords: modeling, hypergraph, configuration, assets, information security management

REFERENCES

1. *Continuous Threat Exposure Management*. Available at: https://xmcyber.com/ctem/ (accessed 01.12.2025).

2. Soloveichik K.A., Svetlov R.V., Arkin P.A. Baiesovskie seti prinyatiya reshenii v zadachakh upravleniya riskami informatsionnoi podsistemy organizatsii [Bayesian decision-making networks in the risk management tasks of the information subsystem of an organization]. *Izvestiya Sankt-Peterburgskogo gosudarstvennogo ekonomicheskogo universiteta*, 2021, no. 2 (128), pp. 88–99. (In Russian).

* *Received 10 November 2025.*

3. Kulikov I., Zhukova N. Practical aspects of using knowledge graphs for modeling telecommunication networks. *Informatics and Automation*, 2020, pp. 1–5.

4. Kasyanov V.N. Metody i sredstva vizualizatsii informatsii na osnove atributirovannykh ierarkhicheskikh grafov s portami [Methods and tools for information visualization on the basis of attributed hierarchical graphs with ports]. *Sibirskii aerokosmicheskii zhurnal* = S *Siberian Aerospace Journal*, 2023, vol. 24, no. 1, pp. 8–17.

5. Chodrow P., Mellor A. Annotated hypergraphs: models and applications. *Applied Network Science*, 2020, vol. 5 (1), p. 9. DOI: 10.1007/s41109-020-0252-y.

6. *Resursno-servisnaya model': chto eto takoe i kakie zadachi reshaet v upravlenii IT-landshaftom* [Main goal: what exactly is it and how would the tasks be aime dat managing the ITsite]. Available at: https://www.naumen.ru/products/bsm/articles/rsm/ (accessed 01.12.2025).

7. Zolotarev V., Gorodetskaya E., Kuznetsov A. Evaluation of approaches to modeling information risk of telecommunication systems based on hypergraphs. *Lecture Notes in Networks and Systems*, 2025, vol. 1456. *AISMA-2025: International Workshop on Advanced Information Security Management and Applications*, pp. 510–521. DOI: 10.1007/978-3-032-07275-7_46.

8. FSTEC of Russia. *Bank dannykh ugroz bezopasnosti informatsii* [Information Security Threat Database]. Available at: https://bdu.fstec.ru/ (accessed 01.12.2025).

9. Kasimova R., Zolotarev V.V., Safiullina L.Kh., Sabirova D.I. Modelirovanie vektora setevykh atak na lokal'nuyu set' s primeneniem bazy MITRE ATT&CK [Modeling the network attack vector on a local network using the MITER ATT&CK]. *Prikaspiiskii zhurnal: upravlenie i vysokie tekhnologii = Caspian Journal: Management and High Technologies*, 2023, no. 4 (64), pp. 88–96. DOI: 10.54398/20741707_2023_4_88.

10. Zolotarev V.V. Formirovanie modeli upravlyaemogo ob"ekta na osnove gipergrafa v tsikle nepreryvnogo detektirovaniya i reagirovaniya na intsidenty informatsionnoi bezopasnosti [Controlled object model based on a hypergraph in the continuous detection and response cycle to information security incidents]. *Prikaspiiskii zhurnal: upravlenie i vysokie tekhnologii = Caspian Journal: Management and High Technologies*, 2024, no. 1 (65), pp. 37–44.

11. Zhukov V.G., Zhukova M.N., Zolotarev V.V., Kovalev I.V. Metodika postroeniya modeli bezopasnosti avtomatizirovannykh sistem [Methodology for constructing a securitymodel for automated systems]. *Programmnye produkty i sistemy = Software and Systems*, 2012, no. 2, pp. 70–74.

Для цитирования:

Городецкая Е.Ю., *Неб А.Ф.* Формирование связей внутренних требований бизнес-процесса с требованиями к информационным системам организации // Безопасность цифровых технологий. – 2025. – № 4 (119). – С. 9–22. – DOI: 10.17212/2782-2230-2025-4-9-22.

For citation:

Gorodetskaya E.Yu., Neb A.F. Formirovanie svyazei vnutrennikh trebovanii biznes-protsessa s trebovaniyami k informatsionnym sistemam organizatsii [Links formation between the internal requirements of the business process and information systems of the organization]. *Bezopasnost' tsifrovykh tekhnologii = Digital Technology Security*, 2025, no. 4 (119), pp. 9–22. DOI: 10.17212/2782-2230-2025-4-9-22.