Ученые записки Крымского федерального университета имени В. И. Вернадского. Экономика и управление. 2024. Т. 10 (76). № 3. С. 45–57.

УДК 004.056.5

АРХИТЕКТУРА НУЛЕВОГО ДОВЕРИЯ КАК ИННОВАЦИОННЫЙ ИНСТРУМЕНТ В СИСТЕМЕ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ КОРПОРАТИВНОЙ ИНФОРМАЦИИ

Кирильчук С. П., Аблитаров Э. Р.

Крымский федеральный университет имени В. И. Вернадского, Симферополь, Российская Федерация
E-mail: ablitaroff@mail.ru

В статье исследована роль архитектуры нулевого доверия как инновационного инструмента в системе обеспечения защиты корпоративной информации, подчеркнуто стратегическое значение информационной безопасности для устойчивого развития хозяйствующих субъектов. Представлены основные детерминанты внедрения архитектуры нулевого доверия в корпоративные информационные системы, отразившие такие тенденции, как рост рынка решений нулевого доверия, увеличение адаптации данного подхода предприятиями и недостаточность традиционных моделей защиты периметра в противостоянии современным киберугрозам. Компаративный анализ традиционных и инновационных методических инструментов защиты корпоративной информации показал более высокую эффективность принципов нулевого доверия, характеризующихся постоянной аутентификацией и авторизацией, микросегментацией и принципом минимальных привилегий, которые позволяют повысить уровень безопасности и снизить риски, связанные с кибератаками и утечками данных. В исследовании очерчены основные препятствия устойчивого внедрения архитектуры нулевого доверия, такие как отсутствие единых стандартов и моделей реализации, сложность интеграции в существующую инфраструктуру и значительные первоначальные инвестиции, исходя из которых предложены меры совершенствования системы информационной безопасности предприятия, включая соблюдение национальных стандартов и системный подход к внедрению.
Ключевые слова: архитектура нулевого доверия, информационная безопасность, инструменты защиты, киберугрозы, предприятие, барьеры внедрения.

ВВЕДЕНИЕ

Масштабное распространение информационно-коммуникационных технологий, рост объемов корпоративных данных и увеличение числа киберугроз формируют новые вызовы для бизнеса, требующие инновационных и эффективных решений. В современных реалиях информационная безопасность становится неотъемлемой частью конкурентоспособности организаций, а обеспечение защиты корпоративной информации – ключевым фактором их успешной деятельности, что также подтверждается заявлением Президента Российской Федерации: «В современных условиях, когда киберугрозы становятся все более изощренными, развитие комплексных стратегий информационной безопасности является приоритетной задачей для обеспечения национальной безопасности страны».

На современном этапе цифровой трансформации и глобализации информационных процессов актуальность и перспективы внедрения архитектуры нулевого доверия в корпоративные информационные системы представляют собой ключевые векторы обеспечения информационной безопасности предприятий, что обусловлено такими уникальными характеристиками данного подхода, как повышенная адаптивность к современным киберугрозам и способность к быстрой

реакции на инциденты безопасности. Обозначенные аспекты подчеркивают потенциал архитектуры нулевого доверия как инновационного инструмента, способствующего укреплению защиты корпоративных данных и инфраструктуры, а также повышению устойчивости бизнеса в условиях постоянно меняющейся цифровой среды. Данные особенности предопределяют возможности ускоренного внедрения принципов нулевого доверия, которые могут стать локомотивом развития современных систем информационной безопасности в условиях постоянных трансформаций глобальной и национальной экономической системы.

Однако в результате усложнения киберугроз и увеличения числа точек доступа к корпоративным ресурсам предприятия столкнулись с серьезными препятствиями, затрудняющими эффективную защиту информации. Снижение эффективности традиционных моделей защиты периметра, нехватка средств для обеспечения комплексной безопасности, а также рост удаленной работы и использования облачных сервисов обозначили критическую необходимость выработки и реализации инновационных подходов, нацеленных на усиление информационной безопасности. По данным отчета о кибербезопасности компании «Microsoft», «96 % руководителей ИБ–подразделений считают разработку стратегии Zero Trust главным приоритетом в области безопасности, критически важным для успеха их организации» [1, с. 5]. Данное утверждение подчеркивает актуальность перехода к новым концепциям защиты информации и необходимости системного подхода к внедрению архитектуры нулевого доверия.

Вышеприведенные негативные аспекты угроз информационной безопасности усугубляются тем, что несмотря на высокую заинтересованность в архитектуре нулевого доверия, единых стандартов и моделей ее реализации не существует. Каждое предприятие обладает уникальной инфраструктурой, бизнес–процессами и требованиями к безопасности, что затрудняет универсальное применение концепции нулевого доверия. В частности, у крупных организаций с разветвленной структурой и наследованными системами возникают сложности при интеграции новых подходов без ущерба для текущих бизнес–операций.

Актуальность исследования заключается в острой необходимости выявления критериев и разработки модели интеграции архитектуры нулевого доверия в корпоративные информационные системы с учетом специфики предприятия, существующей инфраструктуры и требований к безопасности. Необходимость решения данной проблемы также обусловлена возрастанием числа кибератак, сложностью современных угроз информационной безопасности и недостаточной эффективностью традиционных методов защиты.

Проблемы обеспечения информационной безопасности в условиях цифровой трансформации широко освещаются в отечественных и зарубежных исследованиях. Иванов П. А., Капгер И. В. и Шабуров А. С. [2] изучили модели управления доступом к информационным активам в контуре концепции нулевого доверия, подчеркивая необходимость перехода от традиционных моделей защиты периметра к более адаптивным системам, способным эффективно противостоять современным киберугрозам. Авторы акцентировали внимание на важности многофакторной аутентификации и микросегментации сети для повышения уровня безопасности.

Астахова Л. В. [5] рассматривала влияние модели нулевого доверия на информационное поведение сотрудников организаций. Исследование подчеркивает, что внедрение данной концепции требует не только технических изменений, но и перестройки корпоративной культуры, что способствует повышению общей устойчивости предприятия к внутренним и внешним угрозам. Кроме того, отчет консалтинговой компании Gartner [13] предоставил базу для определения экономических преимуществ архитектуры нулевого доверия, ключевым среди которых обозначено снижение финансовых потерь от кибератак для организаций, внедривших эту концепцию.

В отчете зарубежной компании «Microsoft» [1] подчеркивается глобальная тенденция к внедрению стратегии нулевого доверия как приоритета в информационной безопасности. Согласно отчету, «96% руководителей ИБ–подразделений считают разработку стратегии нулевого доверия критически важной для успеха их организации».

Нормативно-правовые аспекты внедрения архитектуры нулевого доверия отражены в национальных стандартах Российской Федерации, таких как ГОСТ Р 59993–2022 [8], ГОСТ Р 59344–2021 [9] и ГОСТ Р 59990–2022 [10]. Стандарты устанавливают основные положения системного анализа и требования к процессам управления инфраструктурой, что создает базис для успешного внедрения концепции нулевого доверия.

Тем не менее, несмотря на обширный спектр исследований в области архитектуры нулевого доверия, недостаточно изучены критерии и модели интеграции данной архитектуры в корпоративные информационные системы с учетом специфики предприятий, их существующей инфраструктуры и требований к безопасности. Отсутствие единых стандартов и методик внедрения затрудняет универсальное применение концепции нулевого доверия, что обуславливает актуальность настоящего исследования. Необходимость решения данной проблемы также обусловлена возрастанием числа кибератак, усложнением современных угроз информационной безопасности и недостаточной эффективностью традиционных методов защиты.

Приведенные неразрешенные вопросы усугубляются отсутствием единых стандартов и моделей реализации концепции нулевого доверия на предприятии, как подчеркивается в работе Валеева С. С., Кондратьевой Н. В. и Мельникова А. В. [11], в которой авторы выделяют основные этапы реинжиниринга информационной системы предприятия в рамках технологии нулевого доверия и обращают внимание на сложности интеграции в существующую ИТ–инфраструктуру предприятия, а именно, необходимость кардинального пересмотра существующих политик безопасности и обеспечения полной совместимости с уже используемыми системами и приложениями.

Цель исследования состоит в разработке рекомендаций по интеграции архитектуры нулевого доверия в корпоративные информационные системы с учетом специфики предприятия, существующей инфраструктуры и требований к безопасности.

В качестве эмпирической базы исследования использовались данные отчетов ведущих организаций в области информационной безопасности, в том числе, Microsoft [1], Gartner [13] и Value Market Research [3], а также нормативно-правовые документы Российской Федерации, в частности, национальные стандарты ГОСТ [8–10]. Проведен анализ существующих решений на рынке информационной безопасности, таких как системы SearchInform, Solar Dozor, Forcepoint, ИНСАЙДЕР и Perimetrix [6], для оценки их соответствия принципам архитектуры нулевого доверия и возможности интеграции в корпоративную среду.

Методологическую основу исследования составили: методы системного и компаративного анализа (при сравнении традиционных и инновационных инструментов защиты корпоративной информации), метод синтеза (для разработки модели интеграции архитектуры нулевого доверия в корпоративные информационные системы), методы обобщения и синтеза (для формирования перспективных направлений внедрения архитектуры нулевого доверия). Также проведен анализ действующих национальных стандартов в области системной инженерии и защиты информации для обеспечения соответствия разработанных рекомендаций требованиям законодательства.

Для оценки экономической эффективности внедрения архитектуры нулевого доверия использовались статистические данные и аналитические отчеты, позволяющие сравнить затраты и выгоды от применения данной концепции в корпоративной практике.

ОСНОВНОЙ МАТЕРИАЛ

Концепция нулевого доверия основана на принципе «никому не доверять, все проверять», другими словами, полного недоверия ко всем субъектам и объектам доступа [2, с. 149]. Подразумевается, что доступ к корпоративным ресурсам предоставляется только после тщательной аутентификации и авторизации каждого запроса независимо от их расположения внутри или вне корпоративной сети. В отличие от традиционных моделей, где основное внимание уделяется защите периметра, концепция нулевого доверия фокусируется на защите самих ресурсов и данных. Согласно прогнозам поставщика отчетов о маркетинговых исследованиях «Value Market Research», «рынок архитектуры нулевого доверия был оценен в 16,9 млрд долл. США, при этом прогнозируется среднегодовой темп роста более 16,5 % в период с 2024 по 2030 годы» [3], что подчеркивает глобальную ориентацию на внедрение концепции нулевого доверия в корпоративную практику (таблица 1).

Таблица 1. Прогноз динамики роста рынка архитектуры нулевого доверия в период с 2024 по 2030 гг.

Год	Оценка рынка, млрд долл. США	Среднегодовой темп роста, %
2024	19,7	X
2025	22,9	16,5
2030	58,58	18,12

Источник: составлено авторами.

Как видно из таблицы 2, предприятия в практике обеспечения информационной безопасности используют различные методические инструменты ее защиты, которые можно условно разделить на организационные и технические меры. К организационным мерам относятся разработка и внедрение политики конфиденциальности, обучение сотрудников принципам информационной безопасности, регулярное тестирование и аудит системы защиты. Технические меры включают аппаратную и программную защиту серверов и рабочих станций, использование сетевых экранов, VPN, систем контроля доступа и других средств [4, с. 610].

Таблица 2. Сравнительный анализ методических инструментов защиты корпоративной информации

Инструмент	Содержание	Преимущества	Недостатки
Политика конфиденциальности	Требования к неразглашению информации и материальная ответственность	Повышение осведомленности сотрудников; юридическая защита	Зависимость от человеческого фактора; возможны нарушения
Аппаратная и программная защита	Антивирусы, резервное копирование данных	Защита от вредоносного ПО; сохранность данных при сбоях	Незащищенность от внутренних угроз; требуется регулярное обновление
Защита от корпоративных атак	Сетевые экраны, защищенные протоколы, VPN	Предотвращение внешних атак; контроль сетевого трафика	Сложность настройки; неэффективность против инсайдерских угроз
Физическое ограничение доступа	Системы контролируемого доступа к серверным помещениям	Защита критической инфраструктуры; контроль физического доступа	Существенные затраты на оборудование; незащищенность от кибератак
Регулярное тестирование безопасности	Аудит и оценка уязвимостей системы	Выявление слабых мест; возможность своевременного исправления	Ресурсоемкость; необходима высокая квалификация специалистов
Обучение сотрудников	Тренинги и семинары по информационной безопасности	Повышение уровня знаний персонала; снижение рисков человеческой ошибки	Трудоемкость; возможна низкая вовлеченность сотрудников

Источник: составлено авторами.

Каждый из представленных в таблице 2 инструментов обеспечения информационной безопасности предприятий обладает уникальными преимуществами и недостатками. Однако общий недостаток традиционных методов заключается в том, что они не обеспечивают должного уровня защиты в условиях современных киберугроз, особенно связанных с внутренними угрозами и мобильностью бизнеса.

Отсюда следует, что традиционные методические инструменты обеспечения защиты корпоративной информации не в полной мере отвечают современным вызовам кибербезопасности. Архитектура нулевого доверия выступает как инновационный инструмент, способный усилить защиту за счет применения принципов микросегментации, минимальных привилегий и постоянной аутентификации. «Для предприятия, стремящегося сохранить конкурентоспособность и обеспечить устойчивое развитие в цифровой экономике, внедрение концепции нулевого доверия становится не просто желательным, а необходимым шагом» [5, с. 17].

В этой связи актуализируется вопрос применения специализированных систем защиты корпоративной информации, реализующих принципы архитектуры нулевого доверия. Рассмотрим наиболее распространенные решения на финтех рынке [6, с. 65]:

1. SearchInform. Система «СерчИнформ Контур информационной безопасности» предоставляет инструменты для анализа корпоративных сетей, контроля действий сотрудников в реальном времени, блокировки передачи данных на внешние устройства и архивирования активности.

2. Solar Dozor. Система предназначена для контроля общения сотрудников, предотвращения хищения данных и выявления фактов мошенничества. Система анализирует широкий спектр данных, включая текстовые и голосовые сообщения, техническую документацию, и формирует скриншоты рабочих столов, что в совокупности закладывает базис для автоматического анализа поведения пользователей и выявления внутренних мошеннических действий.

3. Forcepoint. Система защищает данные как внутри сети предприятия, так и за ее пределами; использует поведенческий анализ для определения потенциально опасных пользователей, что сокращает количество ложных срабатываний и повышает эффективность системы безопасности.

4. ИНСАЙДЕР. Высокотехнологичная система для контроля коммуникаций персонала и выявления утечек информации. Обеспечивает диагностику ПК сотрудников в реальном времени, фиксирует скриншоты рабочих столов и анализирует цифровые отпечатки персонала.

5. Perimetrix. Система ориентирована на введение и поддержку режима секретности в крупных организациях. Контролирует полный жизненный цикл корпоративных данных от момента их создания до утилизации, обеспечивая высокий уровень защиты.

Синтезируя направленность представленных ИТ–решений защиты корпоративной информации, приведем сравнительную характеристику представленных систем (таблица 3).

Таблица 3. Сравнительный анализ систем защиты корпоративной информации

Система	Основные функции	Преимущества	Недостатки
SearchInform	Анализ сетей, контроль действий, блокировка передачи данных	Реальный контроль; предотвращение утечек	Требует интеграции с существующей инфраструктурой
Solar Dozor	Контроль общения, перехват сообщений, скриншоты	Широкий спектр анализируемых данных; глубокий контроль	Возможны вопросы конфиденциальности сотрудников
Forcepoint	Защита данных внутри и вне сети, поведенческий анализ	Снижение ложных срабатываний; адаптивная безопасность	Высокая стоимость внедрения и поддержки
ИНСАЙДЕР	Контроль коммуникаций, диагностика ПК, анализ отпечатков	Высокотехнологичность; детальный контроль	Требует обученного персонала для управления
Perimetrix	Управление жизненным циклом данных, поддержка секретности	Полная интеграция с процессами; высокий уровень защиты	Подходит для крупных организаций; сложность внедрения

Источник: составлено авторами.

Стоит отметить, что выбор конкретного инструмента или системы зависит от потребностей предприятия, его масштабов, отраслевой специфики и имеющихся ресурсов [7, с. 1370]. Однако все перечисленные решения в той или иной степени реализуют принципы архитектуры нулевого доверия, что подтверждает практическую применимость данной концепции.

Для более глубокого понимания правовой среды функционирования архитектуры нулевого доверия обратимся к основным положениям, закрепленным в национальных стандартах Российской Федерации:

1. ГОСТ Р 59993–2022 «Системная инженерия. Системный анализ процесса управления инфраструктурой» устанавливает основополагающие требования к процессам управления инфраструктурой системы, количественным показателям, способам формализации, моделям, методам и критериям, что является базисом для внедрения нулевого доверия [8].

2. ГОСТ Р 59344–2021 «Системная инженерия. Защита информации в процессе анализа бизнеса или назначения системы» устанавливает положения системного анализа для процесса анализа бизнеса или назначения системы применительно к вопросам защиты информации в системах различных областей приложения, что по своей сути обеспечивает успех в вопросах защиты информации в различных системах [9].

3. ГОСТ Р 59990–2022 «Системная инженерия. Системный анализ процесса оценки и контроля проекта» устанавливает основные положения системного анализа процесса оценки и контроля проекта, связанного с созданием (модернизацией, развитием) и эксплуатацией систем различных областей применения, что неизбежно обеспечивает успешное внедрение инновационных систем защиты информации [10].

Учет нормативных требований обеспечивает не только соответствие законодательству, но и повышает доверие со стороны партнеров и клиентов, что важно для репутации предприятия. Ключевым дополнением к соблюдению данных требований является учет основных принципов архитектуры нулевого доверия [2, с. 157]:

1) постоянная проверка и аутентификация: каждый запрос на доступ к ресурсу должен быть проверен, а пользователь или устройство аутентифицированы. Для этого используются многофакторная аутентификация (MFA), контроль подлинности устройств и проверка соответствия политикам безопасности;

2) микросегментация сети: разделение сети на небольшие сегменты или зоны безопасности позволяет ограничить распространение угрозы в случае компрометации одного из сегментов, что достигается с помощью виртуальных локальных сетей (VLAN), программно-определяемых сетей (SDN) и систем предотвращения вторжений (IPS).

3) принцип минимальных привилегий: каждому пользователю, устройству или приложению предоставляются только те права доступа, которые необходимы для выполнения их функций. Это снижает риск неправомерного доступа и злоупотребления привилегиями;

4) контекстуальный доступ: решения о предоставлении доступа принимаются на основе анализа контекста запроса, включая местоположение, время, тип устройства и поведение пользователя, что позволяет более точечно оценивать риски и предотвращать потенциальные угрозы;

5) непрерывный мониторинг и аналитика: постоянное отслеживание активности в сети и анализ поведения пользователей и устройств позволяют своевременно обнаруживать аномалии и реагировать на инциденты безопасности.

Обозначенные принципы нулевого доверия закладывают основу для успешной реализации данной концепции тем, что каждый участник системы, будь то пользователь, устройство или приложение, рассматривается как потенциально небезопасный, и все действия должны быть подтверждены и проверены перед тем, как предоставлять доступ к данным или ресурсам системы. Это означает, что даже если участники системы считаются надежными, необходимы механизмы, которые обеспечивают их подлинность, целостность и конфиденциальность, чтобы обезопасить систему от внутренних и внешних угроз.

На базе приведенных принципов [2, с. 157–160] реализуется механизм функционирования архитектуры нулевого доверия (рисунок 1).

Рисунок 1. Мультипликативная модель функционирования архитектуры нулевого доверия на предприятии

Источник: разработано авторами.

Таким образом, основополагающий принцип данной архитектуры состоит в том, что ни один пользователь или устройство не получает доступа к ресурсам без предварительной многофакторной аутентификации и авторизации, подкрепленной микросегментацией сети и постоянным мониторингом. В соответствии с этим утверждением внедрение архитектуры нулевого доверия в систему защиты корпоративной информационной безопасности предполагает комплексную перестройку подходов к безопасности. В частности, интегрируются следующие компоненты (таблица 4):

Таблица 4. Сравнительный анализ методических инструментов защиты корпоративной информации

Компонент	Функции
Системы IAM	Управление идентификацией, правами доступа
Многофакторная аутентификация (MFA)	Улучшение аутентификации пользователей
Программно-определяемые периметры (SDP)	Динамическое управление границами безопасности
Системы MDM и MAM	Контроль и защита устройств и приложений
Системы SIEM	Мониторинг анализ событий безопасности

Источник: разработано авторами.

Важно отметить, что архитектура нулевого доверия не является конкретным продуктом или технологией, а представляет собой концептуальную модель, которую предприятие адаптирует под специфику своей деятельности [11, с. 140]. Рассматриваемая концепция требует системного подхода к ее внедрению, включающего следующие этапы (рисунок 2):

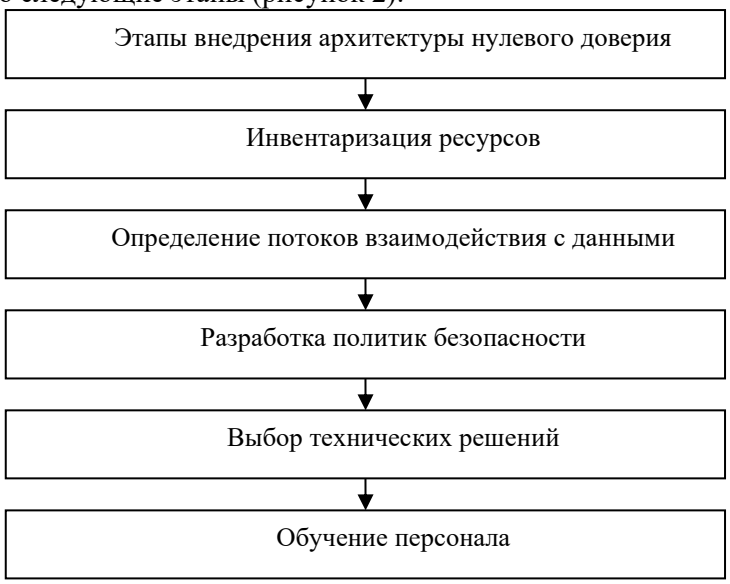

Рисунок 2. Этапы внедрения архитектуры нулевого доверия на предприятии

Источник: разработано авторами.

На первом этапе происходит идентификация всех пользователей, устройств, приложений и данных, а также оценка их ценности и уязвимостей.

На втором этапе проводится анализ того, как данные перемещаются внутри организации и как взаимодействуют различные компоненты системы.

На третьем этапе формируются правила и процедуры, регулирующие доступ к ресурсам на основе принципов нулевого доверия.

На четвертом этапе происходит интеграция необходимых инструментов и технологий, соответствующих разработанным политикам.

На заключительном этапе обеспечивается понимание концепции нулевого доверия среди сотрудников и формируется культура безопасности.

«Одной из ключевых задач при внедрении нулевого доверия является достижение баланса между повышением уровня безопасности и финансовым благополучием предприятия» [12, с. 51]. Поскольку внедрение архитектуры нулевого доверия, с одной стороны, связано с затратами на ИТ–технологии, обучение персонала и затратами на обновлении ИТ–инфраструктуры, а с другой, – повышает уровень информационной безопасности хозяйствующего субъекта, данные издержки следует рассматривать как стратегические вложения в снижение рисков кибератак, утечек данных и связанных с ними финансовых и репутационных потерь.

По данным консалтинговой компании в области информационных технологий «IBM», средняя стоимость утечки данных для предприятия в 2024 году составила 4,45 млн. долл. США. При этом компании, внедрившие принципы нулевого доверия, снижают риск утечек на 43 % по сравнению с организациями, использующими традиционные методы защиты [13]. Более детальный анализ приведен в таблице 5.

Таблица 5. Сравнительный анализ архитектуры нулевого доверия по принципу «выгоды–затраты»

Показатель	Без внедрения	С внедрением
Средняя стоимость утечки данных	4,45 млн. долл. США	2,45 млн. долл. США
Инвестиции в безопасность	1 млн. долл. США	2 млн. долл. США
Вероятность успешной кибератаки	Высокая	Низкая
Репутационные риски	Высокие	Низкие
Общий экономический эффект	Отрицательный	Положительный

Источник: составлено авторами по данным [13].

Из таблицы 5 видно, что несмотря на более высокие первоначальные затраты на внедрение архитектуры нулевого доверия, общий экономический эффект для предприятия положительный за счет снижения вероятности киберинцидентов и связанных с ними расходов. Это объясняется тем, что концепция нулевого доверия сокращает поверхность атаки за счет ограничения прав доступа и сегментирования корпоративной сети. Следовательно, сокращается время, необходимое для обнаружения взлома, что позволяет минимизировать ущерб и ограничить утечку данных.

Учитывая вышеизложенное, сущность применения архитектуры нулевого доверия на базе предприятия заключается в том, что система автоматически проводит процедуру аутентификации и авторизации пользователя, прежде чем предоставить ему доступ к какому-либо приложению, базе данных или другим ресурсам организации. В рамках этой концепции при допуске к активам или учетным записям пользователей осуществляется постоянная проверка их местоположения, идентификатора устройства, типа операционной системы, особенностей использования активов.

ВЫВОДЫ

Проблематика обеспечения информационной безопасности корпоративных систем в современных условиях связана с усложнением киберугроз и неэффективностью традиционных моделей защиты периметра. Среди ключевых проблем необходимо отметить увеличение числа точек доступа к корпоративным ресурсам, рост удаленной работы, использование облачных сервисов и отсутствие единых стандартов внедрения архитектуры нулевого доверия. В совокупности данные факторы затрудняют эффективную защиту корпоративной информации и повышают риск кибератак и утечек данных, что негативно сказывается на устойчивом развитии предприятий.

Для повышения уровня информационной безопасности представляется целесообразным рассмотреть следующие предложения. Во–первых, необходимо интегрировать принципы архитектуры нулевого доверия в корпоративные информационные системы, что подразумевает постоянную аутентификацию и авторизацию пользователей и устройств, микросегментацию сети и применение принципа минимальных привилегий. Данное предложение позволит повысить уровень защиты корпоративных ресурсов, снизить риски несанкционированного доступа и оперативно реагировать на инциденты безопасности.

Во–вторых, целесообразно осуществить системный подход к внедрению архитектуры нулевого доверия, учитывающий специфику предприятия, существующую инфраструктуру и требования к безопасности. Необходимо провести инвентаризацию ресурсов, определить потоки данных, разработать политики безопасности и выбрать подходящие технические решения. Данное решение позволит обеспечить интеграцию новых подходов без ущерба для текущих операций и повысить эффективность системы информационной безопасности в целом.

В качестве дополняющей меры рекомендуется соблюдать национальные стандарты в области информационной безопасности и активно обучать персонал принципам нулевого доверия. Данный шаг укрепит культуру безопасности внутри организации, повысит осведомленность сотрудников о современных киберугрозах и способах их предотвращения. Важно также обеспечить доступность данных инструментов для всех подразделений предприятия, включая удаленные офисы и филиалы. Приведенные меры позволят создать надежную экосистему защиты корпоративной информации, стимулировать инновационное развитие и обеспечить устойчивость бизнеса в условиях цифровой трансформации.

В качестве дальнейших перспектив исследования представляется целесообразным выработка эффективных мер упрощения интеграции элементов архитектуры нулевого доверия в существующие ИТ–системы хозяйствующих субъектов, оптимизация первоначальных инвестиций посредством масштабирования ИТ–решений, а также совершенствование системы информационной безопасности предприятия с учетом системного подхода к внедрению архитектуры нулевого доверия.

Список литературы

1. Microsoft. Zero Trust Adoption Report. 2021. 24 p. [Электронный ресурс]. URL: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWGWha.

2. Иванов П. А., Капгер И. В., Шабуров А. С. Модель реализации управления доступом к информационным активам в концепции нулевого доверия // Вестник Пермского национального исследовательского политехнического университета. Электротехника, информационные технологии, системы управления. 2023. № 45. С. 147–163. DOI 10.15593/2224-9397/2023.1.07.

3. Value Market Research. Глобальный рынок архитектуры нулевого доверия [Отчет]. 2024. [Электронный ресурс]. URL: https://www.valuemarketresearch.com/ru/report/zero-trust-architecture-market/toc.

4. Kirilchuk S. P., Reutov V. E., Nalivaychenko E. V. [et al.] Ensuring the security of an automated information system in a regional innovation cluster // X International Scientific Siberian Transport Forum – TransSiberia 2022, Novosibirsk, 02–05 марта 2022 года. Novosibirsk: Elsevier B. V., 2022. P. 607–617. DOI 10.1016/j.trpro.2022.06.054.

5. Астахова Л. В. Модель нулевого доверия как фактор влияния на информационное поведение сотрудников организации // Научно-техническая информация. Серия 1: Организация и методика информационной работы. 2022. № 3. С. 13–17. DOI 10.36535/0548-0019-2022-03-2.

6. Методика оценки уровня критичности уязвимостей программных, программно-аппаратных средств // Вестник ветеринарии. 2023. № 1 (104). С. 64–67.

7. Скользнев Г. О., Канапухин П. А. Анализ эффективности и влияния корпоративной разведки на конкурентоспособность компаний в современной экономике // Экономика и предпринимательство. 2023. № 5 (154). С. 1368–1371. DOI 10.34925/EIP.2023.154.5.273.

8. ГОСТ Р 59993–2022. Национальный стандарт Российской Федерации. Системная инженерия. Системный анализ процесса управления инфраструктурой системы» (утв. и введен в действие Приказом Росстандарта от 17.08.2022 № 773–ст) // СПС КонсультантПлюс. [Электронный ресурс]. URL: https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=OTN&n=34152#k4k4EUUWeWcUxMYD1.

9. ГОСТ Р 59344–2021. Национальный стандарт Российской Федерации. Системная инженерия. Защита информации в процессе анализа бизнеса или назначения системы» (утв. и введен в действие Приказом Росстандарта от 28.04.2021 № 316–ст) // СПС КонсультантПлюс. [Электронный ресурс]. URL: https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=OTN&n=30728#JUS6EUUsvQUQXCKu.

10. ГОСТ Р 59990–2022. Национальный стандарт Российской Федерации. Системная инженерия. Системный анализ процесса оценки и контроля проекта» (утв. и введен в действие Приказом Росстандарта от 17.08.2022 № 770–ст) // СПС КонсультантПлюс. [Электронный ресурс]. URL: https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=OTN&n=30728#JUS6EUUsvQUQXCKu.

11. Валеев С. С., Кондратьева Н. В., Гузаиров М. Б., Мельников А. В. Этапы реинжиниринга информационной системы предприятия в рамках технологии нулевого доверия // Вестник Российского нового университета. Серия: Сложные системы: модели, анализ и управление. 2023. № 3. С. 136–143. DOI 10.18137/RNU.V9187.23.03.P.136.

12. Валеев С. С., Кондратьева Н. В., Мельников А. В. Архитектура предприятия и архитектура нулевого доверия // Вестник УрФО. Безопасность в информационной сфере. 2023. № 2 (48). С. 49-53. DOI 10.14529/secur230204.

13. IBM. Cost of a Data Breach Report. 2024. [Электронный ресурс]. URL: https://www.ibm.com/downloads/documents/us-en/107a02e94948f4ec.

Статья поступила в редакцию 15.11.2024