Научная статья
УДК 004; DOI: 10.61260/2218-13X-2024-2-126-135

АНАЛИЗ УСЛОВИЙ РЕАЛИЗАЦИИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ЧЕРЕЗ ЭКСПЛУАТАЦИЮ УЯЗВИМОСТЕЙ ИНФОРМАЦИОННЫХ АКТИВОВ

✉**Комаров Валерий Валерьевич;**
Мезинова Наталья Алексеевна;
Евдокимова Елена Александровна.
АНО ДПО «Центр повышения квалификации «АИС», Москва, Россия
✉***vinnipux1@rambler.ru***

Аннотация. Целью исследования является анализ предпосылок и условий для реализации угроз безопасности посредством эксплуатации уязвимостей информационных активов.

Методы исследования заключаются в обобщении и анализе сложившегося подхода к предотвращению угроз информационной безопасности в органах государственной власти Российской Федерации посредством эксплуатации уязвимостей, а также в прогнозировании тенденций и перспектив роста уязвимостей информационных активов.

Научная новизна исследования заключается в анализе эффективности существующих процессов управления уязвимостями информационной инфраструктуры, реализуемых без использования специализированных средств автоматизации процесса.

Ключевые слова: угроза информационной безопасности, уязвимость информационного актива, киберугроза, компьютерная атака, устранение уязвимости

Для цитирования: Комаров В.В., Мезинова Н.А., Евдокимова Е.А. Анализ условий реализации угроз безопасности информации через эксплуатацию уязвимостей информационных активов // Науч.-аналит. журн. «Вестник С.-Петерб. ун-та ГПС МЧС России». 2024. № 2. С. 126–135. DOI: 10.61260/2218-13X-2024-2-126-135.

Scientific article

ANALYSIS OF THE CONDITIONS FOR THE IMPLEMENTATION OF INFORMATION SECURITY THREATS THROUGH THE EXPLOITATION OF INFORMATION ASSET VULNERABILITIES

✉**Komarov Valery V.;**
Mesinova Natalia A.;
Evdokimova Elena A.
ANO DPO «Center for advanced training «AIS», Moscow, Russia
✉***vinnipux1@rambler.ru***

Abstract. The purpose of the study is to analyze the prerequisites and conditions for the implementation of security threats through the exploitation of vulnerabilities of information assets.

The research methods consist in generalizing and analyzing the established approach to preventing threats to information security in the public authorities of the Russian Federation through the exploitation of vulnerabilities, as well as in predicting trends and prospects for the growth of vulnerabilities of information assets.

The scientific novelty of the research lies in the analysis of the effectiveness of existing information infrastructure vulnerability management processes implemented without the use of specialized process automation tools.

Keywords: threat to information security, vulnerability of an information asset, cyber threat, computer attack, vulnerability elimination

For citation: Komarov V.V., Mesinova N.A., Evdokimova E.A. Analysis of the conditions for the implementation of information security threats through the exploitation of information assets vulnerabilities // Scientific and analytical journal «Vestnik Saint-Petersburg university of State fire service of EMERCOM of Russia». 2024. № 2. P. 126–135. DOI: 10.61260/2218-13X-2024-2-126-135.

Введение

В настоящее время информационная инфраструктура в органах (организациях) субъектов Российской Федерации (органы (организации) сталкивается с большим количеством попыток реализации угроз безопасности информации [1, 2].

Согласно аналитическому отчету о киберугрозах по итогам 2023 г.[1] общее число атак выросло на 11 % по сравнению с отчетным периодом предыдущего года.

По информации Федеральной службы по техническому и экспортному контролю (ФСТЭК России)[2] основными причинами реализации угроз безопасности информации в органах (организациях) является несвоевременное устранение уязвимостей владельцами информационных активов[3] [3], а также непринятие компенсирующих мер в случае невозможности устранения уязвимостей.

Отказ от зарубежных производителей программного обеспечения и программно-аппаратных комплексов, используемых в работе информационных активов российских органов (организаций), привел к невозможности оперативного устранения уязвимостей.

Кроме того, существует угроза целенаправленного внедрения вредоносного программного обеспечения в пакеты обновлений от зарубежных поставщиков из недружественных стран или с поддельных веб-сайтов разработчиков программного обеспечения.

Реализация нарушителем угрозы информационной безопасности возможна только при наличии в информационных системах органов (организации) уязвимостей[4].

Угроза целенаправленных действий нарушителей приводит к недопустимым для органов (организаций) событиям[5] [4, 5]. Эта угроза привела к необходимости проведения внеплановых мероприятий по оценке уровня защищенности информационной инфраструктуры с целью повышения устойчивости и безопасности функционирования информационных ресурсов субъектов Российской Федерации[6] для обеспечения их конфиденциальности, доступности и целостности [6].

Система защиты информации, не учитывающая важность процессов управления уязвимостями, эффективно нейтрализует актуальные угрозы безопасности информации [7] исключительно на момент аттестационных испытаний на соответствие требованиям безопасности информации и деградирует с течением времени в связи с выявлением новых уязвимостей, используемых нарушителями для реализации угроз безопасности информации[7] [8].

---

[1] Итоги года. 2023. Jet Security team. URL: https://jetcsirt.su/upload/godovoy_otchet__jet_2023.pdf (дата обращения: 29.01.2024).

[2] Выступление Андреева И.Ю.: ТБ Форум-2024. ФСТЭК России. URL: https://2037604.fs1.hubspotusercontent-eu1.net/hubfs/2037604/Digital/SS/SS_ADAPT/Cybersecurity_TFB_130224_Andreev.pdf (дата обращения: 29.01.2024).

[3] ГОСТ Р ИСО/ТО 13569–2007. Национальный стандарт Российской Федерации. Финансовые услуги. Рекомендации по информационной безопасности» (утв. приказом Ростехрегулирования от 27 дек. 2007 г. № 514-ст) // ЭЛЕКТРОННЫЙ ФОНД правовой и нормативно-технической документации. URL: http://www.docs.cntd.ru (дата обращения: 29.01.2024).

[4] ГОСТ Р 56546–2015. Национальный стандарт Российской Федерации. Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем (утв. и введен в действие приказом Росстандарта от 19 авг. 2015 г. № 1181-ст) // ЭЛЕКТРОННЫЙ ФОНД правовой и нормативно-технической документации. URL: http://www.docs.cntd.ru (дата обращения: 29.01.2024).

[5] О дополнительных мерах по обеспечению информационной безопасности Российской Федерации: Указ Президента Рос. Федерации от 1 мая 2022 г. № 250. Доступ из справ.-правовой системы «КонсультантПлюс».

[6] Типовое техническое задание на выполнение работ по оценке уровня защищенности информационной инфраструктуры. URL: https://digital.gov.ru/ru/documents/8235/ (дата обращения: 29.01.2024).

[7] Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах: приказ ФСТЭК России от 11 февр. 2013 г. № 17. Доступ из справ.-правовой системы «КонсультантПлюс».

12 мая 2017 г. российские органы (организации) подверглись компьютерным атакам, с использованием специально разработанного вредоносного программного обеспечения со встроенным механизмом криптографической модификации информации (шифровальщик) «WannaCry»[8], а также аналогичного вредоносного программного обеспечения «Petya» и «Misha».

При этом еще 11 марта 2017 г. компания Microsoft опубликовала Сводку бюллетеня Microsoft по безопасности[9] (CVE-2017-0199), а ФСТЭК России 12 апреля 2017 г. внесла данные об этих уязвимостях в Банк данных угроз безопасности информации (БДУ) (BDU:2017-01034, BDU:2017-01095, BDU:2017-01096, BDU:2017-01097, BDU:2017-01098, BDU:2017-01099, BDU:2017-01100).

Несмотря на наличие всей необходимой информации о конкретных уязвимостях и способах их устранения, владельцы информационных активов, в том числе органы государственной власти Российской Федерации (Министерство внутренних дел Российской Федерации, Следственный комитет Российской Федерации, Министерство здравоохранения Российской Федерации, Министерство Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий), Сбербанк, операторы сотовой связи (Мегафон, Yota, Билайн) и др.,[10] столкнулись с нарушением работы своих информационных активов (компьютерными инцидентами).

Расследование произошедших компьютерных инцидентов показало, что реализация угрозы безопасности с использованием вышеуказанного вредоносного программного обеспечения осуществлялась за счет эксплуатации уязвимости операционной системы Windows и пакета программ Microsoft Office, а также уязвимостей протокола SMB v.1, позволяющих нарушителю выполнить произвольный код.

К аналогичным выводам о причинах неэффективности систем защиты информации органов (организаций) пришла ФСТЭК России, проведя анализ сложившейся ситуации[11].

По данным ФСТЭК России[12], количество записей об уязвимостях программного обеспечения в БДУ с каждым годом только растет. В 2022 г. оно увеличилось, по сравнению с 2021 г., на 7 532 и составило 44 284 записи, а к концу 2023 г. –53 430, что на 9 146 записей больше, по сравнению с 2022 г., при этом ФСТЭК России, осуществляя проверки контроля состояния технической защиты информации в информационных и автоматизированных системах органов государственной власти и организаций, до сих пор выявляет неустраненные уязвимости «WannaCry», «Petya», «Misha» и их модификации.

Аналитическая часть

По состоянию на 1 марта 2024 г. в БДУ[13] содержится 55 077 записей по уязвимостям, то есть количество уязвимостей увеличилось на 1 647 за два месяца 2024 г. (рис. 1).

[8] WannaCry. URL: https://ru.wikipedia.org/wiki/WannaCry (дата обращения: 29.01.2024).

[9] Microsoft Security Bulletin Summary for March 2017. URL: https://learn.microsoft.com/en-us/security-updates/securitybulletinsummaries/2017/ms17-mar#affected-software (дата обращения: 29.01.2024).

[10] URL: https://zoom.cnews.ru/soft/news/top/2017-05-16_mvd_provodit_sluzhebnuyu_proverku_po_faktu_zarazheniya (дата обращения: 29.01.2024); WannaCry (вирус-вымогатель). URL: https://www.tadviser.ru/index.php/Статья:WannaCry_(вирус-вымогатель)#.D0.90.D1.82.D0.B0.D0.BA.D0.B0_.D0.BD.D0.B0_.D0.A1.D0.B1.D0.B5.D1.80.D0.B1.D0.B0.D0.BD.D0.BA (дата обращения: 29.01.2024).

[11] О мерах по защите информации, направленных на нейтрализацию угроз безопасности информации, связанных с проникновением и распространением вредоносного программного обеспечения WannaCry, Petya, Misha и их модификаций: информационное сообщение ФСТЭК России от 2 июля 2017 г. № 240/22/3171. URL: https://safe-surf.ru/specialists/normative-materials/normativnye-pravovye-akty-federalnykh-organov-ispolnitelnoy-vlasti/5106/ (дата обращения: 29.01.2024).

[12] Доклад начальника управления ГНИИИ ПТЗИ ФСТЭК России Суховеркова А. на конференции «Актуальные вопросы защиты информации» 14 февр. 2024 г. URL: https://www.tbforum.ru/2024/program/information-security (дата обращения: 29.01.2024).

[13] Банк данных угроз безопасности информации. URL: https://bdu.fstec.ru/vul/ (дата обращения: 29.01.2024).

Рис. 1. **Количество опубликованных записей об уязвимостях в БДУ ФСТЭК России с 2021 по 2024 г.**

То есть на сегодняшний день из-за роста количества уязвимостей владельцы информационных активов органов (организаций) все чаще сталкиваются с ситуацией несвоевременного устранения уязвимостей, когда публикуют информацию о новой уязвимости, а ранее опубликованные уязвимости еще не устранены [9].

4 апреля 2022 г. ФСТЭК России внесла данные об уязвимости CVE-2022-27228 (BDU:2022-01141) в БДУ[14], а 12 июля 2022 г. Национального координационного центра по компьютерным инцидентам (НКЦКИ) предупредил об угрозе заражения сайтов под управлением «Bitrix» посредством эксплуатации критической уязвимости в CMS Bitrix[15].

Более чем через год, уже 26 мая 2023 г. произошёл масштабный дефейс[16] веб-серверов национального сегмента сети интернет. В качестве цели атаки выступила CMS «Bitrix». Согласно данным производителя только 10 % пользователей на момент эксплуатации уязвимости обновили программное обеспечение.

Компьютерным атакам подверглись официальные сайты Министерства строительства и жилищно-коммунального хозяйства Российской Федерации, Росреестра, Совета по правам человека, сайты российских вузов.

Таким образом, на сегодняшний день владельцы информационных активов органов (организаций), имея необходимую информацию от ФСТЭК России и НКЦКИ о мерах по повышению защищенности информационной инфраструктуры Российской Федерации, оказываются не готовы к реализации нарушителем угрозы информационной безопасности, по причине несвоевременного устранения уязвимостей [10–12].

Вышеуказанной исходной информации, приведенной на рис. 1, достаточно для проведения анализа, позволяющего спрогнозировать темп прироста количества новых уязвимостей.

Рассчитаем среднегодовое количество новых уязвимостей в БДУ ФСТЭК России по формуле:

[14] Банк данных угроз безопасности информации. URL: https://bdu.fstec.ru/vul/2022-01141 (дата обращения: 29.01.2024).

[15] Угроза заражения веб-сайтов под управлением Bitrix. URL: https://safe-surf.ru/upload/ALRT/ALRT-20220712.1.pdf (дата обращения: 29.01.2024).

[16] Дефейс (от англ. deface – «портить», «уродовать») – взлом сайта и публикация на нем сообщения злоумышленников. URL: https://encyclopedia.kaspersky.ru/glossary/deface/ (дата обращения: 29.01.2024).

$$\overline{Y_i} = \frac{Y_i}{n},$$

где $\overline{Y_i}$ – среднегодовое количество новых уязвимостей, прирост уязвимостей в году по отношению к предыдущему; n – полное число месяцев, за которое рассчитывается прирост уязвимостей.

$$\overline{Y_1} = \frac{6431}{12} = 535{,}9 \approx 536;$$
$$\overline{Y_2} = \frac{7532}{12} = 627{,}6 \approx 628;$$
$$\overline{Y_3} = \frac{9146}{12} = 762{,}1 \approx 762;$$
$$\overline{Y_4} = \frac{1647}{2} = 823{,}5 \approx 824.$$

Вышеуказанные показатели приведены на графике (рис. 2).

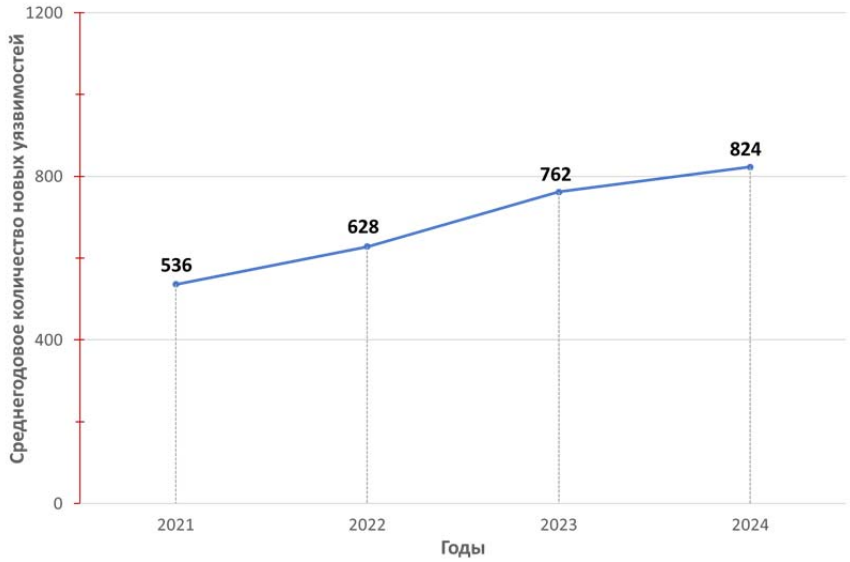

Рис. 2. **Среднегодовой прирост новых уязвимостей**

Определим показатель динамики абсолютного прироста, который определяется в разностном сопоставлении двух уровней ряда динамики в единицах измерения исходной информации:

$$\Delta Y_i = \overline{Y_i} - \overline{Y}_{i-1},$$

где ΔY_i – абсолютный прирост; $\overline{Y_i}$ – последующее значение количества уязвимостей; $\overline{Y}_{i-1}$ – предыдущее значение количества уязвимостей.

$$\Delta Y_2 = \overline{Y_2} - \overline{Y_1} = 628 - 536 = 92;$$
$$\Delta Y_3 = \overline{Y_3} - \overline{Y_2} = 762 - 628 = 134;$$
$$\Delta Y_4 = \overline{Y_4} - \overline{Y_3} = 824 - 762 = 62.$$

Темп роста характеризует отношение двух уровней ряда и выражается в процентах:

$$T_{\text{пр}i} = \frac{\Delta Y_i}{\overline{Y}_{i-1}} \times 100,$$

где $T_{\text{пр}i}$ – темп роста; ΔY_i – абсолютный прирост; $\overline{Y}_{i-1}$ – предыдущее значение количества уязвимостей.

$$T_{\text{пр}2} = \frac{\Delta Y_2}{\overline{Y}_1} \times 100 = \frac{92}{536} \times 100 = 17{,}2\ \%;$$

$$T_{\text{пр3}} = \frac{\Delta Y_3}{\bar{Y}_2} \times 100 = \frac{134}{628} \times 100 = 21{,}3\ \%;$$
$$T_{\text{пр4}} = \frac{\Delta Y_4}{\bar{Y}_3} \times 100 = \frac{62}{762} \times 100 = 8{,}1\ \%.$$

В таблице приведены расчетные значения абсолютного прироста уязвимостей и темпы роста количества уязвимостей.

Таблица

Год	Среднегодовое количество новых уязвимостей	Абсолютный прирост, ΔY_i	Темп роста, $T_{\text{пр4}}$ (%)
2021	536	–	–
2022	628	92	17,2
2023	762	134	21,3
2024	824	62	8,1
Итого:	2 750		

Средний уровень ряда динамики характеризует типическую величину абсолютных уровней. Средний уровень интервального ряда, то есть среднее количество уязвимостей, рассчитывается по формуле:

$$\bar{Y} = \frac{\sum \bar{Y}_i}{n} = \frac{536+628+762+824}{4} = \frac{2750}{4} = 687{,}5,$$

где $\bar{Y}$ – среднее количество уязвимостей; $\sum \bar{Y}_i$ – сумма всех уязвимостей; n – количество расчетных периодов.

Среднее значение появления новых уязвимостей с 2021 по 2024 г. составило $\bar{Y} = 687{,}5$.

Средний темп роста рассчитывается по формуле.

$$\overline{T_p} = \sqrt[n-1]{\frac{\overline{Y_n}}{\overline{Y_1}}} = \sqrt[3]{\frac{\overline{Y_4}}{\overline{Y_1}}} = \sqrt[3]{\frac{824}{536}} = 1{,}154,$$

где $\overline{T_p}$ – средний темп роста; $\overline{Y_n}$ – количество уязвимостей на последний рассматриваемый период; Y_n – количество уязвимостей на первый рассматриваемый период.

Зная средний темп роста количества новых уязвимостей, можно сделать прогноз на следующие два периода, используя формулу:

$$\bar{Y}_{n+1} = \bar{Y}_n \times \overline{T_p}\ ,$$

где $\bar{Y}_{n+1}$ – прогнозное значение среднегодового количества уязвимостей; $\bar{Y}_n$ – крайнее известное значение среднегодового количества уязвимостей; $\overline{T_p}$ – средний темп роста.

$$\bar{Y}_4 = 823 \times 1.154 \approx 950;$$
$$\bar{Y}_5 = 950 \times 1.154 \approx 1097.$$

Исходя из расчетных значений, построим график с прогнозными значениями среднегодового прироста новых уязвимостей (рис. 3).

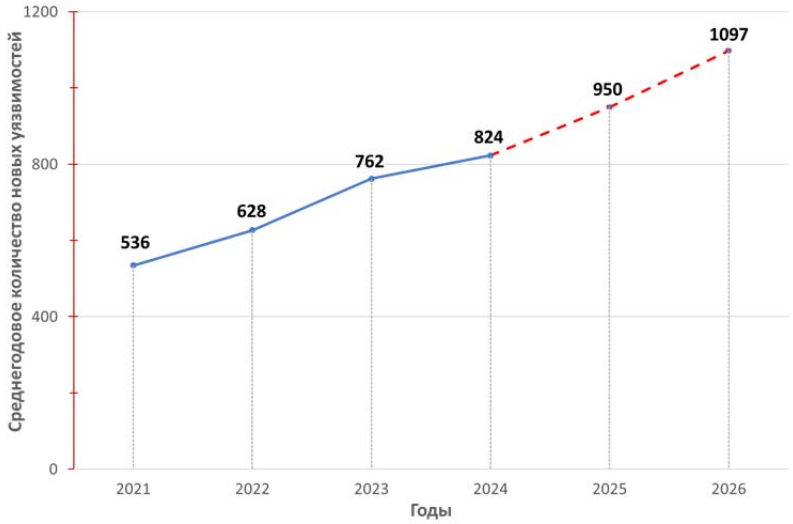

Рис. 3. **Прогнозные значения среднегодового прироста новых уязвимостей на 2025 и 2026 г.**

Согласно Методическому документу[17] на устранение уязвимостей, в зависимости от уровня критичности, отводится до 24 ч (для критически опасных уязвимостей), до четырех месяцев (для уязвимостей с низким уровнем опасности), а согласно п.п. 3.2 и 3.3 табл. 1 Методического документа, опубликованного ФСТЭК России на официальном сайте,[18] значения частных показателей безопасности информации равны нулю, если уязвимости критического уровня опасности не устранены по истечении 30 дней со дня публикации обновлений (компенсирующих мер) в БДУ ФСТЭК России.

На рис. 4 приведена зависимость значимости уязвимостей от сроков их устранения.

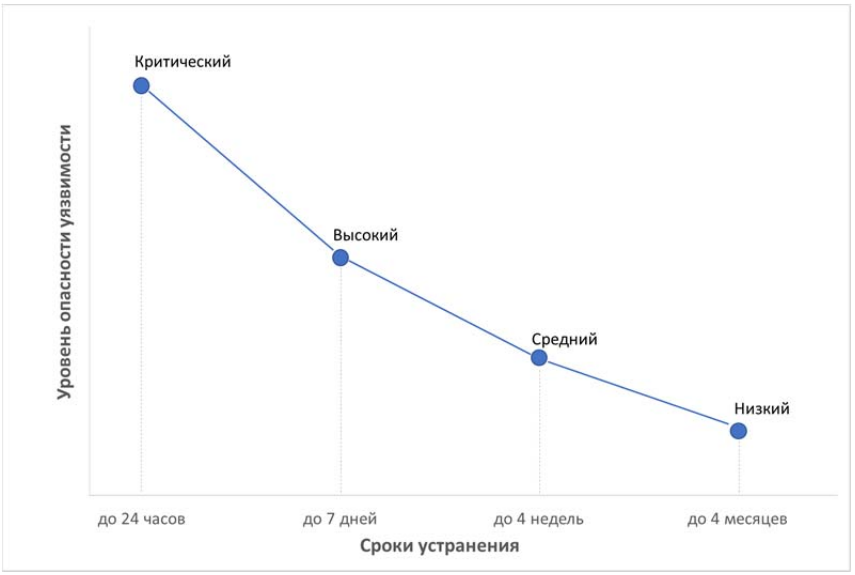

Рис. 4. **График зависимости значимости уязвимости от сроков их устранения**

[17] Руководство по организации процесса управления уязвимостями в органе (организации): Методический документ (утв. ФСТЭК России 17 мая 2023 г.). URL: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-17-maya-2023-g (дата обращения: 29.01.2024).

[18] Методика оценки показателя состояния технической защиты информации и обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации: Методический документ (утв. ФСТЭК России 2 мая 2024 г.). URL: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-2-maya-2024-g (дата обращения: 29.01.2024)

В связи с вышеизложенным, а также исходя из проведенного анализа расчета значений среднегодового прироста новых уязвимостей (рис. 3), можно сделать вывод, что актуальность выстраивания процесса управления уязвимостями с каждым годом будет увеличиваться, а за счет этого в большинстве организаций будет остро стоять вопрос об обеспечении кадровыми и техническими ресурсами [13] для качественного выстраивания процесса, в связи с этим данный процесс требует автоматизированных средств управления уязвимостями для выстраивания очередности устранения большого количества уязвимостей ограниченными ресурсами не только путем решения задачи приоритезации уязвимостей, но и приоритезации информационных активов [14, 15].

Методика расчета количественных показателей эффективности процессов управления уязвимостями для выстраивания очередности устранения большого количества уязвимостей ограниченными ресурсами путем решения задачи приоритезации информационных активов в органе (организации) будет рассмотрена в последующих статьях.

Заключение

В настоящей статье рассмотрена проблематика управления уязвимостями информационной инфраструктуры органов государственной власти Российской Федерации как децентрализованная и не автоматизированная. Обоснована необходимость повышения эффективности системы управления уязвимостями для обеспечения адекватного уровня безопасности информационной инфраструктуры органов государственной власти Российской Федерации от актуальных угроз безопасности информации. Указана взаимосвязь времени устранения уязвимостей с реализацией компьютерных атак на информационную инфраструктуру.

Полученные результаты позволяют сформировать выводы о целесообразности принятия мер по созданию (внедрению) средств автоматизации в процесс управления уязвимостями информационной инфраструктуры и обосновать необходимость формирования методики расчета количественных показателей эффективности процессов управления уязвимостями для выстраивания очередности устранения большого количества уязвимостей ограниченными ресурсами путем решения задачи приоритезации информационных активов.

Список источников

1. Максимова Е.А. Когнитивное моделирование деструктивных злоумышленных воздействий на объектах критической информационной инфраструктуры // Труды учебных заведений связи. 2020. Т. 6. № 4. С. 91–103. DOI: 10.31854/1813-324X-2020-6-4-91-103.

2. Кузьмин В.Н., Менисов А.Б. Исследование путей и способов повышения результативности выявления компьютерных атак на объекты критической информационной инфраструктуры // Информационно-управляющие системы. 2022. № 4. С. 29–43. DOI: 10.31799/1684-8853-2022-4-29-43.

3. Разработка специальной классификации информационных активов в сфере информационной безопасности / А.В. Манжосов [и др.] // Вестник Пермского университета. Математика. Механика. Информатика. 2022. № 4 (59). С. 54–60. DOI: 10.17072/1993-0550-2022-4-54-60.

4. Бакшеев А.С., Лившиц И.И. Разработка методики контроля уровня защищенности информационных объектов критической информационной инфраструктуры // Вопросы кибербезопасности. 2023. № 2 (54). С. 85–95. DOI: 10.21681/2311-3456-2023-2-85-98.

5. Гаськова Д.А., Массель А.Г. Технология анализа киберугроз и оценка рисков нарушения кибербезопасности критической инфраструктуры // Вопросы кибербезопасности. 2019. № 2 (30). С. 42–49. DOI: 10.21681/2311-3456-2019-2-42-49.

6. Лапсарь А.П., Назарян С.А., Владимирова А.И. Повышение устойчивости объектов критической информационной инфраструктуры к целевым компьютерным атакам // Вопросы кибербезопасности. 2022. № 2 (48). С. 43–51. DOI: 10.21681/2311-3456-2022-2-39-51.

7. Суханов И.Д., Рыбкина О.В. Новые подходы к моделированию угроз безопасности информации. Научно-техническое и экономическое сотрудничество стран АТР в XXI веке: труды Всерос. науч.-практ. конф. Хабаровск, 2021. С. 277–282.

8. Актуальные вопросы проблематики оценки угроз компьютерных атак на информационные ресурсы значимых объектов критической информационной инфраструктуры / С.В. Скрыль [и др.] // Безопасность информационных технологий. 2021. Т. 28. № 1. С. 84–94. DOI: 10.26583/bit.2021.1.07.

9. Захарченко Р.И., Королев И.Д. Методика оценки устойчивости функционирования объектов критической информационной инфраструктуры, функционирующей в киберпространстве // Наукоемкие технологии в космических исследованиях Земли. 2018. Т. 10. № 2. С. 52–61.

10. Соловьев С.В., Язов Ю.К. Информационное обеспечение деятельности по технической защите информации // Вопросы кибербезопасности. 2021. № 1 (41). С. 69–79. DOI: 10.21681/2311-3456-2021-1-69-79.

11. Состояние и перспективы развития методического обеспечения технической защиты информации в информационных системах / С.В. Соловьев [и др.] // Вопросы кибербезопасности. 2022. № 1 (53). С. 41–57. DOI: 10.21681/2311-3456-2023-1-41-57.

12. Модель оценки ущерба от инцидентов информационной безопасности / М.О. Таныгин [и др.] // Безопасность информационных технологий. 2021. № 2. С. 98–106. DOI: 10.26583/bit.2021.2.09.

13. Микиденко Н.Л., Сторожева С.П., Струкова Е.Г. Кадровое обеспечение образовательных программ в области информационной безопасности: проблемы проектирования и развития // Вестник СибГУТИ. 2022. № 3. С. 84–100. DOI: 10.55648/1998-6920-2022-16-3-84-100.

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

15. Маслова М.А. Анализ и определение рисков информационной безопасности // Научный результат. Информационные технологии. 2019. Т. 4. № 1. С. 31–37. DOI: 10.18413/2518-1092-2019-4-1-0-5.

References

1. Maksimova E.A. Kognitivnoe modelirovanie destruktivnyh zloumyshlennyh vozdejstvij na ob"ektah kriticheskoj informacionnoj infrastruktury // Trudy uchebnyh zavedenij svyazi. 2020. T. 6. № 4. S. 91–103. DOI: 10.31854/1813-324X-2020-6-4-91-103.

2. Kuz'min V.N., Menisov A.B. Issledovanie putej i sposobov povysheniya rezul'tativnosti vyyavleniya komp'yuternyh atak na ob"ekty kriticheskoj informacionnoj infrastruktury // Informacionno-upravlyayushchie sistemy. 2022. № 4. S. 29–43. DOI: 10.31799/1684-8853-2022-4-29-43.

3. Razrabotka special'noj klassifikacii informacionnyh aktivov v sfere informacionnoj bezopasnosti / A.V. Manzhosov [i dr.] // Vestnik Permskogo universiteta. Matematika. Mekhanika. Informatika. 2022. № 4 (59). S. 54–60. DOI: 10.17072/1993-0550-2022-4-54-60.

4. Baksheev A.S., Livshic I.I. Razrabotka metodiki kontrolya urovnya zashchishchennosti informacionnyh ob"ektov kriticheskoj informacionnoj infrastruktury // Voprosy kiberbezopasnosti. 2023. № 2 (54). S. 85–95. DOI: 10.21681/2311-3456-2023-2-85-98.

5. Gas'kova D.A., Massel' A.G. Tekhnologiya analiza kiberugroz i ocenka riskov narusheniya kiberbezopasnosti kriticheskoj infrastruktury // Voprosy kiberbezopasnosti. 2019. № 2 (30). S. 42–49. DOI: 10.21681/2311-3456-2019-2-42-49.

6. Lapsar' A.P., Nazaryan S.A., Vladimirova A.I. Povyshenie ustojchivosti ob"ektov kriticheskoj informacionnoj infrastruktury k celevym komp'yuternym atakam // Voprosy kiberbezopasnosti. 2022. № 2 (48). S. 43–51. DOI: 10.21681/2311-3456-2022-2-39-51.

7. Suhanov I.D., Rybkina O.V. Novye podhody k modelirovaniyu ugroz bezopasnosti informacii. Nauchno-tekhnicheskoe i ekonomicheskoe sotrudnichestvo stran ATR v XXI veke: trudy Vseros. nauch.-prakt. konf. Habarovsk, 2021. S. 277–282.

8. Aktual'nye voprosy problematiki ocenki ugroz komp'yuternyh atak na informacionnye resursy znachimyh ob"ektov kriticheskoj informacionnoj infrastruktury / S.V. Skryl' [i dr.] // Bezopasnost' informacionnyh tekhnologij. 2021. T. 28. № 1. S. 84–94. DOI: 10.26583/bit.2021.1.07.

9. Zaharchenko R.I., Korolev I.D. Metodika ocenki ustojchivosti funkcionirovaniya ob"ektov kriticheskoj informacionnoj infrastruktury, funkcioniruyushchej v kiberprostranstve // Naukoemkie tekhnologii v kosmicheskih issledovaniyah Zemli. 2018. T. 10. № 2. S. 52–61.

10. Solov'ev S.V., Yazov Yu.K. Informacionnoe obespechenie deyatel'nosti po tekhnicheskoj zashchite informacii // Voprosy kiberbezopasnosti. 2021. № 1 (41). S. 69–79. DOI: 10.21681/2311-3456-2021-1-69-79.

11. Sostoyanie i perspektivy razvitiya metodicheskogo obespecheniya tekhnicheskoj zashchity informacii v informacionnyh sistemah / S.V. Solov'ev [i dr.] // Voprosy kiberbezopasnosti. 2022. № 1 (53). S. 41–57. DOI: 10.21681/2311-3456-2023-1-41-57.

12. Model' ocenki ushcherba ot incidentov informacionnoj bezopasnosti / M.O. Tanygin [i dr.] // Bezopasnost' informacionnyh tekhnologij. 2021. № 2. S. 98–106. DOI: 10.26583/bit.2021.2.09.13.

13. Mikidenko N.L., Storozheva S.P., Strukova E.G. Kadrovoe obespechenie obrazovatel'nyh programm v oblasti informacionnoj bezopasnosti: problemy proektirovaniya i razvitiya // Vestnik SibGUTI. 2022. № 3. S. 84–100. DOI: 10.55648/1998-6920-2022-16-3-84-100.

14. Obespechenie informacionnoj bezopasnosti kiberfizicheskih ob"ektov na osnove prognozirovaniya i obnaruzheniya anomalij ih sostoyaniya / V.I. Vasil'ev [i dr.] // Sistemy upravleniya, svyazi i bezopasnosti. 2021. № 6. S. 90–119. DOI: 10.24412/2410-9916-2021-6-90-119.

15. Maslova M.A. Analiz i opredelenie riskov informacionnoj bezopasnosti // Nauchnyj rezul'tat. Informacionnye tekhnologii. 2019. T. 4. № 1. S. 31–37. DOI: 10.18413/2518-1092-2019-4-1-0-5.

Информация о статье:
Статья поступила в редакцию: 01.04.2024; одобрена после рецензирования: 13.06.2024;
принята к публикации: 16.06.2024
Information about the article:
The article was submitted to the editorial office: 01.04.2024; approved after review: 13.06.2024;
accepted for publication: 16.06.2024

Сведения об авторах:
Комаров Валерий Валерьевич, преподаватель АНО ДПО «Центр повышения квалификации «АИС» (111123, Москва, ул. Плеханова, д. 4а), сертифицированный ведущий аудитор ISO/IEC 27001, e-mail: vinnipux1@rambler.ru, https://orcid.org/0009-0000-9872-9358
Мезинова Наталья Алексеевна, АНО ДПО «Центр повышения квалификации «АИС» (111123, Москва, ул. Плеханова, д. 4а), e-mail: natali.mezinova@icloud.com, https://orcid.org/0009-0000-8357-9641
Евдокимова Елена Александровна, АНО ДПО «Центр повышения квалификации «АИС» (111123, Москва, ул. Плеханова, д. 4а), e-mail: evdokimovaelena151@gmail.com, https://orcid.org/ 0009-0006-2019-3171

Information about the authors:
Komarov Valery V., teacher of the Autonomous non-profit organization of additional professional education «Center for advanced training «AIS» (111123, Moscow, Plekhanova str., 4a), certified lead auditor ISO/IEC 27001, e-mail: vinnipux1@rambler.ru, https://orcid.org/0009-0000-9872-9358
Mesinova Natalia A., Autonomous non-profit organization of additional professional education «Center for advanced training «AIS» (111123, Moscow, Plekhanova str., 4a), e-mail: natali.mezinova@icloud.com, https://orcid.org/0009-0000-8357-9641
Evdokimova Elena A., Autonomous non-profit organization of additional professional education «Center for advanced training «AIS» (111123, Moscow, Plekhanova str., 4a), e-mail: evdokimovaelena151@gmail.com, https://orcid.org /0009-0006-2019-3171