Бурцев Михаил Николаевич,
магистр 1го курса,
Информационная безопасность
Санкт-Петербургский государственный университет телекоммуникаций
им. проф. М.А. Бонч-Бруевича
Россия, Санкт-Петербург

ОЦЕНКА ЭФФЕКТИВНОСТИ СИСТЕМ ЗАЩИТЫ ОТ НЕСАНКЦИОНИРОВАННОГО ПОДКЛЮЧЕНИЯ ВРЕДОНОСНЫХ АППАРАТНЫХ МОДУЛЕЙ В КОРПОРАТИВНОЙ СРЕДЕ

Аннотация. Статья посвящена проблеме защиты корпоративной инфраструктуры от несанкционированного подключения вредоносных аппаратных модулей. Рассматриваются типы угроз, возникающие при использовании аппаратных средств атаки, приводится обзор существующих систем защиты, включая аппаратные и программные решения. Описана методика комплексной оценки эффективности на основе нормированных критериев, учитывающих долю блокировки подключений, частоту ложных срабатываний, время обнаружения угрозы и удобство администрирования. Приведены примеры расчётов показателей эффективности для различных классов защитных систем.

Ключевые слова:Информационная безопасность, корпоративная сеть, вредоносные аппаратные модули, контроль устройств, мониторинг подключений, предотвращение угроз, оценка эффективности, аппаратные средства защиты, программные политики, физическая безопасность, системы контроля доступа, защита от вторжений, киберугрозы, корпоративная защита данных.

Annotation The article is devoted to the problem of protecting corporate infrastructure from unauthorized connection of malicious hardware modules. The types of threats that arise when using hardware attack tools are considered, and an overview of existing protection systems, including hardware and software solutions, is provided. A methodology for a comprehensive assessment of effectiveness based on standardized

criteria is described, taking into account the proportion of connection blocking, the frequency of false alarms, the time of threat detection and the convenience of administration. Examples of calculations of efficiency indicators for various classes of protective systems are given.

Keywords: Information security, corporate network, malicious hardware modules, device control, connection monitoring, threat prevention, performance assessment, hardware protection, software policies, physical security, access control systems, intrusion protection, cyber threats, corporate data protection.

В условиях стремительной цифровизации корпоративной инфраструктуры возрастает угроза несанкционированного подключения вредоносных аппаратных модулей, таких как USB-устройства, способных нарушить информационную безопасность организаций. Современные киберпреступники активно используют подобные методы для обхода традиционных средств защиты и получения несанкционированного доступа к конфиденциальным данным [1].

Согласно отчету компании RED Security, в 2024 году количество кибератак на российские компании увеличилось в 2,5 раза по сравнению с предыдущим годом, достигнув почти 130 тысяч инцидентов. Примечательно, что около 45% атак на промышленный сектор происходили в нерабочее время, что свидетельствует о целенаправленном использовании уязвимостей в периоды сниженного контроля [2,3].

Особую опасность представляют вредоносные аппаратные модули, такие как USB Rubber Ducky и Malduino, которые могут быть использованы для внедрения шпионского ПО или получения удаленного доступа к корпоративным системам. Эти устройства способны обходить традиционные средства защиты, что делает их эффективным инструментом в арсенале киберпреступников.

В связи с этим актуальной задачей является оценка эффективности существующих систем защиты от несанкционированного подключения вредоносных аппаратных модулей в корпоративной среде. Данная статья направлена на анализ текущих угроз, обзор существующих решений и

разработку методики оценки их эффективности для обеспечения надежной защиты корпоративной информации.

В корпоративной среде подключение внешних аппаратных устройств традиционно рассматривается как потенциальная угроза информационной безопасности. Вредоносные аппаратные модули представляют собой устройства, которые могут быть физически подключены к корпоративным компьютерам, серверам или сетевому оборудованию с целью нарушения работы систем, кражи данных, установки вредоносного программного обеспечения или создания каналов несанкционированного доступа.

Одной из основных категорий подобных угроз являются устройства имитации HID (Human Interface Device), такие как USB Rubber Ducky, Malduino и их аналоги. Эти устройства внешне напоминают обычные флеш-накопители, однако после подключения к компьютеру они эмулируют клавиатуру, выполняя заранее запрограммированные команды: открытие терминала, загрузку и установку вредоносного ПО, изменение конфигураций безопасности и создание скрытых учетных записей.

Вторую важную категорию составляют шпионские устройства, маскирующиеся под стандартные элементы периферии (зарядные устройства, мыши, клавиатуры). Они способны незаметно осуществлять перехват данных с клавиатуры (кейлоггеры), запись экрана, аудио и видео, а также передавать полученную информацию злоумышленникам через скрытые радиоканалы или при последующем извлечении устройства.

Особую угрозу представляют устройства с функцией автоматического внедрения вредоносного кода в системы через использование уязвимостей операционных систем или драйверов [4]. Такие устройства способны обходить традиционные антивирусные решения, так как на уровне сетевой активности или файловой системы их действия могут оставаться незаметными до момента реализации атаки.

Важно отметить, что атаки с использованием вредоносных аппаратных модулей зачастую происходят в условиях частичного или полного отсутствия

физического контроля за рабочими местами, особенно в периоды технического обслуживания, сменной работы персонала или в помещениях с открытым доступом [5].

Для предотвращения угроз, связанных с несанкционированным подключением вредоносных аппаратных модулей, применяются различные технические и программные решения. Краткий обзор систем представлен в таблице 1.

Таблица 1. Классификация существующих систем защиты от подключения вредоносных аппаратных модулей

Класс системы	Описание	Примеры решений
Аппаратные блокировки портов	Физическая блокировка USB-портов с помощью замков или заглушек	USB Lock RP, Smart Keeper
Программные политики контроля устройств	Ограничение работы портов на уровне операционной системы или через политики безопасности	Microsoft Device Control (GPO), Symantec DLP
Системы мониторинга активности USB	Отслеживание всех событий подключения устройств с регистрацией и анализом	Safend Protector, Endpoint Protector
Специализированные решения для защиты	Детектирование и блокирование опасных HID-устройств, контроль типов подключаемых устройств	Cisco ISE, CrowdStrike Falcon Device Control

Для объективного анализа различных систем защиты от несанкционированного подключения вредоносных аппаратных модулей определены следующие ключевые критерии:

- P_{block} — доля успешно заблокированных попыток подключения (от 0 до 1). Чем выше значение, тем лучше система предотвращает угрозы.
- F_{false} — частота ложных срабатываний (от 0 до 1). Чем ниже значение, тем меньше система ошибочно блокирует легитимные устройства.

- T_{detect} — среднее время обнаружения вредоносного устройства (в секундах). Чем меньше время, тем быстрее реагирует система.
- U_{admin} — удобство администрирования системы, выраженное по экспертной шкале от 1 (очень неудобно) до 5 (очень удобно).

Данные параметры выбраны не случайно: они охватывают как техническую сторону безопасности, так и практическую сторону эксплуатации систем в реальной корпоративной среде.

Для расчёта общей эффективности введем следующую формулу 1:

$$E = \alpha \times P_{block} + \beta \times \left(1 - F_{false}\right) + \gamma \times \left(\frac{1}{T_{detect}}\right) + \delta \times \left(\frac{U_{admin}}{5}\right) \quad (1)$$

Где $\alpha, \beta, \gamma, \delta$ — весовые коэффициенты важности критериев:

- $\alpha = 0.4$ (главный упор на предотвращение угроз);
- $\beta = 0.3$ (важность уменьшения ложных срабатываний);
- $\gamma = 0.2$ (скорость обнаружения как важный, но менее критичный параметр);
- $\delta = 0.1$ (удобство управления, учитывающее эксплуатационные затраты).

Пояснение: значение P_{block} и выражение $1 - F_{false}$ находятся в прямой зависимости от итоговой эффективности системы: чем выше эти показатели, тем выше итоговое значение эффективности. Параметр T_{detect} включается в расчёт в обратной зависимости: чем быстрее происходит обнаружение угрозы (то есть чем меньше значение T_{detect}), тем выше общий показатель эффективности системы. Показатель U_{admin} нормализуется путем деления на максимальный балл 5, что позволяет привести его к единой шкале измерения с другими критериями.

Для анализа были выбраны три широко применяемых решения, что отображено в таблице 2.

Таблица 2. Выбранные решения для оценки эффективности

Система	Доля блокировок (P_{block})	Ложные срабатывания (F_{false})	Время обнаружения (T_{detect})	Удобство администрирования (U_{admin})
Аппаратная блокировка (USB Lock RP)	1.00	0.00	1	4
Программная политика (GPO Windows)	0.85	0.10	5	5

Продолжение таблицы 2

Система	Доля блокировок (P_{block})	Ложные срабатывания (F_{false})	Время обнаружения (T_{detect})	Удобство администрирования (U_{admin})
Мониторинг активности (Safend)	0.90	0.05	10	3

Значения, представленные в таблице 2, основаны на данных, опубликованных в технической документации производителей, обзорах независимых исследований, а также обобщённых результатах практического применения указанных систем в корпоративной среде. В частности, для аппаратной блокировки (USB Lock RP) принято значение доли блокировок P_{block} равное «1.00», поскольку физическая блокировка полностью предотвращает подключение устройств. Частота ложных срабатываний F_{false} принята равной «0.00», что отражает отсутствие необходимости различать устройства. Время обнаружения T_{detect} условно установлено как 1 секунда — фактически мгновенное действие, связанное с невозможностью физического подключения без ключа или снятия защиты. Удобство администрирования U_{admin} оценено на уровне 4 баллов из 5, учитывая необходимость периодического обслуживания замков и ключей.

Для программной политики контроля устройств на базе групповых политик Windows (GPO) доля блокировок P_{block} составляет «0.85», что отражает высокую, но не абсолютную эффективность из-за возможности обхода настроек. Частота ложных срабатываний F_{false} указана на уровне «0.10», связанная с возможными ошибками классификации легитимных устройств. Время обнаружения T_{detect} установлено на уровне 5 секунд, поскольку активация политик может требовать дополнительного времени при подключении устройства. Удобство администрирования U_{admin} оценено на максимальные 5

баллов благодаря встроенным средствам централизованного управления в Windows.

Для системы мониторинга активности USB-портов (Safend Protector) доля блокировок P_{block} установлена на уровне «0.90», поскольку системы могут иметь ограничения при определении новых или нестандартных устройств. Частота ложных срабатываний F_{false} оценена в «0.05», что указывает на относительно высокую точность фильтрации подключений. Время обнаружения T_{detect} составляет около 10 секунд, что обусловлено необходимостью анализа событий подключения и возможной задержкой обработки данных. Удобство администрирования U_{admin} оценено в 3 балла, поскольку такие системы требуют отдельной настройки, обслуживания серверов отчетности и постоянного обновления правил безопасности.

Теперь рассчитаем интегральный показатель E для каждой системы согласно формуле 1:

1. Аппаратная блокировка USB Lock RP: $E = 0{,}4 \times 1{,}00 + 0{,}3 \times (1 - 0{,}00) + 0{,}2 \times \left(\frac{1}{1}\right) + 0{,}1 \times \left(\frac{4}{5}\right) = 0.4 + 0.3 + 0.2 + 0.08 = 0.98$

Итог: очень высокая эффективность — почти идеальная защита.

2. Программная политика GPO Windows: $E = 0{,}4 \times 0{,}85 + 0{,}3 \times (1 - 0{,}10) + 0{,}2 \times \left(\frac{1}{5}\right) + 0.1 \times \left(\frac{5}{5}\right) = 0{,}34 + 0{,}27 + 0{,}04 + 0{,}1 = 0{,}75$

Итог: Хорошая эффективность, но ниже из-за задержки обнаружения и небольшого числа ложных срабатываний.

3. Мониторинг активности Safend Protector: $E = 0{,}4 \times 0{,}90 + 0{,}3 \times (1 - 0{,}05) + 0{,}2 \times \left(\frac{1}{10}\right) + 0.1 \times \left(\frac{3}{5}\right) = 0{,}36 + 0{,}285 + 0{,}02 + 0{,}06 = 0{,}725$

Итог: Эффективность чуть ниже, особенно из-за более долгого времени реакции.

Защита корпоративной среды от несанкционированного подключения вредоносных аппаратных модулей является важнейшим элементом обеспечения информационной безопасности организации. Проведённый анализ показал, что наиболее высокую эффективность демонстрируют аппаратные решения,

обеспечивающие физическую недоступность портов для подключения посторонних устройств. Программные политики и системы мониторинга предоставляют гибкость в управлении и более высокий уровень контроля, но в одиночку не обеспечивают полной защиты от всех типов атак, особенно при наличии человеческого фактора и сложных сценариев обхода.

Оценка эффективности различных подходов, выполненная на основе комплексной методики с использованием нормированных критериев, позволила обоснованно выделить сильные и слабые стороны каждой из рассмотренных систем. Расчёты подтвердили необходимость комбинирования аппаратных и программных мер для достижения максимально возможного уровня безопасности.

Список источников информации

1. Число кибератак в России и в мире // TAdviser. URL: https://www.tadviser.ru/index.php/Статья:Число_кибератак_в_России_и_в_мире (дата обращения: 28.04.2025).
2. RED Security SOC: в I квартале 2025 г. количество атак на финансовый сектор выросло более чем в два раза // CNews. URL: https://safe.cnews.ru/news/line/2025-04-21_red_security_soc_v_i_kvartale_2025 (дата обращения: 28.04.2025).
3. Число кибератак выросло в 2,5 раза за 2024 год и достигло 130 тысяч случаев // Смотрим. URL: https://smotrim.ru/article/4307761 (дата обращения: 28.04.2025).
4. Гельфанд А. М. и др. Анализ и управление рисками информационной безопасности объекта критической информационной инфраструктуры //Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия. – Т. 1. – С. 21-27.
5. Штеренберг С. И., Бударный Г. С., Чумаков И. В. Методика обеспечения безопасности доменных систем доверенной зоны //Региональная информатика и информационная безопасность. – 2022. – С. 621-625.