ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ
INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

УДК 004.05

DOI: 10.21822/2073-6185-2026-53-1-193-199 Оригинальная статья/ Original article

Распределение ресурсов защиты автоматизированных систем органов внутренних дел Российской Федерации и их реализация

А.И. Янгиров[1], Е.А. Рогозин[2], И.В. Атласов[3], С.Б. Ахлюстин[2]
[1] ФКУ «НИЦ «Охрана» Росгвардии,
[1]111539, г. Москва, ул. Реутовская, 12Б, Россия,
[2] Воронежский институт МВД России,
[2]394065, г. Воронеж, проспект Патриотов, 53, Россия,
[3] Московский университет МВД России имени В.Я. Кикотя,
[3]117997, г. Москва, ул. Академика Волгина, д. 12, Россия

Резюме. Цель. Формирование надежной системы безопасности АС ОВД РФ требует рационального распределения ресурсов. В работе рассматривается подход к определению приоритетов при реализации защитных мер. **Метод.** Исследование основано на анализе данных из банка данных угроз ФСТЭК России, а также на изучении научных публикаций, специализированной литературы и интернет-источников. **Результат.** Предложен вариант распределения ресурсов защиты автоматизированных систем органов внутренних дел Российской Федерации (далее – АС ОВД РФ), а также рассмотрены возможные варианты мер защиты. Представлен подход к распределению ресурсов безопасности для АС ОВД РФ, а также предложены возможные варианты защитных мероприятий. **Вывод.** Отмечается необходимость применения комплексного подхода к обеспечению защиты АС ОВД РФ с применением не только программных, но и аппаратных средств защиты.

Ключевые слова: информационная система, приоритизация, органы внутренних дел, распределение ресурсов, меры защиты

Для цитирования: А.И. Янгиров, Е.А. Рогозин, И.В. Атласов, С.Б. Ахлюстин. Распределение ресурсов защиты автоматизированных систем органов внутренних дел Российской Федерации и их реализация. Вестник Дагестанского государственного технического университета. Технические науки. 2026;53(1):193-199. DOI:10.21822/2073-6185-2026-53-1-193-199

Allocation of resources for the protection of automated systems of the internal affairs bodies of the russian federation and their implementation

A.I. Yangirov[1], E.A. Rogozin[2], I.V. Atlasov[3] S.B. Akhlyustin[2]
[1] FSI «SRC «OKHRANA» of the Federal service of National Guard of Russia,
[1] 12B Reutovskaya St., Moscow 111539, Russia,
[2]Voronezh Institute of the Ministry of Internal Affairs of Russia,
[2] 53 Patriots Ave. Voronezh 394065, Russia,
[3] V.Y. Kikot Moscow University of Russian Ministry of Internal Affairs,
[3]12 Akademika Volgina St., Moscow 117997, Russia

Abstract. Objective. Building a reliable security system for the automated systems of the internal affairs agencies of the Russian Federation requires a rational allocation of resources. This paper examines an approach to determining priorities in the implementation of protective measures. **Method.** This study is based on an analysis of data from the FSTEC of Russia's threat database, as well as a review of scientific publications, specialized literature, and online sources. **Result.** A proposed approach to allocating security resources for automated systems of the Russian Federation's internal affairs agencies (hereinafter referred to as the RF IAS) is presented, and possible protective measures are discussed. An approach to allocating security resources for the RF

IAS is presented, along with possible protective measures. **Conclusion.** The need for a comprehensive approach to ensuring the protection of the RF IAS is emphasized, utilizing both software and hardware protection.

Keywords: information system, prioritization, internal affairs agencies, allocation of resources, protection measures.

For citation: A.I. Yangirov, E.A. Rogozin, S.B. Akhlyustin. Allocation of resources for the protection of automated systems of the internal affairs bodies of the Russian Federation and their implementation. Herald of Daghestan State Technical University. Technical Sciences. 2026;53(1):193-199. (In Russ) DOI:10.21822/2073-6185-2026-53-1-193-199.

Введение. BIOS (Basic Input-Output System) и его современный аналог UEFI (Unified Extensible Firmware Interface) являются ключевыми компонентами в процессе загрузки многих АС ОВД РФ. Эти компоненты, выполняющие критически важные функции инициализации оборудования и запуска операционной системы (ОС,) с каждым годом становятся все более привлекательными целями для злоумышленников.

На этом этапе злоумышленники могут внедрить вредоносный код, который останется незамеченным для традиционных средств защиты. BIOS (или UEFI), будучи низкоуровневым программным обеспечением, уязвим к различным видам атак.

Атаки можно разделить на три категории: внешние угрозы; внутренние угрозы; угрозы, вызванные техническими сбоями.

К внешним угрозам относятся атаки, осуществляемые удаленно или через физический доступ к оборудованию.

Например, эксплуатация уязвимостей в сетевых интерфейсах, позволяющих злоумышленнику модифицировать прошивку без прямого контакта с устройством. Особую опасность представляют атаки, направленные на подмену кода BIOS до загрузки ОС. Методы подобные Bootkit или Rootkit позволяют злоумышленникам сохранять работоспособность вредоносных программ даже после переустановки ОС. Одной из последних подобных атак стала обнаруженная в 2018 году уязвимость в UEFI, позволяющая выполнять код через поддельные обновления [1].

К внутренним угрозам могут быть отнесены действия инсайдеров или применение вредоносного программного обеспечения, которое уже получило привилегии в системе. Например, вредоносные программы, способные перезаписать BIOS через уязвимости в драйверах или системных утилитах.

Угрозы, вызванные техническими сбоями, также могут повлиять на работоспособность системы и защиты АС ОВД РФ. Ошибки в коде BIOS (или UEFI), сбои питания или некорректные обновления могут привести к повреждению прошивки, что сделает устройство неработоспособным или уязвимым для последующих атак.

Постановка задачи. Разработка эффективной стратегии защиты АС ОВД РФ требует научно обоснованного подхода к распределению ресурсов. В настоящем исследовании рассматривается приоритизация при распределении мер защиты.

Методы исследования. Исследование основано на анализе угроз из банка данных ФСТЭК России, а также различных источников научной литературы, публикаций и интернет-ресурсов.

Обсуждение результатов. Вопросы защиты автоматизированных систем рассматривались в следующих исследованиях [2-4]. Базовые системы ввода-вывода современных компьютеров представляют собой сложные программно-аппаратные комплексы, уязвимости в которых могут быть использованы для реализации особо опасных атак.

В отличие от угроз ОС, атаки на BIOS/UEFI обладают рядом уникальных особенностей, делающих их исключительно опасными.

1. Они действуют на более низком уровне, чем традиционное вредоносное программное обеспечение;

2. Компрометация BIOS/UEFI сохраняется даже после переустановки ОС или замены жесткого диска;
3. Современные BIOS/UEFI обладают сетевыми возможностями, что потенциально позволяет проводить атаки удаленно.

Современные исследования демонстрируют несколько ключевых векторов атак на BIOS/UEFI. Наиболее распространенным является модификация прошивки с целью внедрения постоянно действующего вредоносного кода. Такие атаки могут осуществляться как с физическим доступом к оборудованию, так и через уязвимости в механизмах обновления прошивки. Другим опасным сценарием является подмена или модификация модулей BIOS/UEFI, которые могут выполняться на ранних этапах загрузки системы.

Приоритезация защитных мер должна учитывать не только частоту угроз, но и их потенциальный ущерб. Хотя угроз BIOS/UEFI значительно меньше, чем угроз ОС, их реализация может привести к не менее катастрофическим последствиям.

Поэтому защита BIOS требует качественно иных подходов, часто включающих аппаратные решения. Современные системы защиты BIOS/UEFI должны обеспечивать три ключевых функции: контроль целостности прошивки, защиту от несанкционированной модификации и механизмы безопасного восстановления.

Разработка эффективной стратегии защиты требует научно обоснованного подхода к распределению ресурсов. Основываясь на данных ФСТЭК России, можно вывести оптимальное соотношение мер защиты [5].

В банке данных угроз ФСТЭК России по состоянию на 26.04.2025 г. 222 угрозы. Угрозы в банке данных угроз ФСТЭК России представлены в следующих видах (рис. 1-3). К каждой из 222 угроз представлено описание с указанием того, откуда могут поступать эти самые угрозы (от внешних нарушителей, от внутренних нарушителей или от внешних и внутренних нарушителей).

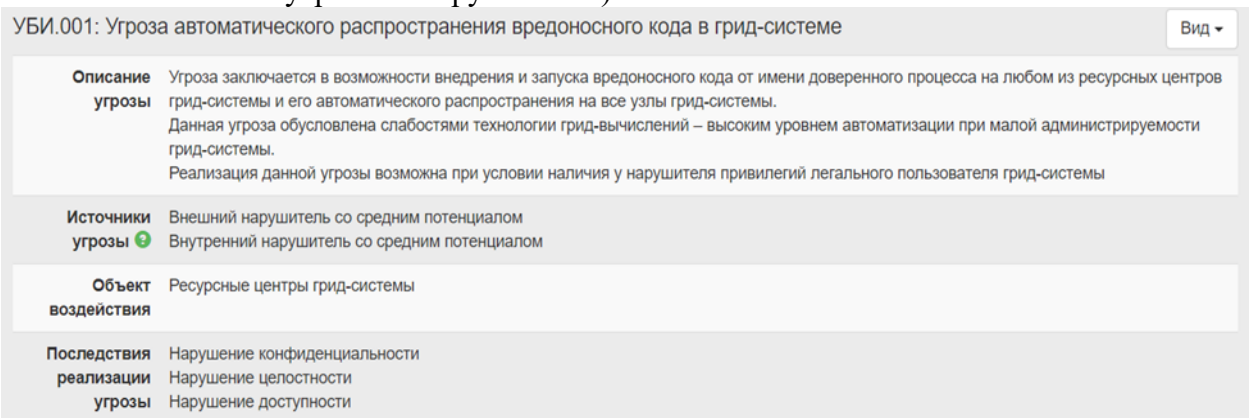

Рис. 1 – Вариант представления угроз в банке данных угроз ФСТЭК России
Fig. 1 – Option for representing threats in the FSTEC of Russia threat database

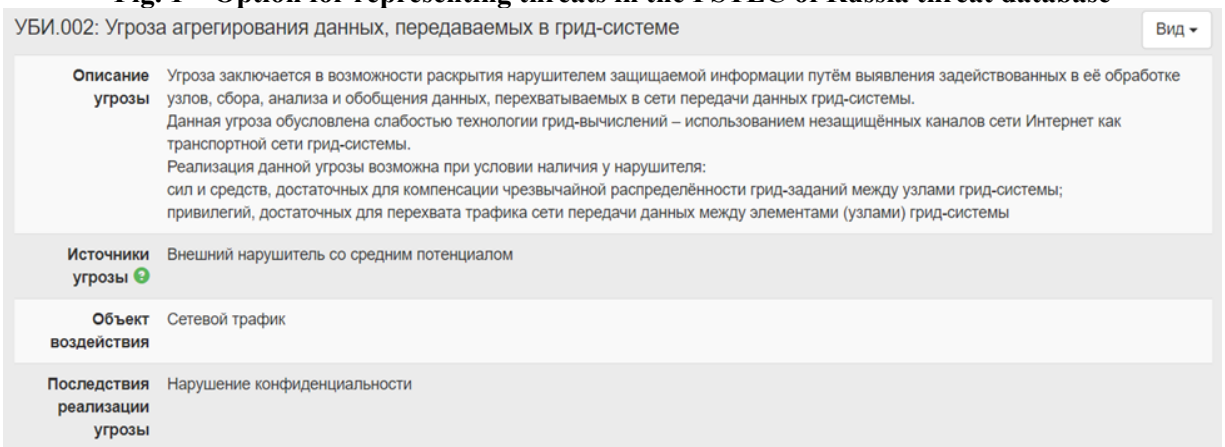

Рис. 2 – Вариант представления угроз в банке данных угроз ФСТЭК России
Fig. 2 – Option for representing threats in the FSTEC of Russia threat database

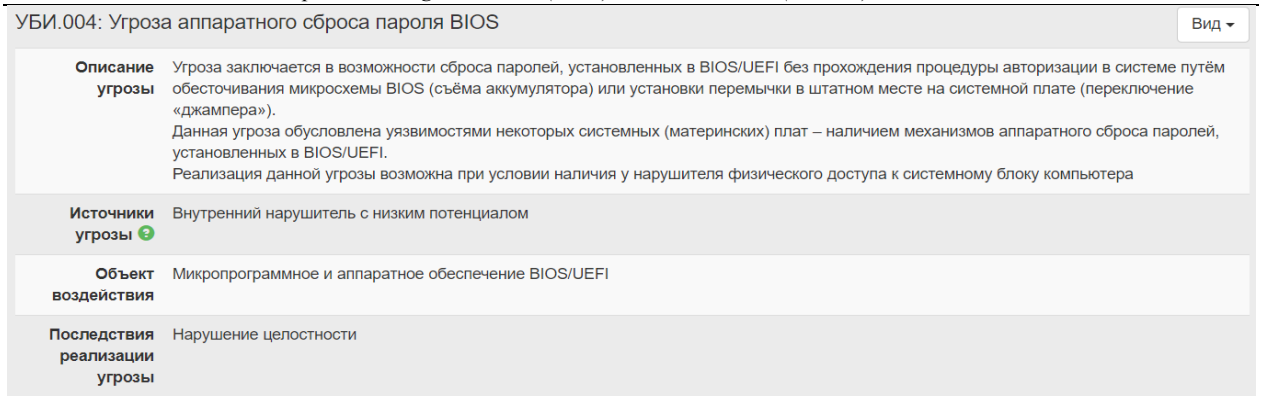

Рис. 3 – Вариант представления угроз в банке данных угроз ФСТЭК России
Fig. 3 – Option for representing threats in the FSTEC of Russia threat database

Также, кроме представленных вариантов, есть угрозы, которые не поступают от внешних или внутренних нарушителей (рис. 4), а могут возникнуть сами по себе из-за технического сбоя или ошибок (человеческого фактора).

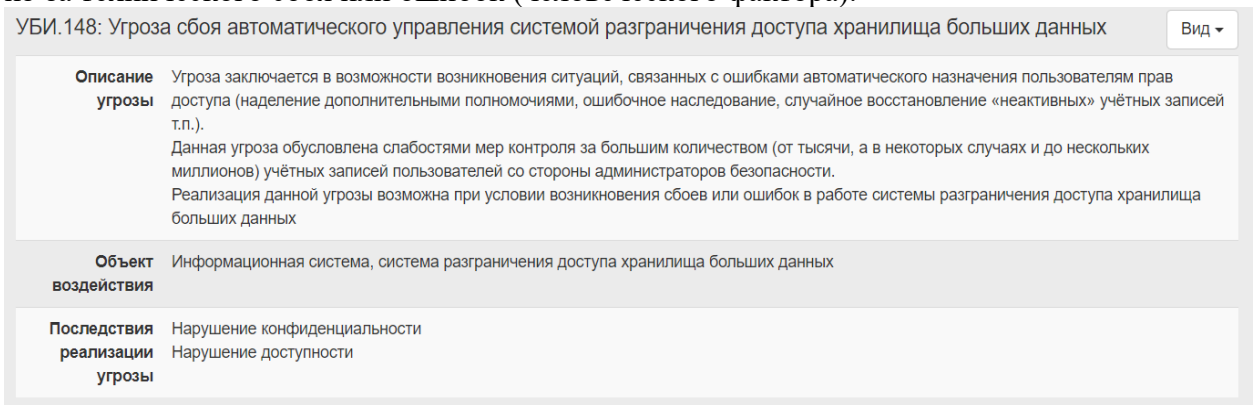

Рис. 4 – Вариант представления угроз в банке данных угроз ФСТЭК России
Fig. 4 – Option for representing threats in the FSTEC of Russia threat database

Если учитывать откуда могут поступить эти угрозы от внешнего нарушителя, от внутреннего нарушителя или из-за различных ошибок, то общее количество угроз возрастает до 321 из них: внешние угрозы: 166; внутренние угрозы: 153; угрозы из-за технического сбоя, ошибок (человеческого фактора): 2.

На открытые ОС могут быть воздействия, в том числе, через BIOS/UEFI, с помощью простого физического воздействия, а не только программным, аппаратным или программно-аппаратным способом. А значит, при защите открытых ОС должны быть, в том числе приняты и такие меры, которые бы позволяли защититься от таких угроз.

Из этих 321 угрозы на BIOS могут повлиять 18. А на физическую защиту в базе данных ФСТЭК представлена 1 единственная угроза (рис. 5).

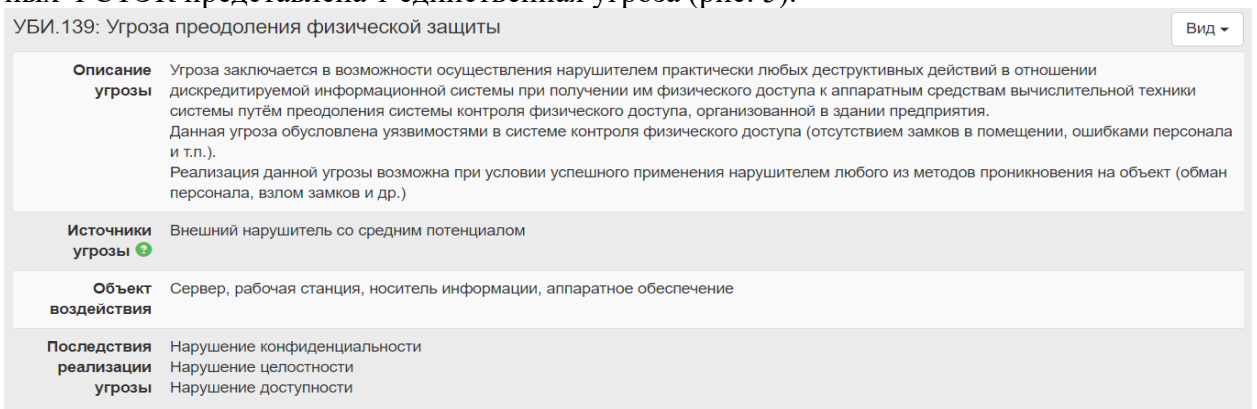

Рис. 5 – Угроза преодоления физической защиты в банке данных угроз ФСТЭК России
Fig. 5 – Threat to overcome physical security in the FSTEC of Russia threat database

Полученные статистические значения могут быть использованы в рамках методики количественной оценки защищенности открытых ОС [6] в процентном соотношении:

1) угрозы, воздействующие на открытую ОС: 302 (94%);

2) угрозы, воздействующие на BIOS: 18 (5,6%);

3) угроза физического воздействия: 1 (0,31%).

Исходя из произведенных расчетов, 94% мер следует направлять на защиту ОС, 5,6% – на обеспечение безопасности BIOS/UEFI, и 0,31% – на физическую защиту.

Основной объем защитных мер, как показывает статистика, должен быть направлен на обеспечение безопасности ОС. Современные подходы к защите ОС включают многоуровневую систему безопасности, сочетающую превентивные, детективные и реагирующие меры. Наиболее эффективными являются системы мониторинга целостности, обеспечивающие контроль критически важных системных файлов, реестра и конфигураций.

Особое внимание уделяется механизмам разграничения доступа и минимальных привилегий. Современные ОС реализуют сложные модели управления правами пользователей, позволяющие минимизировать потенциальный ущерб от компрометации учетных записей. Важным компонентом защиты являются системы обнаружения вторжений, анализирующие аномальную активность и подозрительное поведение процессов.

Защита базовой системы ввода-вывода требует специальных аппаратных решений, так как традиционные программные методы неэффективны на этапе до загрузки ОС. Одним из наиболее перспективных направлений является использование доверенных платформенных модулей (TPM), которые могут хранить криптографические ключи и обеспечивать проверку целостности прошивки (рис. 6).

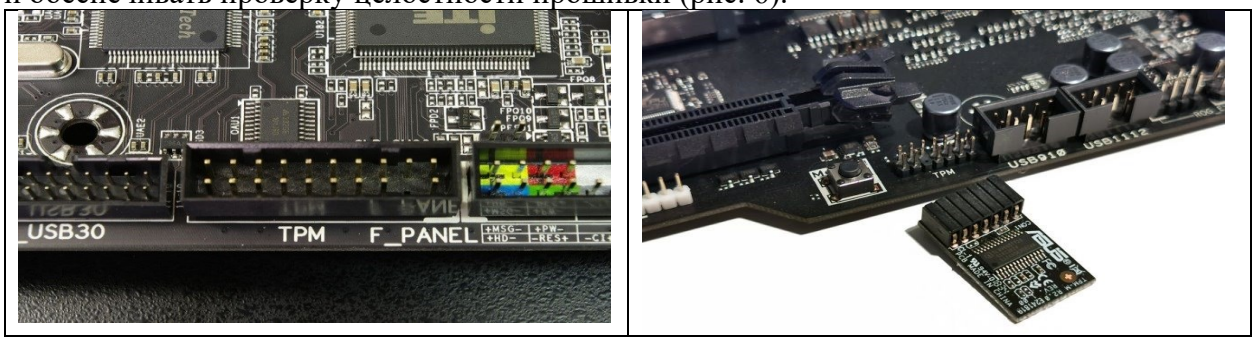

Рис. 6 – Доверенный платформенный модуль (TPM)
Fig. 6 – Trusted Platform Module (TPM)

Современные подходы к защите BIOS/UEFI включают несколько ключевых технологий. Технология безопасной загрузки (Secure Boot) обеспечивает проверку цифровых подписей всех компонентов, загружаемых до ОС.

Аппаратные механизмы защиты от записи в чип BIOS/UEFI предотвращают несанкционированную модификацию прошивки. Решения на основе изолированных исполняемых сред (Trusted Execution Environment) позволяют выполнять критические операции защиты в безопасном окружении.

Хотя угрозы физического уровня составляют лишь небольшую долю от общего числа, их важность нельзя недооценивать. Физическая безопасность включает несколько аспектов: контроль доступа к оборудованию, защиту от перехвата данных через побочные каналы, противодействие аппаратным закладкам. Особое значение физическая защита приобретает в условиях, когда злоумышленник может получить непосредственный доступ к оборудованию.

Современные подходы к физической защите включают использование специализированных корпусов с датчиками вскрытия, системы видеонаблюдения и контроля доступа, защитные покрытия, затрудняющие физический анализ чипов.

Для критически важных систем применяются методы активного противодействия, включая механизмы самоуничтожения данных при попытке несанкционированного доступа. Например, Transcend предлагает SATA 3 SSD в различных форм-факторах,

которые могут поставляться с функцией аппаратного стирания для возможности быстрого и безопасного стирания данных (рис. 7).

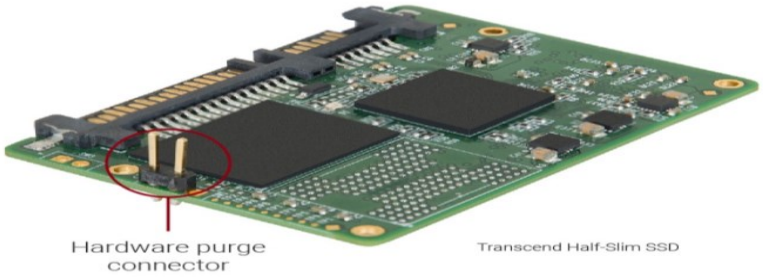

Рис. 7 – SATA 3 SSD с функцией аппаратного стирания
Fig. 7 – SATA 3 SSD with hardware erase function

При замыкании контактов аппаратного стирания, активируется функция быстрого стирания, и все данные, записанные на накопитель, полностью стираются. Стертые данные не подлежат восстановлению, это значит, что вся конфиденциальная информация была уничтожена [7].

Эффективная защита АС ОВД РФ требует не просто набора отдельных мер, а их тщательной интеграции в единый комплекс. Особое внимание должно уделяться взаимодействию между защитными механизмами разных уровней.

Например, система защиты BIOS/UEFI может быть согласована с механизмами безопасности ОС, создавая непрерывную цепочку доверия от момента включения питания до полной загрузки системы. Развитие технологий защиты должно идти параллельно с эволюцией угроз. Одним из наиболее перспективных направлений является использование технологий искусственного интеллекта и машинного обучения для прогнозирования и предотвращения атак. Эти технологии особенно эффективны для анализа больших объемов данных безопасности и выявления сложных аномалий.

Другим перспективным направлением может стать развитие концепции «нулевого доверия» (Zero Trust), которая предполагает постоянную проверку всех компонентов системы, независимо от их местоположения или предполагаемого уровня доверия. Эта концепция особенно актуальна для защиты BIOS/UEFI и других низкоуровневых компонентов.

Вывод. Проведенные исследования демонстрируют необходимость комплексного подхода к защите АС ОВД ОФ, учитывающего как количественные показатели угроз, так и их качественные характеристики. Хотя статистика показывает, что основное внимание следует уделять защите ОС, безопасность BIOS/UEFI также требует особых, часто аппаратных решений, несмотря на меньшую долю соответствующих угроз.

Оптимальная стратегия защиты должна основываться на тщательном анализе рисков, учитывающем как вероятность реализации угроз, так и потенциальный ущерб. При этом особое внимание следует уделять интеграции защитных механизмов разных уровней, создавая единую, взаимосвязанную систему безопасности. Предлагаемый системный подход может обеспечить надежную защиту современных АС ОВД РФ от большинства известных угроз.

Библиографический список:

1. LoJax: первый известный UEFI руткит, используемый во вредоносной кампании // ESET URL: https://www.esetnod32.ru/upload/iblock/24b/03.10.2018-LoJax_pervyy-izvestnyy-UEFI-rutkit_-ispolzuemyy-vo-vredonosnoy-kampanii.pdf (дата обращения: 26.04.2025).
2. Мониторинг операционной системы как средство защиты информации/ А.Ю. Лабинский //Природные и техногенные риски (физико-математические и прикладные аспекты). –2024.– № 1(49). - С.16-23. DOI 10.61260/2307-7476-2024-1-16-23. EDN RKKXYG.
3. Защита персонального компьютера на уровне / Е.Н. Дорожкин // Информационные технологии обеспечения комплексной безопасности в цифровом обществе: сборник материалов IV Всероссийской молодежной научно-практической конференции с международным участием, Уфа, 21–22 мая 2021 года. – Уфа: Башкирский государственный университет, 2021. – С. 192-194. – EDN FYFTNZ.

4. Подход к повышению уровня доверия к аппаратно-программным платформам информационных систем критически важных инфраструктур в целях предупреждения компьютерных атак с использованием уязвимостей в ПО BIOS / А.Ю. Боровиков, О.А. Маслов, С. Е. Кузнецов, И.А. Козлов // Наноиндустрия. – 2021. – Т. 14, № S7(107). – С. 338-339. – DOI 10.22184/1993-8578.2021.14.7s.338.339. – EDN KDYCTC.
5. Банк данных угроз безопасности информации – [Электронный ресурс] – Режим доступа. – URL: https://bdu.fstec.ru/ (Дата обращения: 26.04.2025).
6. Методический подход к количественной оценке защищенности открытых операционных систем АС ОВД / А.И. Янгиров, И.М. Янгиров, Е.А. Рогозин, С.Б. Ахлюстин // Вестник Дагестанского государственного технического университета. Технические науки. 2024;51(3):163-171. https://doi.org/10.21822/2073-6185-2024-51-3-163-171.
7. Аппаратное уничтожение данных // Transcend Information. Inc. URL: https://ru.transcend-info.com/embedded/technology/hardware-purge (дата обращения: 26.04.2025).

References:

1. LoJax: the first known UEFI rootkit used in a malicious campaign // ESET URL: https://www.esetnod32.ru/upload/iblock/24b/03.10.2018-LoJax_pervyy-izvestnyy-UEFI-rutkit_-ispolzue-myy-vo-vredonosnoy-kampanii.pdf (date of request: 04.26.2025).
2. Monitoring of the operating system as a means of information protection / A.Y. Labinsky. *Natural and man-made risks (physico-mathematical and applied aspects).* 2024;1(49):16-23. DOI 10.61260/2307-7476-2024-1-16-23. – EDN RKKXYG.
3. Personal computer protection at the level / E.N. Dorozhkin // Information technologies for ensuring integrated security in a digital society: collection of materials of the IV All-Russian Youth Scientific and Practical Conference with international participation, Ufa, May 21-22, 2021. Ufa: Bashkir State University, 2021;192-194. EDN FYFTNZ.
4. An approach to increasing the level of trust in hardware and software platforms of information systems of critical infrastructures in order to prevent computer attacks using vulnerabilities in BIOS software / A.Y. Borovikov, O.A. Maslov, S.E. Kuznetsov, I.A. Kozlov. *Nanoindustria.* 2021;14(S7(107):338-339. – DOI 10.22184/1993-8578.2021.14.7s.338.339. – EDN KDYCTC.
5. Data bank of information security threats – [Electronic resource] – Access mode. – URL: https://bdu.fstec.ru / (Date of request: 04.26.2025).
6. Methodological approach to quantitative assessment of the security of open operating systems AS of the Internal Affairs Bodies. A.I. Yangirov, I.M. Yangirov, E.A. Rogozin, S.B. Akhlyustin. *Herald of Dagestan State Technical University. Technical Sciences*. 2024;51(3):163-171. (In Russ) DOI.org/10.21822/2073-6185-2024-51-3-163-171.
7. https://ru.transcend-info.com/embedded/technology/hardware-purge (date of request: 04.26.2025). Hardware data destruction. *Transcend Information. Inc*.

Сведения об авторах:

Адиль Илдарович Янгиров, начальник отделения лабораторных исследований и испытаний; adil-yan@yandex.ru

Евгений Алексеевич Рогозин, доктор технических наук, профессор, профессор кафедры автоматизированных информационных систем ОВД; evgenirogozin@yandex.ru

Атласов Игорь Викторович, доктор физико-математических наук, профессор, профессор кафедры естественнонаучных дисциплин учебно-научного комплекса информационных технологий; mathematic1@rambler.ru

Ахлюстин Сергей Борисович, кандидат технических наук, начальник кафедры тактико–специальной подготовки, Воронежский институт МВД России; cerg7676@yandex.ru

Information about authors:

Adil I. Yangirov, Head of the Laboratory Research and Testing; adil-yan@yandex.ru

Evgeny A. Rogozin, Dr. Sci. (Eng.), Assoc. Prof., Prof., Department of Automated Information Systems of Internal Affairs Bodies; evgenirogozin@yandex.ru

Igor V. Atlasov, Dr. Sci. (Physico-Mathemat.), Assoc. Prof., Prof., Department of Natural Sciences of the Educational and Scientific Complex of Information Technologies, Sciences; mathematic1@rambler.ru

Sergey B. Ahlyustin, Cand. Sci. (Eng.), Head of the department of tactical and special training; cerg7676@yandex.ru

Конфликт интересов/Conflict of interest.

Авторы заявляют об отсутствии конфликта интересов/The authors declare no conflict of interest.

Поступила в редакцию/Received 20.06.2025**.**

Одобрена после рецензирования/Reviced 17.08.2025.

Принята в печать/Accepted for publication 16.01.2026.