УДК 33 DOI: 10.14451/2.188.97

Кибербезопасность в информационных системах управления: вызовы и решения

© 2024 **Петрова Елена Анатольевна**
Генеральный директор. HTBS-FZCO, Москва.
E-mail: htbselena@gmail.com

Ключевые слова: информационные системы управления, безопасность информационных систем, угроза внешних кибератак, внутренние уязвимости системы, киберпреступники, доступ к конфиденциальной информации, кибербезопасность.

С развитием технологий и увеличением зависимости бизнеса, государственных структур и общества в целом от информационных систем, возрастает и сложность задач, связанных с обеспечением их безопасности. Информационные системы управления, являясь ключевым элементом в структуре любой организации, сталкиваются с угрозами внешних кибератак, внутренними уязвимостями системы и прочими рисками. С одной стороны, информационные системы повышают эффективность работы организаций, обеспечивая оперативное управление ресурсами, быстрое принятие решений и обмен данными. С другой стороны, они становятся мишенью для киберпреступников, стремящихся получить доступ к конфиденциальной информации, нарушить работоспособность систем или даже причинить ущерб на национальном уровне. Таким образом, вопросы кибербезопасности в информационных системах управления обретают стратегическое значение и требуют комплексного подхода к решению. **Объектом исследования** являются информационные системы управления в различных организационных контекстах, а также аспекты кибербезопасности, связанные с этими системами. **Целью исследования** является анализ рисков кибербезопасности, с которыми сталкиваются информационные системы управления, и характеристика решений для противодействия этим угрозам. **Методы исследования –** исследование научных трудов по теме исследования, общие научные методы (анализ, синтез, обобщение). **Научная новизна исследования:** исследование учитывает последние достижения в области информационных технологий и их применение в области кибербезопасности. Исследование направлено на идентификацию существующих и потенциальных уязвимостей в системах, оценку эффективности текущих мер безопасности и применение новых подходов и технологий для повышения уровня защиты информационных систем управления.

Введение

В информационных системах управления одной из ключевых задач является предотвращение рисков, особенно связанных с кибератаками. Слово «кибер» связано с информационными технологиями, а киберпространство описывает среду для обмена данными через компьютерные сети. Кибератака — это враждебная операция в киберпространстве, способная нанести ущерб информационной системе, объектам или людям.

Кибербезопасность определяется как способность системы управления справляться с задачами при кибератаках и технических неисправностях. Основные угрозы включают в себя неавторизованный доступ, скрытые функции в программном обеспечении и системные сбои. Полностью исключить все угрозы нереально, поэтому компании, как правило, фокусируются на стратегиях уменьшения рисков и разработке систем адекватной защиты.

Целью исследования является анализ рисков кибербезопасности, с которыми сталкиваются информационные системы управления, и характеристика решений для противодействия этим угрозам.

Актуальность исследования обусловлена прогнозируемым ростом объемов глобального ущерба от киберпреступности с 8,44 трлн долл. в 2022 году до 23,84 трлн долл. к 2027 году.

Материалы и методы

Методы исследования — исследование научных трудов по теме исследования, общие научные методы (анализ, синтез, обобщение). Научная новизна исследования: исследование учитывает последние достижения в области информационных технологий и их применение в области кибербезопасности. Исследование направлено на идентификацию существующих и потенциальных уязвимостей в системах, оценку эффективности текущих мер безопасности и применение новых подходов и технологий для повышения уровня защиты информационных систем управления.

Результаты и обсуждение

Информационные атаки путем неавторизованного доступа нацелены на серверы, пользовательские станции, коммуникационное оборудование путем использования специализированных программ для автоматизации атак.

Отметим, что количество организаций, так или иначе пострадавших от атак различных вредоносных программ, в том числе и программ-вымогателей, каждый год только увеличивается.

По данным Cybersecurity Ventures, глобальный годовой ущерб от киберпреступности, по прогнозам, достигнет 9,5 триллионов долларов США в 2024 году. Это усугубляется ростом стоимости ущерба от киберпреступности, который, как ожидается, достигнет 10,5 триллиона долларов США к 2025 году.

Фазы кибератаки [10, с. 34]:

- разведка — сбор данных о цели для планирования атаки;
- проникновение — доступ к ресурсам без разрешения;
- осуществление атаки — достижение конечных целей атаки, включая удаление или изменение данных и маскировку вторжения;
- расширение атаки — внедрение вредоносного ПО для атаки на другие части системы.

Виды вредоносных программ: [2, с. 6]

- DoS-атаки, целью которых является нарушение работы системы и блокировка доступа пользователей;
- троянские программы, нарушающие целостность данных и распространяющие вирусы, с возможностью сбора конфиденциальной информации;
- программы для несанкционированного управления, включая различные типы вирусов и червей.

Атаки путем неавторизованного доступа влекут за собой компрометацию конфиденциальности и нарушение целостности данных, а также ограничивают доступ к системам и их содержимому. Конфиденциальность подвергается угрозе при утечке или краже данных. Ограничение доступности возникает из-за блокировки системы или данных и потери средств доступа, включая пароли. Целостность данных страдает от их несанкционированной модификации или введения ложных данных.

Скрытые функции в программах и оборудовании могут влиять на доступность, целостность и конфиденциальность данных. Эти функции, не указанные в документации, могут быть как программными, так и аппаратными.

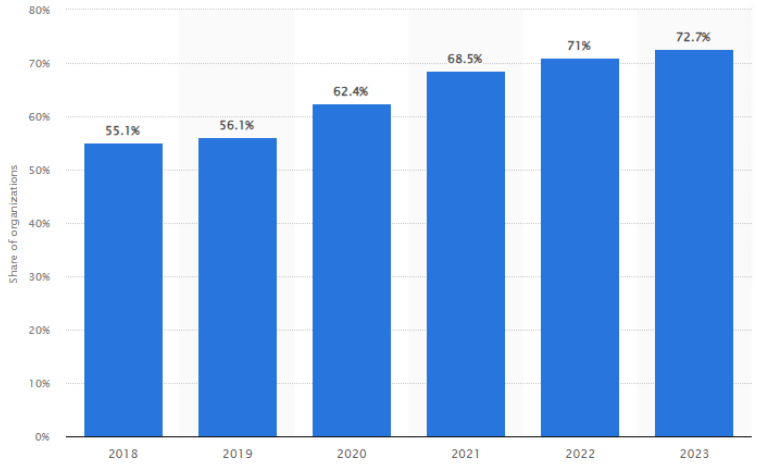

Рис. 1. Годовая доля организаций, пострадавших от атак программ-вымогателей по всему миру, с 2018 по 2023 год [13].

Системные сбои представляют собой значительные препятствия в работе информационных систем, возникающие вследствие различных технических неисправностей или ошибок в программном обеспечении. Эти сбои могут привести к временной потере функциональности, недоступности данных или даже к полному отказу систем. Отличаясь от умышленных кибератак, системные сбои чаще всего являются результатом внутренних недочетов, таких как ошибки в коде, неполадки оборудования, или неправильное управление ресурсами системы.

В сфере защиты от киберугроз и обеспечения функциональной надежности информационных систем управления, рекомендуется следовать основополагающим принципам: [5, с. 18]

1. Гарантированная кибербезопасность (устойчивость, надежность) в управляющих системах — недостижимый идеал.
2. Увеличение сложности системы и разнообразие ее функций пропорционально снижают уровень кибербезопасности.
3. Для укрепления кибербезопасности системы важно использовать резервирование в сочетании с продуманным контроллингом.
4. Обеспечение кибербезопасности в информационных системах управления необходимо на каждом этапе их жизненного цикла.

Уровень кибербезопасности системы, как правило, ограничен экономическим потенциалом заказчика. Полная кибербезопасность недостижима, поскольку устранение определенных уязвимостей не исключает возникновение новых. Кроме того, по мере развития защитных технологий, эволюционируют и методы атаки, и в условиях недостижимости абсолютной безопасности важно оценить уровень оставшихся рисков и обосновать меры безопасности системы.

Структура управления информационной безопасностью включает политики и методы контроля для управления безопасностью и рисками на корпоративном уровне. Эти меры могут следовать установленным стандартам безопасности или быть адаптированы под конкретные отраслевые требования. Компании должны разработать или адаптировать существующие системы кибербезопасности, чтобы они отражали реальные потребности в управлении безопасностью.

Система управления кибербезопасностью должна включать инструменты и процедуры для комплексного управления рисками и повышения осведомленности сотрудников. Она интегрируется в основные процессы организации, обеспечивая: [12, с. 29]

- планирование аварийного восстановления и оценку рисков;
- мониторинг и минимизацию рисков от постав-

щиков;
- оптимизированное управление рисками;
- соответствие нормативным стандартам.

Управление рисками играет ключевую роль в пресечении угроз на ранних стадиях. В современной цифровой эпохе составляющие системы кибербезопасности включают следующие элементы: [4, с. 210]

- защита кадров — развитие политик и стратегий, связанных с персоналом, в том числе снижение внутренних угроз и обучение для предотвращения ошибок в безопасности;
- урегулирование инцидентов информационной безопасности — оперативное решение ИТ-проблем, с ограничением их влияния на работу;
- операционное управление и коммуникация — поддержание политик безопасности в ходе эксплуатации систем;
- регулирование доступа — ограничение доступа персонала и мониторинг аномалий в сети;
- использование криптографии — управление криптографическими методами защиты;
- структурирование информационной безопасности — предотвращение угроз в корпоративной сети;
- управление связями с поставщиками — контрольные меры для минимизации рисков от доступа третьих лиц;
- стратегии информационной безопасности — создание специфических политик безопасности в компании;
- развитие и поддержка информационных систем — применение мер безопасности на всех этапах их жизненного цикла;
- соблюдение законодательства;
- активное управление активами и защита ресурсов компании;
- стратегии по минимизации потерь и восстановлению систем;
- физическая и окружающая безопасность — обеспечение надежности ИТ-оборудования.

Приведенные элементы формируют многоуровневую защиту против разнообразных киберугроз.

Рассмотрим примеры инновационных решений для улучшения управления информационной безопасностью: [1, с. 42]

1. EDR (Endpoint Detection and Response) — это передовая система безопасности для защиты конечных устройств от угроз. Она интегрирует активный мониторинг и сбор данных о конечных точках (ПЭВМ) в реальном времени, обеспечивая эффективное реагирование на сложные угрозы. Система непрерывно следит за конечными точками, обеспечивая оперативное реагирование на кибератаки. Данные анализируются в централизованной базе, что позволяет проводить тщательный анализ и составлять отчеты.

EDR повышает защиту пользователей вне корпоративного периметра от безфайловых атак и инфицированных устройств, а также дополняет традиционные меры безопасности для ликвидации уязвимостей в корпоративной сети.

EDR применяется для выявления различных угроз на основе анализа поведенческих паттернов, а не только стандартных индикаторов, таких как вирусы или нарушения брандмауэра. Вначале злоумышленники могут без препятствий управлять целевыми устройствами, однако последующие попытки расширения доступа или перехода к другим системам, вероятно, будут выявлены системой EDR или оставят заметные следы для специалистов по кибербезопасности.

Ключевым вызовом для компаний является представление срочных оповещений в доступном формате для упрощения идентификации угрозы и составления плана ответных действий. Обычные методы защиты нередко оставляют аналитиков без необходимой информации, затрудняя анализ и расследование угроз.

Типичные решения безопасности часто не фиксируют достаточно данных о деятельности в конечных точках. EDR решает эту проблему, предлагая возможности аудита и исследования угроз, давая более глубокое понимание стратегий злоумышленников [7, с. 38].

Таким образом, EDR дополняет традиционные

решения, обеспечивая детальный анализ и обзор после нарушения. Эти системы отслеживают все операции в конечных точках, выявляя направленные угрозы, перемещение внутри сети, использование скомпрометированных данных, внутренние угрозы и другие нетипичные действия. EDR записывает все сетевые события и активности на устройствах, предоставляя полезные данные для исследований и решения проблем безопасности, предлагая преимущества как в техническом, так и в бизнес-аспекте.

Недостатки EDR заключаются в неспособности отображать активность конечных точек без установленного агента EDR, требовании в квалифицированном персонале для эффективного выявления и реакции на инциденты, а также в ограниченной видимости сетевых операций, что позволяет скрытым угрозам незаметно перемещаться и взаимодействовать с удаленными серверами.

2. PIM/PAM/PUM — управление привилегированными аккаунтами. Данные системы предоставляют эффективный контроль доступа, включая управление паролями и учетными записями. Администраторы и пользователи с расширенными правами могут выполнять скрытые действия, представляя риск для информационных систем. [9, с. 125]

Привилегии, включающие права на настройку и выключение системы, управление учетными записями, становятся потенциальным источником проблем как из-за случайных ошибок, так и из-за умышленных действий. Управление привилегированным доступом включает в себя централизованное управление аутентификацией, аудит активности сети, мониторинг сессий и контроль над запуском приложений и выполнением команд.

Аналитические возможности системы управления привилегированным доступом предоставляют специалистам по безопасности инструменты для быстрого выявления подозрительных действий и сбора необходимых данных. В эту систему входят следующие ключевые компоненты: [11, с. 65]

- привилегированное управление идентификацией (PIM) — регламентирует доступ привилегированных пользователей к ресурсам и осуществляет мониторинг критических ресурсов;
- управление привилегированным доступом (PAM) — сосредоточено на менеджменте учетных записей с расширенными правами, устанавливая стратегии защиты конфиденциальных данных;
- управление привилегированными пользователями (PUM) — отвечает за контроль над пользователями, обладающими особыми правами.

Эти компоненты способствуют эффективному контролю доступа, уменьшают возможности для кибератак и помогают снизить ущерб от внешних нарушений, служебных злоупотреблений или невнимательности.

3. SIEM — это система, сочетающая управление информацией о безопасности (SIM) и управление событиями безопасности (SEM), которая обеспечивает комплексное управление инцидентами для организаций всех размеров. В его функции входят агрегация и анализ данных из разнообразных компонентов ИТ-структуры, а также представление обзора состояния информационной безопасности предприятия [3, с. 71].

SIEM объединяет хранение и интерпретацию данных журналов SEM с аналитическими возможностями SIM, что позволяет оперативно идентифицировать инциденты безопасности в реальном времени. Это решение выступает в роли защитного барьера для бизнес-процессов, распознавая различные виды киберугроз. Примером может служить распознавание обычной рабочей активности и подозрительных действий, в частности при попытках несанкционированного доступа.

SIEM ведет мониторинг журналов приложений, действий пользователей, состояния файлов и системных журналов. Ее задача — собирать и объединять данные из различных источников, включая сетевые и безопасностные устройства. Системы SIEM упрощают для сотрудников процесс

выявления проблем, ускоряя анализ активности и файлов, что способствует более эффективной отчетности в организации.

4. Программа Security Awareness — это образовательный сервис по информационной безопасности, разработанный для улучшения понимания сотрудниками протоколов безопасности, особенно тех, кто использует интернет в своей работе. Этот сервис повышает компетенции персонала в сфере безопасного обращения с информацией, тем самым снижая вероятность стоимостных инцидентов безопасности и утечек данных. Обучение помогает сотрудникам узнать больше о киберугрозах и приватности в интернете, делая их важной частью защиты информационных активов организации.

Сервис предназначен не только для службы безопасности и HR, но и для всего персонала. Он нацелен на уменьшение рисков, связанных с ошибками сотрудников, и на усиление ответственности каждого за соблюдение корпоративной политики безопасности. Постоянное обучение особенно важно в области постоянно меняющихся киберугроз и хакерских методов.

5. Кибербразведка (Threat Intelligence) представляет собой процесс сбора важной информации, который помогает компаниям осознавать и анализировать потенциальные угрозы безопасности. Данный подход включает анализ данных о возможных и текущих кибератаках для защиты ключевых корпоративных активов.

Автоматизированные платформы для кибербразведки эффективно обрабатывают обширные объемы информации, способствуя своевременному предотвращению и нейтрализации угроз. Эти системы предоставляют необходимые сведения о киберугрозах, включая их природу, методы, индикаторы, возможные последствия и конкретные рекомендации для действий.

Основные функции кибербразведки включают: [6, с. 28]

- аккумуляцию первичных данных о новейших и актуальных угрозах;
- проведение анализа и фильтрации информации, связанной с угрозами, для укрепления безопасности;
- предоставление информации о сложных угрозах, таких как продвинутые долгосрочные атаки, эксплойты неизвестных уязвимостей;
- оповещение о случаях нарушения безопасности данных и сервисов;
- сбор и обобщение данных об атаках, направленных как на саму компанию, так и на ее клиентов.

6. UAM (мониторинг активности пользователей) является неотъемлемым инструментом для защиты важных корпоративных данных в интернете, что напрямую влияет на безопасность и репутацию любого бизнеса. Эти системы обеспечивают наблюдение за действиями сотрудников онлайн, предотвращая угрозы безопасности.

UAM отслеживает действия пользователей на корпоративных устройствах, в сетях и облачных сервисах, обнаруживая утечки конфиденциальной информации и другие неправомерные действия. Возможности UAM включают определение устройств и рабочих мест, используемых сотрудниками; установление внутренних и внешних коммуникаций сотрудника; анализ собранной информации для выявления рисков; категоризацию наблюдаемых сотрудников для более эффективного управления [8, с. 157].

Таким образом, проведенное исследование показало, что эффективное решение проблем кибербезопасности требует комплексного подхода, включающего в себя не только технические, но и правовые и организационные аспекты, а также обучение и повышение осведомленности пользователей. Использование современных технологий защиты является необходимым, но недостаточным условием. Важно также уделять внимание правовому регулированию, разработке стандартов и протоколов, а также созданию организационных политик и процедур, которые помогут минимизировать риски и быстро реагировать на инциденты. Также стоит отметить важность непрерывного мониторинга и анализа угроз, что позволяет оперативно обновлять

стратегии и меры безопасности. В долгосрочной перспективе необходима постоянная работа над улучшением технологий кибербезопасности и адаптация к изменяющимся условиям киберпространства.

Выводы

Исследование подтвердило, что кибербезопасность в информационных системах управления — это не статичная дисциплина, а динамичная область, требующая непрерывного развития, обучения и адаптации. Учитывая быстро меняющуюся природу киберугроз, ключевым фактором успеха в области кибербезопасности является гибкость и готовность к постоянному обновлению знаний и практик. В заключение можно отметить, что реализация мероприятий по обеспечению кибербезопасности в информационных системах управления является не просто технической необходимостью, но и стратегическим приоритетом, способствующим устойчивому развитию и надежной работе организаций в условиях постоянно развивающегося цифрового мира.

Библиографический список

1. *Бабуханян А. Б.* Информационная и кибербезопасность в условиях цифровизации государственного управления // Научные труды Северо-Западного института управления РАНХиГС. — 2018. — Т. 9, 4 (36). — С. 39—43.
2. *Барашков А. И.* Обеспечения кибербезопасности систем управления в электроэнергетике // Студенческий. — 2018. — 11—7(31). — С. 5—8.
3. *Васильев В. И., Кириллова А. Д., Кухарев С. Н.* Кибербезопасность автоматизированных систем управления промышленных объектов (современное состояние, тенденции) // Вестник УрФО. Безопасность в информационной сфере. — 2018. — 4(30). — С. 66—74.
4. *Власенко В. Э.* Кибератаки: как государства реагируют на инциденты, затрагивающие кибербезопасность информационных систем на современном этапе международного информационного права // Молодой ученый. — 2021. — 48(390). — С. 208—211.
5. *Золотарев П. С.* О подходах к обеспечению кибербезопасности систем управления ядерным оружием // США и Канада: экономика, политика, культура. — 2020. — Т. 50, № 10. — С. 5—25.
6. Кибербезопасность РЗА и систем управления современных объектов электроэнергетики // Вести в электроэнергетике. — 2021. — 2 (112). — С. 24—31.
7. *Киселев И. В., Рубан К. А.* Кибербезопасность компании: сравнительный анализ отечественных систем управления событиями и информацией о безопасности (SIEM) // Корпоративная экономика. — 2022. — 4(32). — С. 34—39.
8. *Леладзе Д., Сванадзе В.* Проблемы и решения для управления кибербезопасностью и информационной безопасностью в организациях // Научный журнал Власть и общество (История, Теория, Практика). — 2021. — 2(58). — С. 152—169.
9. *Мироненко И. Н.* Искусственный интеллект и кибербезопасность как основа управления экономическими системами // Экономика и управление: проблемы, решения. — 2021. — Т. 6, 12 (120). — С. 121—132.
10. *Московченко В. М., Гудков М. А., Лаута О. С.* Робототехническая система анализа кибербезопасности информационных систем и сетей связи // НБИ технологии. — 2018. — Т. 12, № 2. — С. 30—38.
11. *Промыслов В. Г., Семенков К. В., Шумов А. С.* Синтез архитектуры кибербезопасности для систем управления атомных электростанций // Проблемы управления. — 2019. — № 3. — С. 61—71.
12. *Ронжина Н. А., Глазатов А. А.* Развитие системы кибербезопасности в Российской Федерации как основное условие обеспечения национальной информационной безопасности // Право. Безопасность. Чрезвычайные ситуации. — 2023. — 1(58). — С. 24—34.
13. Annual share of organizations affected by ransomware attacks worldwide from 2018 to 2023 / Statista. — 2024. — URL: https://www.statista.com/statistics/204457/businesses-ransomware-attack-rate.
14. *Fleck A.* Cybercrime Expected To Skyrocket in Coming Years / Statista. — 2024. — URL: https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027.