Бетин В.В., Мордвинова А.Ю. Исследование категорий нарушителей и спектра их потенциальных возможностей// Международный журнал информационных технологий и энергоэффективности.– 2026. –Т. 11 № 6(68) Ч.1 с. 112–116

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/



УДК 004.056

ИССЛЕДОВАНИЕ КАТЕГОРИЙ НАРУШИТЕЛЕЙ И СПЕКТРА ИХ ПОТЕНЦИАЛЬНЫХ ВОЗМОЖНОСТЕЙ

Бетин В.В., [1]**Мордвинова А.Ю**.
ФГАОУ ВО "СЕВАСТОПОЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ", Севастополь, Россия (299053, город Севастополь, Университетская ул., зд. 33), e-mail: [1] aumordvinova@mail.sevsu.ru

Статья анализирует актуальные угрозы кибербезопасности в условиях цифровизации, опираясь на статистику Роскомнадзора и классификацию ФСТЭК России. Рассматриваются типы нарушителей — внешние и внутренние, — а также их градация по уровням возможностей (от В.1 до В.4). Обсуждается степень опасности каждого класса с примерами атак и предлагаются targeted меры защиты: от базовых обновлений ПО для новичков до многоуровневых стратегий против государственных спецслужб. Материал подчеркивает важность адаптированных подходов для надежной охраны информационных систем.

Ключевые слова: Кибератаки, нарушители ИБ, классификация ФСТЭК, внешние угрозы, внутренние угрозы, уровни возможностей, защита информации, zero trust; цепочка поставок, национальная безопасность.

A STUDY OF INVULNER CATEGORIES AND THEIR RANGE OF POTENTIAL CAPABILITIES

Betin V.V., [1]Mordvinova A. Yu.
SEVASTOPOL STATE UNIVERSITY, Sevastopol, Russia (299053, Sevastopol, Universitetskaya st., 33), e-mail: [1] aumordvinova@mail.sevsu.ru

This article analyzes current cybersecurity threats in the context of digitalization, based on Roskomnadzor statistics and the classification of the Federal Service for Technical and Export Control of Russia. The article examines the types of intruders—external and internal—as well as their gradation by capability level (from B.1 to B.4). The danger level of each class is discussed, with attack examples and targeted security measures proposed, ranging from basic software updates for beginners to multi-layered strategies against government intelligence agencies. The material emphasizes the importance of tailored approaches for reliably protecting information systems.

Keywords: Cyberattacks, information security violators, FSTEC classification, external threats, internal threats, capability levels, information security, zero trust; supply chain, national security.

В эпоху цифровизации, нарушение информационной безопасности угрожает не только государственным учреждениям и частным компаниям, но и каждому пользователю глобальной сети. По данным Роскомнадзора в третьем квартале 2025 года произошло около 42 000 кибератак – 40% от общего числа компьютерных инцидентов за год. [1] Нарушители информационной безопасности – это основные исполнители большинства инцидентов в информационных инфраструктурах. Понимание их видов и способностей помогает выстраивать эффективную защиту информационной системы.

На данный момент нарушителей классифицирует ФСТЭК России, а именно в банке данных угроз ФСТЭК. Согласно данному документу, выделяют следующие виды нарушителей:

1. Внешние нарушители: специальные службы иностранных государств; террористические, экстремистские группировки; преступные группы (криминальные структуры); отдельные физические лица (хакеры); конкурирующие организации; лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем; бывшие работники (пользователи).

2. Внутренние нарушители: разработчики программных, программно-аппаратных средств; поставщики вычислительных услуг, услуг связи; лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ; лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора (администрация, охрана, уборщики и т. д.); авторизованные пользователи систем и сетей; системные администраторы и администраторы безопасности.

Также, согласно данному нормативному акту, нарушители классифицируются по категориям возможности, В.1 – В.4. Рассмотрим подробнее каждый из них.

Категория В.1: Нарушитель с базовыми возможностями.

Характеристики: использует только известные уязвимости, скрипты и общедоступные инструменты; обладает минимальными знаниями механизмов функционирования вредоносного ПО; имеет базовые компьютерные навыки на уровне пользователя; может осуществлять физические воздействия при наличии доступа к техническим средствам.

Типы нарушителей: физическое лицо (хакер); лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем; лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора (администрация, охрана, уборщики и т.д.); авторизованные пользователи систем и сетей; бывшие работники (пользователи).

Особенности реализации угроз: способны реализовать только известные угрозы, направленные на задокументированные уязвимости; используют общедоступные инструменты и данные из сети «Интернет»; ограничены в возможности реализации атак ; не разрабатывают собственные вредоносные программы.

Категория В.2: Нарушитель с базовыми повышенными возможностями.

Характеристики: хорошо владеет общедоступными средствами реализации угроз; понимает принципы работы инструментов и может вносить изменения для повышения эффективности; обладает фреймворками и наборами специализированных инструментов; имеет навыки самостоятельного планирования сценариев угроз; знаком с защитными механизмами программного обеспечения; обладает практическими знаниями о функционировании систем и сетей.[2]

Типы нарушителей: преступные группы (два лица и более, действующие по единому плану); конкурирующие организации; поставщики вычислительных услуг, услуг связи; лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ; системные администраторы и администраторы безопасности.

Особенности реализации угроз: способны реализовывать угрозы, направленные на недокументированные уязвимости; используют специально созданные инструменты, свободно распространяемые в Интернете; не имеют возможности атаковать физически изолированные сегменты систем; могут координировать действия в рамках группы.

Категория В.3: Нарушитель со средними возможностями.

Характеристики: имеет доступ к специализированным платным ресурсам (биржам уязвимостей); может приобретать дорогостоящие средства и инструменты для реализации угроз; способен самостоятельно разрабатывать инструменты для атак; имеет доступ к анализу встраиваемого ПО, системного и прикладного ПО; обладает навыками анализа программного кода для выявления уязвимостей; имеет глубокое понимание защитных механизмов; может действовать в составе группы специалистов.

Типы нарушителей: террористические, экстремистские группировки; разработчики программных, программно-аппаратных средств.[3]

Особенности реализации угроз: способны реализовывать угрозы на выявленные ими неизвестные уязвимости; используют самостоятельно разработанные инструменты; не имеют возможностей для атак на физически изолированные сегменты систем; обладают организационной структурой для координации атак.

Категория В.4: Нарушитель с высокими возможностями.

Характеристики: имеет доступ к исходному коду программного обеспечения для выявления уязвимостей «нулевого дня»; способен внедрять программные и программно-аппаратные закладки на этапах поставки; может создавать методы и средства реализации угроз с привлечением научных организаций; имеет возможность привлекать специалистов разных категорий возможностей; создает и применяет специальные технические средства для добывания информации через физические поля; способен долговременно и незаметно реализовывать угрозы; обладает исключительными знаниями о конкретных защитных механизмах атакуемых систем.

Типы нарушителей: специальные службы иностранных государств.

Особенности реализации угроз: имеют практически неограниченные возможности реализации угроз; используют недекларированные возможности и закладки, встроенные в компоненты систем; способны атаковать физически изолированные сегменты; обладают значительными ресурсами и государственной поддержкой; могут осуществлять долгосрочные операции по сбору информации.

Далее проведем анализ опасности данных классов нарушителей. Анализ представлен в порядке от самого опасного класса до менее опасного.

Класс нарушителя В.4 Тип нарушителя: Внешний Вид нарушителя: Специальные службы иностранных государств. Способности нарушителя: предоставляет угрозу национальной безопасности; обладает неограниченными возможностями; использует самые современные методы и средства. Пример атаки: атаки на критическую инфраструктуру России, шпионаж в военной и промышленной сферах.

Класс нарушителя В.3 Тип нарушителя: Внешний Вид нарушителя: Террористические и экстремистские группировки. [4] Способности нарушителя: дестабилизация общественной безопасности; использование информационных технологий для пропаганды и координации действий; атака на системы жизнеобеспечения. Пример атаки: атаки на системы управления транспортом, энергетическими объектами.

Класс нарушителя В.2 Тип нарушителя: Внутренний Вид нарушителя: Системные администраторы и администраторы безопасности. Способности нарушителя: максимальный уровень легального доступа; знание архитектуры и защитных механизмов сети; маскируют

свои действия под легитимные операции. Пример атаки: кража конфиденциальной информации, установка бэкдоров.

Класс нарушителя В.3 Тип нарушителя: Внутренний Вид нарушителя: Разработчики программных средств. Способности нарушителя: имеют доступ к исходным кодам приложений; могут внедрять скрытые функции и закладки; знакомы с внутренней архитектурой защищаемых систем. Пример атаки: внедрение троянов в банковское ПО, закладки в системное ПО.[5]

Класс нарушителя В.1 Тип нарушителя: Внешний Вид нарушителя: Хакеры-одиночки. Способности нарушителя: часто действуют из любопытства или для демонстрации своих возможностей; используют готовые инструменты и скрипты; ориентированы на массовые атаки на уязвимые системы. Пример атаки: взлом сайтов, DDoS-атаки на доступные ресурсы.

Класс нарушителя В.1 Тип нарушителя: Внутренний Вид нарушителя: Авторизованные пользователи и персонал. Способности нарушителя: могут случайно или намеренно нарушать политики безопасности; часто являются источником утечек из-за неосторожности; могут передавать учетные данные третьим лицам. Пример атаки: передача паролей, подключение несанкционированных устройств.

Теперь, когда были определены возможности и опасность нарушителей, рассмотрим рекомендации по защите от данных категорий нарушителей. Первоначально рассмотрим защиту от нарушителей категории В.1: Регулярное обновление ПО для закрытия известных уязвимостей. Базовое обучение пользователей основам ИБ. Контроль физического доступа к техническим помещениям. Простые, но эффективные парольные политики. Антивирусная защита и базовые средства обнаружения вторжений.

Защита от нарушителей категории В.2: Внедрение систем обнаружения аномального поведения. Разграничение прав доступа по принципу минимальных привилегий. Регулярный аудит действий администраторов и привилегированных пользователей. Контроль подключаемых устройств и внешних носителей. Внедрение систем предотвращения утечек данных (DLP)

Защита от нарушителей категории В.3: Глубокий анализ трафика и поведения в сети. Использование средств защиты от неизвестных угроз (песочницы, машинное обучение). Контроль цепочки поставок программного и аппаратного обеспечения. Внедрение принципа нулевого доверия (Zero Trust). Регулярное тестирование на проникновение силами независимых экспертов.

Защита от нарушителей категории В.4: Физическая изоляция критически важных сегментов. Использование отечественного оборудования и ПО с открытым кодом. Внедрение многоуровневых систем защиты с разными вендорами. Постоянный мониторинг на наличие скрытых закладок и аномальной активности. Взаимодействие со спецслужбами и участие в государственных программах защиты. Проведение регулярных проверок на электромагнитные утечки.

Таким образом, понимание классификации нарушителей информационной безопасности является ключевым элементом в построении эффективной системы защиты. Каждая категория нарушителей требует разработки специфических мер противодействия, соответствующих их возможностям и целям.

Список литературы

1. Россия под атакой. Под ударом хакеров телекоммуникации, ИТ и финансовый сектор // Cnews : сайт. – URL: https://www.cnews.ru/news/top/2025-11-05_s_iyulya_po_sentyabr_2025_goda.
2. БДУ ФСТЭК России - Нарушители // ФСТЭК России : сайт. – URL: https://bdu.fstec.ru/threat-section/potential
3. Карцан И.Н., Мордвинова А.Ю. Система управления информационными рисками. В сборнике: Вопросы контроля хозяйственной деятельности и финансового аудита, национальной безопасности, системного анализа и управления. Материалы VII Всероссийской научно-практической конференции. Москва, 2022. С. 141-146.
4. Мордвинова А.Ю., Нуриев С.А. Исследование уязвимостей и угроз безопасности стандарта IEEE 802.11. Современные инновации, системы и технологии. 2023. Т. 3. № 3. С. 117-131.
5. Мордвинова А.Ю., Жуков А.О., Аверьянов В.С., Карцан И.Н. Нейросетевая обработка информации в социокиберфизичеких системах. Информационные и телекоммуникационные технологии. 2021. № 52. С. 8-12.

References

1. Russia Under Attack. Telecommunications, IT, and the Financial Sector Under Hacker Attack // Cnews: website. – URL: https://www.cnews.ru/news/top/2025-11-05_s__iyulya_po_sentyabr_2025_goda.
2. BDU FSTEC of Russia - Violators // FSTEC of Russia: website. – URL: https://bdu.fstec.ru/threat-section/potential
3. Kartsan I.N., Mordvinova A.Yu. Information Risk Management System. In the collection: Issues of Control over Economic Activity and Financial Audit, National Security, Systems Analysis and Management. Proceedings of the VII All-Russian Scientific and Practical Conference. Moscow, 2022. pp. 141-146.
4. Mordvinova A.Yu., Nuriyev S.A. Study of Vulnerabilities and Security Threats of the IEEE 802.11 Standard. Modern Innovations, Systems, and Technologies. 2023. Vol. 3. No. 3. pp. 117-131.
5. Mordvinova A.Yu., Zhukov A.O., Averyanov V.S., Kartsan I.N. Neural Network Information Processing in Sociocyber-Physical Systems. Information and Telecommunication Technologies. 2021. No. 52. pp. 8-12.