Министерство образования Республики Беларусь
Учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

УДК 004.492.2

СОЛОДКИЙ
Денис Валерьевич

СИСТЕМА КОНТРОЛЯ ДОСТУПА ПОЛЬЗОВАТЕЛЕЙ К ИНФОРМАЦИОННОЙ СЕТИ ОРГАНИЗАЦИИ

АВТОРЕФЕРАТ
диссертации на соискание степени магистра

по специальности 7-06-0611-02 Информационная безопасность

Минск 2026

Работа выполнена на кафедре защиты информации учреждения образования «Белорусский государственный университет информатики и радиоэлектроники»

Научный руководитель:	**БУДНИК Артур Владимирович,** доцент кафедры защиты информации учреждения образования «Белорусский государственный университет информатики и радиоэлектроники», кандидат технических наук, доцент
Рецензент:	**ГЕРМАН Олег Витольдович,** доцент кафедры информационных технологий автоматизированных систем учреждения образования «Белорусский государственный университет информатики и радиоэлектроники», кандидат технических наук, кандидат технических наук, доцент

Защита диссертации состоится «20» января 2026 г. года в $14^{\underline{30}}$ часов на заседании Государственной экзаменационной комиссии по защите магистерских диссертаций в учреждении образования «Белорусский государственный университет информатики и радиоэлектроники» по адресу: 220089, Минск, ул. П. Бровки, 10, копр. 3, ауд. 506.

ВВЕДЕНИЕ

Современные организации, включая предприятия лесного хозяйства, функционируют в условиях постоянного роста угроз информационной безопасности. Для таких организаций, как **Кобринский опытный лесхоз**, информационные ресурсы имеют стратегическое значение: это базы данных по лесному фонду, геоинформационные системы, бухгалтерская и кадровая документация, а также специализированные приложения для планирования и учёта лесохозяйственных мероприятий. Утечка или несанкционированный доступ к этим данным может привести не только к экономическим потерям, но и к нарушению экологических и нормативных обязательств.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования

Одним из ключевых элементов защиты корпоративных ресурсов является система контроля доступа, обеспечивающая разграничение прав пользователей и предотвращение несанкционированного доступа к критически важной информации. Традиционные модели аутентификации, основанные преимущественно на паролях, демонстрируют уязвимость перед современными методами атак, что требует внедрения более надёжных и комплексных решений. В условиях цифровизации лесного хозяйства, интеграции с государственными информационными системами и ужесточения нормативных требований (ГОСТ, ISO/IEC 27001, национальные стандарты в области защиты информации) проблема разработки и анализа эффективных систем контроля доступа приобретает особую актуальность.

Цель и задачи исследования

Целью работы является разработка и анализ системы контроля доступа, обеспечивающей высокий уровень информационной безопасности в корпоративной сети **Кобринского опытного лесхоза**.

Для достижения цели решаются следующие задачи:

- провести классификацию и сравнительный анализ существующих моделей контроля доступа (DAC, MAC, RBAC, ABAC);
- исследовать современные концепции обеспечения доступа (Zero Trust, passwordless-аутентификация, многофакторная аутентификация);
- проанализировать угрозы и уязвимости, связанные с использованием парольных систем в условиях лесохозяйственного предприятия;
- выполнить оценку рисков с применением международных и национальных методик (ISO/IEC 27005, ГОСТ Р ИСО/МЭК 27005-2010);

- разработать архитектуру системы контроля доступа на базе pfSense и LDAP/AD с интеграцией VPN и MFA, адаптированную к инфраструктуре организации;
- провести анализ эффективности предложенной системы и определить перспективы её развития.

Область исследования

Объектом исследования являются системы контроля доступа в корпоративных сетях организаций лесного хозяйства. Предметом исследования выступают методы и средства разграничения прав доступа, а также механизмы аутентификации и авторизации пользователей в условиях **Кобринского опытного лесхоза**.

Теоретическая и методологическая основа исследования

В основу диссертации легли работы белорусских и зарубежных ученых в области информационной безопасности и построения компьютерных систем и сетей, а также анализ технических нормативных правовых актов по рассматриваемой тематике.

Информационная база исследования сформирована на основе литературы, открытой информации, технических нормативно-правовых актов, сведений из электронных ресурсов, а также материалов научных конференций и семинаров.

Научная новизна, теоретическая и практическая значимость

Научная новизна работы заключается в комплексном подходе к разработке системы контроля доступа, сочетающем классические модели разграничения прав с современными концепциями Zero Trust и многофакторной аутентификации. В работе предложена архитектура, ориентированная на интеграцию с существующей корпоративной инфраструктурой лесхоза и учитывающая актуальные нормативные требования Республики Беларусь и международных стандартов.

Теоретическая значимость работы заключается в анализе защищенности современных систем контроля доступа к информационным сетям организаций.

Практическая значимость исследования состоит в возможности непосредственного применения разработанной системы в организациях для повышения уровня защищённости информационных ресурсов. Предложенные решения могут быть использованы при проектировании корпоративных сетей организаций, а также при модернизации существующих систем информационной безопасности.

Основные положения, выносимые на защиту

1. Анализ архитектуры систем парольной защиты, способов хранения паролей и факторов, влияющие на их стойкость. Расчет стойкости паролей с учетом современных способов преодоления парольной защиты.

2. Систематизация основных способов преодоления систем парольной защиты, анализ соответствующих угроз информационной безопасности и мер противодействия, направленные на повышение надёжности и устойчивости механизмов аутентификации

3. Анализ архитектуры системы контроля доступа, перечень событий, подлежащих контролю, а также требования к системе парольной защиты как базовому компоненту аутентификации, интегрированному в общую модель безопасности организации.

4. Разработка и практическая реализация системы контроля доступа, описание этапов настройки и интеграции её компонентов, а также результаты тестирования.

Публикации

Изложенные в диссертации основные положения и выводы опубликованы в 2 печатных работах.

Общий объем публикаций по теме диссертации составляет 19 страниц.

Структура и объем работы

Диссертация состоит из введения, общей характеристики работы, четырех глав с краткими выводами по каждой главе, заключения и библиографического списка.

- В первой главе рассмотрены теоретические основы систем контроля доступа и нормативные требования.
- Во второй главе проведён анализ угроз и рисков, связанных с использованием различных моделей аутентификации применительно к лесохозяйственным организациям.
- В третьей главе представлена разработка и анализ системы контроля доступа на базе современных технологий с учётом специфики лесхоза.
- В четвёртой главе проведена практическая реализация системы pfSense+VPN+LDAP в инфраструктуре **Кобринского опытного лесхоза**.

В заключении сформулированы основные выводы и перспективы дальнейших исследований.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

В первой главе в ходе анализа архитектуры и алгоритмов функционирования систем парольной аутентификации установлено, что данный метод остаётся базовым и наиболее распространённым способом идентификации пользователей в корпоративных информационных системах. Его популярность объясняется простотой реализации, низкой стоимостью и универсальностью применения. Для Кобринского опытного лесхоза парольная аутентификация является фундаментом разграничения доступа к бухгалтерским системам, базам данных лесного фонда, геоинформационным сервисам и внутренним корпоративным приложениям.

Рассмотренные архитектурные основы показали, что система строится вокруг трёх ключевых процессов — идентификации, аутентификации и авторизации, которые образуют логическую последовательность, обеспечивающую контроль доступа к ресурсам. Важным элементом является использование современных криптографических алгоритмов хэширования (bcrypt, Argon2), а также внедрение дополнительных механизмов защиты, таких как блокировка учётных записей при множественных ошибках и аудит действий пользователей.

Анализ способов хранения паролей продемонстрировал эволюцию от небезопасных решений (хранение в открытом виде) к современным адаптивным алгоритмам и аппаратным модулям безопасности (HSM). Сравнительная оценка методов показала, что минимальным требованием для корпоративных систем является использование хэширования с солью, а для критически важных инфраструктур — применение специализированных аппаратных средств.

Исследование факторов стойкости пароля подтвердило, что длина, сложность и уникальность являются ключевыми характеристиками, определяющими устойчивость к атакам перебора и словарным методам. Формализованная оценка энтропии показала экспоненциальный рост стойкости при увеличении длины и разнообразия символов. Современные стандарты (NIST SP 800-63B, ISO/IEC 27002) акцентируют внимание на необходимости использования длинных и уникальных паролей, а также интеграции проверок по базам утёкших комбинаций.

Таким образом, глава 1 демонстрирует, что парольная аутентификация, несмотря на свои ограничения, остаётся важнейшим элементом защиты корпоративных информационных систем. Её эффективность определяется не только техническими аспектами хранения и проверки паролей, но и соответствием международным и национальным стандартам, а также интеграцией с многофакторными методами аутентификации. Для лесохозяйственного предприятия это означает необходимость постоянного совершенствования архитектуры систем защиты, внедрения адаптивных алгоритмов и обеспечения комплексного подхода к управлению доступом.

Во второй главе проведённый анализ показал, что системы парольной аутентификации обладают рядом фундаментальных уязвимостей, которые могут быть использованы злоумышленниками для получения

несанкционированного доступа. Угрозы охватывают как технические аспекты (слабые пароли, отсутствие шифрования, эксплуатация уязвимостей протоколов), так и организационные факторы (повторное использование паролей, недостаточный аудит, ошибки администрирования). Существенную роль играет человеческий фактор, проявляющийся в низкой дисциплине пользователей и их подверженности методам социальной инженерии.

Матрица рисков показала, что наиболее критическими угрозами для лесхоза являются фишинг и повторное использование паролей, так как они сочетают высокую вероятность реализации и значительный ущерб. Высокий уровень риска также характерен для слабых паролей и утечек баз данных, что подтверждает необходимость внедрения комплексных мер защиты. Средние риски связаны с угрозами, которые могут быть контролируемы техническими средствами, но требуют постоянного мониторинга и регулярного обновления инфраструктуры.

Анализ способов противодействия угрозам продемонстрировал, что повышение устойчивости возможно только при сочетании технических, организационных и концептуальных мер. Технические меры включают использование современных алгоритмов хэширования, защищённых каналов связи и систем мониторинга. Организационные меры направлены на формирование культуры информационной безопасности, обучение сотрудников и регулярный аудит прав доступа. Концептуальные подходы, такие как многофакторная аутентификация, Zero Trust и passwordless модели, позволяют существенно снизить зависимость от человеческого фактора и повысить общий уровень защищённости.

Таким образом, традиционная парольная аутентификация не может рассматриваться как достаточный инструмент защиты в условиях Кобринского опытного лесхоза. Только комплексный подход, включающий технические средства, организационные меры и современные концепции аутентификации, способен обеспечить надёжную защиту корпоративных информационных систем. Данный вывод определяет необходимость перехода к рассмотрению современных моделей аутентификации и их интеграции в комплексные системы защиты, что станет предметом анализа в следующей главе.

В третьей главе анализ архитектуры и алгоритмов функционирования системы контроля доступа показал, что данный механизм является ключевым элементом обеспечения информационной безопасности корпоративных систем. В отличие от единичного процесса аутентификации, контроль доступа представляет собой комплексное решение, включающее формализацию политик, принятие решений, принудительное их исполнение, аудит и мониторинг.

Рассмотренные архитектурные модели (DAC, MAC, RBAC, ABAC) продемонстрировали различия в гибкости, защищённости и масштабируемости. Для Кобринского опытного лесхоза оптимальным является соче-

тание RBAC и ABAC, обеспечивающее баланс между простотой администрирования и контекстной чувствительностью. RBAC позволяет разграничивать доступ по должностям и ролям, а ABAC учитывает дополнительные параметры — время, устройство, геолокацию, что особенно важно для удалённых сотрудников лесничеств.

Перечень идентификаторов событий информационной безопасности подтвердил, что надёжность системы контроля доступа напрямую зависит от способности фиксировать и анализировать критические события. Ключевыми индикаторами являются превышение числа неудачных попыток входа (AUTH_FAIL_EXCESS), попытки повышения привилегий (PRIV_ESCALATION_ATTEMPT), массовая выгрузка данных (DATA_EXFIL_INDICATOR) и нарушения политик доступа (POLICY_VIOLATION). Их корреляция в SIEM и анализ с использованием UEBA позволяют своевременно выявлять угрозы и предотвращать инциденты.

Определение требований к системе парольной защиты показало, что парольная аутентификация остаётся фундаментальным элементом идентификации, но её эффективность зависит от соответствия современным стандартам. Ключевыми требованиями являются использование адаптивных алгоритмов хэширования (bcrypt, Argon2), проверка паролей на утечки, защита от перебора, интеграция с MFA и контекстной авторизацией. Дополнительно требуется формирование политики сложных паролей, обучение пользователей и регулярный аудит.

Таким образом, система контроля доступа в лесхозе должна рассматриваться как многоуровневый механизм, объединяющий технические, организационные и концептуальные меры. Только комплексный подход, включающий RBAC и ABAC, интеграцию с LDAP/AD, применение MFA, SIEM и UEBA, способен обеспечить устойчивость к современным угрозам и соответствие международным стандартам информационной безопасности.

В четвёртой главе практическая реализация подтвердила, что комплексный подход, включающий технические средства (pfSense, LDAP, FreeRADIUS, VPN), организационные меры (централизованное управление, аудит, обучение пользователей) и современные концепции (MFA, Zero Trust), обеспечивает надёжную защиту корпоративных информационных систем лесхоза. Полученные результаты могут быть масштабированы и адаптированы для других организаций лесного хозяйства, что делает предложенную модель универсальной и перспективной.

Интеграция с каталогом пользователей обеспечивает централизованное управление доступом, а использование многофакторной аутентификации существенно снижает риск компрометации учётных записей. Внедрение VPN позволяет безопасно подключать удалённых сотрудников, а централизованный аудит и SIEM обеспечивают своевременное выявление и реагирование на инциденты. Результаты тестирования системы сведены в таблицу 4.1

Таблица 4.1 – Результаты тестирования системы контроля доступа

№	Сценарий	Тип угрозы	Ожидаемый результат	Фактический результат
1	Brute Force-атака	Подбор паролей	Блокировка учётной записи после нескольких неудачных попыток; запись события в SIEM	Учётная запись блокируется после 5 попыток; событие фиксируется в SIEM
2	Фишинговая атака	Компрометация пароля	Вход невозможен без второго фактора (OTP)	Попытка входа с украденным паролем отклонена; требуется OTP
3	Попытка доступа к запрещённым ресурсам	Несанкциониро-ванный доступ	Отказ в доступе; регистрация события POLICY_VIOLATION	Доступ отклонён; событие POLICY_VIOLATION зафиксировано
4	Удалённое подключение через VPN	Подключение извне	Доступ предоставляется только после успешной MFA-аутентификации	Подключение установлено только после ввода пароля и OTP

Результат внедрения системы в сравнении с исходным состоянием представлен в таблице 4.2.

Таблица 4.2 – Сравнение «До внедрения / После внедрения»

Критерий	**До внедрения**	**После внедрения**
Аутентификация	Только пароль	Пароль + MFA
Управление доступом	Локально на каждом сервисе	Централизованно через LDAP
VPN	Отсутствует	OpenVPN/IPsec
Журналирование	Частично	Централизованное, SIEM
Устойчивость к атакам	Низкая	Высокая

ЗАКЛЮЧЕНИЕ

Основные результаты диссертации:

- Систематизированы архитектурные основы парольной аутентификации и контроля доступа, показана эволюция методов хранения паролей от открытых решений до адаптивных алгоритмов и аппаратных модулей безопасности.
- Проведён анализ угроз информационной безопасности, выявлены наиболее критические риски (фишинг, повторное использование паролей, слабые комбинации, утечки баз данных) и предложены меры противодействия.
- Рассмотрены модели контроля доступа (DAC, MAC, RBAC, ABAC), проведён их сравнительный анализ и обоснован выбор комбинации RBAC и ABAC для лесхоза как оптимального решения.
- Определён перечень ключевых событий информационной безопасности, требующих обязательного мониторинга и корреляции в SIEM, что обеспечивает своевременное выявление инцидентов.
- Сформулированы требования к системе парольной защиты, включающие адаптивное хэширование, проверку на утечки, защиту от перебора, интеграцию с MFA и контекстной авторизацией.
- Реализована практическая архитектура системы контроля доступа на базе pfSense, LDAP/Active Directory, FreeRADIUS и VPN, проведено тестирование, подтвердившее эффективность предложенной модели.

Перспективы дальнейших исследований.
Дальнейшее развитие работы связано с:

- интеграцией системы с платформами мониторинга и анализа событий безопасности (SIEM),
- применением методов машинного обучения для выявления аномалий в поведении пользователей,
- расширением концепции Zero Trust в условиях гибридных и облачных инфраструктур,
- адаптацией решений к специфике государственных информационных систем лесного хозяйства Республики Беларусь.

СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ

Статьи в сборниках научных трудов

1. Методы обеспечения конфиденциальности персональных данных пользователей / Д.В. Солодкий // Интеграция, аналитика и геоинформационный сервис: сб. науч. трудов по материалам междунар. заоч. науч.−практич. конф., / гл. ред. В.Я. Цветков; отв. за вып. С.В. Шайтура; Институт гуманитарных наук, экономики и информационных технологий. – Бургас: ИГНЭИТ, 2025 – 142-148.

2. Организация системы парольной аутентификации пользователя информационной системы/ Д.В. Солодкий // Интеграция, аналитика и геоинформационный сервис: сб. науч. трудов по материалам междунар. заоч. науч.−практич. конф., / гл. ред. В.Я. Цветков; отв. за вып. С.В. Шайтура; Институт гуманитарных наук, экономики и информационных технологий. – Бургас: ИГНЭИТ, 2025 – 295-305.

РЭЗЮМЭ

Салодкі Дзяніс Валер'евіч

Сістэма кантролю доступу карыстальнікаў да інфармацыйнай сеткі арганізацыі

Ключавыя словы: інфармацыйная бяспека, парольная аўтэнтыфікацыя, кампраметацыя ўліковых дадзеных, кіберпагрозы, абарона інфармацыі, MFA, палітыка пароляў.

Мэта працы: Мэтай працы з'яўляецца распрацоўка і аналіз сістэмы кантролю доступу, якая забяспечвае высокі ўзровень інфармацыйнай бяспекі ў карпаратыўнай сетцы арганізацыі.

Атрыманыя вынікі і іх навізна: навуковая навізна працы заключаецца ў комплексным падыходзе да распрацоўкі сістэмы кантролю доступу, які спалучае класічныя мадэлі размежавання правоў з сучаснымі канцэпцыямі Zero Trust, шматфактарнай аўтэнтыфікацыі і SIEM сістэмамі. У працы прапанавана архітэктура, арыентаваная на інтэграцыю з існуючай карпаратыўнай інфраструктурай лясгаса і якая ўлічвае актуальныя нарматыўныя патрабаванні Рэспублікі Беларусь і міжнародных стандартаў.
Тэарэтычная значнасць працы заключаецца ў аналізе абароненасці сучасных сістэм кантролю доступу да інфармацыйных сетак арганізацый.
Практычная значнасць даследавання складаецца ў магчымасці непасрэднага прымянення распрацаванай сістэмы ў арганізацыях для павышэння ўзроўню абароненасці інфармацыйных рэсурсаў. Прапанаваныя рашэнні могуць быць выкарыстаны пры праектаванні карпаратыўных сетак арганізацый, а таксама пры мадэрнізацыі існуючых сістэм інфармацыйнай бяспекі.

Ступень выкарыстання: вынікі ўкаранёны ў сістэму інфармацыйнай бяспекі дзяржаўнай доследнай лесагаспадарчай установы «Кобрынскі доследны лясгас»

Вобласць ужывання: інфармацыйная бяспека карпаратыўных сетак у арганізацыях і прадпрыемствах.

РЕЗЮМЕ

Солодкий Денис Валерьевич

Система контроля доступа пользователей к информационной сети организации

***Ключевые слова*:** информационная безопасность, парольная аутентификация, компрометация учетных данных, киберугрозы, защита информации, MFA, политика паролей.

Цель работы: Целью работы является разработка и анализ системы контроля доступа, обеспечивающей высокий уровень информационной безопасности в корпоративной сети организации.

***Полученные результаты и их новизна*:** научная новизна работы заключается в комплексном подходе к разработке системы контроля доступа, сочетающем классические модели разграничения прав с современными концепциями Zero Trust, многофакторной аутентификации и SIEM системами. В работе предложена архитектура, ориентированная на интеграцию с существующей корпоративной инфраструктурой лесхоза и учитывающая актуальные нормативные требования Республики Беларусь и международных стандартов.

Теоретическая значимость работы заключается в анализе защищенности современных систем контроля доступа к информационным сетям организаций.

Практическая значимость исследования состоит в возможности непоредственного применения разработанной системы в организациях для повышения уровня защищённости информационных ресурсов. Предложеные решения могут быть использованы при проектировании корпоративных сетей организаций, а также при модернизации существующих систем информационной безопасности.

***Степень использования*:** результаты внедрены в систему информационной безопасности государственного опытного лесохозяйственного учреждения «Кобринский опытный лесхоз»

***Область применения*:** информационная безопасность корпоративных сетей в организациях и предприятиях.

SUMMARY

Denis Solodkiy

User Access Control System for an Organization's Information Network

Keywords: information security, password authentication, credential compromise, cyber threats, information protection, MFA, password policy.

***The object of study*:** The objective of this study is to develop and analyze an access control system that ensures a high level of information security in an organization's corporate network.

Results and Novelty: The scientific novelty of this study lies in its integrated approach to access control system development, combining classical privilege delimitation models with modern concepts of Zero Trust, multifactor authentication, and SIEM systems. The study proposes an architecture oriented toward integration with the existing corporate infrastructure of the forestry enterprise and takes into account current regulatory requirements of the Republic of Belarus and international standards. The theoretical significance of this work lies in its analysis of the security of modern access control systems for organizational information networks.

The practical significance of the study lies in the potential for the direct application of the developed system in organizations to improve the security of information resources. The proposed solutions can be used in the design of corporate networks, as well as in the modernization of existing information security systems.

***Degree of use*:** The results have been implemented in the information security system of the state experimental forestry institution "Kobrin Experimental Forestry."

Sphere of application: Information security of corporate networks in organizations and enterprises.