МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНСТИТУТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И АНАЛИЗА ДАННЫХ
КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

КУРСОВОЕ ПРОЕКТИРОВАНИЕ 1

Анализ современных способов разграничения доступа

Студент _____ В. В. Карпов

Руководитель
канд. экон. наук, доцент _____ Е.Г. Шумик

Нормоконтролер
канд. экон. наук, доцент _____ Е.Г. Шумик
(нормоконтролер руководитель)

Владивосток 2026

Содержание

Введение

В современной экономике, динамично растущей цифровизации информации стала важнейшим активом организаций. Все виды бизнес-процессов, все формы государственных услуг, производства и управления предполагают работу с большими данными в системах разных типов. На фоне роста процессов цифровизации наблюдается одновременный рост угроз информационной безопасности – это несанкционированный доступ к данным, утечки информации, злоупотребление полномочий пользователей, различные типы атак на корпоративные ИС и другие угрозы. Отсюда следует высокая важность обеспечения качественного разграничения доступа к информационным ресурсам.

Разделение прав доступа – это меры, как административные так технические, позволяющие предоставить пользователям информацию или ресурсы в объеме исключительно необходимом им для работы. Использование такого принципа помогает защитить информационные системы от утечки информации, несанкционированного изменения и получения данных, тем самым избежать рисков ИБ [1]. В наше время системы контроля доступа являются неотъемлемой частью любой корпоративной информационной среды, вне зависимости от отрасли.

Эволюция средств управления доступом шла параллельно с развитием информационной техники. Для начальных этапов развития ИТ были характерны примитивные средства управления доступом, рассчитанные на малый круг субъектов и объектов. Усложнение корпоративных информационных систем, появление распределенных вычислений, облачных вычислений, мобильных терминалов стали причиной резкого усложнения процессов администрирования прав. Сформировалась потребность в создании новых решений для обеспечения надежности использования ИС без ущерба для их доступности.

Наиболее распространенными являются дискреционные, мандатные и ролевые схемы контроля доступа [2]. Все они имеют свои плюсы и минусы. У дисперсионной модели есть возможность гибкого контроля прав пользователей,

но при этом возможен рост избыточных прав и ошибок в управлении. При использовании мандатного подхода контроль доступа жестко регламентируется по уровням безопасности, зато не хватает гибкости. Ролевая модель дает возможность значительно облегчить контроль над правами доступа, т. к. при ее использовании происходит консолидация прав по категориям должностей работников организации. По этой причине данная модель активно применяется в коммерческих компаниях и на уровне органов государственного управления.

Современные тенденции развития информационных технологий способствуют появлению новых моделей управления доступом. Особую популярность приобретают атрибутивные механизмы, учитывающие широкий набор характеристик пользователей, информационных ресурсов и условий выполнения запросов. Значительное внимание уделяется концепции Zero Trust, предполагающей постоянную проверку субъектов доступа независимо от их местоположения в корпоративной сети [3]. Кроме того развиваются такие направления как управление привилегированными учетными записями (PAM), многоуровневая аутентификация и анализ рисков для принятия решений. Благодаря применению таких технологий компании смогут успешно бороться с актуальными проблемами безопасности информации и гарантировать сохранность корпоративных ресурсов.

Для отечественных компаний актуальны вопросы классификации доступа. Активное развитие процессов цифровизации, импортозамещения ПО и построения объектов КИИ обусловливает необходимость использования новейших средств обеспечения информационной безопасности в соответствии с законодательством Российской Федерации и требованиями регулирующих органов. Федеральной службой по техническому и экспортному контролю Российской Федерации, Федеральную службу безопасности Российской Федерации. Актуальные вопросы идентификации, аутентификации и управления доступом в информационных системах разных уровней защищенности рассматривались этими ведомствами [3] В этой связи актуализируется

потребность во внедрении новых моделей разграничения доступа как средства защиты данных, так и обеспечения комплаенса (compliance).

Примером практического использования актуальных методов управления доступом может служить большая российская ИТ-компания, имеющая мощную информационную систему. Примером такой компании является Sitronics Group. Она занимается реализацией проектов по цифровой трансформации, ЦОД, разработкой ПО, инфраструктурным решениям и системам безопасности информации. Масштабы деятельности требуют разработки многоуровневой системы управления правами доступа, гарантирующей сохранность как внутренних данных предприятия, так и информации пользователей. Исследование действующей практики Sitronics Group дает возможность рассмотреть результативность применяемых на практике методов защиты прав доступа и выявить специфические черты их реализации на предприятии крупного российского игрока рынка.

Объект изучения - система разграничения прав доступа на предприятиях корпоративных информационных систем.

Предмет исследования: актуальные технологии и механизмы контроля доступа к информации на предприятии России.

Целью данного исследования является рассмотреть виды разграничения доступа и изучить специфику их применения на практике на примере организации Sitronics Group.

Для выполнения данной работы требуется выполнить следующие задания: проанализировать принципы разграничения доступа, существующие модели разграничения прав пользователей; рассмотреть актуальные технологии организации контроля доступа; выявить методы разграничения доступа в компании Sitronics Group; сформировать перечень показателей оценки современных моделей управления доступом; провести сопоставительный анализ методов разграничения доступа, применяемых компанией Sitronics Group и оценка эффективности их применения.

Актуальность исследования определяется увеличением числа кибератак, ростом сложности корпоративных информационных сред и потребностью в обеспечении информационной безопасности активов при развитии электронной экономики. Разграничение прав доступа - один из важнейших методов защиты информации организаций. Метод обеспечивает снижение вероятности несанкционированного доступа к объектам ИБ организации, предотвращает утечку конфиденциальной информации, обеспечивает выполнение требований нормативных правовых актов РФ в области защиты информации. Актуальность темы исследования. Анализ современных решений в области контроля доступа и их реализация на практике (на материале Sitronics Group) имеет большую научную и практическую ценность в плане оценки действенности данных подходов к обеспечению безопасности информации для реалий сегодняшней российской ИТ инфраструктуры.

1. Теория разграничения прав доступа

1.1 Определения и термины

Доступ (разграничение) – комплекс организационных и технических средств для ограничения полномочий субъектов, процессов и информационно-логических ресурсов при взаимодействии с ИР. На сегодняшний день это важнейшее средство обеспечения информационной безопасности ввиду предотвращения несанкционированного просмотра информации; её изменения, удаления либо копирования. В отечественном опыте вопросам разграничения доступа посвящены многие положения как систем защиты информации, так и отдельных документов – требований Федеральной службы по техническому и экспортному контролю (ФСТЭК России) и Федеральной службы безопасности Российской Федерации (ФСБ России).

Субъект доступа - это пользователь, программа или устройство, обращающееся за исполнением определённой операции. Объект доступа – ресурс, к которому обращаются [4] К объектам доступа относятся файлы, базы данных, сетевые ресурсы, инфраструктурные ресурсы, программные модули и другие объекты информационной системы. Субъект и объект имеют между собой соглашения по взаимодействию, согласованные правила операций и требования к выполнению этих операций.

Одним из основных является понятие – прав доступа. Правом доступа определяется возможность производить определенное действие по отношению к ресурсу. К основным видам относятся: чтение, запись, удаление, изменение и выполнение. В современных ИС список разрешенных действий достаточно обширный и включает в себя кроме указанных выше возможности для управления ресурсами, назначение прав другим пользователям (делегирование), управление политикой безопасности, реализацию дополнительных специализированных возможностей.

Предоставление прав доступа реализуется через процессы идентификации, аутентификации и авторизации. Процесс идентификации идентифицирует субъект по уникальному свойству, например по учетной записи.

Аутентификация же удостоверяет личность заявляемого субъекта с помощью пароля, сертификата, биометрии или других способов. Авторизация – решение вопроса о возможности совершения запрошенного действия при условии установления идентичности субъекта.

В российской практике акцент делается на принципе наименьших привилегий. По этому принципу у субъекта должны быть лишь те права, которые нужны ему для выполнения своих задач. Применение этого принципа значительно уменьшает риски злоупотребления правами; предотвращает негативные последствия взлома учетных записей; повышает общую безопасность информационного ресурса.

Другой не менее значимый термин - это политика доступа. Это набор регламентов и запретов, описывающий механизм взаимодействия субъектов и объектов. Политику доступа могут задавать на основании должностей пользователя, географического расположения, применяемого устройства, доверия к пользователю внутри системы и многого другого. В настоящее время в российских компаниях доступ всё чаще воспринимается не просто как фиксированная мера, а как гибкое средство регулирования безопасности - то есть адаптивная система контроля за безопасностью.

1.2. Классические модели

Развитие способов разграничения прав осуществлялось в соответствии с развитием средств вычислительной техники. Если изначально вопросы информационной безопасности рассматривались только в государственных или вооруженных структурах и здесь была крайне важна секретность данных - то были созданы базовые принципы управления доступом, повлиявшие на построение многих систем защиты информации.

Наиболее распространенной ее разновидностью являются дискреционные модели управления доступа [3]. В этом случае право определять, кому будет доступен объект, возлагается на владельца этого объекта. Данный механизм реализован практически во всех файловых системах и ОС общего назначения.

Основным преимуществом модели является гибкость, однако высокая степень свободы пользователей нередко приводит к ошибкам конфигурирования и появлению избыточных полномочий.

Большое воздействие на теорию безопасности имело применение модели управления доступом по принципам мандатов. При таком подходе каждый субъект и объект имеют присвоенные уровни доступа. Доступ определяется сравнением уровней безопасности субъектов и объектов, причем решение не зависит от волеизъявления владельца объекта. Эта модель широко использовалась в правительстве и других организациях, которые обрабатывают секретную информацию. В РФ реализованы принципы мандатной системы безопасности в различных защищенных ОС и специализированных ПЭОМ.

Особую роль в формировании современных моделей доступа сыграла реализация ролевой модели контроля доступа. Появление этой модели обусловлено развитием структур организаций, ростом числа пользователей, а также потребностью в централизации управления правами доступа на уровне всей организации. Назначение прав персонифицированно (по одному субъекту) заменено их привязкой к роли – должностной функции, определяющей положение сотрудника в структуре компании. Набор прав пользователь получает через присвоенную ему роль. Такой метод очень хорошо облегчает процесс управления и дает больше управление в управлении правами доступа.

В России данная ролевая модель активно применяется во всех видах информационных систем государственного сектора, банковских организациях и корпоративных ИС. Актуальность данной модели обусловлена способностью к описанию структуры организации в целом и согласованности выполняемых функций сотрудниками с правами доступа.

Хотя модели отличаются, все они имеют ценность для теории информации о безопасности. Практически никогда не применяется чистая модель в современном решении. Как правило используются элементы разных моделей с целью достичь баланса между уровнем обеспечения безопасности, эксплуатационным удобством и эффективностью администрирования.

1.3 Современные модели разграничения доступа

В современном мире наблюдается активное внедрение облачных вычислений, мобильной техники, распределенных систем и удаленного доступа, в результате чего классические методы контроля доступа стали недостаточны и возникла потребность в построении адаптивных моделей.

Одним из самых многообещающих вариантов выступает атрибутивная модель контроля доступа. Суть данной модели в том, что субъект, объект и среда описываются набором атрибутов. При определении того, можно ли предоставить или нет пользователю доступ к ресурсу все эти атрибуты анализируются. Так, система может знать уровень доступа сотрудника, отдел компании, время запроса, адрес нахождения человека и статус его терминала. Этот метод обеспечивает большую гибкость, а также позволяет внедрять различные политики безопасности.

Атрибутивный подход начал применяться в крупнейших российских корпорациях и в рамках систем государственной информатизации. Этот метод нашел свое применение особенно активно при проведении цифровых преобразований, поскольку пользователи обращаются к ресурсам с разных мест и на разных устройствах, а учет контекста обращения может повысить безопасность без заметной потери пользовательского комфорта.

Особый интерес сегодня представляет идея Zero Trust. В этом случае считается, что ни один пользователь не заслуживает автоматического доверия без учёта своего местоположения – как внутри сети предприятия, так и снаружи её границ. Любой запрос на использование ресурса сопровождается аутентификацией, анализом целостности терминала и множеством других факторов риска. Модель Zero Trust нельзя назвать отдельным подходом к управлению доступом как таковым, но тем не менее она сильно влияет на реализацию современных систем управления доступом.

Организации России все чаще начинают применять идеи Zero Trust из-за роста числа удаленно работающих сотрудников и усиления угроз

информационным активам. Отечественные вендоры решений по защите информации внедряют в свои приложения механизмы многоуровневой идентификации, постоянного контроля активности пользователей, оценку ситуации при доступе. Это дает возможность применять новые формы контроля доступа, соответствующие национальным правовым нормам и особенностям локальной вычислительной среды.

Еще один подход это риск-ориентированный контроль доступа. Данный подход предполагает принятие решения о предоставлении доступа с учетом уровня риска той операции, которая будет выполнена пользователем. При обнаружении системы угроз в поведении пользователя возможно применение дополнительных процедур подтверждения или ограничение срока действия разрешений. Применение поведенческого анализа пользователей и машинного обучения помогает идентифицировать отклонения и действовать на опережение при подозрениях.

Развитие отечественных платформ для программного обеспечения позволяет дополнительно улучшить инструменты управления доступом. Для импортозамещения приоритетное значение имеют разработки отечественных ОС, системы контроля идентификации, решения классу IAM [5]. Они предназначены для соблюдения регуляторных требований и повышения защищенности критической информационной инфраструктуры (КИИ).

Подводя итоги, можно сказать что современные модели разграничения доступа характеризуется движением от жестких назначений прав к динамическим системам оценки. Российская практика показывает применение атрибутивной модели, риск-ориентированной и модели нулевое доверие. Это дает возможность организации защищать себя от современных угроз, соответствовать регламентированным требованиям и находить золотую середину между безопасностью и использованием информационно-телекоммуникационных систем.

1.4 Инструменты идентификации, аутентификации, авторизации

Идентификация, аутентификация и авторизация - это основные элементы информационной безопасности, они являются фундаментальными компонентами в системах разграничения доступа. При использовании всех трех элементов можно определить кто пользователь, проверить его личность, дать ему доступ к необходимым ресурсам для решения определенной задачи.

Идентификация определяется как присвоение субъекту идентификатора. Идентификатором может служить логин, email-адрес, номер учетной записи, сертификат, и другие специфические метки. Задача идентификации сводится к однозначной идентификации пользователя или программного процесса, делающему запрос на доступ к информационным ресурсам.

Следующий этап – это аутентификация. Аутентификация нужна для проверки на подлинность личности субъекта. Самый простой способ - это пароли, но эффективность этого метода напрямую связана с надежностью установленных паролей и поведением пользователей.

Сейчас очень часто используется многофакторная аутентификация. При ее использовании применяют несколько разных независимых факторов подтверждения личности пользователя. Чаще всего используют что-то, что пользователь знает (пароль), имеет у себя устройство и свои биометрические данные. Несколько факторов при этом делают гораздо меньше шансов на успешную компрометацию учетной записи.

Важное значение имеют биометрические способы авторизации. Биометрия использует различные уникальные характеристики человека такие как отпечаток пальца, лицо, голос и тд.. Биометрические системы вводят высокую степень удобств и повышает безопасность информационных систем.

После авторизации происходит авторизация пользователя. Определяет какие ресурсы доступны пользователю и какие операции он может выполнять. Авторизация основывается на правилах безопасности, моделях управления

правами доступа. Результат работы от этого этапа напрямую влияет на безопасность корпоративной системы.

Одним из ключевых элементов таких систем является единый вход. С его помощью пользователь может совершить аутентификацию единожды, чтобы получить доступ ко многим информационным системам. Внедрение таких технологий снижает трудоемкость работы персонала, но также усиливает контроль со стороны администраторов информационной безопасности.

В российских компаниях политика процессы идентификации, аутентификации и авторизации определяется законами страны и инструкциями от регуляторов. Применение сертифицированной защиты информации, ведение логов доступа — это тоже необходимые вещи для безопасности.

Идентификация, аутентификация и авторизация - это взаимодополняющие процедуры управления доступом, позволяющие эффективно ограничивать права пользователей на использование информационных ресурсов.

1.5 Технологии управления привилегированным доступом

Управление привилегированным доступом – одно из приоритетных направлений развития современных средств обеспечения ИБ. Привилегированные пользователи – это администраторы, операторы информационных систем, а также иные сотрудники, имеющие широкие права управления ключевыми информационными ресурсами предприятия..

Утрата контроля над привилегированными аккаунтами может стать причиной: · Утечки данных; · Сбоев в функционировании информационного оборудования; · Блокировки доступов. За счет этого контроль привилегий является одним из главных элементов информационной безопасности.

Для реализации этой задачи используют средства класса Privileged Access Management[6], реализующие централизованные механизмы управления привилегированными учетными записями, контроля доступа к использованию административных прав и аудита действий пользователей. Применение таких

средств значительно уменьшает риски злоупотреблений и усиливает наблюдаемость деятельности администраторов.

Один из самых удачных вариантов это временное присвоение прав. Административный доступ выдается пользователю временно, то есть в течение определенного времени выполнения поставленной задачи. Когда работа будет выполнена, доступ автоматически убирается. Это обеспечивает принцип наименьших привилегий.

В современных системах управления привилегиями применяются механизмы безопасного хранения учетных данных. Парольные и ключевые данные помещаются в единое защищенное хранилище для предотвращения утечки и обеспечивают строгий контроль над ними.

Большое значение имеет журналирование действий пользователей. Все операции, выполняемые администраторами, регистрируются и могут быть использованы для проведения аудита или расследования инцидентов информационной безопасности. Дополнительно могут записываться экранные сессии и команды, выполняемые в процессе администрирования.

Для усиления защиты в рамках системы PAM используются интеграции с IAM-системами, системами безопасности (SIEM) и SOAR-платформами. Интеграция дает возможность построить многоуровневую модель управления доступом и вовремя заметить аномальное поведение пользователей или систем.

Российские организации широко используют системы управления привилегированным доступом, в особенности это относится к органам государственной власти, финансовым учреждениям и критическим информационным системам. Применение этих решений дает возможность значительно увеличить защищенность информационных ресурсов предприятия.

1.6 Концепция Zero Trust и перспективы развития систем разграничения доступа

Zero Trust – одна из самых актуальных концепций в области защиты информации. Возникла она как ответ на трансформацию корпоративной инфраструктуры: расширение облачных технологий, работа за пределами офисов, использование периферийных устройств и тд. Классическая схема защиты - "если ты внутри сети – тебе можно верить" – все чаще перестает работать.

Базовая идея Zero Trust состоит в том, что никакому субъекту доступа автоматически не может быть доверяемо. Для обращения к любому информационному ресурсу необходимо проводить аутентификацию вне зависимости от локации пользователя и типа подключенного им к сети оборудования. Это уменьшает риски несанкционированного доступа.

Для этого подхода характерна постоянная проверка безопасности. Пользователя проверяют не только при входе, а на протяжении всей сессии работы. Если будет обнаружена попытка взлома – доступ ограничивают либо блокируют его полностью.

Внедрение модели Zero Trust подразумевает использование множественных факторов аутентификации, политик центрального управления правами доступа, анализ поведения пользователей и контроль за устройством пользователя. Поддерживается системами обнаружения угроз (Threat detection) и Machine Learning для определения подозрительной активности [7].

Подход Zero Trust активно развивает идеи атрибутивных моделей доступа. Доступ к ресурсам осуществляется по совокупности факторов: роли пользователя, устройства и его геолокации, а также оценка риска в данный момент времени. Благодаря этому достигается большая степень эластичности и адаптивности политики безопасности.

В России интерес к Zero Trust неослабно растет. Связано это с усилением внимания к вопросам защиты критической информационной инфраструктуры,

развитием цифровой экономики, увеличением количества кибератак. Отдельные отечественные разработчики внедряют принципы Zero Trust в свою продукцию.

Тенденции в развитии механизмов контроля доступа Направления совершенствования Контроль доступа будет еще больше автоматизирован. Сегодня с помощью искусственного интеллекта уже анализируют много данных и заранее замечают угрозы. В дальнейшем появятся системы защиты, которые сами будут менять правила доступа в зависимости от опасности.

2 Исследование опыта применения методов разделения прав доступа на компании Sitronics Group.

2.1 О компании Sitronics Group и ее ИТ инфраструктуре

Sitronics Group – Российская IT-компания которая занимается разработкой цифровых решений для государства и бизнеса в сфере информационных технологий, цифровой трансформации, телекоммуникаций, транспорта, промышленной автоматизации, центров обработки данных, информационной безопасности. Sitronics Group построила целую экосистему цифровых сервисов за время своего существования для разработки и поддержки инфраструктурных high-tech решений.

Особенностью деятельности компании является широкий спектр реализуемых проектов. Решения Sitronics Group применяются в транспортной отрасли, энергетике, промышленности, государственном управлении и городской инфраструктуре. Работа с большим количеством заказчиков требует обработки значительных объемов информации и использования развитой информационной инфраструктуры, способной обеспечить высокую доступность сервисов и необходимый уровень защиты данных.

Современная ИТ-инфраструктура компании состоит из вычислительных мощностей, информационных систем предприятия, средств виртуализации, сетевой инфраструктуры, облачных сервисов и дата-центров. Многие службы работают в распределенной среде, поэтому необходимо применять централизованное управление идентификацией пользователей и управлением

доступом. Такая структура организации работы предприятия свойственна для крупного IT-предприятия работающего в сфере предоставления цифровых сервисов и поддержки комплексных программно- аппаратных систем.

Важную роль в инфраструктуре Sitronics Group играют центры обработки данных. Компания участвует в проектировании и эксплуатации ЦОД, а также предоставляет решения для хранения и обработки информации. Использование подобных технологий предполагает наличие строгих механизмов контроля доступа как к программным ресурсам, так и к физическим объектам инфраструктуры.

Вопросами информационной безопасности следует выделить применение централизованных механизмов аутентификации. В условиях крупных организаций ручное ведение тысяч учетных записей становится неприемлемым подходом с позиций организационного менеджмента и усиливает фактор риска. Крупные компании активно применяют системы типа Identity and Access Management для автоматизации выдачи и ревукации доступов.

На основании анализа открытых источников компании можно говорить о внедрении технологий single sign-on, central authentication authority, privileged account management. В совокупности данные решения дают возможность реализовать единый принцип доступа при наличии значительного числа информационных систем и пользователей.

Одной из главных особенностей проектируемой ИТ-инфраструктуры является учет российского законодательства о защите информации, так как компания работает над государственными проектами и сотрудничает с такими предприятиями, которые нуждаются в большей степени защиты информации. Аудит действий пользователя, журналирование событий и управление доступом должны быть предусмотрены в системе управления правами.

Кроме того, рост облачной вычислительной техники влияет на структуру предприятия. В связи с этим появление виртуальных ресурсов приводит к необходимости разработки новых средств авторизации и управления правами доступа. Особую актуальность приобретает управление доступом в среде

распределенных приложений, где требуются единый центр идентификации пользователей и система многоуровневой аутентификации.

Отдельный вопрос – взаимодействие работников организации с удаленными сервисами и информационными ресурсами организаций-заказчиков. Безопасность данных процессов обеспечивается за счет защищенных каналов передачи информации, средств криптографии для защиты информации, а также применением дополнительных факторов идентификации пользователей.

Таким образом, ИТ инфраструктура Sitronics Group состоит из множества взаимосвязанных информационных систем и сервисов, в которой обязательным условием являются системы разграничения доступа. Современный подход к обеспечению безопасности корпоративной среды включает использование средств единого управления идентификаторами пользователей, а также единого централизованного механизма аутентификации и контроля привилегий учетных записей.

2.2 Определение способов разграничения доступа

Sitronics Group – крупнейшая российская компания в сфере информационных технологий. Компания обеспечивает решения цифровой трансформации бизнеса и госструктур через разработку ПО, создание инфраструктурных решений, строительство ЦОДов, внедрение виртуальных сред и информационной безопасности. За счет масштаба работы требуется выстроенный контроль доступа к информационным активам.

Согласно открытым источникам компании можно заключить, что компания использует современные решения в области управления идентификацией и доступом. Среди решений по защите информации Sitronics Group отмечены Identity Management (IDM) / Identity and Access Management (IAM), Single Sign-On (SSO), решения типа Privileged Identity Management и Privileged User Management. Использование таких систем говорит о том, что управление доступами реализовано на высоком уровне.

Ролевая модель является основой модели управления доступом. В больших компаниях права определяются на основе роли сотрудника в компании - то есть назначается ему роль в соответствии с его обязанностями. Применение IAM систем позволяет централизованно управлять учетными данными работников компании и осуществлять контроль над распространением прав внутри подразделений.

Единый вход (Single Sign On) — это механизм, позволяющий пользователю авторизироваться в корпоративных сервисах единожды для последующего использования сразу нескольких услуг. Единый вход удобно применять для централизации доступа к ресурсам организации, что не только делает использование систем удобнее, но также помогает в администрировании прав доступа.

Не меньшее внимание уделяется управлению привилегированным доступом. При работе с критической инфраструктурой, дата-центрами, ГИС контроль действий администраторов является востребованной функцией. PIM и PUM решения обеспечивают возможность отслеживания действий пользователей с расширенными правами и снижения рисков их неправомерного использования.

Еще одним средством защиты являются двухэтапная (многофакторная) аутентификация и использование криптографических средств защиты информации. Они же служат для усиления уровня безопасности, минимизирования рисков злоумышленников получить доступ к учетным записям.

2.3 Критерии оценки различных методов определения границ доступа

Для оценки различных методов разделения доступа предлагается применить комплекс показателей, которые дадут возможность качественно оценить и сопоставить разные системы разграничения прав. Важнейшими

требованиями в настоящее время являются – защита информации; адаптивность решения; масштабируе-мость; простота в управлении.

Главный показатель эффективности – безопасность. Модель разграничения доступа не позволяет посторонним лицам получить доступ к информации и обеспечивает защиту информационных активов от рисков внешних и внутренних угроз. Безопасность системы зависит от того насколько точно она контролирует действия пользователей.

Далее это гибкость. Структура большой компании меняется регулярно, появляютсяеждаются новые проекты и отделы, поэтому система прав доступа должна позволять оперативно менять привилегии не сильно усложняя процесс управления ими.

Масштабируемость особенно важна для крупных ИТ-компаний. Используемая модель должна эффективно работать при большом количестве пользователей, информационных систем и сервисов. Недостаточная масштабируемость приводит к росту затрат на сопровождение и снижению эффективности управления безопасностью.

Не последнюю роль играет также соблюдение нормативных требований. Предприятия России должны защищать персональные данные граждан, коммерческую тайну и иную информацию ограниченного доступа. А потому современные системы управления доступом обязаны включать возможности аудита и ведения логов операций пользователей.

Также не менее важным показателем - защищенность от внутриорганизационных угроз. Множество инцидентов информационной безопасности происходит из-за действий персонала организаций, именно поэтому современные механизмы должны реализовывать мониторинг за привилегированными пользователями и возможности временного ограничения их прав.

Другой не менее важный критерий это уровень аудита и мониторинга пользовательских действий. Новые системы разграничения доступа должны обеспечивать возможность учета всех операций по предоставлению,

модификации и использованию прав доступа. Ведение детальных логов событий дает возможность проводить расследование инцидентов информационной безопасности, фиксировать нарушения действующих политик, подтверждать соответствие регуляторным требованиям. Для больших компаний функция аудита очень важна, так как она помогает контролировать потоки доступа и предупреждать возможные проблемы заранее.

Огромную роль играет совместимость системы контроля доступа с остальными компонентами ИБ. В настоящие времена контроль над доступом работает в связке с системами логирования безопасности, антивирусными программами, системами менеджмента идентификации пользователей, системами анализа угроз. Степень интеграции определяет насколько эффективно организации могут оперативно реагировать на проблемы и давать им всеобъемлющий контроль над инфраструктурой компании. Это важно для организаций с большой территориальной разбросанностью ИТ-инфраструктуры или же в том случае если есть множество различных интегрированных информационных систем.

2.4 Анализ методов разделения доступа на объекте Sitronics Group

По результатам исследования можно заключить о том, что в Sitronics Group применяются элементы нескольких современных решений по управлению доступом. Такой вид организации может быть типичным для компаний с высокоуровневой информационной системой.

Самым ярко выраженным в этом случае будет ролевое управление доступом. За счет него, происходит централизованная передача полномочий сотрудникам компании. В свою очередь достигается соответствие прав доступа с должностными обязанностями сотрудников предприятия. Благодаря этому для большого предприятия создается высокий уровень контролируемости и наглядности в вопросах безопасности.

Вместе с тем наблюдается тенденция к применению атрибутивных механизмов. Компания ведет работу в разных секторах экономики, работает с госорганом и крупными компаниями. При этом доступ определяется не столько должностью пользователя, сколько его проектом, подразделением, категорией доступа.

Большим плюсом атрибтивной модели является её адаптивность. Благодаря ей можно использовать другие характеристики и создать лучше политика безопасности. А минус в том, что она очень сложно управляется и нужно следить за тем чтобы используемые атрибуты были актуальны. Отдельный интерес представляют методы управления особым уровнем доступа. Для инфраструктурной компании результаты действий администратора напрямую влияют на работу информационных систем и сервисов.

Использование технологий PIM и PUM обеспечивает дополнительный контроль над критически важными ресурсами и позволяет реализовать принцип минимально необходимых привилегий. Использование технологии Single Sign-On способствует повышению удобства работы сотрудников и снижению нагрузки на службу информационной безопасности. Централизованное управление учетными записями упрощает аудит и позволяет оперативно блокировать доступ при изменении статуса пользователя.

Распространение облачных технологий, а также использование виртуализации открывают перспективы использования подхода Zero Trust. В этом случае любой запрос на получение доступа считается подозрительным и должен быть подвергнут анализу. Это намного надежнее в плане безопасности чем привычные методы обеспечения защищенности.

Проведенный анализ различных подходов к реализации сегментации продемонстрировал оптимальность комбинации рассмотренных методов в контексте потребностей Sitronics Group. Ролевая модель формирует каркас RBAC, атрибуты расширяют его возможности, средства ограничения

привилегий администраторов дополняются элементами Zero Trust для защиты особо значимых ресурсов.

Практика применения решений компании Sitronics Group отражает современные подходы к построению систем безопасности в России. Комплексная система управления доступом объединяет решение для централизованного управления пользователями, инструменты мониторинга учетных записей с повышенными правами доступа, средства проверки идентичности пользователей и системы контроля за действиями пользователей.

2.5 Анализ эффективности текущей реализации разграничения доступа

Оценка эффективности реализации механизма разграничения прав доступа входит в число ключевых задач при анализе защищенности ИС. Данная процедура дает возможность оценить уровень адаптации применяемых к настоящему моменту средств обеспечения информационной безопасности; установить достоинства имеющейся архитектуры ИС; выделить возможные направления ее дальнейшей эволюции.

По результатам исследования было установлено, что механизмы разграничения прав в рамках системы управления доступом Sitronics Group базируются на реализации передовых концепций управления идентификацией субъектов и их правами. Реализация решений централизованного типа класса IAM гарантирует эффективное управление учетными данными пользователей и автоматизирует большинство задач администрирования.

Еще одним достоинством рассматриваемой системы является ролевое назначение прав, так как именно рольовый подход дает меньше возможностей для ошибок при присвоении полномочий и позволяет соблюдать принцип соответствия прав сотрудникам с их должностными обязанностями. Для большой компании такой способ управления правами будет самым оптимальным с точки зрения удобств в использовании и масштабирования.

Хорошую результативность показывает применение решений на базе единства входа. Единство в аутентификации пользователей облегчает задачи для персонала и вместе с тем усиливает контроль корпоративных аккаунтов. Меньшее количество логин-парольных комбинаций сокращают риск человеческого фактора и управление жизненным циклом учетной записи становится более простым.

Также важным аспектом служит использование механизмов контроля доступа с правами администратора. В целях уменьшения внутренних угроз за счет проведения мониторинга операций административных и иных лиц имеющих расширенные права доступа. Возможность анализа деятельности пользователей за счет применения средств журнализации и аудита.

С позиции выполнения нормативных требований действующая система показывает достаточно высокую степень зрелости. Применяемые решения отвечают актуальным стандартам информационной безопасности и дают возможность организовать доступ к наиболее значимым активам. Централизованное администрирование пользователей позволяет улучшить наблюдаемость в вопросах безопасности.

Однако в связи с развитием инфраструктуры и ростом числа предоставляемых цифровых сервисов появляютсяются новые сложности. Возможные ограничения традиционных ролевых моделей при работе со сложными политикатиками доступа делают перспективной применение атрибутивных моделей управления доступом, которые позволяют использовать дополнительные свойства пользователей и запроса к ресурсам.

Отдельного внимания заслуживает проблема удаленного доступа. Распространение дистанционных форм работы требует постоянного контроля безопасности пользовательских устройств и оценки уровня риска каждой операции. В связи с этим перспективным направлением развития является внедрение элементов концепции Zero Trust, предусматривающей непрерывную проверку пользователей и устройств.

Одним из ключевых аспектов, способствующих улучшению уровня защиты является увеличение доля многофакторной аутентификации. Использование такого вида аутентификация получило широкое распространение в корпоративных средах, ее применение позволит дополнительно исключить возможность несанкционированным доступом к учетным записям, повысить стойкость инфраструктуры к новым векторам атак.

Одним из перспективных направлений становится применение систем анализа поведения пользователей. Данные решения позволяют обнаруживать необычную деятельность, в результате чего система может самостоятельно принимать решения по противодействию возможному риску. Включение аналогичных решений в систему управления доступом даст возможность увеличить степень автоматизации процедур защиты.

Подводя итог проделанной работе можно сказать что разработанная политикаразграничения доступа Sitronics Group отвечает принципам информационной безопасности и позволяет защищать информационные ресурсы компании. Реализация единого управления доступом к учетным записям пользователей, привилегированным учетным записям, механизмам аудита, а также применение современных методов аутентификации позволяют обеспечить высокий уровень защиты информации предприятия.

При этом развитие системы должно подразумевать переход к риск-ориентированным алгоритмам принятия решений, увеличение доли атрибутивных моделей доступа и внедрение принципов Zero Trust. Учет указанных факторов позволит достигнуть необходимой степени устойчивости инфраструктурных элементов перед лицом современных угроз и привести их в соответствие с будущими стандартами цифрового периметра.

3. Методы определения порядка разграничения прав доступа

3.1 Общие критерии выбора модели разграничения прав доступа

Выбор метода реализации контроля доступа определяется спецификой функционирования компании, топологией ИС и степенью чувствительности данных. Практика показывает, что единая модель доступа неприменима ни к одному предприятию. Следовательно разработка политики доступа должна базироваться на исследовании бизнес-процессов, групп пользователей, потребностей безопасности информации.

Первый принцип - согласованность модели доступа с оргструктурой организации. При несоответствии системы контроля доступа реально существующим должностным обязанностям возникает риск возникновения лишних прав и ошибок в администрировании. В этом случае уменьшается защита информации и труднее осуществлять контроль доступа.

Особую роль в этом играет принцип наименьших привилегий. Пользователю предоставляется лишь необходимый минимум прав доступа для выполнения поставленных служебных задач. Применением этого принципа можно минимизировать ущерб от возможной компрометации учетных записей и уменьшить угрозы со стороны сотрудников. Аудит полномочий необходимо проводить периодически с последующим удалением ненужных прав доступа к ресурсам системы.

3.2 Предложения для использования традиционных схем доступа

Дискреционные модели управления доступом применяются для защиты информационных систем небольшого числа пользователей, а также систем со сравнительно низкой степенью сложности в описании связей субъектов и объектов доступа. Это преимущество обеспечивается высокой гибкостью такого подхода - владелец ресурса сам решает, кому предоставляет права доступа. Однако с ростом количества пользователей существенно увеличивается риск возникновения ошибок при настройке системы и возникновения излишних прав доступа.

Мандатная модель хорошо подходит организациям, которые работают с секретными данными. Этот тип модели даёт отличный контроль благодаря уровням безопасности и регламенту предоставления доступа. Однако у этой модели низкая адаптивность, а также высокие административные расходы на поддержку.

Ролевая модель доступа считается самым гибким подходом к управлению доступом в компании. Ролевая модель обеспечивает возможность группировки прав по функциональным ролям пользователей и значительно снижает нагрузку при администрировании систем. Именно ролевой модели преимущественно используют большинство отечественных компаний для реализации политик управления доступом за счет максимальной эффективности сочетания принципов защиты, простоты использования и ценового фактора ее внедрения.

3.3 Применение современных моделей разграничения доступа

Возникновение цифровых технологий породило новые модели управления доступом. Перспективным направлением в этом плане является атрибутивный подход. Атрибутивный метод отличается от ролевого тем, что он учитывает атрибуты как субъектов так и объектов а также контекст запроса. Благодаря этому удается создать гибкие политики безопасности для обеспечения правил доступа к ресурсам.

Атрибутивную модель целесообразно применять в масштабе крупных предприятий с распределённой организацией, множеством проектов и усложнённым взаимодействием между подразделениями. В ней учитываются не только факт принадлежности сотрудника к проекту, но и его уровень доступа, устройство, местоположение и многое другое. При этом при её внедрении необходимо иметь инфраструктуру управления идентификацией, а также требовать ресурсов по дальнейшему обслуживанию.

Специально стоит отметить применение риск-ориентированных механизмов решения задач. Механизмы основанные на анализе контекста обращения, вероятности появления угроз и т д при обнаружении подозрительной

активности могут требовать дополнительной проверки пользователя или временный блокировки доступа к ресурсам. Применение риск-ориентированного подхода помогает обеспечить безопасность в той же мере что и строгие меры безопасности не нарушая удобство работы сотрудников.

3.4 Использование IAM, PAM и Multi-factor Authentication

Современные предприятия требуют централизованного контроля за учетными записями пользователей. Предлагаем применение решений категории Identity and Access Management (IAM). Эти системы позволяют автоматизировать процессы создания/удаления учетных записей, управлять ролями и правами доступа, вести контроль по действиям пользователей. Внедрение IAM дает высокую результативность в области управления безопасностью и уменьшает число ручных операций администратора.

Особое внимание следует уделить мониторингу привилегированных пользователей. Пользователи с повышенными правами доступа получают доступ к важнейшим ресурсам в организации. Для снижения угрозы рекомендуется применение средств класса Privileged Access Management [8]. С их помощью осуществляется управление выдачей прав доступа, ведется регистрация действий администратора и достигается еще один слой управления для критических операций.

Одним из важнейших элементов безопасности сегодня является применение многофакторной аутентификации. Применение нескольких факторов авторизации, как правило, делает практически невозможным взлом учетных записей. Многократно подтверждается факт того, что если известны только пароли пользователей, но есть еще один фактор подтверждения, то злоумышленник вряд ли сможет получить доступ к информации компании.

3.5 Перспективы развития систем разграничения доступа

Среди главных достижений последних лет - появление подхода Zero Trust. Суть этого подхода состоит в том, что для любого пользователя или устройства

не предполагается никаких гарантий на доверие. Любое обращение к данным рассматривается как злонамеренное и должно быть подвергнуто проверке. Это дает преимущество перед классическими методами обеспечения безопасности.

Появление облачных сред и развитие удаленных форм работы делают принцип Zero Trust крайне востребованным. С развитием распределенных информационных систем у которых имеется доступ из разных мест мира защита периметра не всегда эффективна, поэтому требуется проверка всех обращений.

Для отечественных компаний целесообразен переходной вариант - сочетание элементов Zero Trust с ролевой и атрибутивной моделями доступа, что позволит максимально использовать сильные стороны уже действующих систем управления доступом при повышении защищенности инфраструктур от современных угроз. Лучшая практика – это создание единого контура безопасности на базе IAM + PAM, MFA, логирования активности пользователей и контекстного анализа доступа.

Таким образом, модели для разграничения доступа следует выбирать с учетом совокупности организационных, технических и правовых аспектов. Оптимальным вариантом оказывается применение гибридных решений, сочетающих сильные стороны традиционных и новых подходов к управлению доступом. Только на их основе можно достичь достаточной защиты информационных систем при соблюдении актуальных требований информационного обеспечения.

Заключение

В процессе работы изучены теоретические принципы разграничения доступа в информационно-логических системах, рассмотрены основные понятия разграничения доступа, рассмотрена классическая модель разграничения доступа - дискреционная модель разграничения доступа, мандатная модель разграничения доступа, ролевая модель разграничения доступа Отдельно рассмотрены современные способы управления доступом такие как, атрибутивный подход, Zero Trust, мультимодальная аутентификация и управление привилегиями.

В ходе работы практическая часть состояла в изучении применения методов разделения доступа на примере Sitronics Group. По открытым источникам информации, имеющимся у организации были выделены ключевые способы контроля доступа внутри предприятия. Установлено применение компанией: централизованной системы управления идентификацией пользователей, решений для единого входа (Single Sign-On), средств контроля привилегированных учетных записей и реализации современных методов аутентификации. Представленные рекомендации дают возможность надёжно обеспечить защиту информационных ресурсов, ответить на вызовы современности.

Для сопоставления рассмотренных решений использованы следующие параметры сравнительного анализа существующих механизмов контроля доступа: безопасность, адаптивность политики доступа, масштабирование, простота управления, соблюдение законодательных актов, защита от инсайдеров. Сделан вывод о том, что наиболее эффективным является комплексный подход, объединяющий возможности различных методов контроля доступа и гибкость в подборе меры безопасности под организацию.

Исследованию подвержены вопросы: - Результаты проведенного исследования дают возможность заключить что системы разграничения доступа

представляют собой один из основных средств защиты информации на предприятии. На примере Sitronics Group показано примнение механизмов ролевого и атрибутивного управления доступом на основе технологий контроля привилегированного пользователя и принципов нулевого доверия для обеспечния эффективной защиты ИС в условиях угроз информационной безопасности, роста числа атак и повышения степени цифровизации бизнес-процессов.,ролевого и атрибутивного управления доступом на основе технологий контроля привилегированного пользователя и принципов нулевого доверия для обеспечения эффективной защиты ИС в условиях угроз информационной безопасности, роста числа атак и повышения степени цифровизации бизнес-процессов.

Список использованных источников

1 Васильков И.А. Безопасность и управление доступом в информационных системах. – Москва: Форум, 2020. – 368 с.

2 Девянин П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками. – Москва: Телеком, 2023. – 352 с.

3 Бондарев В.В. Введение в информационную безопасность автоматизированных систем. – Москва: МГТУ им. Н.Э. Баумана, 2021. – 252 с.

4 Мельников Д.А. Информационная безопасность открытых систем – Москва: Флинта, 2019. – 444 с.

5 Курило А.П. Толстой А.И. Основы управления информационной безопасностью / А. П. Курило, Н. Г. Милославская, М. Ю. Сенаторов – Москва: Телеком, 2016. – 244 с.

6 OWASP Foundation. Access Control [Электронный ресурс] // OWASP Foundation: официал. сайт – Режим доступа: https://owasp.org/www-community/Access_Control.

7 OWASP Foundation. Broken Access Control [Электронный ресурс] // OWASP Foundation: официал. сайт – Режим доступа: https://owasp.org/www-community/Broken_Access_Control.

8 OWASP Foundation. Enforce Access Controls [Электронный ресурс] // OWASP Foundation: официал. сайт – Режим доступа: https://devguide.owasp.org/en/04-design/02-web-app-checklist/07-access-controls.

9 The Web SSO Standard OpenID Connect: In-Depth Formal Security Analysis and Security Guidelines [Электронный ресурс] / D. Fett, R. Küsters, G. Schmitz // arxiv.org: open-access articles archive – Режим доступа: https://arxiv.org/abs/1704.08539/.