УДК 004.738

С.В. Корякин srgkoryakin1@gmail.com
Институт машиноведения автоматики и геомеханики НАН КР
Д.О. Кошевой d.o.koshevoi@gmail.com
Институт информационных технологий КГТУ им. И. Раззакова

МЕТОДЫ И СРЕДСТВА АППАРАТНЫХ И ПРОГРАММНЫХ ТЕХНОЛОГИЙ ДЛЯ КОНТРОЛЯ ПЕРЕДАЧИ ИНФОРМАЦИИ ПРИ ИСПОЛЬЗОВАНИИ USB

В данной статье представлен обзор современных аппаратных и программных решений, направленных на контроль и предотвращение несанкционированной передачи данных через USB-интерфейсы. Актуальность темы обусловлена растущим числом инцидентов информационной безопасности, связанных с утечками конфиденциальной информации, где USB-носители остаются одним из ключевых векторов угроз. Рассмотрены основные архитектуры, функциональные возможности и ограничения различных подходов к обеспечению безопасности USB-портов, включая физическую блокировку, политики операционных систем, а также специализированные системы, такие как DLP (Data Loss Prevention), EDR (Endpoint Detection and Response) и UEBA (User and Entity Behavior Analytics).

Ключевые слова: конфиденциальная информация; USB-интерфейс; аппаратная блокировка; программный контроль; Data Diode; DLP; EDR; UEBA; виртуализация рабочих сред (VDI); фильтрация USB-трафика; групповые политики ОС; белые и чёрные списки USB-устройств; мониторинг USB-активности; SIEM-интеграция; BadUSB-атаки

Введение

В эпоху цифровизации и расширения периметра вычислительных сетей обеспечение информационной безопасности становится одной из приоритетных задач. Прогнозируется, что глобальные затраты на противодействие киберпреступности значительно возрастут, достигнув $13.82 триллиона к 2028 году [1]. Этот подчеркивает острую необходимость в усилении бдительности и инновациях в стратегиях защиты информационных систем. Комплексная защита данных требует детального анализа всех потенциальных каналов, через которые может произойти несанкционированный доступ или утечка конфиденциальной информации. Среди этих каналов USB-интерфейсы занимают особое место, представляя собой один из наиболее распространенных и одновременно уязвимых векторов угроз [2, 25].

Широкое распространение USB-устройств, от флэш-накопителей до принтеров и прочих внешних устройств, обусловлено их универсальностью и простотой использования [2]. Однако именно эта универсальность и создает значительные риски [43].

Во-первых, повсеместное распространение USB-накопителей и их кажущаяся безобидность часто приводят к недостаточному вниманию к их безопасности. Во-вторых, злоумышленники постоянно совершенствуют методы эксплуатации USB, переходя от примитивных вредоносных программ к сложным атакам на уровне прошивки, способным имитировать доверенные устройства или даже вызывать физические повреждения [49]. В-третьих, существование скрытых каналов передачи данных через USB, например, посредством электромагнитного излучения, показывает, что информация может быть получена даже из изолированных систем с использованием нетрадиционных и крайне скрытных методов [38].

Подключение внешних устройств может привести к следующим инцидентам [38, 43]:

1. Всегда существует риск **внедрения вредоносного кода** в устройство. Неосторожное подключение заражённого USB-накопителя может привести к распространению по корпоративной сети вирусов, червей, программам-вымогателей или шпионского ПО. Приведем примеры значимых инцидентов и их последствия:

- **Stuxnet (2010)** — сложное кибероружие, нацеленное на ядерную программу Ирана, предположительно распространялось через зараженные USB-накопители.

- **FIN7, Raspberry Robin (2022)** — в данном случае устройствами распространялись программы-вымогатели, парализуя корпоративные сети и вызывая значительную потерю данных. Raspberry Robin, червь для Windows, был обнаружен на машинах Windows, устанавливая вредоносное ПО и повышая привилегии.

И хотелось бы отметить, что данные примеры — лишь часть подобных инцидентов угроз и не являются окончательными.

2. USB-устройства могут быть перепрограммированы таким образом, чтобы эмулировать легитимные устройства (например, клавиатуру), выполняя вредоносные команды на подключенном компьютере без ведома пользователя и тем самым реализовывать **атаки типа BadUSB** [49].

3. Основной причиной **утечки конфиденциальных данных** можно выделить и то, что сотрудники (как преднамеренно, так и по неосторожности) могут копировать конфиденциальную информацию на личные USB-накопители. Данные действия приводят к нарушению политик безопасности и потенциальным финансовым и репутационным потерям.

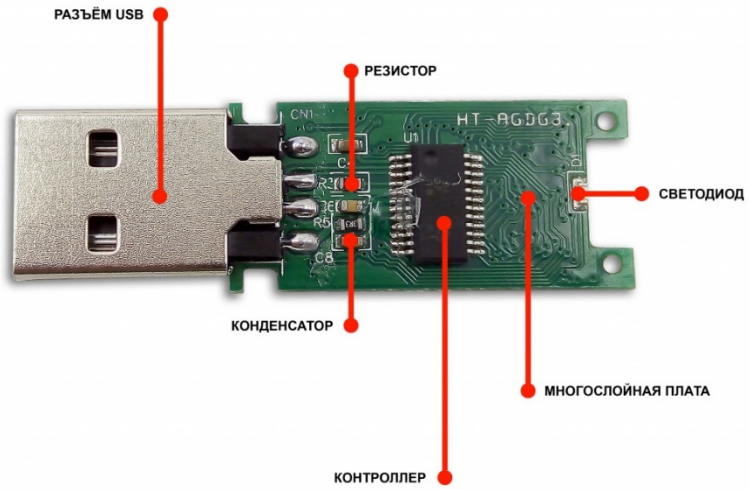

Рисунок 1 — Пример технической реализации устройства с USB-интерфейсом

Основной вопрос состоит в том, способны ли существующие технологии в полной мере обеспечить цельный уровень защиты от утечек конфиденциальной информации через USB-интерфейсы.

Несмотря на множество технологий для контроля передачи данных через USB, ключевая проблема заключается в их фрагментированности и неполноте при изолированном применении. Каждое рассмотренное решение (аппаратная блокировка, системные политики, DLP, EDR/UEBA, шифрование, виртуализация) эффективно компенсирует лишь определенный спектр угроз, оставляя уязвимыми другие векторы атак. Приведем некоторые примеры:

1. Физическая блокировка бессильна против авторизованных, но скомпрометированных устройств (BadUSB).
2. Политики ОС и белые списки уязвимы к подделке идентификаторов и не контролируют содержимое передаваемых данных.
3. DLP-системы, анализируя только контент, могут пропускать сложные атаки на уровне прошивки или скрытые каналы передачи.
4. EDR/UEBA выявляют аномалии, не предотвращая утечку в реальном времени.
5. Шифрование защищает данные на носителе, но не препятствует их несанкционированной *передаче* на само устройство.

Таким образом, основной проблемой является невозможность достижения комплексной и устойчивой защиты от всего спектра USB-угроз с помощью какой-либо одной технологии. Существующие решения, каждое из которых обладает различными преимуществами и

ограничениями, зачастую создает фрагментированную систему защиты, где остаются критически важные «окна» уязвимости [4, 40]. Соответственно целью данного аналитического обзора является систематизирование этих ограничений, выявление компенсируемых уязвимостей каждой технологии и обоснование необходимости продуманной, многоуровневой (гибридной) стратегии защиты, объединяющей сильные стороны различных методов для устранения их взаимных недостатков и создания системы контроля передачи информации при использовании технологии USB.

Проблема же заключается не только в наличии или отсутствии конкретной технологии, но и в сложности их интеграции, администрирования, а также в способности противостоять постоянно развивающимся методам обхода и новым типам угроз, использующим как неосторожность пользователей, так и уязвимости протоколов и аппаратных компонентов USB [38]. Поэтому совершенно необходим не просто набор отдельных решений, а продуманная, интегрированная и гибридная стратегия, способная обезопасить от большинства рисков, связанных с USB-трафиком.

Учитывая комплексный характер проблемы, её эффективное решение требует внедрения механизмов (реализации подсистем защиты), которые сочетают как аппаратные, так и программные меры контроля. Поэтому одна из целей данного исследования — проведение системного анализа существующих подходов к защите от утечек информации по USB-каналу, рассмотреть основные технологии, их принципы работы, преимущества и недостатки, а также определить их роль в общей архитектуре информационных систем и подсистем защиты информации[16, 18]. Таким образом, необходима систематизация существующих решений и построение модели многоуровневой защиты, учитывающей как технические, так и организационные аспекты.

Следует отметить, что исследование направлено на изучение технологий, которые позволяют:

1. **Ограничивать физический доступ** к USB-интерфейсам на устройствах, а также получение через них информации.
2. **Управлять политиками безопасности** в среде операционных систем для контроля подключаемых устройств [7, 9].
3. **Внедрять средства анализа поведения пользователей** и агентов для контроля содержимого передаваемых данных [20, 22].

Прежде чем приступить к описанию конкретных решений, важно разобраться с тем, как USB-интерфейс функционирует на уровне операционной системы и как происходит процесс взаимодействия с аппаратной частью. Каждое USB-устройство имеет уникальные идентификаторы (Vendor ID – VID и Product ID – PID), по которым ОС определяет его тип и назначение [2, 27]. Взаимодействие осуществляется через драйверные модули ядра операционной системы [2].

Методы обеспечения безопасности USB-интерфейсов традиционно разделяются на две большие группы. В ***первой*** группе представлены **аппаратные решения.** Данные методы направлены на работу на физическом уровне. К ним относятся физическая блокировка портов, фильтрация электрических сигналов и использование изолирующих средств и компонентов. Их главное преимущество — независимость от программной среды, что делает их устойчивыми к некоторым типам программных обходов. Они представляют собой первый эшелон защиты, действуя на физическом уровне вне зависимости от состояния операционной системы. Они надежны, так как обход этих мер зачастую требует физического доступа к оборудованию [3, 30]. Во ***второй*** группе представлены **программные решения.** Данные методы реализуются на уровне операционной системы или с помощью специального программного обеспечения (агентов). Сюда входят специализированные средства контроля устройств (**Device Control**), системы предотвращения утечек (**DLP**), платформы обнаружения и реагирования на инциденты (**EDR**), а также средства анализа поведения пользователей и сущностей (**UEBA**), а также настройки политик безопасности ОС [16, 18,

20]. Их внедрение в существующую инфраструктуру информационной системы требует понимания особенностей архитектуры и возможных моделей угроз.

В рамках исследования рассмотрены наиболее распространённые **аппаратные решения:**

1. **Физические заглушки и замки** являются самым простым и доступным методом. Это механические устройства, которые вставляются в USB-порты и блокируют их использование. Они предотвращают случайное или несанкционированное подключение любых USB-устройств.

2. **USB Data Diode** представляет собой специализированное устройство, которое физически разрешает передачу данных только в одном направлении, например, только *из* сети *в* USB-устройство или наоборот. Это полностью исключает обратный канал ввода/вывода, что критически важно в сетях передачи информации информационных систем, где требуется предотвратить попытку извлечения или внедрения данных [6].

3. Более сложные решения представляют собой **аппаратные фильтры и контроллеры**, которые могут быть реализованы на уровне BIOS/UEFI компьютера или как внешние устройства. Они перехватывают и анализируют USB-сигналы, позволяя определять устройства и классифицировать их по типу (например, HID – Human Interface Device, Mass Storage – накопитель), а затем блокировать их подключение по заданным критериям (например, по уникальному идентификатору производителя – VID, или продукта – PID, а также по серийному номеру) [27, 28]. С результатами сравнительного анализа данных методов, включая компенсируемые уязвимости и ключевые ограничения, можно ознакомиться в таблице 1.

Таблица 1 — Сравнительный анализ аппаратных методов контроля и компенсируемые уязвимости

Решение	Ключевые возможности	Компенсируемые уязвимости	Основные ограничения
Физические заглушки/замки	Полная блокировка порта	Физический доступ устройств	Нулевая функциональность
	Низкая стоимость	Кража данных через прямое копирование	Легкий физический обход
USB Data Diode	Гарантированная однонаправленность передачи	Извлечение данных	Ограниченная функциональность (1 направление)
		Загрузка вредоносного кода	Высокая стоимость
Аппаратные фильтры (BIOS/UEFI/контроллеры)	Гибкая фильтрация по VID/PID/классу	BadUSB-атаки	Уязвимость к подделке идентификаторов
	Централизованное управление	Подключение запрещенных устройств	Сложность актуализации списков
		Скрытые каналы	

После рассмотрения аппаратных мер защиты, действующих на физическом уровне и исключающих возможность подключения нежелательных устройств, перейдем к средствам, работающим внутри операционной системы и анализирующим поведение и содержимое данных. Программные решения дополняют защиту аппаратной составляющей, позволяя гибко управлять политиками, обнаруживать аномалии и предотвращать утечки на уровне процессов и файлов. Встроенные в операционные системы механизмы позволяют администраторам управлять доступом к USB-устройствам на уровне базовых политик. Это наиболее распространенный и экономически выгодный способ базовой защиты [7, 9, 11].

В рамках исследования были рассмотрены следующие наиболее распространённые, основанные на политиках операционных систем, решения:

1. Подсистема ядра Linux «**udev»** позволяет динамически управлять устройствами. С

помощью udev-правил можно идентифицировать USB-устройства по различным характеристикам (производитель, модель, тип) и выполнять предопределенные действия, такие как автоматическое монтирование, блокировка или запуск скриптов при подключении [9, 10].

2. В доменной среде Windows администраторы могут централизованно настраивать разрешения на установку и использование USB-устройств, используя **групповые политики Windows (GPO)**. Например, можно запретить подключение всех съемных накопителей, разрешить только чтение данных с них или допускать только заранее определенные модели устройств [7, 8].

3. **Инструменты MDM (Mobile Device Management)** используются для централизованного управления политиками доступа к сменным носителям на мобильных устройствах и конечных точках, которые интегрированы в облачную инфраструктуру (**Пример инструмента: Microsoft Intune)** [11, 13].

Сравнительные характеристики решений представлены в таблице 2.

Таблица 2 — Сравнительный анализ методов контроля USB на уровне операционных систем

Решение	Ключевые возможности	Компенсируемые уязвимости	Основные ограничения
udev (Linux)	Динамическое управление через правила, идентификация по атрибутам (VID/PID, класс)	Подключение запрещенных типов устройств, BadUSB-атаки, скрытые каналы	Отсутствие централизованного управления, сложность администрирования, уязвимость к подделке ID
GPO (Windows)	Централизованное управление через AD, блокировка/разрешение классов или моделей	Подключение запрещенных типов устройств, BadUSB-атаки, скрытые каналы	Эффективно только в доменной среде, уязвимо к действиям локальных администраторов, нет контентного анализа
MDM	Централизованное облачное управление, Политики для мобильных и обычных устройств	Подключение запрещенных устройств, несанкционированное копирование, упрощение соблюдения политик	Зависит от интернета и облака провайдера, ограниченная поддержка сложных USB, высокая стоимость лицензий

Среди программных мер выделяют, в частности, системы предотвращения утечек (DLP), которые анализируют контекст и содержимое передаваемых данных [16], а платформы EDR мониторят активность конечных точек, выявляя подозрительные операции с USB-устройствами. Эти технологии интегрируются с остальными компонентами ИБ, обеспечивая многоуровневый подход к защите. DLP-системы являются одним из наиболее эффективных инструментов для контроля USB-трафика, так как их основная задача — предотвращение несанкционированной передачи конфиденциальных данных [16, 47].

Типичная DLP-система состоит из агентской части, которая устанавливается на конечные точки (рабочие станции, серверы), и центрального сервера управления, где хранятся политики безопасности и логи событий. Агенты перехватывают все операции с данными, включая попытки копирования на внешние USB-устройства [16].

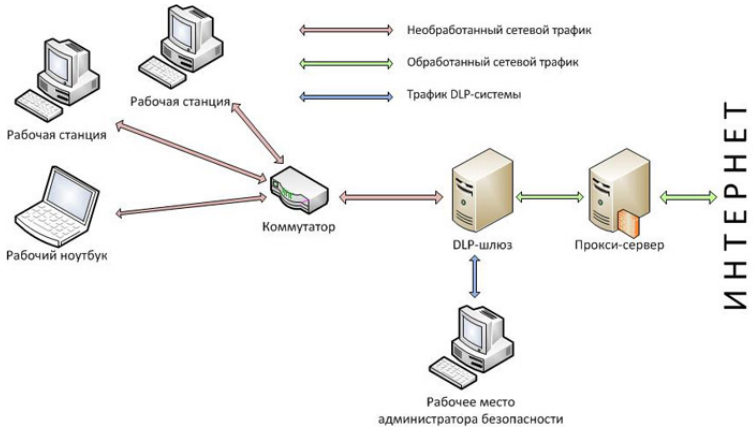

Рисунок 2 — Пример организации вычислительной сети с использованием технологии DLP

Методы DLP реализуются последовательно и просто. Сначала действует *контекстный контроль. Реализуется* анализ метаданных процесса, а именно, кто, когда, откуда и куда пытается передать данные, какой тип устройства используется, какой размер файла. Это позволяет сразу блокировать потенциально угрожающие безопасности данных операции без углубления в содержимое [16].

Если контекстовая проверка не срабатывает, подключается *контентный контроль*. В нем используются:

- Регулярные выражения для поиска известных шаблонов (номера карт, ИНН и т. п.) [16].
- Цифровые отпечатки заранее известных конфиденциальных документов, чтобы обнаружить даже слегка изменённые копии [29].
- Поиск по классификаторам и ключевым словам, чтобы поймать материалы, попадающие под правила (например, персональные данные или коммерческая тайна) [16].

Наконец, DLP фиксирует каждую попытку передачи: в логах остаются сведения обо всех операциях, а файлы по необходимости сохраняются как теневые копии [16]. Это даёт возможность не только блокировать нежелательное копирование, но и потом расследовать события, восстановив, что именно и когда пытались передать.

Методы реализации DLP-защиты систематизированы в таблице 3.

Таблица 3 — Сравнительный анализ методов DLP

Методы (DLP)	Ключевые возможности	Компенсируемые уязвимости	Основные ограничения
Контекстный контроль	Анализ метаданных (пользователь, устройство, размер файла), быстрая блокировка подозрительных операций	Несанкционированная передача по разрешенным устройствам, копирование неклассифицированных данных	Не анализирует содержимое, ложные срабатывания при аномальном поведении
Регулярные выражения	Поиск структурированных шаблонов (номера карт, ИНН), обнаружение известных форматов конфиденциальных данных	Утечка данных с известными шаблонами, прямое копирование чувствительной информации	Уязвимость к изменению формата данных, неэффективность для неструктурированного контента
Цифровые отпечатки	Точное обнаружение известных документов, выявление модифицированных копий, защита специфических файлов	Утечка зарегистрированных конфиденциальных документов, копирование критичных файлов	Бесполезен для новых/неизвестных документов, требует предварительной регистрации файлов

Методы (DLP)	Ключевые возможности	Компенсируемые уязвимости	Основные ограничения
Поиск по классификаторам	Обнаружение неструктурированных данных по тематике, гибкие правила для категорий информации (ПДн, коммерческая тайна)	Утечки по смысловому содержанию, передача скрытой конфиденциальной информации	Риск ложных срабатываний на синонимы, зависимость от качества классификаторов
Теневые копии и логи	Фиксация всех операций передачи, возможность постфактум анализа и расследований, доказательная база для инцидентов	Скрытие следов инсайдерской деятельности, анализ причин утечек	Не предотвращает утечку в реальном времени, требует ресурсов для хранения данных

После описания возможностей DLP, обеспечивающих превентивное блокирование несанкционированных копирований, следующим уровнем защиты становятся системы, ориентированные на обнаружение уже начавших развиваться инцидентов. Платформы EDR отслеживают поведение процессов и файлов на конечных точках, фиксируя подозрительные операции с USB-устройствами и своевременно реагируя на них [18]. При этом UEBA усиливает анализ за счёт моделирования нормального поведения пользователей и устройств, позволяя выявлять скрытые или инсайдерские угрозы [20, 22]. Совместное применение EDR и UEBA дополняет превентивные меры DLP, формируя реактивный и аналитический уровень защиты.

Системы **EDR (Endpoint Detection and Response)** непрерывно собирают данные об активности на конечной точке (системные вызовы, сетевые соединения, файловые операции, запущенные процессы). Они анализируют эти данные, выявляют подозрительные процессы и коррелируют их с базами данных известных индикаторов компрометации (IOC) и техниками атак (например, матрица MITRE ATT&CK) [18, 34]. В контексте USB-трафика EDR может обнаружить:

- Необычно большой объем данных, скопированных на USB-накопитель.
- Попытки запуска исполняемых файлов с USB-носителей, которые не соответствуют установленным политикам [18].
- Подозрительные действия, указывающие на попытку обхода средств контроля USB (например, изменения в реестре или запуск специальных утилит) [44].

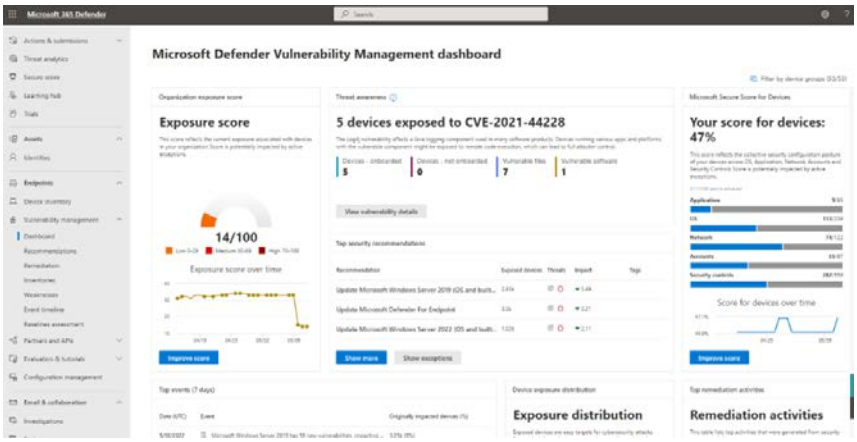

Рисунок 3 — Пример интерфейса одной из EDR-систем

Системы **UEBA (User and Entity Behavior Analytics)** основываются на построении моделей поведения пользователей и сущностей (устройств, приложений) на основе проанализированной информации о действиях и операциях, происходивших в системе. Они идентифицируют отклонения от этих моделей [20, 21]. Например, если сотрудник, который

обычно не использует USB-накопители для передачи больших объемов данных, внезапно начинает копировать крупные файлы на флешку в нерабочее время, UEBA может расценить это как аномалию и сформировать предупреждение [22].

События, выявленные EDR и UEBA, как правило, внедряются в централизованные системы управления событиями безопасности (SIEM) для дальнейшего анализа, сопоставления с данными из других источников (сетевое оборудование, серверы) и автоматизации реагирования на инциденты [23].

Сравнение платформ EDR и UEBA приведено в таблице 4.

Таблица 4 — Сравнительный анализ EDR и UEBA

Критерий/Технология	EDR (Endpoint Detection and Response)	UEBA (User and Entity Behavior Analytics)	Комбинированное решение (EDR + UEBA)
Основная функция	Мониторинг активности процессов и файлов в реальном времени	Анализ поведенческих паттернов пользователей и сущностей	Комплексный анализ угроз с двойной верификацией
Компенсируемые уязвимости	BadUSB-атаки, запуск вредоносного ПО с носителей, попытки обхода контроля USB	Скрытые инсайдерские угрозы, нестандартное использование устройств, аномальные действия пользователей	Комбинированные атаки, сложные инциденты с участием USB, целевые компрометации
Ключевые возможности	Обнаружение массовой передачи данных, фиксация запуска исполняемых файлов, выявление изменений системных настроек	Построение поведенческих базовых профилей, выявление отклонений от нормы, контекстный анализ временных паттернов	Корреляция событий EDR с поведенческими аномалиями, автоматизация реагирования
Технологии анализа	IOC-сканирование, MITRE ATT&CK mapping, анализ цепочек процессов	Машинное обучение, статистическое моделирование, анализ временных рядов	Гибридные алгоритмы, системы приоритизации инцидентов
Интеграция с SIEM	Прямая передача событий для корреляции	Обогащение данных контекстом поведения	Сквозная видимость угроз на всех уровнях
Примеры детекции	Копирование 50 ГБ на USB за 5 мин, запуск скрытого.exe с носителя, изменение реестровых ключей USB	Копирование файлов в нерабочее время, использование нехарактерных устройств, резкий рост активности	Одновременная массовая передача + аномальное поведение пользователя
Преимущества	Высокая точность детекции известных TTP, быстрое реагирование	Обнаружение неизвестных угроз, выявление инсайдерских рисков	Максимальный охват угроз, снижение ложных срабатываний
Ограничения	Зависимость от сигнатур IOC, слепота к контексту пользователя	Требует длительного обучения моделей, сложность настройки	Экстремальная ресурсоемкость, требовательность к экспертизе
Ресурсные затраты	Высокие требования к CPU/памяти на конечных точках	Высокие требования к хранилищам данных	Критически высокие требования к инфраструктуре

При этом следует отметить, что контроль списков доверия (белых и чёрных) является фундаментальным для многих решений по контролю устройств, а данные методы рассматриваются в качестве дополнительных программных механизмов.

1. В подходе, основанном на **белых списках (whitelist)**, разрешается подключение и использование только тех USB-устройств, которые были предварительно зарегистрированы и признаны доверенными. Идентификация происходит по уникальным параметрам, таким как VID (Vendor ID), PID (Product ID) и/или серийный

номер [26, 27]. Все остальные устройства по умолчанию блокируются.

2. В отличие от белых в **чёрные списки (blacklist)** вносятся устройства, которые считаются потенциально опасными или нежелательными, и их использование блокируется [26].

Управление списками может осуществляться через групповые политики Windows, специализированные агентские решения (так называемые **Device Control** модули, часто входящие в состав EDR или DLP), а также встроенные контроллеры устройств в операционных системах [7, 26].

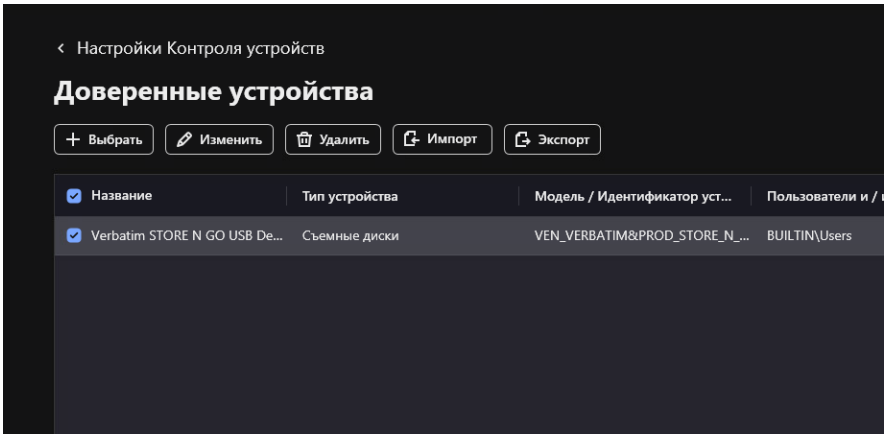

Рисунок 4 —Пример создания списка доверенных устройств на базе ПО Kaspersky Endpoint Security Cloud

Обобщая сказанное выше, можно говорить о том, что контроль списков доверия является фундаментальным механизмом. Его характеристики отражены в таблице 5.

Таблица 5 — Сравнительный анализ методов контроля списков доверия USB

Метод	Ключевые возможности	Компенсируемые уязвимости	Основные ограничения
Белые списки (Whitelist)	Разрешение только доверенных устройств, идентификация по VID/PID/серийному номеру, централизованное управление (GPO, MDM, EDR/DLP)	Подключение неавторизованных устройств, использование неконтролируемых носителей, массовое распространение неизвестных угроз	Высокие административные затраты на регистрацию, уязвимость к подделке идентификаторов, негибкость при частой смене устройств
Черные списки (Blacklist)	Блокировка известных вредоносных устройств, быстрое реагирование на новые угрозы, простота начальной настройки	Подключение устройств с известными признаками вредоносности, использование массово распространяемых уязвимых устройств	Неэффективность против неизвестных/кастомных угроз, постоянная необходимость обновления списка, ложное чувство безопасности

Шифрование данных является важным компонентом стратегии защиты информации, передаваемой или хранящейся на USB-устройствах. Оно обеспечивает защиту данных «в покое» (data at rest) [29, 30].

1. Существуют **аппаратные шифрующие накопители**, которые представляют собой USB-устройства со встроенными криптопроцессорами (например, использующими алгоритм AES-256), которые автоматически шифруют и дешифруют данные «на лету». Доступ к таким накопителям обычно защищен паролем или биометрическими данными [29, 31]. В случае утери или кражи устройства данные остаются защищенными.

2. Также не стоит забывать про **программное шифрование,** включающее использование клиентских приложений для шифрования отдельных файлов, папок или

целых разделов на USB-накопителях (например, BitLocker To Go в Windows, VeraCrypt). В корпоративной среде эти решения часто интегрируются с системами управления ключами (PKI – Public Key Infrastructure, HSM – Hardware Security Module) для централизованного контроля и восстановления ключей [15, 29].

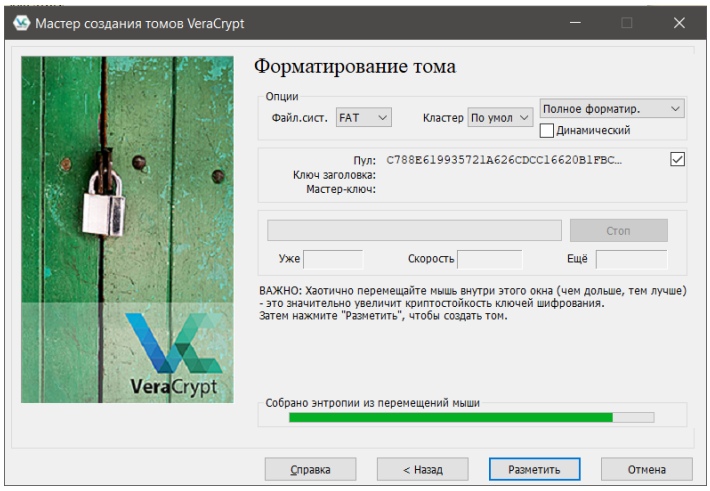

Рисунок 5 — Пример работы программного обеспечения для шифрования накопителей

Шифрование данных — критический компонент защиты. Оценка методов представлена в таблице 6.

Таблица 6 — Сравнительный анализ методов шифрования USB-носителей

Метод	Ключевые возможности	Компенсируемые уязвимости	Основные ограничения
Аппаратное шифрование	Автоматическое шифрование «на лету», защита паролем/биометрией, независимость от ОС, физическая защита чипа	Доступ к данным при утере/краже носителя, физический доступ к устройству, кража информации с потерянных носителей	Ограниченная функциональность (только хранение), высокая стоимость устройств, риск потери доступа при утере ключа
Программное шифрование	Шифрование файлов/разделов/целых носителей, интеграция с PKI/HSM, гибкие политики, поддержка различных ОС	Несанкционированный доступ к данным на носителе, кража информации, перехват данных при передаче незашифрованных файлов	Зависимость от ПО и ОС, снижение производительности, риск компрометации ключей на хосте

3. Помимо традиционных программных и аппаратных методов, важную роль в обеспечении безопасности информационных систем играют **токены**. Эти компактные аппаратные устройства служат надёжными хранилищами для криптографических ключей и сертификатов, а также используются для строгой аутентификации пользователей [5]. Они могут быть выполнены в различных форм-факторах, от **USB-ключей** до **смарт-карт**, и взаимодействуют с операционной системой через стандартизированные интерфейсы. Благодаря своей способности выполнять криптографические операции внутри себя, не раскрывая секретные данные вне системы, токены значительно повышают уровень защиты от несанкционированного доступа и утечек информации [5, 46], дополняя существующие меры безопасности.

Их возможности систематизированы в таблице 7.

Таблица 7 — Сравнительный анализ токенов и систем управления ключами

Метод	Ключевые возможности	Компенсируемые уязвимости	Основные ограничения

Криптографические токены (например, eToken)	Безопасное хранение ключей/сертификатов, двухфакторная аутентификация (2FA), аппаратная изоляция криптоопераций, поддержка цифровых подписей	Кража учетных данных (логин/пароль), несанкционированный доступ к системам, компрометация ключей на хосте	Ограниченная емкость хранилища, зависимость от совместимости драйверов/ПО, риск физической утери/повреждения, дополнительные затраты на инфраструктуру
Системы управления ключами (PKI/HSM)	Централизованное хранение и генерация ключей, автоматическая ротация и отзыв ключей, строгий аудит криптоопераций, высокая отказоустойчивость	Компрометация ключей шифрования, несанкционированный доступ к ключам, отсутствие контроля за жизненным циклом ключей	Высокая стоимость внедрения и лицензий, требовательность к администрированию, сложность интеграции с legacy-системами

Подходы, основанные *на виртуализации и контейнеризации*, предоставляют мощные механизмы изоляции, которые могут значительно снизить риски, связанные с USB-устройствами, путем ограничения прямого физического доступа [32, 35].

1. Технология VDI (Virtual Desktop Infrastructure) позволяет пользователям работать в виртуальной машине, которая размещается на централизованном сервере. USB-устройства могут быть «проброшены» в эту виртуальную машину, но с изолированным контролем [32]. Это означает, что физический доступ к USB-портам на локальном тонком клиенте или ПК может быть полностью ограничен, а все операции с USB-устройствами происходят в изолированной виртуальной среде, где их легче контролировать.

2. Контейнеры (например, Docker) позволяют изолировать приложения и их зависимости. В контексте USB можно настроить механизмы изоляции (например, через namespaces, cgroups, AppArmor/SELinux), чтобы ограничить доступ приложений внутри контейнера к USB-устройствам [35]. Это может быть полезно для запуска потенциально небезопасных приложений в контролируемой среде.

Подходы на основе виртуализации предоставляют механизмы изоляции. Их сравнительные характеристики приведены в таблице 8.

Таблица 8 — Сравнительный анализ методов изоляции

Метод	Ключевые возможности	Компенсируемые уязвимости	Основные ограничения
VDI (Virtual Desktop Infrastructure)	Централизованное размещение рабочих столов на сервере, полный запрет физического доступа к USB на клиентских устройствах, изолированный проброс USB в виртуальную среду, централизованный мониторинг операций	Физический доступ к USB-портам клиента, кража данных через прямое подключение носителей, заражение клиентских устройств через USB	Высокие требования к серверным ресурсам и сети (латенция 20–50 мс), ограниченная поддержка специфичных USB-устройств (только 75–85% устройств), годовая стоимость лицензий ($100-250/пользователь)

Контейнеризация (Docker, Podman)	Изоляция приложений с помощью namespaces/cgroups, гранулярный контроль доступа через SELinux/AppArmor, быстрое развертывание изолированных сред, низкие накладные расходы (1–5% производительности)	Доступ приложения к нежелательным USB-устройствам, распространение вредоносного кода через USB на хост-систему, компрометация приложения через USB-уязвимости	Сложность конфигурации USB-passthrough (требует прав root), ограниченная поддержка USB 3.0+ (только 60% устройств), риск утечек через shared kernel vulnerabilities

Для комплексной защиты рассматриваются специализированные решения. Их параметры отражены в таблице 9.

Таблица 9 — Сравнительный анализ дополнительных решений для контроля USB

Метод	Ключевые возможности	Компенсируемые уязвимости	Основные ограничения
Аппаратная виртуализация (Гипервизор 1 типа)	Полная изоляция USB-контроллера, прямой доступ к устройству из VM, защита на уровне микроядра (например, Qubes OS)	Компрометация хоста через уязвимости драйверов, перехват USB-трафика	Высокие требования к ресурсам (8+ ГБ RAM/VM), сложность администрирования, Ограниченная поддержка GPU/USB 3.1
USB over IP решения	Перенаправление USB по сети, централизованное хранение устройств в защищенной зоне, шифрование трафика TLS 1.3	Физический доступ к устройствам, кража носителей, несанкционированное подключение	Зависимость от сетевой инфраструктуры (требует 1 Гбит/с+), задержки >100 мс, стоимость шлюзов ($500-2000/устройство)

По завершении исследования существующих решений был проведён сравнительный анализ. Комплексная оценка рассмотренных методов демонстрирует, что каждый из них имеет свои сильные и слабые стороны, а оптимальная стратегия защиты зачастую заключается в их комбинации. Итоговая оценка эффективности технологий представлена в таблице 10.

Таблица 10 — Комплексный анализ технологий контроля USB-трафика и их эффективности

Категория	Технология/Метод	Ключевые возможности	Компенсируемые уязвимости	Ограничения	Эффективность решения проблемы	Уровень защиты
Аппаратные решения	Физические заглушки	Блокировка физического доступа к портам	Физический доступ к портам	Нулевая функциональность, легко обойти	Низкая (1)	Физический
	USB Data Diode	Гарантированная однонаправленная передача	Извлечение/внедрение данных через двунаправленные порты	Ограниченная функциональность, высокая стоимость	Средняя (2)	Физический
	Аппаратные фильтры	Фильтрация по VID/PID/классу устройств	Подключение неавторизованных устройств, BadUSB-атаки	Уязвимость к подделке ID, сложность управления	Высокая (3)	Физический/логический

Категория	Технология/Метод	Ключевые возможности	Компенсируемые уязвимости	Ограничения	Эффективность решения проблемы	Уровень защиты
Политики ОС	udev (Linux)	Динамическое управление устройствами	Подключение запрещенных устройств	Отсутствие централизованного управления	Средняя (2)	Логический
	GPO (Windows)	Централизованное управление доступом	Массовые атаки через USB	Уязвимость к правам администратора	Высокая (3)	Логический
	MDM	Облачное управление политиками	Несанкционированное использование мобильных устройств	Зависимость от облака, высокая стоимость	Высокая (3)	Логический
DLP-системы	Контекстный контроль	Анализ метаданных передач	Передача данных через разрешенные устройства	Нет анализа содержимого	Средняя (2)	Контентный
	Контентный анализ	Обнаружение конфиденциальных данных	Утечки структурированных/неструктурированных данных	Ложные срабатывания, ресурсоемкость	Высокая (3)	Контентный
Мониторинг/Анализ	EDR	Обнаружение подозрительных операций	Запуск вредоносного ПО, массовая передача данных	Зависимость от сигнатур	Высокая (3)	Поведенческий
	UEBA	Выявление аномалий поведения	Инсайдерские угрозы, скрытые действия	Требует обучения моделей	Высокая (3)	Поведенческий
Контроль устройств	Белые списки	Разрешение только доверенных устройств	Подключение неавторизованных устройств	Административные затраты	Высокая (3)	Логический
	Черные списки	Блокировка известных угроз	Использование уязвимых устройств	Неэффективен против новых угроз	Средняя (2)	Логический
Шифрование	Аппаратное	Автоматическое шифрование «на лету»	Доступ к данным при утере устройства	Высокая стоимость, ограниченная функциональность	Высокая (3)	Защита данных
	Программное	Гибкое шифрование файлов/разделов	Несанкционированный доступ к данным	Снижение производительности	Высокая (3)	Защита данных
Безопасность ключей	Крипто-токены	Безопасное хранение ключей, 2FA	Кража учетных данных	Риск физической утери	Высокая (3)	Аутентификация
	PKI/HSM	Централизованное управление ключами	Компрометация ключей	Высокая стоимость, сложность интеграции	Высокая (3)	Инфраструктура

Категория	Технология/Метод	Ключевые возможности	Компенсируемые уязвимости	Ограничения	Эффективность решения проблемы	Уровень защиты
Виртуализация	VDI	Полная изоляция USB-операций	Физический доступ к клиентским портам	Высокие требования к инфраструктуре	Высокая (3)	Архитектурный
	Контейнеризация	Изоляция приложений	Доступ приложений к USB	Сложность настройки, ограниченная поддержка	Средняя (2)	Прикладной
Дополнительные	USB over IP	Централизованное хранение устройств	Физический доступ к устройствам	Сетевая зависимость, задержки	Средняя (2)	Архитектурный

Итак, аппаратные решения обеспечивают максимальный уровень жёсткости контроля, но их внедрение может быть дорогостоящим и менее гибким. Программные решения демонстрируют большую гибкость и масштабируемость, но требуют дополнительной защиты от привилегированных атак и могут быть ресурсоёмкими. Системы DLP обеспечивают высокую степень видимости операций и контентный контроль, в то время как EDR и UEBA дополняют их аналитическим компонентом, позволяя выявлять отклонения от нормального поведения и реагировать на сложные угрозы.

Рациональным подходом является внедрение нескольких методов в рамках многоуровневой архитектуры безопасности [4, 40]. Такой подход обеспечивает глубокую и эшелонированную защиту. С учётом возрастающей сложности атак на информационные системы и расширения возможных векторов воздействия наиболее эффективным подходом является реализация **гибридных архитектур безопасности** [39]. Такие архитектуры сочетают в себе:

1. **Физическую изоляцию и аппаратный контроль** для базового уровня защиты.
2. **Глубокий контентный анализ** с использованием DLP-систем для предотвращения передачи конфиденциальных данных [16].
3. **Поведенческий анализ** (UEBA) и **мониторинг активности конечных точек** (EDR) для выявления аномалий и сложных инсайдерских угроз [20, 22].
4. **Шифрование данных** для защиты информации в случае физической утери устройства [29].

Учитывая необходимости **гибридного подхода** [4, 39, 40] для эффективного противодействия угрозам, связанным с рассматриваемой проблемой, предлагается подведение итогов анализа, в результате которого может быть представлена демонстрационная модель системы целевой защиты от ключевых угроз. Основные задачи модели:

1. Интеграция аппаратного контроля, программных политик, контентного анализа (DLP), поведенческого мониторинга (EDR/UEBA) и шифрования в единой управляемой системе.
2. Обеспечение прозрачности и корреляции событий на всех уровнях взаимодействия с USB-устройствами, используя **современные методы анализа данных.**
3. Автоматизированное реагирование на инциденты на основе комбинированных данных от различных модулей системы, что позволяет **динамически адаптировать защитные меры и минимизировать время реакции**.

Модель в итоге должна представлять из себя демонстрационный вариант архитектуры, устойчивой к современным и перспективным угрозам, включая атаки при помощи устройств с модернизированной прошивкой, целенаправленные утечки информации сотрудниками и использование скрытых каналов передачи данных.

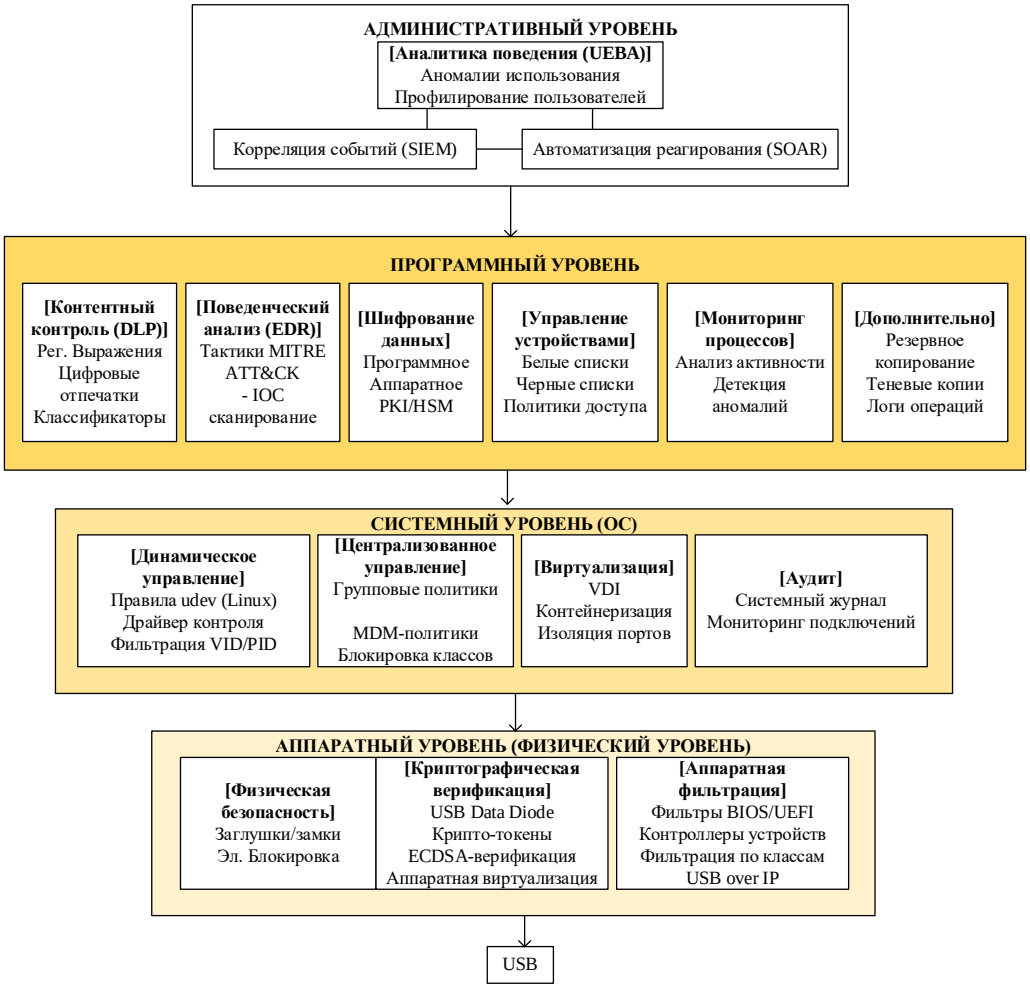

Рисунок 6 — Демонстрационная модель взаимодействия технологий и методов в рамках гибридной системы защиты

Представленная модель является результатом комплексного анализа современных технологий защиты, описывая архитектуру взаимодействия компонентов гибридной системы для противодействия утечкам через USB-интерфейсы. Её ключевая ценность состоит в системном объединении проверенных методов, где каждый уровень решает конкретные задачи безопасности без избыточной сложности.

Подводя итоги, стоит отметить, что защита информации от утечек через USB-интерфейсы представляет собой постоянно актуальную задачу, которая должна учитывать множество различных нюансов и аспектов. Анализ различных аппаратных и программных методов показывает, что каждый из них обладает своими преимуществами и ограничениями. Выбор оптимальной стратегии реализации защиты должен основываться на тщательном анализе угроз, специфики организации, её ИТ-инфраструктуры и доступных ресурсов [40, 47].

Предполагается, что в будущем развитие получат более интеллектуальные и адаптивные решения, основанные на машинном обучении или искусственном интеллекте, а также обладающие способностью к верификации подлинности USB-устройств [22, 48]. Это позволит создавать более устойчивые и комплексные системы информационной безопасности, способные эффективно противостоять постоянно меняющимся угрозам и обеспечивать надежную защиту корпоративных активов.

Литература

1. Statista. Expected Cost of Cybercrime Until 2027 [Электронный ресурс]. — Режим доступа: https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027/ (дата обращения: 06.11.2025).
2. USB [Электронный ресурс] // Википедия. — Режим доступа: https://ru.wikipedia.org/wiki/USB (дата обращения: 06.11.2025).
3. Новости аппаратного обеспечения [Электронный ресурс] // iXBT.com. — Режим доступа: https://www.ixbt.com/news/hard/index.shtml?09/40/88/ (дата обращения: 06.11.2025).
4. Selectel. Анализ технологий USB-безопасности [Электронный ресурс] // Habr.com. — Режим доступа: https://habr.com/ru/companies/selectel/articles/799403/ (дата обращения: 06.11.2025).
5. Токен (авторизации) [Электронный ресурс] // Википедия. — Режим доступа: https://ru.wikipedia.org/wiki/Токен_(авторизации) (дата обращения: 06.11.2025).
6. Однонаправленная сеть [Электронный ресурс] // Википедия. — Режим доступа: https://ru.wikipedia.org/wiki/Однонаправленная_сеть (дата обращения: 06.11.2025).
7. Microsoft. Управление установкой устройств с помощью групповой политики [Электронный ресурс] // Docs.Microsoft.com. — Режим доступа: https://learn.microsoft.com/ru-ru/windows/client-management/client-tools/manage-device-installation-with-group-policy (дата обращения: 06.11.2025).
8. CoreWin. Что такое USB Group Policy? [Электронный ресурс] // CoreWin.ua. — Режим доступа: https://corewin.ua/ru/blog-ru/what-is-usb-group-policy/ (дата обращения: 06.11.2025).
9. ArchWiki. Udev (Русский) [Электронный ресурс]. — Режим доступа: https://wiki.archlinux.org/title/Udev_(Русский) (дата обращения: 06.11.2025).
10. ALT Linux. Как писать правила Udev [Электронный ресурс]. — Режим доступа: https://www.altlinux.org/Как_писать_правила_Udev (дата обращения: 06.11.2025).
11. DIS-Group. Master Data Management: что такое MDM-системы [Электронный ресурс]. — Режим доступа: https://dis-group.ru/blogs/master-data-management-chto-takoe-mdm-sistemy-i-master-dannye/ (дата обращения: 06.11.2025).
12. IBM. Mobile Device Management [Электронный ресурс]. — Режим доступа: https://www.ibm.com/think/topics/mobile-device-management (дата обращения: 06.11.2025).
13. Microsoft. Шифрование устройств через Microsoft Intune [Электронный ресурс] // Docs.Microsoft.com. — Режим доступа: https://learn.microsoft.com/ru-ru/intune/intune-service/protect/encrypt-devices (дата обращения: 06.11.2025).
14. Microsoft. Security baselines в Microsoft Intune [Электронный ресурс] // Docs.Microsoft.com. — Режим доступа: https://learn.microsoft.com/ru-ru/intune/intune-service/protect/security-baselines (дата обращения: 06.11.2025).
15. GlobalSign. Основы PKI [Электронный ресурс] // Habr.com. — Режим доступа: https://habr.com/ru/companies/globalsign/articles/471372/ (дата обращения: 06.11.2025).

16. Предотвращение утечек информации [Электронный ресурс] // Википедия. — Режим доступа: https://ru.wikipedia.org/wiki/Предотвращение_утечек_информации (дата обращения: 06.11.2025).
17. RT-Solar. Solar Dozor: Блог [Электронный ресурс]. — Режим доступа: https://rt-solar.ru/products/solar_dozor/blog/2080/ (дата обращения: 06.11.2025).
18. Kaspersky. Endpoint Detection and Response [Электронный ресурс]. — Режим доступа: https://www.kaspersky.ru/resource-center/preemptive-safety/endpoint-detection-and-response (дата обращения: 06.11.2025).
19. Anti-Malware. Endpoint Detection and Response (EDR) — аналитика рынка [Электронный ресурс]. — Режим доступа: https://www.anti-malware.ru/analytics/Market_Analysis/endpoint-detection-and-response-edr (дата обращения: 06.11.2025).
20. Kaspersky. UEBA (User and Entity Behavior Analytics) [Электронный ресурс]. — Режим доступа: https://encyclopedia.kaspersky.ru/glossary/ueba/ (дата обращения: 06.11.2025).
21. Wikipedia. User behavior analytics [Электронный ресурс]. — Режим доступа: https://en.wikipedia.org/wiki/User_behavior_analytics (дата обращения: 06.11.2025).
22. Habr. Анализ поведения пользователей в информационной безопасности [Электронный ресурс]. — Режим доступа: https://habr.com/ru/articles/878142/ (дата обращения: 06.11.2025).
23. SIEM [Электронный ресурс] // Википедия. — Режим доступа: https://ru.wikipedia.org/wiki/SIEM (дата обращения: 06.11.2025).
24. CoreWin. Monitoring USB drives in Windows using Wazuh [Электронный ресурс]. — Режим доступа: https://corewin.ua/ru/blog-ru/monitoring-usb-drives-in-windows-using-wazuh/ (дата обращения: 06.11.2025).
25. Panda Security. Защита от USB-угроз [Электронный ресурс] // Habr.com. — Режим доступа: https://habr.com/ru/companies/panda/articles/323536/ (дата обращения: 06.11.2025).
26. Kaspersky. Kaspersky Endpoint Security: документация [Электронный ресурс]. — Режим доступа: https://support.kaspersky.com/KESWin/11.4.0/ru-RU/34890.htm (дата обращения: 06.11.2025).
27. FlashBoot. VID/PID база данных [Электронный ресурс]. — Режим доступа: https://flashboot.ru/files/vidpid/ (дата обращения: 06.11.2025).
28. Synology. Как узнать PID/VID USB-устройства [Электронный ресурс]. — Режим доступа: https://kb.synology.com/ru-ru/DSM/tutorial/How_do_I_check_the_PID_VID_of_my_USB_device (дата обращения: 06.11.2025).
29. Kingston Technology. Аппаратное vs программное шифрование [Электронный ресурс] // Habr.com. — Режим доступа: https://habr.com/ru/companies/kingston_technology/articles/521084/ (дата обращения: 06.11.2025).
30. Аппаратное шифрование [Электронный ресурс] // Википедия. — Режим доступа: https://ru.wikipedia.org/wiki/Аппаратное_шифрование (дата обращения: 06.11.2025).
31. Kingston. Hardware vs Software Encryption [Электронный ресурс]. — Режим доступа: https://www.kingston.com/ru/blog/data-security/hardware-vs-software-encryption (дата обращения: 06.11.2025).
32. Microsoft. Настройка перенаправления USB в Azure Virtual Desktop [Электронный ресурс] // Docs.Microsoft.com. — Режим доступа:

https://learn.microsoft.com/ru-ru/azure/virtual-desktop/redirection-configure-usb?tabs=intune&pivots=azure-virtual-desktop (дата обращения: 06.11.2025).

33. ISPsystem. Новости виртуализации [Электронный ресурс] // Habr.com. — Режим доступа: https://habr.com/ru/companies/ispsystem/news/830068/ (дата обращения: 06.11.2025).

34. MITRE. MITRE ATT&CK [Электронный ресурс]. — Режим доступа: https://attack.mitre.org/ (дата обращения: 06.11.2025).

35. Контейнеризация [Электронный ресурс] // Википедия. — Режим доступа: https://ru.wikipedia.org/wiki/Контейнеризация (дата обращения: 06.11.2025).

36. RedOS. Ограничение USB в Red OS [Электронный ресурс]. — Режим доступа: https://redos.red-soft.ru/base/redos-7_3/7_3-equipment/7_3-usb-config/7_3-restriction-usb/ (дата обращения: 06.11.2025).

37. iXBT. Форум по информационной безопасности [Электронный ресурс]. — Режим доступа: https://forum.ixbt.com/topic.cgi?id=7:32719 (дата обращения: 06.11.2025).

38. Otus. Анализ USB-угроз [Электронный ресурс] // Habr.com. — Режим доступа: https://habr.com/ru/companies/otus/articles/767884/ (дата обращения: 06.11.2025).

39. Habr. Современные методы защиты периметра [Электронный ресурс]. — Режим доступа: https://habr.com/ru/articles/790002/ (дата обращения: 06.11.2025).

40. CrowdStrike. Mitigating USB data exfiltration [Электронный ресурс]. — Режим доступа: https://www.crowdstrike.com/en-us/blog/mitigating-usb-data-exfiltration-with-new-capabilities-in-falcon-device-control/ (дата обращения: 06.11.2025).

41. Laboratoria. Классификация рабочих мест [Электронный ресурс]. — Режим доступа: https://laboratoria.by/stati/klassifikacija-rabochih-mest (дата обращения: 06.11.2025).

42. FalconGaze. Управление инцидентами информационной безопасности [Электронный ресурс]. — Режим доступа: https://falcongaze.com/ru/pressroom/publications/incidenty-ib/upravlenie-incidentami-informacionnoy-bezopasnosti-v-kompanii.html (дата обращения: 06.11.2025).

43. Habr. Атаки через USB-устройства [Электронный ресурс]. — Режим доступа: https://habr.com/ru/articles/223363/ (дата обращения: 06.11.2025).

44. Microsoft. USB Event Tracing for Windows [Электронный ресурс] // Docs.Microsoft.com. — Режим доступа: https://learn.microsoft.com/ru-ru/windows-hardware/drivers/usbcon/usb-event-tracing-for-windows (дата обращения: 06.11.2025).

45. RedOS. Логирование USB в Red OS [Электронный ресурс]. — Режим доступа: https://redos.red-soft.ru/base/redos-7_3/7_3-equipment/7_3-usb-config/7_3-usb-log/ (дата обращения: 06.11.2025).

46. Habr. Криптографические методы защиты USB [Электронный ресурс]. — Режим доступа: https://habr.com/ru/articles/907692/ (дата обращения: 06.11.2025).

47. PT. Анализ рынка DLP-систем [Электронный ресурс] // Habr.com. — Режим доступа: https://habr.com/ru/companies/pt/articles/845262/ (дата обращения: 06.11.2025).

48. SecurityLab. Аналитика киберугроз [Электронный ресурс]. — Режим доступа: https://www.securitylab.ru/analytics/550392.php (дата обращения: 06.11.2025).

49. Securelist. Hacking microcontroller firmware through a USB [Электронный ресурс]. — Режим доступа: https://securelist.ru/hacking-microcontroller-firmware-through-a-usb/93623/ (дата обращения: 06.11.2025).

50. Microsoft. What is Incident Response [Электронный ресурс]. — Режим доступа: https://www.microsoft.com/ru-ru/security/business/security-101/what-is-incident-response (дата обращения: 06.11.2025).

51. Корякин, С. В. Аналитический обзор методов построения подсистем аппаратных фаерволов для SOC / С. В. Корякин, Д. А. Ибраимов // Проблемы автоматики и управления. – 2025. – № 2(53). – С. 52-63. – ЭДН ФТВДРМ.

52. Корякин, С. В. Аналитический обзор технологий построения аппаратно-ориентированных облачных систем защиты информации с применением нейросетевых технологий / С. В. Корякин // Проблемы автоматики и управления. – 2025. – № 2(53). – С. 41-51. – EDN RCCRHC.