БЕЗОПАСНОСТЬ ЦИФРОВЫХ ТЕХНОЛОГИЙ. – 2024. – № 4 (115). – 25–36

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 004.056.5 DOI: 10.17212/2782-2230-2024-4-25-36

РАЗРАБОТКА РЕКОМЕНДАЦИЙ ПО ЗАЩИТЕ ИНФОРМАЦИИ ОТ ЭКСПЛУАТАЦИИ АКТУАЛЬНЫХ УЯЗВИМОСТЕЙ 2024 ГОДА*

С.С. ЖУМАЖАНОВА[1], Н.В. ЗУБОВИЧ[2], Д.Е. ОБРЫВАЛИН[3]

[1] *644050, РФ, г. Омск, Проспект Мира, 11, ФГБОУ ВО «Омский государственный технический университет», канд. техн. наук, доцент кафедры «Комплексная защита информации». E-mail: samal_shumashanova@mail.ru*
[2] *644050, РФ, г. Омск, Проспект Мира, 11, ФГБОУ ВО «Омский государственный технический университет», лаборант кафедры «Комплексная защита информации». E-mail: ankerov.n@mail.ru*
[3] *644050, РФ, г. Омск, Проспект Мира, 11, ФГБОУ ВО «Омский государственный технический университет», лаборант кафедры «Комплексная защита информации». E-mail: dimawork3270@gmail.com*

Угрозы информационной безопасности являются одной из наиболее важных проблем современности. Под угрозой в общем смысле понимается потенциально возможное событие, действие (воздействие), процесс или явление, которые могут привести к нанесению ущерба чьим-либо интересам. Существует множество способов реализации угроз ИБ, но одним из основных является эксплуатация уязвимостей ИБ. Согласно недавнему отчету компании Positive Technologies [1], в 2023 году эксплуатация уязвимостей стала одним из основных методов атаки на организации (32 %). Уязвимости эксплуатируются в соответствии с некоторым сценарием проведения атаки, который условно делится на следующие этапы: проведение разведки, проведение атаки, развитие атаки на информационную систему, получение выгоды. Таким образом, настоящая работа посвящена анализу ряда уязвимостей ИБ в 2024 году, моделированию сценариев атак при эксплуатации данных уязвимостей и составлению рекомендаций по устранению возможности эксплуатации уязвимостей на базе организационно-технических мер.

Ключевые слова: информационная безопасность, уязвимости, эксплойт, эксплуатация уязвимости, защита информации, сценарий атаки, меры защиты, системы оценки уязвимостей информационной безопасности

* Статья получена 12 ноября 2024 г.

ВВЕДЕНИЕ

Цифровые технологии в современное время распространились не только на повседневную жизнь людей, но и на крупные отрасли промышленности и многие коммерческие предприятия. Таким образом, угрозы и уязвимости ИБ представляют собой реальную опасность. Уязвимость информационной безопасности – это недоработка или брешь, обнаруженная в компонентах какого-либо продукта или услуги, которая может быть использована с целью намеренно нарушить целостность данных и негативно повлиять на функциональность компонентов продукта или услуги даже при правильной конфигурации. Уязвимость сама по себе – просто характеристика состояния системы, реальные последствия наступают только после ее эксплуатации.

В настоящий момент существует несколько крупных систем оценок и каталогизации уязвимостей, таких как CVE, OWASP, ФСТЭК и др.

Наиболее распространенные уязвимости были собраны в базе данных CVE (Common Vulnerabilities and Exposures) [2]. CVE – это список стандартных идентификаторов для общеизвестных уязвимостей информационной безопасности, созданный с целью объединения различных баз данных уязвимостей и унификации их описания. Каждая отдельная уязвимость в этой базе данных имеет свой идентификационный номер, краткое описание, а также соответствующие ссылки на отчеты об этой уязвимости или рекомендации по ее устранению. Для оценки уязвимостей в CVE используется открытый стандарт – CVSS (Common Vulnerability Scoring System), разработанный для расчета количественных оценок уязвимости в безопасности компьютерной системы. В последней, четвертой, версии стандарта была введена новая группа метрик угроз, предоставлены более подробные определения векторов атак и обновлены метрики взаимодействия с пользователем. Это обеспечивает более простую, адаптивную и точную систему оценки, более точное описание потенциальных опасностей, улучшенное описание реальных рисков, повышенную гибкость и адаптивность, а также улучшенную ясность и простоту [3]. В CVSS для расчета критичности уязвимости рекомендуется опираться не только на базовые метрики, но именно они в конечном итоге учитываются в таких источниках, как NVD [4], где можно найти ссылки на рекомендации по безопасности, способы исправления уязвимостей, которые, как правило, включают обновление ресурса до безопасной версии. Однако предлагаемых решений по предотвращению ущерба, устранению уязвимостей или противодействию их эксплуатации бывает недостаточно, в то же время организации борются с неразрешенными уязвимостями, число которых растет изо дня в день экспоненциально.

Таким образом, настоящая работа посвящена разбору ряда неразрешенных уязвимостей, а также уязвимостей, для устранения которых разработчик предлагает лишь установить обновленную версию ресурса с целью оценки их критичности согласно CVSS 4.0, для построения возможных сценариев эксплуатации уязвимостей, а также организационно-технических методов нейтрализации сопутствующих угроз ИБ.

1. ВЫБОР И ОЦЕНКА УЯЗВИМОСТЕЙ

Оценка уязвимости по стандарту CSVV 4.0 включает в себя описание следующих составляющих.

1. *Базовые*

- Вектор атаки (AV) – сценарий эксплуатации уязвимости злоумышленником.
- Сложность атаки (AC) – степень сложности эксплуатации уязвимости злоумышленником при обходе существующих мер защиты.
- Требования к атаке (AT) – определенные условия или характеристики уязвимой системы, которые позволяют злоумышленнику провести атаку.
- Требуемые привилегии (PR) – уровень привилегий, необходимых злоумышленнику для эксплуатации уязвимости.
- Взаимодействие с пользователем (UI) – необходимость участия пользователя (не злоумышленника) в эксплуатации уязвимости.
- Влияние на конфиденциальность (VC) – степень влияния уязвимости на конфиденциальность данных.
- Влияние на целостность (VI) – степень влияния уязвимости на целостность данных.
- Влияние на доступность (VA) – степень влияния уязвимости на доступность данных.

2. *Временные*

- Эксплуатируемость (E) – степень легкости поиска злоумышленником эксплойта для уязвимости.
- Уровень оповещения (RL) – степень известности уязвимости.

3. *Экологические*

- Влияние на безопасность (SI) – степень влияния уязвимости на безопасность системы или сети.
- Влияние на целостность (II) – степень влияния уязвимости на целостность системы или сети.
- Влияние на доступность (AI) – степень влияния уязвимости на доступность системы или сети.

Перечень и описание рассматриваемых уязвимостей приведены в табл. 1.

Таблица 1

Рассматриваемые уязвимости

Уязвимость	Описание уязвимости	Имеющееся решение/ рекомендации к устранению	Оценка по CVSS
CVE-2024-48902	В JetBrains YouTrack до 2024.3.46677 ненадлежащий контроль доступа позволил пользователям с разрешением на обновление проекта удалять приложения через API	Обновление до новой версии	Отсутствует
CVE-2024-7421	Информация в Devolutions Remote Desktop Manager 2024.2.20.0 и ранее в Windows позволяет внутренним нарушителям с доступом к системным журналам получать учетные данные сеанса через пароли, включенные в аргументы командной строки при запуске сеансов WinSCP	Обновление до Remote Desktop Manager 2024.3.10 или выше	Отсутствует
CVE-2024-38202	Уязвимость повышения привилегий, что потенциально позволяет злоумышленнику с основными привилегиями пользователя повторно использовать ранее смягченные уязвимости или обойти некоторые функции безопасности на основе виртуализации	Microsoft разрабатывает обновление безопасности для смягчения этой угрозы, но оно пока недоступно. Рекомендуется настроить параметр «Аудит доступа к объектам»	Отсутствует

Исходя из этого можно сделать вывод, что, несмотря на наличие решений в виде обновления версий ресурсов до безопасного или общие рекомендации по управлению доступа к объектам, таких мер зачастую бывает недостаточно.

С целью определения критичности этих уязвимостей была проведена их оценка по 11 базовым метрикам CVSS. 4.0 (табл. 2).

Таблица 2

Оценка уязвимостей по CVSS. 4.0

Уязвимость / Метрика	Значение метрики		
	CVE-2024-48902	CVE-2024-7421	CVE-2024-38202
AV	N	L	L
AC	L	L	L
AT	P	P	P
PR	L	L	L
UI	N	N	A
VC	L	H	H
VI	H	N	H
VA	N	N	H
SC	L	H	H
SI	H	N	H
SA	N	N	H
Оценка риска по 4-й версии CVSS	7.1 Высокий	6.8 Средний	7.3 Высокий

Все три уязвимости имеют оценку критичности выше среднего, соответственно их эксплуатация, что может привести организации к существенным материальным, репутационным и иным видам ущерба. Для разработки организационно-технических мер защиты рассмотрим основные сценарии эксплуатации уязвимостей злоумышленником.

1. CVE-2024-48902

Локальный злоумышленник (сотрудник компании либо человек, имеющий доступ к корпоративной сети и проектам) создает через API запрос на удаление проекта, такой запрос должен пройти через процесс авторизации, прежде чем быть выполненным, но из-за отсутствия такового процесса выполняется любой запрос, даже вредоносный. Вследствие этого проект может быть утерян безвозвратно (при отсутствии в других системах резервных версий проекта), что приводит к получению компанией коммерческого ущерба,

связанного с затратами на восстановление проекта, а также репутационного ущерба, связанного с задержкой сдачи утраченного проекта заказчику. Схематически сценарий эксплуатации представлен на рис. 1.

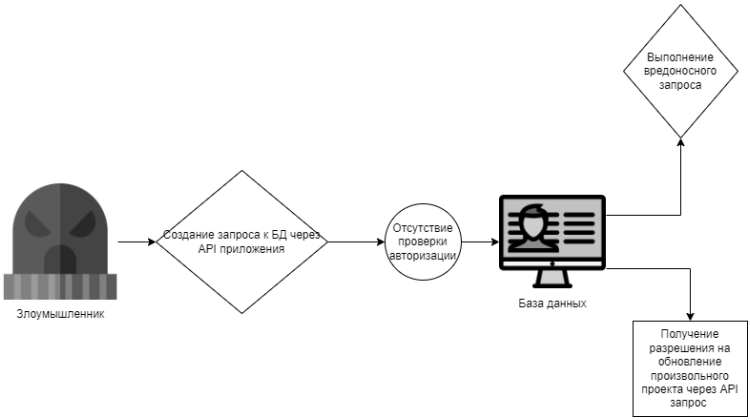

Рис. 1. Сценарий эксплуатации уязвимости CVE-2024-48902

2. CVE-2024-7421

Злоумышленник, имеющий доступ к системным журналам, может отследить события запуска Remote Desktop Manager с вызовом сеансов WinSCP, просмотреть по записям журнала аргументы, передаваемые для запуска сеанса, и найти среди них необходимые учетные данные для развития атаки. С такими данными злоумышленник может получить несанкционированный доступ к аккаунтам и устройствам других сотрудников, что может привести как к утечке и компрометации информации, так и к нарушению доступности этих устройств для санкционированных сотрудников компании. Таким образом, работа компании будет приостановлена до момента обнаружения злоумышленника и устранения всех последствий его вмешательства. Схематический сценарий эксплуатации представлен на рис. 2.

3. CVE-2024-38202

В сценарии эксплуатации этой уязвимости присутствует сразу 2 нарушителя, один из которых имеет базовые права доступа, второй – привилегированные (повышенные). Уязвимость позволяет нарушителю при содействии привилегированного пользователя повысить свои права, что приводит к возможности повторно ввести ранее устраненные уязвимости или обойти некоторые функции Virtualization Based Security (VBS). Эта уязвимость позволяет

группе злоумышленников создать для себя брешь в защите, которая позволит при обнаружении одного нарушителя заменить его другим. Потенциальный ущерб от этой уязвимости представляет собой длительную приостановку работы компании либо возможность для нарушителей в удобный для них момент получить полный доступ к системе и развить свою атаку на любой из ее компонентов за счет внедрения уже устраненных уязвимостей. Схематический сценарий эксплуатации представлен на рис. 3.

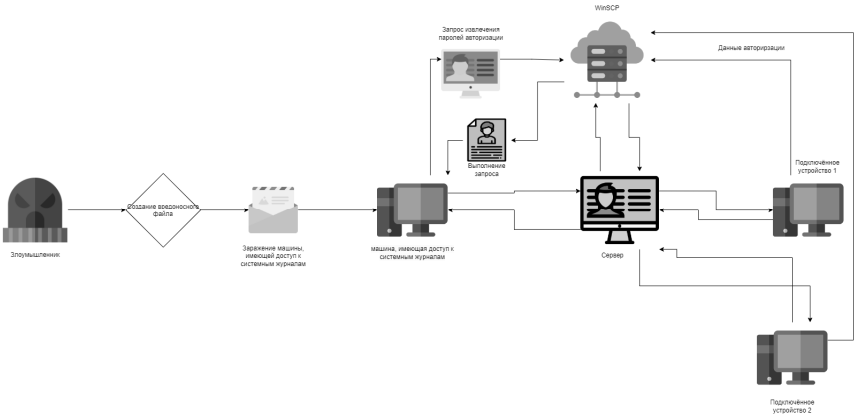

Рис. 2. Сценарий эксплуатации уязвимости CVE-2024-7421

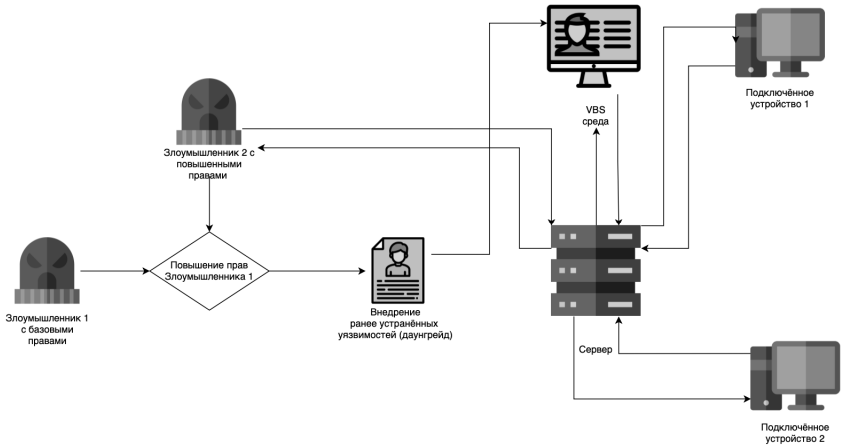

Рис. 3. Сценарий эксплуатации уязвимости CVE-2024-38202

2. МЕРЫ ЗАЩИТЫ

Основной рекомендацией по безопасности для исключения возможности эксплуатации уязвимости CVE-2024-48902 является обновление JetBrains YouTrack до версии 2024.3.46677 или более поздней. В случае если нет возможности провести обновление, рекомендуется рассмотреть возможность внедрения дополнительных средств контроля доступа и мониторинга любых подозрительных вызовов API, связанных с удалением приложений. Необходимо проверить и ограничить разрешения на обновление проекта только для необходимых пользователей и отслеживать действия пользователей, особенно тех, у кого повышенные разрешения. Это поможет снизить риски возможной эксплуатации к минимуму.

В качестве базовой меры по безопасности для исключения возможности эксплуатации уязвимости CVE-2024-7421 является обновление до последней версии. Однако зачастую возникает ситуация, когда установка обновлений невозможна в конкретный момент, особенно с учетом того, что данная уязвимость обнаружена относительно недавно или требует значительных временных затрат. В таком случае можно внедрить собственные меры по защите от эксплуатации уязвимости. Например, рекомендуется ограничить доступ к системным журналам на компьютерах, использующих уязвимое ПО, внедрить более строгий контроль доступа, а также осуществлять мониторинг всех систем, на которых работает Remote Desktop Manager. Более того, стоит рассмотреть альтернативные методы запуска сеансов WinSCP, которые не раскрывают пароли в аргументах командной строки, а также регулярно изменять учетные данные, используемые в сеансах, управляемых уязвимым ПО. Также возможно реализовать принцип наименьших привилегий, подразумевающий выдачу пользователю только тех привилегий, которые абсолютно необходимы для выполнения задач, для учетных записей, используемых с Remote Desktop Manager. Это снизит до минимума вероятность доступа к конфиденциальной информации.

Оптимальным вариантом по безопасности для исключения возможности эксплуатации уязвимости CVE-2024-38202 будет обновление до актуальной версии ПО. В случае возникновения обстоятельств, препятствующих обновлению, рекомендуется настроить параметры «Аудит доступа к объектам» для отслеживания попыток доступа к файлам, таких как создание файлов, операции чтения/записи или изменения дескрипторов безопасности, а также провести аудит пользователей, имеющих разрешение на выполнение операций обновления и восстановления, чтобы убедиться, что выполнять эти операции могут только соответствующие пользователи. Более того, можно реализовать список контроля доступа или списки дискреционного контроля доступа,

чтобы ограничить доступ или изменение файлов обновлений и разрешить выполнять операции восстановления только соответствующим пользователям, например администраторам, несмотря на то что такие действия не устранят возможность эксплуатации уязвимости, но сведут этот риск к минимуму, что позволит выиграть время для последующего обновления.

ЗАКЛЮЧЕНИЕ

В ходе настоящего исследования была проведена оценка уязвимостей 2024 года – CVE-2024-48902, CVE-2024-7421, CVE-2024-38202 – в соответствии с недавно выпущенной версией CVSS 4.0, согласно которой эти уязвимости имеют степень критичности или серьезности выше среднего. Несмотря на это, в качестве базовых мер от защиты эксплуатации этих уязвимостей разработчики рекомендует обновить ресурс до последней «неуязвимой» версии, чего может быть недостаточно в ряде случаев, например при невозможности установки обновления, но необходимости работы сервиса или ресурса. Для разработки рекомендаций по обеспечению информационной безопасности были описаны и схематически изображены практические сценарии эксплуатации рассматриваемых уязвимостей, отражающие поведение злоумышленника при реализации атак. Предлагаемые меры защиты носят больше рекомендательный характер, так как основной способ защиты – при любой возможности установить последние обновления от разработчика. Однако стоит придерживаться основных мер по обеспечению информационной безопасности, например: установка необходимых технических и криптографических средств защиты информации, разработка и внедрение организационных мероприятий, в том числе проведение периодического контроля состояния информационного ресурса или системы, пересмотр модели угроз и нарушителей ИБ [6], назначение доверенных ответственных лиц в организации, своевременный доступный для понимания инструктаж авторизованных пользователей по вопросам ИБ и возможностям злоумышленников, обучение пользователей противодействию современным методам социальной инженерии [7].

СПИСОК ЛИТЕРАТУРЫ

1. Актуальные киберугрозы для организаций: итоги 2023 года // Positive Technologies. – 2024. – 22 апреля. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/aktualnye-kiberugrozy-dlya-organizacij-itogi-2023-goda/ (accessed: 02.12.2024).

2. CVE (Common Vulnerabilities and Exposures): Website. – URL: https://cve.mitre.org/ (accessed: 02.12.2024).

3. CVSS v4.0 Specification Document / FIRST – Forum of Incident Response and Security Teams. – URL: https://www.first.org/cvss/v4.0/specification-document (accessed: 02.12.2024).

4. NVD – Vulnerabilities. – URL: https://nvd.nist.gov/vuln (accessed: 02.12.2024).

5. Common Vulnerability Scoring System Version 4.0 Calculator / FIRST – Forum of Incident Response and Security Teams. – URL: https://www.first.org/cvss/calculator/4.0 (accessed: 02.12.2024).

6. ФСТЭК России. Методический документ от 5 февраля 2021 г. – URL: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g (accessed: 02.12.2024).

7. *Мельников А.И.* Социальная инженерия в цифровой эпохе: анализ методов манипуляции человеческим фактором в целях кибератак // Социально-гуманитарные знания. – 2024. – № 1. – С. 50–54.

Жумажанова Самал Сагидулловна, кандидат технических наук, доцент кафедры «Комплексная защита информации» Омского государственного технического университета. Основное направление научных исследований: информационная безопасность, биометрия, дистанционное определение психофизиологического состояния. E-mail: samal_shumashanova@mail.ru

Зубович Никита Васильевич, лаборант кафедры «Комплексная защита информации» Омского государственного технического университета. Область научных интересов – киберполигоны. E-mail: ankerov.n@mail.ru

Обрывалин Дмитрий Евгеньевич, лаборант кафедры «Комплексная защита информации» Омского государственного технического университета. Область научных интересов – информационная безопасность. E-mail: dimawork3270@gmail.com

DOI: 10.17212/2782-2230-2024-4-25-36

Establishing of recommendations for information protection from exploitation of current vulnerabilities in 2024*

S.S. Zhumazhanova[1], N.V. Zubovich[2], D.E. Obryvalin[3]

[1] *Omsk State Technical University, 11 Prospekt Mira, Omsk, 644050, Russian Federation, Ph.D., associate professor of Complex Information Protection Department. E-mail: samal_shumashanova@mail.ru*

[2] *Omsk State Technical University, 11 Prospekt Mira, Omsk, 644050, Russian Federation, laboratory assistant of Complex Information Protection Department. E-mail: ankerov.n@mail.ru*

[3] *Omsk State Technical University, 11 Prospekt Mira, Omsk, 644050, Russian Federation, laboratory assistant of Complex Information Protection Department. E-mail: dimawork3270@gmail.com*

Information security threats are one of the most important problems of our time. In general, a threat is a potential event, action (impact), process or phenomenon that can lead to damage to someone's interests. There are many ways to implement information security threats, but one of the main ones is the exploitation of information security vulnerabilities. According to a recent report by Positive Technologies [1], in 2023, vulnerability exploitation became one of the main methods of attack on organizations (32 %). Vulnerabilities are exploited in accordance with a certain attack scenario, which is conventionally divided into the following stages: conducting reconnaissance, conducting an attack, developing an attack on an information system, obtaining benefits. Thus, this work is devoted to the analysis of a number of information security vulnerabilities in 2024, modeling attack scenarios when exploiting these vulnerabilities and establishing of recommendations for eliminating the possibility of exploiting vulnerabilities based on organizational and technical measures.

Keywords: information security, vulnerabilities, exploit, vulnerability exploitation, information protection, attack scenario, measures of protection, information security vulnerability assessment systems

REFERENCES

1. Aktual'nye kiberugrozy dlya organizatsii: itogi 2023 goda [Current cyber threats for organizations: 2023 results]. *Positive Technologies*, 2024, 22 April. (In Russian). Available at: https://www.ptsecurity.com/ru-ru/research/analytics/aktualnye-kiberugrozy-dlya-organizacij-itogi-2023-goda/ (accessed 02.12.2024).

2. *CVE (Common Vulnerabilities and Exposures)*. Website. Available at: https://cve.mitre.org/ (accessed 02.12.2024).

* *Received 12 November 2024.*

3. *CVSS v4.0 Specification Document*. FIRST – Forum of Incident Response and Security Teams. Available at: https://www.first.org/cvss/v4.0/specification-document (accessed 02.12.2024).

4. *NVD – Vulnerabilities*. Available at: https://nvd.nist.gov/vuln (accessed 02.12.2024).

5. *Common Vulnerability Scoring System Version 4.0 Calculator*. FIRST – Forum of Incident Response and Security Teams. Available at: https://www.first.org/cvss/calculator/4.0 (accessed 02.12.2024).

6. FSTEC of Russia. *Methodological document from February 5, 2021*. (In Russian). Available at: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g (accessed 02.12.2024).

7. Melnikov A.I. Sotsial'naya inzheneriya v tsifrovoi epokhe: analiz metodov manipulyatsii chelovecheskim faktorom v tselyakh kiberatak [Social engineering in the digital age: analysis of methods of manipulating the human factor for cyber attacks]. *Sotsial'no-gumanitarnye znaniya = Social and Humanitarian Knowledge*, 2024, no. 1, pp. 50–54.

Для цитирования:

Жумажанова С.С., Зубович Н.В., Обрывалин Д.Е. Разработка рекомендаций по защите информации от эксплуатации актуальных уязвимостей 2024 года // Безопасность цифровых технологий. – 2024. – № 4 (115). – С. 25–36. – DOI: 10.17212/2782-2230-2024-4-25-36.

For citation:

Zhumazhanova S.S., Zubovich N.V., Obryvalin D.E. Razrabotka rekomendatsii po zashchite informatsii ot ekspluatatsii aktual'nykh uyazvimostei 2024 goda [Establishing of recommendations for information protection from exploitation of current vulnerabilities in 2024]. *Bezopasnost' tsifrovykh tekhnologii = Digital Technology Security*, 2024, no. 4 (115), pp. 25–36. DOI: 10.17212/2782-2230-2024-4-25-36.