БЕЗОПАСНОСТЬ ЦИФРОВЫХ ТЕХНОЛОГИЙ. – 2025. – № 2 (117). – 76–102

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 004 DOI: 10.17212/2782-2230-2025-2-76-102

ОРГАНИЗАЦИЯ ПРОЦЕССА УПРАВЛЕНИЯ УЯЗВИМОСТЯМИ ПРЕДПРИЯТИЙ ФИНАНСОВОГО СЕКТОРА*

Л.А. ГРИЩЕНКО[1], В.А. ЛЕВИЦКАЯ[2]

[1] *630055, РФ, г. Новосибирск, ул. Шатурская, 2, акционерное общество «Центр финансовых технологий», старший инженер анализа защищенности. E-mail: l.grishhenko@corp.nstu.ru*

[2] *630073, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, лаборант кафедры защиты информации. E-mail: leviczkaya.2020@stud.nstu.ru*

В статье представлен детальный анализ методических документов по управлению уязвимостями, включая как отечественные, так и зарубежные стандарты и руководства. Основной целью данного исследования является определение сильных и слабых сторон каждого рассмотренного источника для последующего построения универсального подхода, объединяющего наиболее эффективные практики. Особое внимание сосредоточено на адаптации предложенного подхода к современным и быстро развивающимся киберугрозам, а также к требованиям информационной безопасности. Результатом работы является комплексная программа управления уязвимостями, сочетающая эффективные методы обнаружения, оценки уязвимостей и активов, ранжирования и устранения уязвимостей, контроля устранения и улучшения процесса управления уязвимостями. Значимость организации такого процесса очевидна, ведь своевременно устраненные уязвимости могут существенно снизить риски и обезопасить организации от потенциальных атак.

Ключевые слова: уязвимости, процесс управления уязвимостями, финтех-компания, IT-инфраструктура, эксплойты, IT-активы, сканирование уязвимостей, патчи

ВВЕДЕНИЕ

В современном информационном обществе, где технологии играют важную роль, вопросы безопасности становятся неотъемлемой частью деловой среды. Уязвимости в информационных системах могут представлять серьез-

* Статья получена 16 мая 2025 г.

ную угрозу для организаций, нанося значительный ущерб и нарушая их деятельность и репутацию [1].

Управление уязвимостями – достаточно трудоемкий процесс, но он необходим организациям, так как направлен на минимизацию рисков и защиту систем от возможных атак, эксплойтов и других форм взлома или нарушений безопасности. Процесс включает выявление, приоритизацию и устранение уязвимостей, а также контроль над процессом. Управление уязвимостями гарантирует, что организация понимает свои слабые места и может планировать соответствующие действия [2].

Процесс управления уязвимостями состоит из нескольких этапов. Каждому из этих этапов следует уделять особое внимание, так как эффективное управление уязвимостями зависит от корректного определения приоритетов и ресурсов, а также от способности оперативного реагирования на выявленные угрозы. Значимость таких процессов очевидна, ведь своевременно устраненные уязвимости могут существенно снизить риски и обезопасить организации от потенциальных атак.

Актуальность темы обусловлена тем, что уязвимости остаются одним из ключевых факторов, угрожающих безопасности инфраструктуры организации. Их эксплуатация может привести к сбоям в работе критически важных систем, к утечке конфиденциальной информации и нанесению финансового ущерба. В связи с этим правильное выстраивание процесса управления уязвимостями является важной задачей.

Целью исследования является организация процесса управления уязвимостями в компании, специализирующейся на разработке финансовых технологий.

Для достижения этой цели необходимо решить ряд задач:

1) изучить отечественные и зарубежные документы;

2) провести сравнительный анализ отечественной и зарубежной документации;

3) проанализировать нормативные и методические документы, касающиеся управления уязвимостями;

4) разработать комплексный подход к организации процесса управления уязвимостями.

1. ИЗУЧЕНИЕ ОТЕЧЕСТВЕННОЙ И ЗАРУБЕЖНОЙ ДОКУМЕНТАЦИИ

Управление уязвимостями – это практика обеспечения безопасности, направленная на упреждающее предотвращение использования IT-уязвимостей, существующих в организации. Целью является сокращение времени и ресурсов на устранение уязвимостей и снижение рисков их использования [3].

Для того чтобы выстроить качественный процесс управления уязвимостями, необходимо изучать существующую документацию по данному процессу – как отечественную, так и зарубежную.

В отечественной документации ключевым является Методический документ ФСТЭК России от 17.05.2023 г. «Руководство по организации процесса управления уязвимостями в органе (организации)» (далее – Руководство), регламентирующий процесс обеспечения безопасности информационных систем от уязвимостей в организациях. Основной целью данного Руководства является минимизация уязвимостей, которые могут быть использованы злоумышленниками для проникновения и эксплуатации информационных систем. В нем описаны принципы управления уязвимостями, требования к их выявлению, анализу, устранению, аудиту и организационной структуре [1].

Зарубежный документ NIST.SP.800-40r2 (далее – NIST) предлагает рекомендации по созданию и внедрению программы управления уязвимостями, включая разработку и тестирование исправлений. Документ ориентирован на менеджеров безопасности и системных администраторов.

2. СРАВНИТЕЛЬНЫЙ АНАЛИЗ ОТЕЧЕСТВЕННОЙ И ЗАРУБЕЖНОЙ ДОКУМЕНТАЦИИ ПО ОРГАНИЗАЦИИ ПРОЦЕССА УПРАВЛЕНИЯ УЯЗВИМОСТЯМИ

Как было понятно из вышесказанного, в качестве отечественной документации был выбран методический документ ФСТЭК от 17.05.2023 г. «Руководство по организации процесса управления уязвимостями в органе (организации)», а зарубежной – NIST SP 800-40.

Перед тем как начать проводить анализ, следует объяснить выбор именно этих двух документов. Руководство предъявляет обязательные требования, соответствующие российскому законодательству, что важно для соблюдения норм в области информационной безопасности. NIST, в свою очередь, предлагает признанные лучшие практики и инструменты для управления патчами и уязвимостями.

NIST охватывает не только управление уязвимостями, но и управление исправлениями, что является одним из отличий этого документа от Руководства. Согласно NIST, исправления – это дополнительные фрагменты кода, разработанные для устранения проблем (обычно называемых багами) в программном обеспечении. Стандарт включает рекомендации по созданию и тестированию исправлений.

Оба документа подчеркивают необходимость создания специализированной группы. В NIST описаны общие обязанности участников, а в Руководстве конкретные роли. Они могут распределяться и (или) совмещаться в зависимости от укомплектованности подразделений. Представлены три роли:

- О (ответственный) – работник, ответственный за завершение выполнения задачи;
- И (исполнитель) – работник, непосредственно выполняющий задачу;
- У (участник) – работник, участие которого требуется для выполнения задачи.

Стоит отметить, что в NIST более подробно написано про инвентаризацию активов, что является основой любой инфраструктуры. Необходимо создание единого реестра активов при условии, что каждый IT-ресурс связан с одной системой.

Также следует отметить, что в NIST есть пункт про тестирование исправлений (патчей). Подчеркивается важность тестирования исправлений перед их развертыванием в производственной среде.

В NIST описаны меры предосторожности перед применением идентифицированного исправления с помощью патча или без него. Рекомендации для тестирования исправлений могут включать следующее:

- убедитесь, что патч получен из официального источника;
- проверьте патч на соответствие методам аутентификации поставщика;
- перед установкой патчей следует провести проверку антивирусом;
- исправления и модификации конфигурации следует тестировать на непроизводственных системах;
- установка одного исправления может случайно удалить или отключить другое исправление, поэтому важно соблюдать последовательность установки и проверять наличие зависимостей;
- тестируйте патчи на системах, отражающих рабочую конфигурацию;
- перед установкой исправления стоит изучить опыт других пользователей;
- если возникнут проблемы с исправлением, нужно оценить, перевешивают ли недостатки преимущества его установки.

3. АНАЛИЗ НОРМАТИВНЫХ И МЕТОДИЧЕСКИХ ДОКУМЕНТОВ, КАСАЮЩИХСЯ УПРАВЛЕНИЯ УЯЗВИМОСТЯМИ

Также, для организации управления уязвимостями следует рассмотреть такие документы:

- ГОСТ Р ИСО/МЭК 27002–2021;
- ГОСТ Р 57580.1–2017;

- ФСТЭК России от 28 октября 2022 г. Методика тестирования обновлений безопасности программных, программно-аппаратных средств;
- ГОСТ Р ИСО/МЭК 27005–2010;
- PCI DSS.

3.1. ГОСТ Р ИСО/МЭК 27002–2021

В этом документе представлена информация по процессу управления техническими уязвимостями. Техническая уязвимость – это недостатки в программном или аппаратном обеспечении.

Кроме того, указано, что необходимо предпринять соответствующие и своевременные меры для выявления потенциальных технических уязвимостей. Для эффективного управления уязвимостями рекомендуется:

1) назначить ответственных за процесс;
2) определить источники информации для выявления и актуализации сведений об уязвимостях;
3) установить сроки реагирования на уведомления;
4) оценить риски и предпринимать меры при выявлении уязвимости;
5) если доступно официальное обновление, следует оценить риски, связанные с его установкой;
6) если исправлений не выпущено, следует рассмотреть иные меры;
7) следует вести журнал всех предпринятых действий;
8) регулярно контролировать и оценивать процесс;
9) приоритет отдавать системе с высоким уровнем риска;
10) при отсутствии готовых решений необходимо оценить риски и разработать временные меры.

3.2. ГОСТ Р 57580.1–2017

В целях повышения эффективности процесса рассматривается возможность применения данного ГОСТа, содержащего оптимальные профессиональные решения. Меры актуальны для процесса VM: ЦЗИ.1 – ЦЗИ.11.

3.3. ФСТЭК РОССИИ ОТ 28 ОКТЯБРЯ 2022 г. МЕТОДИКА ТЕСТРОВАНИЯ ОБНОВЛЕНИЙ БЕЗОПАСНОСТИ ПРОГРАММНЫХ, ПРОГРАММНО-АППАРАТНЫХ СРЕДСТВ

Включает в себя рекомендации по подготовке обновлений, их установку, проведение тестов и анализ результатов для подтверждения отсутствия новых уязвимостей.

3.4. ГОСТ Р ИСО/МЭК 27005–2010

В этом ГОСТе представлены примеры уязвимостей и угроз, которые могут быть полезными во время оценки угроз и уязвимостей для определения сценария значимого инцидента. Следует подчеркнуть, что в некоторых случаях эти уязвимости могут использоваться и другими угрозами.

3.5. PCI DSS

Стандарт включает требование 6 по регулярному выявлению, оценке и устранению уязвимостей с обязательным устранением критических проблем в течение 30 дней. Требование 11 обязывает проводить ежеквартальные сканирования и ежегодные пентесты, а также подтверждать устранение уязвимостей повторными проверками. Все действия должны фиксироваться в логах в соответствии с требованием 10. Стандарт включает в себя требование 2 (по инвентаризации активов) и требование 12 (по политике безопасности), где прописаны роли и сроки реагирования. На практике используются инструменты для сканирования, учета активов и автоматизации устранения уязвимостей.

4. СОЗДАНИЕ КОМПЛЕКСНОГО ПОДХОДА ПО ОРГАНИЗАЦИИ ПРОЦЕССА УПРАВЛЕНИЯ УЯЗВИМОСТЯМИ

Исходя из информации, полученной из руководства ФСТЭК и NIST, было выделено 7 этапов процесса управления уязвимостями. На рис. 1 представлена схема процесса управления уязвимостями.

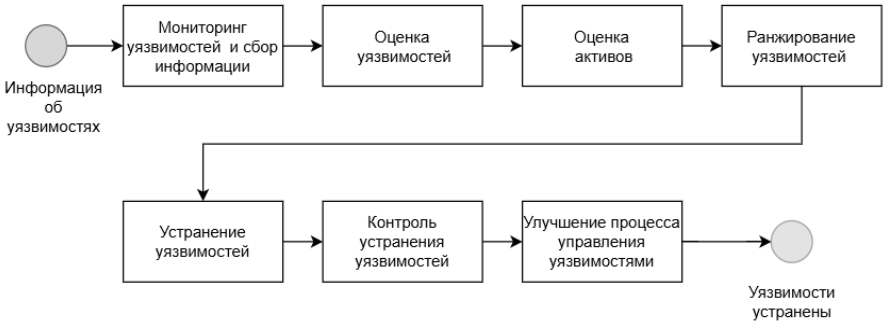

Рис. 1. Схема процесса управления уязвимостями

Fig. 1. Vulnerability management process diagram

4.1. МОНИТОРИНГ УЯЗВИМОСТЕЙ И СБОР ИНФОРМАЦИИ

На этом этапе осуществляется выявление уязвимостей на основании данных, получаемых из внешних и внутренних источников, и принятие решений по их последующей обработке [4].

На основе данных из руководства ФСТЭК и NIST можно сформировать более обширный перечень источников.

К внутренним источникам относятся:

- системы управления информационной безопасностью;
- базы данных управления конфигурациями;
- документация на информационные системы;
- электронные базы знаний органов (организаций);
- данные, полученные от сотрудников организации;
- информация, полученная из отчетов сканеров уязвимостей.

К внешним источникам принадлежат:

- базы данных, содержащие сведения об известных уязвимостях (например, NVD, CVE);
- официальные информационные ресурсы разработчиков программных и программно-аппаратных средств и исследователей в области информационной безопасности;
- доклады и отчеты по безопасности;
- социальные сети;
- информационные рассылки разработчика программного обеспечения;
- информационные рассылки регуляторов в области информационной безопасности.

Источник, не входящий в какую-то из групп, – база данных уязвимостей, содержащаяся в Банке данных угроз безопасности информации ФСТЭК России.

Мониторинг уязвимостей – процесс непрерывного наблюдения за состоянием информационной системы с намерением выявить потенциальный недостаток. Он включает в себя сканирование системы с целью выявления слабых мест, которые могут быть использованы злоумышленниками.

На этом этапе выполняются последовательно несколько операций. Схема процесса представлена на рис. 2.

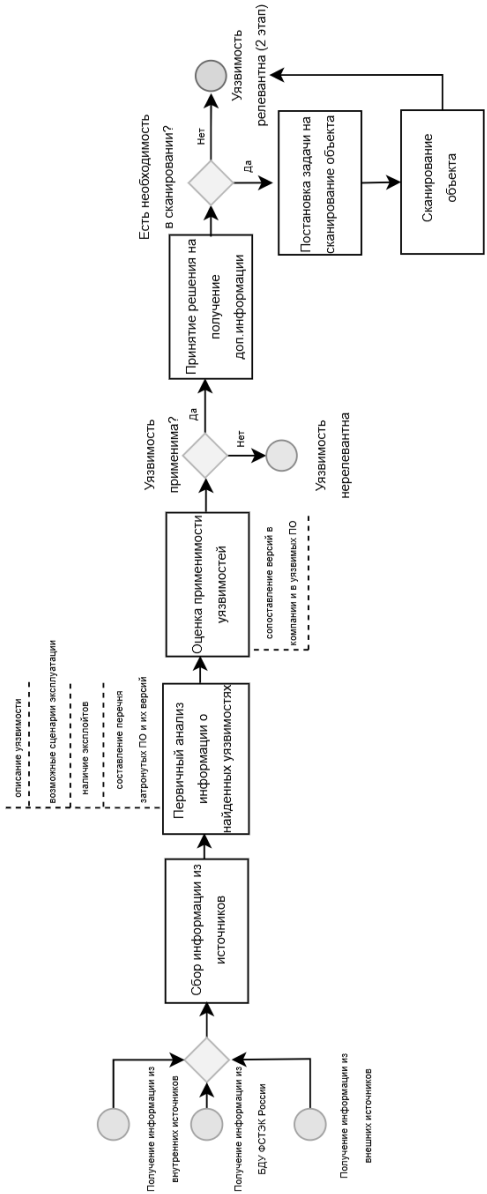

Рис. 2. Схема этапа мониторинга уязвимостей и сбора информации

Fig. 2. Vulnerability monitoring and information collection stage diagram

Рассмотрим каждую операцию подробнее.

Сбор информации из источников

К первой операции этапа относится сбор информации из источников: мониторинг данных из специализированных ресурсов, таких как базы данных уязвимостей, рассылки вендоров, отчеты сканеров и все остальные источники, которые были указаны ранее. Рекомендуется систематизировать процесс сверки внутренних баз уязвимостей с информацией из профессиональных ресурсов и при обнаружении несоответствий вносить корректировки в корпоративную базу.

Первичный анализ информации о найденных уязвимостях

Важным компонентом данного этапа является первичный анализ данных об обнаруженных уязвимостей. Его цель – быстро оценить, насколько критична уязвимость и стоит ли тратить ресурсы на ее более детальную проверку.

В ходе анализа необходимо проверить общую информацию об уязвимости:

- описание уязвимости;
- возможные сценарии эксплуатации;
- наличие эксплойтов.

На основе собранной информации необходимо составить перечень уязвимого ПО с указанием затронутых версий. В список включаются как критичные, так и менее важные уязвимости, которые могут повлиять на функционирование систем. Для каждой уязвимости следует указать точные версии ПО, так как патчи могут касаться не всех версий. Этот перечень позволяет выявить риски и приоритизировать задачи по обновлению.

Оценка применимости уязвимостей

После первичного анализа необходимо провести оценку применимости уязвимости в компании. Для этого нужно проверить, используются ли в организации версии программного обеспечения, содержащие выявленные недостатки. Кроме версии ПО, важно также учитывать, может ли уязвимость быть связана с конкретной конфигурацией системы.

При подтверждении факта эксплуатации уязвимости определяется перечень затрагиваемых информационных систем, сервисов/бизнесов, в которых применяется найденная уязвимость и производится экспертная оценка возможности использования в этих информационных системах.

Принятие решения на получение дополнительной информации

В рамках этого этапа может приниматься решение о необходимости получения дополнительной информации. При сомнениях в актуальности данных о программном обеспечении или обнаружении новых уязвимостей после последней проверки создается запрос для проведения внепланового обследование системы.

Постановка задачи на сканирование объектов

Является необязательной операцией этапа, потому что не всегда есть необходимость ручного планирования сканирования объектов. Для того чтобы провести незапланированное сканирование, необходимо создать заявку для согласования с владельцем системы или объекта сканирования. В ней следует указать цель проверки, перечень затрагиваемых систем и предполагаемые методы обследования. Кроме того, важно определить временные рамки проведения анализа, чтобы минимизировать возможное влияние на работу инфраструктуры.

Сканирование объектов

После получения задачи на сканирование объекта специалист ИБ проводит проверку объекта на наличие уязвимостей и недостатков конфигурации с помощью автоматизированных систем анализа защищенности.

Те уязвимости, которые после проведенного анализа оказались релевантными для компании, переходят на следующий этап процесса VM.

4.2. ОЦЕНКА УЯЗВИМОСТЕЙ

На этом этапе можно определить реальный уровень риска каждой обнаруженной уязвимости, оценить ее потенциальное воздействие на бизнес-процессы и выработать стратегию по ее устранению.

Оценка уязвимостей включает в себя несколько аспектов, представленных на рис. 3.

Рассмотрим каждую операцию подробнее.

Классификация выявленных уязвимостей

Разберем первый аспект – классификацию уязвимостей. Это процесс категоризации выявленных недостатков по различным критериям, что в дальнейшем помогает в анализе, приоритизации и устранении.

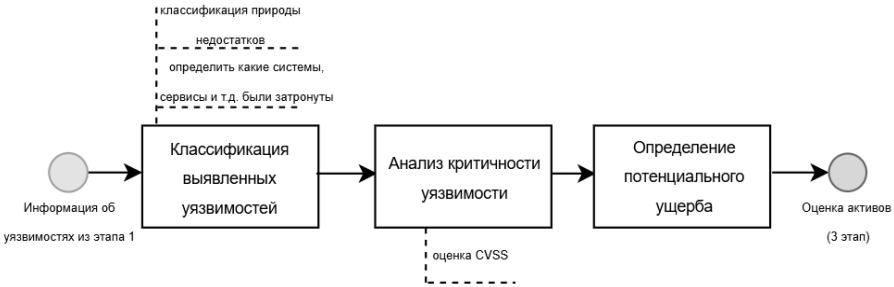

Рис. 3. Схема этапа оценки уязвимостей

Fig. 3. Vulnerability assessment stage diagram

Необходимо классифицировать природу недостатков системы, определяя, связаны ли они с ПО, с конфигурацией системы, сетевыми настройками или человеческим фактором. Такой подход помогает структурировать данные и эффективно распределять ресурсы на устранение наиболее критичных проблем.

Далее необходимо определить, какие системы, сервисы, приложения или компоненты инфраструктуры могут быть подвержены найденными уязвимостями. Это позволяет сфокусировать усилия на критичных элементах.

Анализ критичности уязвимостей

После того как была осуществлена привязка уязвимостей к определенным компонентам инфраструктуры, важно оценить, какое воздействие они могут оказать на эти компоненты. Такая оценка помогает понять, насколько серьезными могут быть последствия эксплуатации уязвимости и какие шаги необходимо предпринять для минимизации рисков.

Системы управления уязвимостями предоставляют различные рейтинги риска и оценки, такие как CVSS, которые помогают определить приоритеты устранения уязвимостей. Однако реальный уровень риска зависит не только от этих стандартных оценок, но и от ряда дополнительных факторов. К ним относятся следующие.

- Является ли уязвимость реальной или ложным срабатыванием?
- Доступна ли она напрямую из Интернета?
- Насколько сложно ее эксплуатировать?

- Существует ли публичный эксплойт для этой уязвимости?
- Каковы потенциальные последствия для бизнеса при ее эксплуатации?
- Есть ли дополнительные меры безопасности, снижающие вероятность или влияние атаки?
- Как давно обнаружена уязвимость и сколько времени она остается нерешенной [5]?

CVSS включает три основные группы метрик:

- базовая оценка;
- временная оценка;
- контекстная оценка.

При анализе базовых показателей следует учитывать, что потенциальный злоумышленник хорошо осведомлен о слабых местах целевой системы, включая ее конфигурацию и встроенные механизмы защиты. Например, если эксплуатация уязвимости приводит к стабильному и предсказуемому успеху, это по-прежнему указывает на низкую сложность атаки, независимо от уровня подготовки атакующего.

Определение потенциального ущерба

На этапе оценки уязвимостей важно не только определить их наличие и вероятность эксплуатации, но и оценить возможные последствия их использования злоумышленниками. Потенциальный ущерб от уязвимостей может проявляться в разных формах, затрагивая финансовые, репутационные, юридические сферы деятельности.

4.3. ОЦЕНКА АКТИВОВ

Этот этап был добавлен на основе сравнительного анализа двух документов: ФСТЭК и NIST.

Часто приоритизация уязвимостей опирается только на CVSS-оценки, но такой подход не всегда эффективен. Уязвимости с высоким баллом не всегда опасны для бизнеса.

Эффективная приоритизация требует оценки критичности активов, на которых обнаружены уязвимости. Это позволяет сфокусироваться на значимых рисках и повысить защищенность организации [6].

Этап «Оценка активов» можно разделить на несколько операций, представленных на рис. 4.

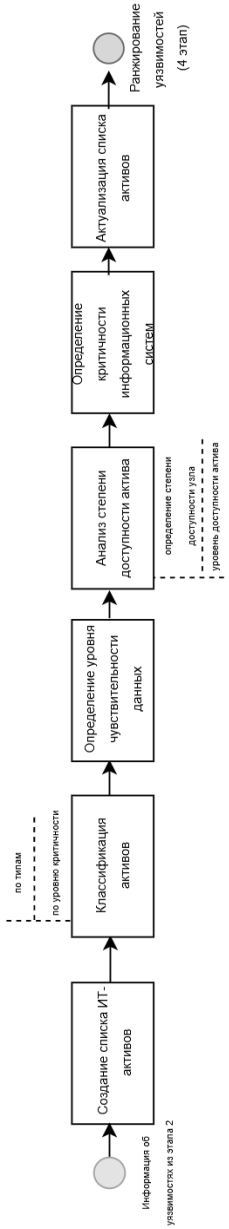

Рис. 4. Схема этапа оценки активов

Fig. 4. Asset valuation stage diagram

Рассмотрим каждую операцию подробнее.

Создание списка IT-активов

Для начала необходимо провести идентификацию активов. Цель этого процесса – сформировать полный и актуальный перечень всех IT-активов, что позволит в дальнейшем оценивать их критичность, выявлять уязвимости и управлять рисками.

Классификация активов

После определения всех активов необходимо провести их категоризацию по нескольким признакам. Это необходимо для определения значимости каждого актива, дальнейшей оценки критичности. Признаки классификации:

- по типам;
- по уровню критичности.

Разделение активов по степени важности позволяет эффективно распределять ресурсы для защиты наиболее значимых объектов.

Также необходимо, чтобы у каждого актива был владелец и ответственный за обслуживание.

Определение уровня чувствительности данных

Все активы обрабатывают определенные данные. Важно установить их уровень чувствительности.

Анализ степени доступности актива

В рамках этапа «Оценка активов» необходимо не только идентифицировать и классифицировать активы, но и проанализировать их доступность для потенциальных злоумышленников. Доступность узла, на котором обнаружена уязвимость, является важным фактором при определении уровня риска.

Определение степени доступности узла. При анализе доступности актива необходимо ответить на несколько ключевых вопросов.

- Может ли внешний злоумышленник получить доступ к узлу без предварительного проникновения в сеть?
- Требуются ли для эксплуатации уязвимости особые привилегии (например, права администратора)?
- Возможно ли использование уязвимости удаленно, или она требует локального присутствия внутри корпоративной сети?

Уровень доступности активов. На основе ответов на эти вопросы можно выделить несколько уровней доступности активов:

- общедоступные узлы (внешние ресурсы);
- граничные системы (размещенные в DMZ);
- внутренние системы (ЛВС, защищенные сегменты).

Приоритизация уязвимостей по доступности активов. После определения уровня доступности узлов важно правильно расставить приоритеты устранения уязвимостей:

- высший приоритет – уязвимости в общедоступных и граничных системах;
- средний приоритет – уязвимости во внутренних системах, если нет признаков компрометации;
- низкий приоритет – уязвимости в изолированных средах, если не предусмотрены сценарии атак с физическим доступом [6].

Определение критичности информационных систем

Дальше нужно определить критичность информационных систем. Она определяется на основе их назначения, сетевого размещения и роли в бизнес-процессах, а также важности данных, которые они обрабатывают, и последствий для компании при их недоступности или компрометации.

Актуализация списка активов

В рамках оценки активами важно понимать, что инфраструктура компании постоянно изменяется: появляются новые системы, изменяется конфигурация существующих, выводятся из эксплуатации устаревшие ресурсы. Без регулярного обновления данных об активах невозможно эффективно управлять уязвимостями и оценивать риски.

Без своевременного обновления данных о ресурсах возможны следующие риски:

- отсутствие контроля над новыми активами;
- забытые и неконтролируемые системы;
- неточность в приоритизации уязвимостей.

4.4. РАНЖИРОВАНИЕ УЯЗВИМОСТЕЙ

Как говорилось ранее, стандартная оценка CVSS не дает полной картины критичности уязвимости и не позволяет правильно определить порядок ее устранения. Причина в том, что каждая компания имеет уникальную IT-инфраструктуру, критически важные сервисы и бизнес-процессы [7].

Схема данного этапа представлена на рис. 5.

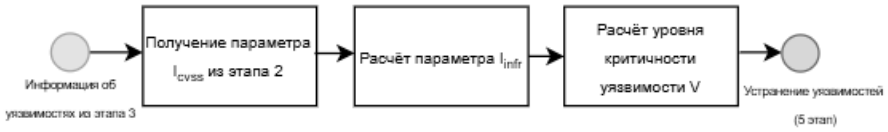

Рис. 5. Схема этапа ранжирования уязвимостей

Fig. 5. Vulnerability ranking stage diagram

Воспользуемся формулой (1) для определения уровня критичности уязвимости (V), которая приведена в методическом документе ФСТЭК «Методика оценки уровня критичности уязвимостей программных, программно-аппаратных средств». Она имеет следующий вид:

$$V = I_{\text{CVSS}} I_i, \tag{1}$$

где I_{CVSS} – показатель опасности уязвимости, рассчитанный в соответствии с методикой CVSS 3.1; I_i – показатель, отражающий степень воздействия уязвимости программных, программно-аппаратных средств на функционирование ИС.

Параметр I_{CVSS} определяется на этапе «Оценка уязвимостей». Показатель I_{infr} рассчитывается по формуле

$$I_i = kK + lL + pP, \tag{2}$$

где K – показатель, характеризующий тип компонента ИС, подверженного уязвимости; L – показатель, учитывающий масштаб распространения уязвимости в системе; P – показатель, характеризующий влияние уязвимого компонента на защищенность периметра ИС; k, l, p – весовые коэффициенты, присваиваемые каждому параметру. Веса данных параметров можно посмотреть в методике ФСТЭК.

На основе результатов расчета уровень критичности уязвимости определяется в соответствии со значениями, приведенными в таблице.

Результаты расчета уровня критичности уязвимости

The results of calculating the vulnerability criticality level

Суммарное количество баллов уязвимости	Оценка уровня критичности уязвимости
$7{,}0 \le V \le 10{,}0$	Критичный
$4{,}5 \le V \le 7{,}0$	Высокий
$1{,}5 \le V \le 4{,}5$	Средний
$V < 1{,}5$	Низкий

Этот метод ранжирования уязвимостей дополняет оценку CVSS, так как помогает решить ее главный недостаток – учитывает, насколько конкретная уязвимость критична для инфраструктуры. Этот подход позволяет лучше понимать, какие риски критичны для бизнеса.

4.5. УСТРАНЕНИЕ УЯЗВИМОСТЕЙ

На данном этапе принимаются меры, направленные на устранение или исключение возможности использования уязвимостей.

Он включает в себя следующие операции, которые продемонстрированы на рис. 6.

Рассмотрим каждую операцию подробнее.

Определение методов устранения уязвимостей или компенсирующих мер, а также лиц, ответственных за их реализацию

В зависимости от вектора эксплуатации уязвимости, ее релевантности и приоритета устранения выбираются следующие варианты закрытия уязвимости:

- уязвимость закрыта;
- применение компенсирующих мер;
- уязвимость принята.

Методы устранения уязвимостей могут варьироваться в зависимости от типа уязвимостей, специфики системы и доступных ресурсов.

Установка патчей и обновлений – это один из ключевых методов. Патчи и обновления представляют собой исправления, разработанные вендорами для устранения уязвимостей в ПО.

После идентификации уязвимости необходимо проверить, доступен ли патч от производителя. Но перед его установкой нужно проанализировать совместимость с текущей версией ПО, так как есть риск того, что после установки патча он может вызвать проблемы в других системах [8].

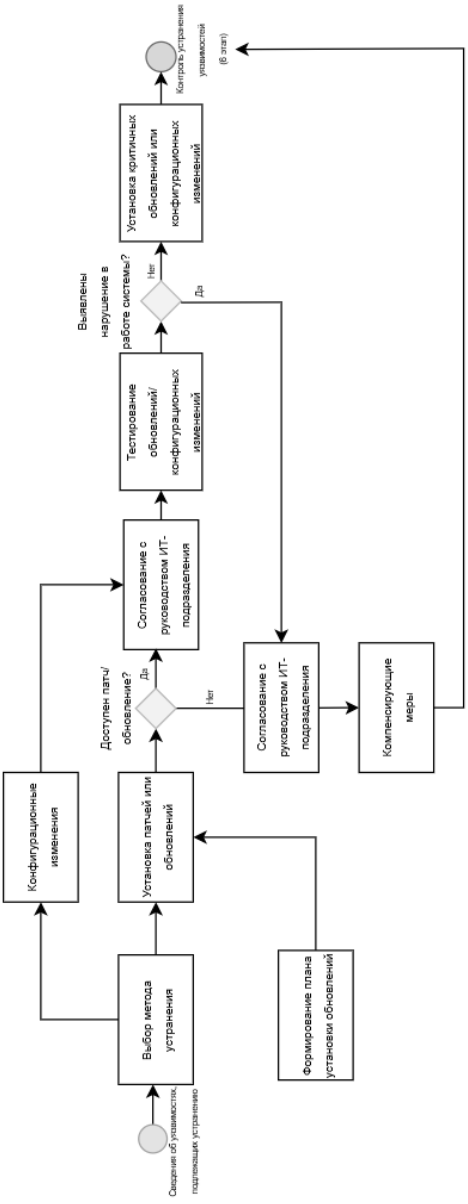

Рис. 6. Схема этапа устранения уязвимостей

Fig. 6. Vulnerability elimination stage diagram

Конфигурационные изменения. Этот способ устранения заключается в изменении настроек системы или приложений для повышения уровня безопасности и снижения вероятности эксплуатации уязвимостей. Такие изменения могут быть как временной мерой до выхода патча, так и полноценным решением [2].

Важный момент заключается в том, что любые конфигурационные изменения должны быть задокументированы и протестированы. Некорректная настройка может привести к нарушению работы сервисов или снижению доступности систем.

Компенсирующие меры. Когда патчи еще не доступны или стало известно, что они могут вызвать проблемы в системе, необходимо применить компенсирующие меры устранения, для того чтобы снизить риски до выхода патча. Они позволяют ограничить доступ злоумышленникам к уязвимым компонентам. Вот некоторые примеры:

- использование Firewall;
- изоляция уязвимых компонентов или сервисов;
- ограничение прав доступа;
- сегментация сети;
- WAF;
- другие компенсирующие меры.

Принятие уязвимости. В рамках этого процесса организация может принять решение не устранять ту или иную уязвимость. Причиной может стать то, что затраты на устранение превосходят последствия эксплуатации. Также уязвимость может быть признана незначительной, если ее использование маловероятно или она не представляет серьезной угрозы для безопасности.

Следует регламентировать время устранения уязвимости в зависимости от критичности:

- критический уровень опасности – до 24 часов;
- высокий уровень опасности – до 5 дней;
- средний уровень опасности – до 3 недель;
- низкий уровень опасности – до 4 месяцев.

Согласование любых изменений с руководством подразделения IT

Необходимо согласовать установку обновлений, конфигурационные изменения или реализацию компенсирующих мер с руководством подразделения IT. Этот шаг важен для оценки рисков, связанных с изменениями, и их потенциального воздействия на инфраструктуру; для принятия решения

о том, как и когда будет выполнены изменения; для утверждения временных рамок и ресурсного обеспечения при выполнении операций.

Тестирование обновлений / конфигурационных изменений

Для проверки нужно протестировать патч или конфигурационные изменения в специальных средах, так называемых «песочницах». Тестирование осуществляется для обнаружения потенциально опасных функций, которые могли быть внедрены без официального указания разработчика [9]. Проверке подлежат обновления безопасности, направленные на устранения уязвимостей, уровень критичности которых определен в соответствии с этапом «Ранжирование уязвимостей».

Установка критичных обновлений

Если в системе обнаруживается серьезная уязвимость, то сотрудники IT-подразделения вынуждены экстренно обновлять уязвимое ПО на всех затронутых компонентах инфраструктуры.

Формирование плана установки обновлений

После успешного тестирования необходимо сформировать план установки обновлений. Необходимо определить очередь размещения их в систему. План создается для того, чтобы минимизировать риски и время простоя в условиях зависимости. Уязвимости, для которых не установлена необходимость срочного размещения обновлений, устраняются в процессе планового обновления системы.

Установка плановых обновлений

В отличие от экстренного патчинга, плановое обновление происходит по графику, сформированному на предыдущей операции. Это часть процесса, направленного не на реакцию на конкретный инцидент, а на предотвращение ранее выявленных уязвимостей.

4.6. КОНТРОЛЬ УСТРАНЕНИЯ УЯЗВИМОСТЕЙ

Этот этап включает проверку устранения уязвимостей или подтверждения внедрения компенсирующих мер, снижающих риск до приемлемого уровня, соблюдение установленных сроков, дальнейший мониторинг состояния инфраструктуры для выявления новых уязвимостей. Кроме того, на этом этапе

проводится анализ причин отклонений и неисполнений заявок на устранение уязвимостей. После получения результатов последующих сканирований можно оценить количественные показатели уязвимостей: сколько из них было устранено, сколько обнаружено новых и какие остались неустраненными.

Процесс контроля устранения уязвимостей состоит из следующих операций (рис. 7).

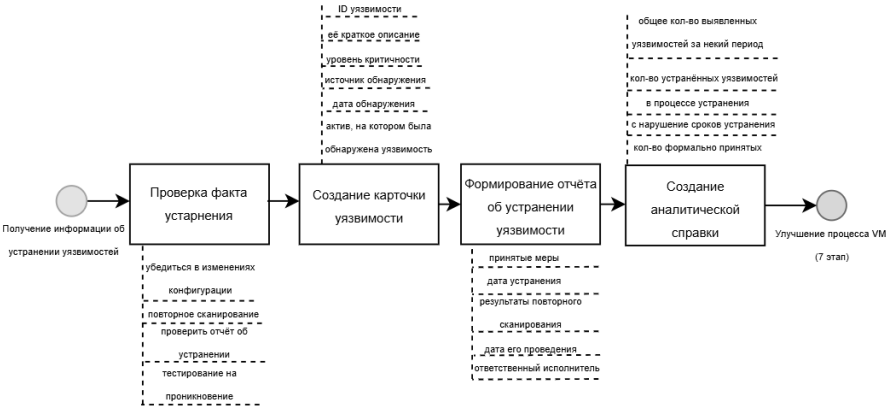

Рис. 7. Схема этапа контроля устранения уязвимостей

Fig. 7. The scheme of the vulnerability elimination control stage

Рассмотрим каждую операцию подробнее

Получение информации об устранении уязвимостей

Для начала IT-специалисты должны проинформировать специалистов ИБ о том, что меры для устранения уязвимостей были применены. Для этого нужно направить отчет. Это можно сделать либо с помощью инструментов, где заводилась задача на устранение, или в виде документов. В отчете нужно указать, кем, когда и каким образом была устранена уязвимость.

Проверка факта устранения

После предоставления информации специалисты подразделения информационной безопасности должны проконтролировать факт устранения уязвимостей. NIST предлагает несколько способов контроля устранения уязвимостей, а именно:

- необходимо убедиться, что файлы или параметры конфигурации, отправленные на исправление, были изменены, как указано в документации поставщика и/или в бюллетенях;
- еще раз просканировать хост с помощью сканера уязвимостей, который способен обнаруживать известные уязвимости;
- проверить, правильно ли были установлены рекомендованные исправления;
- использовать процедуры эксплойта или код и попробовать проэксплуатировать уязвимость (т. е. выполнить тест на проникновение).

В данной операции важно убедиться, что устранение было выполнено в установленные сроки.

Создание карточки уязвимости

После того как специалист по ИБ убедился в том, что уязвимости были устранены, следует составить карточку уязвимости. Она должна включать:

- идентификатор уязвимости;
- ее краткое описание;
- уровень критичности;
- источник обнаружения;
- дата обнаружения;
- актив, на котором была обнаружена уязвимость.

Формирование отчета об устранении уязвимости

Также следует сформировать отчет об устранении, который должен включать следующую информацию:

- принятые меры по устранению;
- дату устранения;
- результаты повторного сканирования и дату его проведения;
- ответственного исполнителя.

Можно включить подтверждающие документы: скриншоты, отчеты сканера, логи и т. п.

Создание аналитической справки

Финальной операцией данного этапа является формирование аналитической справки, в которой специалист по ИБ указывает статусы устранения уязвимостей. Она должна включать следующие сведения:

- общее количество выявленных уязвимостей за некий период;

- количество устраненных уязвимостей;
- количество уязвимостей, находящихся в процессе устранения;
- количество уязвимостей с нарушением сроков устранения;
- количество формально принятых уязвимостей.

Таким образом, этап «Контроль устранения уязвимостей» позволяет не только убедиться, что уязвимости были устранены, но и зафиксировать все действия и результаты для дальнейшего анализа, что поможет на следующем этапе.

4.7. УЛУЧШЕНИЕ ПРОЦЕССА УПРАВЛЕНИЯ УЯЗВИМОСТЯМИ

Этот этап является заключительным в рамках процесса управления уязвимостями, но очень важной составляющей. Он направлен на устранение слабых мест, повышение качества выявления и обработки уязвимостей, а также развитие компетенций участников процесса.

Этап состоит из нескольких операций, которые продемонстрированы на рис. 8.

Рис. 8. Схема этапа улучшения процесса управления уязвимостями

Fig. 8. The scheme of the stage of improvement of the vulnerability management process

Рассмотрим каждую операцию подробнее.

Анализ причин невыявления уязвимостей

Эта операция позволяет понять, почему конкретные уязвимости не были обнаружены своевременно, и предотвратить подобные ситуации в будущем.

Сначала следует проверить, входит ли затронутая система в зону охвата сканирования, была ли она доступна во время проведения анализа. Также важно убедиться, что настройки сканеров были корректны. Например, использовались ли актуальные политики и не были ли отключены важные модули.

Кроме того, стоит проанализировать актуальность перечня активов в компании, так как недостаток информации или некорректное описание ресурсов может привести к неохваченным зонам при сканировании.

Иногда уязвимость могла быть проигнорирована из-за неправильно настроенных фильтров, ограничений на нагрузку или исключений, добавленных вручную.

Результаты анализа фиксируются, чтобы на их основе можно было обновить процедуры, внести изменения в настройки инструментов и провести обучение [10].

Обновление документации

Обновление документации позволяет обеспечить актуальность процессов и повысить прозрачность действий для всех участников. По результатам необнаруженных или повторно возникающих уязвимостей необходимо вносить изменения в регламенты, инструкции и политики, чтобы устранить системные причины.

Обучение и повышение осведомленности сотрудников

Эта операция является неотъемлемой частью процесса VM, поскольку человеческий фактор часто играет решающую роль в успешности предотвращения угроз. Обучение должно быть направлено не только на участников процесса, но и на всех сотрудников компании.

Важно сказать, что этот этап позволяет организациям устранять не только уязвимости, но и причины их появления и недочеты в процессе.

ЗАКЛЮЧЕНИЕ

В ходе исследования был выстроен комплексный подход к организации процесса управления уязвимостями. Он охватывает ключевые этапы – от выявления и анализа уязвимостей до их устранения и последующего контроля эффективности принимаемых мер. Предложенная модель учитывает специфику бизнес-процессов и особенности IT-инфраструктуры.

Практическая значимость представленного решения заключается в его применимости для повышения уровня информационной безопасности организаций финансового сектора. Внедрение разработанного процесса позволяет сократить время реагирования на выявленные угрозы от момента обнаружения уязвимости до постановки задачи на ее устранение.

Таким образом, построение эффективной системы управления уязвимостями требует комплексного подхода, сочетающего технические инструменты, организационные меры и систематическую работу с персоналом. Только при условии сбалансированного взаимодействия этих компонентов возможно минимизировать риски и обеспечить надежную защиту информационных систем. Важно, чтобы организации постоянно адаптировались к изменениям в области кибербезопасности с внедрением новых технологий и методов, а также с учетом лучших практик отрасли.

СПИСОК ЛИТЕРАТУРЫ

1. *Трубина М.Е.* Организация процесса управления уязвимостями // Безопасность информационного пространства: сборник трудов XXII Всероссийской научно-практической конференции студентов, аспирантов и молодых ученых, 30 ноября 2023 года. – Челябинск, 2024 – С. 57–60.

2. CRR Supplemental Resource Guide: Vulnerability Management // CISA. – Washington, D.C., 2016. – 36 p.

3. R-Vision. Управление уязвимостями: ключевые проблемы и практические советы. – URL: https://www.rvision.ru/blog-posts/upravlenie-uyazvimostyami-klyuchevye-problemy-i-prakticheskie-sovety (дата обращения: 11.06.2025).

4. Реализация процедуры мониторинга в ходе процесса управления уязвимостями / С.Ю. Силимгереев, Д.В. Сенин, Т.В. Минкина, В.Е. Рачков // Инновационные тренды и драйверы устойчивого развития социально-экономических процессов в условиях перехода к цифровому обществу: сборник научных статей по материалам Международной научно-практической конференции, Ставрополь, 16–17 октября 2023 года. – Ставрополь: Изд-во СГАУ, 2023. – С. 669–674.

5. Softprom. Управление уязвимостями: часто задаваемые вопросы. – URL: https://softprom.com/ru/Vulnerability-Management-FAQ (дата обращения: 16.06.2025).

6. Менеджмент уязвимостей: инструкция по применению. – Positive Technologies, 2022. – URL: https://pt-corp.storage.yandexcloud.net/upload/corporate/ru-ru/analytics/Vulnerability-management-instructions-for-use_RUS.pdf (дата обращения: 16.06.2025).

7. *Ременчик В.* О приоритизации устранения уязвимостей. – 2024. – URL: https://mte-cyber.by/mte-blog/o-prioritizaczii-ustraneniya-uyazvimostej/ (дата обращения: 16.06.2025).

8. *Скоробогатов Р.Г.* Идентификация уязвимостей, анализ рисков, разработка рекомендаций по устранению уязвимостей и обеспечению безопасности активов организации // Современные наука и образование: достижения и перспективы развития: сборник материалов XXX международной очно-заочной научно-практической конференции: в 4 т. – М.: Империя, 2023. – Т. 3. – С. 126–128.

9. Методика тестирования обновлений безопасности программных, программно-аппаратных средств: методический документ ФСТЭК России от 28 октября 2022 г. – URL: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-28-oktyabrya-2022-g (дата обращения: 16.06.2025).

10. Социальная инженерия: современные подходы и примеры атак. – URL: https://www.securitylab.ru/analytics/515888.php (дата обращения: 15.04.2025).

Грищенко Лев Аркадьевич, старший инженер анализа защищенности АО «ЦФТ». Основное направление научных исследований – информационная безопасность. E-mail: l.grishhenko@corp.nstu.ru

Левицкая Вероника Андреевна, лаборант кафедры защиты информации Новосибирского государственного технического университета. Основное направление научных исследований – информационная безопасность. E-mail: leviczkaya.2020@stud.nstu.ru

DOI: 10.17212/2782-2230-2025-2-76-102

Organization of the vulnerability management process of financial sector companies*

L.A. Grishchenko[1], V.A. Levitskaya[2]

[1] *Joint-Stock Company "Financial Technologies Center", 2 Shaturskaya Street, Novosibirsk, 630055, Russian Federation, senior security analysis engineer. E-mail: l.grishhenko@corp.nstu.ru*
[2] *Novosibirsk State Technical University, 20 Karl Marx Avenue, Novosibirsk, 630073, Russian Federation, laboratory assistant of the Department of Information Security. E-mail: leviczkaya.2020@stud.nstu.ru*

The article analyzes methodological documents related to vulnerability management, both domestic and foreign. The purpose of the analysis is to identify the strengths and weaknesses of each methodology and develop a comprehensive solution that combines best practices from different approaches. This solution is aimed at creating a comprehensive and effective vulnerability management program that meets modern threats and security requirements.

Keywords: vulnerabilities, vulnerability management process, fintech company, IT infrastructure, exploits, IT assets, vulnerability scanning, patches

REFERENCES

1. Trubina M.E. [Organization of the vulnerability management process]. *Bezopasnost' informatsionnogo prostranstva* [Security of information space]. Proceedings of the XXII All-Russian scientific and practical conference of students, postgraduates and young scientists. Chelyabinsk, 2024, pp. 57–60. (In Russian).

2. CRR Supplemental Resource Guide: Vulnerability Management. *CISA*. Washington, D.C., 2016. 36 p.

3. R-Vision. *Upravlenie uyazvimostyami: klyuchevye problemy i prakticheskie sovety* [Vulnerability management: key issues and practical tips]. Available at: https://www.rvision.ru/blog-posts/upravlenie-uyazvimostyami-klyuchevye-problemy-i-prakticheskie-sovety (accessed 11.06.2025).

* *Received 16 May 2025.*

4. Silimgereev S.Yu., Senin D.V., Minkina T.V., Rachkov V.E. [Realization of the monitoring procedure during the vulnerability management process]. *Innovatsionnye trendy i draivery ustoichivogo razvitiya sotsial'no-ekonomicheskikh protsessov v usloviyakh perekhoda k tsifrovomu obshchestvu* [Innovative trends and drivers of sustainable development of socio-economic processes in the context of transition to a digital society]. Collection of scientific articles on the materials of the International scientific-practical conference, Stavropol, 2023, pp. 669–674. (In Russian).

5. Softprom. *Upravlenie uyazvimostyami: chasto zadavaemye voprosy* [Vulnerability Management: frequently asked questions]. (In Russian). Available at: https://softprom.com/ru/Vulnerability-Management-FAQ (accessed 16.06.2025).

6. *Menedzhment uyazvimostei: instruktsiya po primeneniyu* [Instructions on vulnerability management]. Positive Technologies, 2022. (In Russian). Available at: https://pt-corp.storage.yandexcloud.net/upload/corporate/ru-ru/analytics/Vulnerability-management-instructions-for-use_RUS.pdf (accessed 16.06.2025).

7. Remenchik V. *O prioritizatsii ustraneniya uyazvimostei* [On the prioritization of vulnerability remediation]. Available at: https://mte-cyber.by/mte-blog/o-prioritizaczii-ustraneniya-uyazvimostej/ (accessed 16.06.2025).

8. Skorobogatov R.G. [Identification of vulnerabilities, risk analysis, development of recommendations to eliminate vulnerabilities and ensure the safety of the organization's assets]. *Sovremennye nauka i obrazovanie: dostizheniya i perspektivy razvitiya* [Modern science and education: achievements and prospects of development]. Proceedings of the XXXth International scientific-practical conference. Moscow, Imperiya Publ., 2023, pp. 126–128. (In Russian).

9. FSTEC of Russia Methodological document, October 28, 2022 “Methodology for testing security updates of software, software and hardware”. (In Russian). Available at: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-28-oktyabrya-2022-g (accessed 16.06.2025).

10. *Sotsial'naya inzheneriya: sovremennye podkhody i primery atak* [Social engineering: modern approaches and examples of attacks]. (In Russian). Available at: https://www.securitylab.ru/analytics/515888.php (accessed 15.04.2025).

Для цитирования:

Грищенко Л.А., *Левицкая В.А.* Организация процесса управления уязвимостями предприятий финансового сектора // Безопасность цифровых технологий. – 2025. – № 2 (117). – С. 76–102. – DOI: 10.17212/2782-2230-2025-2-76-102.

For citation:

Grishchenko L.A., Levitskaya V.A. Organizatsiya protsessa upravleniya uyazvimostyami predpriyatiy finansovogo sektora [Organization of the vulnerability management process of financial sector companies]. *Bezopasnost' tsifrovykh tekhnologii = Digital Technology Security*, 2025, no. 2 (117), pp. 76–102. DOI: 10.17212/2782-2230-2025-2-76-102.