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

УДК 004.075:004.056

МАРЦИНКЕВИЧ
Владислав Антонович

ЗАЩИЩЕННАЯ КОРПОРАТИВНАЯ СЕТЬ С БЕСПРОВОДНЫМ ДОСТУПОМ

АВТОРЕФЕРАТ
диссертации на соискание степени магистра

по специальности 7-06-0611-06 Системы и сети инфокоммуникаций

Минск 2026

ВВЕДЕНИЕ

Современные корпоративные сети представляют собой сложные распределённые инфраструктуры, обеспечивающие доступ к информационным ресурсам, сервисам и вычислительным платформам, необходимым для функционирования организаций. Рост объёмов передаваемой информации, широкое распространение беспроводных технологий и увеличение числа мобильных пользователей приводят к усложнению архитектуры сетей и повышению требований к их защищённости.

Особую значимость вопросы информационной безопасности приобретают в организациях с распределённой структурой, включая образовательные учреждения, где одновременно функционируют административные, учебные, исследовательские и гостевые сегменты. Такие сети характеризуются высокой динамичностью, разнообразием типов пользователей и устройств, а также необходимостью обеспечения непрерывного доступа к критически важным сервисам. Нарушение конфиденциальности, целостности или доступности данных может привести к финансовым потерям, репутационным рискам и нарушению ключевых бизнес-процессов.

В условиях роста числа кибератак, усложнения методов их реализации и появления новых векторов угроз возрастает необходимость разработки архитектурных решений, обеспечивающих высокий уровень защищённости корпоративной сети. При этом важным является не только применение отдельных средств защиты, но и построение модульной архитектуры, в которой каждый компонент выполняет строго определённые функции, а взаимодействие модулей обеспечивает целостность и управляемость всей инфраструктуры.

Дополнительную сложность вносит необходимость соответствия нормативным требованиям в области информационной безопасности. Международные и национальные стандарты (ГОСТ, СТБ, ISO/IEC, NIST) предъявляют требования к сегментации, контролю доступа, журналированию, аутентификации, защите беспроводных сетей и управлению инфраструктурой. В этих условиях актуальной задачей является формирование архитектуры, которая одновременно учитывает технические, организационные и нормативные аспекты.

Одним из ключевых элементов проектирования защищённой сети является оценка её защищённости. Традиционные подходы, основанные на качественных характеристиках, не позволяют объективно сравнивать архитектурные решения и обосновывать выбор конкретных механизмов защиты. Поэтому особую значимость приобретает разработка методики оценки количественных характеристик защищённости, включающей

показатели сегментации, изоляции, полноты журналирования, соответствия нормативным требованиям и устойчивости к угрозам.

В связи с этим актуальной является задача разработки модульной архитектуры защищённой корпоративной сети с беспроводным доступом, а также методики её оценки, позволяющей формализовать и количественно измерять уровень защищённости. Практическая апробация архитектуры на примере университетской сети подтверждает её применимость в условиях распределённой инфраструктуры и возможность масштабирования на другие типы организаций.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования

Современные корпоративные сети представляют собой распределённые инфраструктуры, обеспечивающие доступ к критически важным ресурсам и сервисам. Рост числа мобильных пользователей, распространение беспроводных технологий и усложнение методов кибератак повышают требования к их защищённости. Особенно актуально это для образовательных учреждений, где одновременно функционируют административные, учебные, исследовательские и гостевые сегменты, а нарушение конфиденциальности, целостности или доступности данных может привести к значительным рискам.

В условиях необходимости соблюдения международных и национальных нормативных требований (СТБ ISO/IEC 27001, СТБ 34.101.6–2013, ГОСТ Р 50922–2006, ГОСТ МЭК 62443–3–3–2013) важной задачей является разработка архитектурных решений, обеспечивающих высокий уровень защищённости корпоративной сети с беспроводным доступом, а также методики количественной оценки её защищённости.

Степень разработанности проблемы

Вопросы построения защищённых корпоративных сетей рассматриваются в работах отечественных и зарубежных исследователей, а также в нормативных документах Республики Беларусь и международных стандартах. Однако существующие исследования преимущественно описывают отдельные аспекты защиты — сегментацию, межсетевое экранирование, беспроводной доступ, мониторинг — без их интеграции в единую архитектуру. Недостаточно проработаны вопросы количественной оценки защищённости, что затрудняет сравнение решений и их практическое применение.

Цель и задачи исследования

Цель исследования – повышение защищённости корпоративной сети с беспроводным доступом, включая анализ архитектурных решений, нормативных аспектов и количественных показателей безопасности.

Для достижения цели решены следующие задачи:

1 Систематизированы нормативные требования, архитектурные принципы и технологии, определяющие построение защищённой корпоративной сети образовательного учреждения.

2 Проанализированы архитектурные варианты подключения подразделений к корпоративной сети, учитывая критерии безопасности, управляемости и масштабируемости.

3 Предложена и апробирована методика количественной оценки защищённости корпоративной сети на основе реализованных архитектурных решений, а также сформулировать рекомендации по её практическому применению в университетской инфраструктуре.

Объект и предмет исследования

Объект исследования – архитектурные решения построения корпоративной сети с беспроводным доступом.

Предмет исследования – влияние архитектурных решений на уровень защищённости корпоративной сети.

Методы исследования

В работе использованы методы архитектурного анализа, моделирования сетевой инфраструктуры, сравнительного анализа механизмов защиты, методы количественной оценки защищённости, а также нормативно правовой анализ требований информационной безопасности.

Научная новизна, теоретическая и практическая значимость

Научная новизна работы заключается в предложении методики оценки защищённости корпоративной сети, которая сочетает количественные показатели с качественными параметрами нормативного соответствия. В отличие от традиционных методик, ориентированных преимущественно на процессы или уязвимости, предложенный подход связывает архитектурные решения с объективными метриками. Такой формат обеспечивает комплексность анализа и возможность применения в различных корпоративных инфраструктурах, включая образовательные учреждения.

Теоретическая значимость состоит в формализации классификации сетевых сервисов по функциональным группам и построении архитектурной модели, обеспечивающей концептуальную основу проектирования корпоративных сетей в соответствии с национальными и международными стандартами.

Практическая значимость определяется возможностью применения предложенной архитектуры и методики оценки при проектировании и модернизации корпоративных сетей. Разработанные рекомендации по совершенствованию систем защиты, включая внедрение защищённого беспроводного доступа как составной части корпоративной инфраструктуры, позволяют повысить уровень сегментации, управляемости и соответствия нормативным требованиям в образовательных учреждениях, государственных органах, промышленных предприятиях и коммерческих организациях.

Основные положения, выносимые на защиту

1 Результаты анализа нормативных требований и архитектурных принципов, включая предложенную классификацию сетевых сервисов по функциональным группам, обеспечивающую структурирование архитектуры.

2 Оценка архитектурных вариантов подключения подразделений, выявившие баланс безопасности, управляемости и масштабируемости и положенные в основу модульной архитектуры корпоративной сети с беспроводным доступом.

3 Методика количественной оценки защищённости корпоративной сети, дополненная качественными параметрами нормативного соответствия, апробированная на примере университетской инфраструктуры и подтверждающая универсальность применения в различных корпоративных средах.

Апробация диссертации и информация об использовании ее результатов

Результаты исследований, вошедшие в диссертацию, докладывались и обсуждались на X Международной научно-практической конференции «BIG DATA и анализ высокого уровня» (г. Минск, Беларусь, 13 марта 2024 г), Международной научно-методической конференции «Инженерное образование в цифровом обществе» (г. Минск, Беларусь, 14 марта 2024 г), XXII Белорусско-Российской научно-технической конференции «Технические средства защиты информации» (г. Минск, Беларусь, 12 июня 2024 года), VII Всероссийской молодежной научно-практической конференции с международным участием «Информационные технологии обеспечения комплексной безопасности в цифровом обществе» (г. Уфа, Российская Федерация, 25-25 мая 2024 г.), II Международной научно-практической конференции (г. Пенза, Российская Федерация 28 февраля 2025 г), Международном научно-техническом семинаре «Технологии передачи и обработки информации» (г. Минск, Беларусь, апрель 2025 г).

Рекомендации, разработанные в 3-й главе диссертации, использованы при модернизации архитектуры корпоративной сети учреждения образования БГУИР, включая организацию защищённого беспроводного доступа.

Публикации

Изложенные в диссертации основные положения и выводы опубликованы в 7 печатных работах. В их числе 6 статей в сборниках научных трудов, 1 тезис доклада на научных конференциях.

Общий объем публикаций по теме диссертации составляет 29 страниц.

Структура и объем работы

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

В **первой главе** рассмотрены теоретические основы построения защищённой корпоративной сети в условиях распределённой инфраструктуры, проанализирована роль централизованных сервисов и предложена классификация сетевых сервисов по функциональным группам с учётом нормативных требований.

Во **второй главе** выполнен анализ архитектурных вариантов подключения подразделений, включая сегментацию, межсетевое экранирование, защищённый беспроводной доступ, удалённый доступ и изолированные сегменты. На основе анализа сформирована целевая модульная архитектура, соответствующая требованиям национальных и международных стандартов.

В **третьей главе** проведена практическая апробация архитектуры в тестовой среде, реализованы различные сценарии подключения и разработана методика оценки количественных характеристик защищённости, что позволило перейти от описательного анализа к измеримым метрикам и подтвердить универсальность предложенных решений.

В приложении представлен обзор маршрутизирующих решений с учётом импортозамещения, графический материал, акт внедрения в производство и справка проверки на плагиат.

Общий объем диссертационной работы составляет 108 страниц. Из них 95 страниц основного текста, 34 иллюстрации на 24 страницах, библиографический список из 76 наименований на 5 страницах, список собственных публикаций соискателя из 7 наименований на 2 страницах, 4 приложения на 13 страницах.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

В первой главе рассмотрены теоретические основы построения защищённой корпоративной сети на примере образовательного учреждения. Показано, что корпоративная сеть представляет собой многоуровневую систему, включающую ядро, уровень распределения и уровень доступа, а также центр обработки данных и периферийные подразделения. Особое внимание уделено специфике университетской среды, где одновременно функционируют административные, учебные, научные и гостевые сегменты, что требует масштабируемости и гибкости архитектуры.

Проанализированы централизованные сетевые сервисы, обеспечивающие унификацию политики безопасности и упрощение администрирования. Для их систематизации предложена функционально нормативная классификация, отражающая соответствие сервисов международным и национальным стандартам, приведённая в таблице 1.

Таблица 1 – Функционально нормативная классификация сервисов

Группа сервисов	Примеры компонентов	Релевантные нормативные источники
Идентификация и авторизация	RADIUS, LDAP, Kerberos	RFC 2865; ISO/IEC 27002:2022; NIST SP 800-63
Адресация и маршрутизация	DHCP, DNS, NAT	RFC 2131; RFC 1918; СТБ 34.101.6-2013
Мониторинг и управление	SNMP, Syslog, Netflow	ISO/IEC 27001:2022; RFC 5424; NIST SP 800-92
Защита и фильтрация	Firewall, ACL, DPI	ISO/IEC 27033:2020; RFC 4301; СТБ 34.101.5-2011
Хранение и резервное копирование	NFS, FTP, Backup-серверы	ISO/IEC 27040:2024; NIST SP 800-57; Постановление № 66 от 16.02.2009 (РБ)
Доступ к образовательным ресурсам	VPN, LMS-портал, прокси	ISO/IEC 27033; RFC 5280; Локальные политики доступа учреждений

Приведённая классификация демонстрирует прямую связь архитектурных решений с нормативными источниками, что подтверждает соответствие проектируемой сети требованиям информационной безопасности.

Отдельное внимание уделено организации беспроводного доступа. Рассмотрены принципы использования нескольких SSID, их привязка к VLAN

и аутентификация через 802.1X с применением WPA3. Такая модель обеспечивает разграничение доступа для сотрудников, студентов и гостей, а также соответствует современным требованиям безопасности.

В работе также раскрыты подходы к защите внутренних компонентов сети: сегментация, контроль доступа, использование межсетевых экранов, журналирование и мониторинг. На рисунке 1 представлена концептуальная схема, иллюстрирующая применение модели Zero Trust, микросегментации, управления политиками и механизмов постоянной проверки.

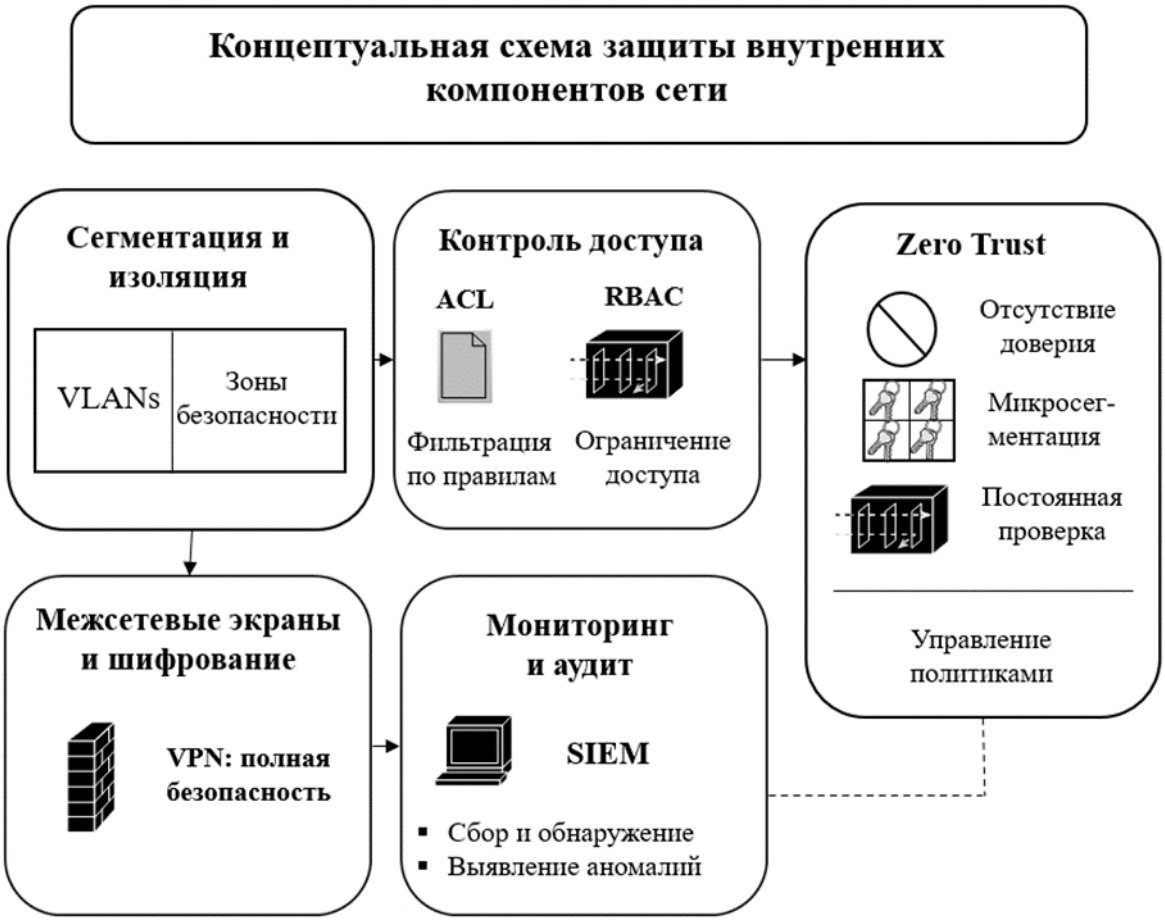

Рисунок 1.6 — Концептуальная схема защиты внутренних компонентов сети

Данная схема визуализирует архитектурные принципы, соответствующие требованиям ISO/IEC 27001, ISO/IEC 27033 и национальным регламентам, и служит основой для практической реализации защищённой корпоративной сети.

Завершающая часть главы посвящена применяемым стандартам и нормативным требованиям. Приведены национальные акты Республики Беларусь и международные стандарты, определяющие требования к защите информации и влияющие на архитектурные решения.

Таким образом, первая глава формирует теоретическую и нормативную основу исследования, выявляет недостатки существующих подходов и обосновывает необходимость разработки модульной архитектуры корпоративной сети с беспроводным доступом и методики оценки её защищённости.

Во второй главе рассмотрены архитектурные решения подключения подразделений к корпоративной сети университета. На основе методологического подхода проведён SWOT анализ, показавший необходимость модульной архитектуры, включающей сегментацию по VLAN, централизованную маршрутизацию и фильтрацию через NGFW, аутентификацию в Active Directory, контроль доступа с использованием ACL, поддержку беспроводного и удалённого доступа, а также возможность полной изоляции отдельных сегментов.

Предложены ключевые архитектурные модули:

– Модуль сегментации — реализация VLAN и ACL для разграничения доступа между подразделениями.

– Модуль защищённого беспроводного доступа — использование 802.1X, WPA3 и привязки SSID к VLAN.

– Модуль удалённого доступа — организация VPN подключения с аутентификацией через корпоративные учётные данные.

– Модуль изолированных сегментов — автономные зоны без выхода в интернет, предназначенные для научных лабораторий и критичных узлов.

Систематизации компонентов архитектуры приведена в таблице 2.

Таблица 2 — Ключевые компоненты методологии построения защищённой корпоративной сети

Компонент	**Назначение**	**Применение в архитектуре**	**Архитектурный уровень**
VLAN (IEEE 802.1Q)	Логическая сегментация сети	Разделение трафика по подразделениям, реализация зон безопасности	Уровень доступа
Межсетевой экран (NGFW)	Централизованная маршрутизация и фильтрация	Контроль межсегментного взаимодействия, NAT, VPN, инспекция трафика	Ядро сети
Active Directory + 802.1X	Аутентификация и авторизация	Единое управление учётными записями, интеграция с Wi-Fi и VPN	Уровень доступа / ядро
ACL	Контроль доступа	Ограничение взаимодействия между VLAN, принцип минимальных привилегий	Уровень распределения

Продолжение таблицы 2

Компонент	Назначение	Применение в архитектуре	Архитектурный уровень
Wi-Fi (WPA3)	Безопасный беспроводной доступ	Привязка SSID к VLAN, шифрование, разграничение доступа	Уровень доступа
VPN	Защищённый удалённый доступ	Подключение вне кампуса с аутентификацией через AD	Ядро сети
Изолированные сегменты	Полная автономность	Лаборатории без выхода в интернет, строго регламентированные ACL	Уровень доступа / распределения

Все модули объединены в целевую архитектуру защищённой корпоративной сети (рисунок 2), охватывающую проводные и беспроводные подключения, VPN доступ и изолированные сегменты. Архитектура обеспечивает централизованное управление, гибкость масштабирования и соответствие нормативным требованиям.

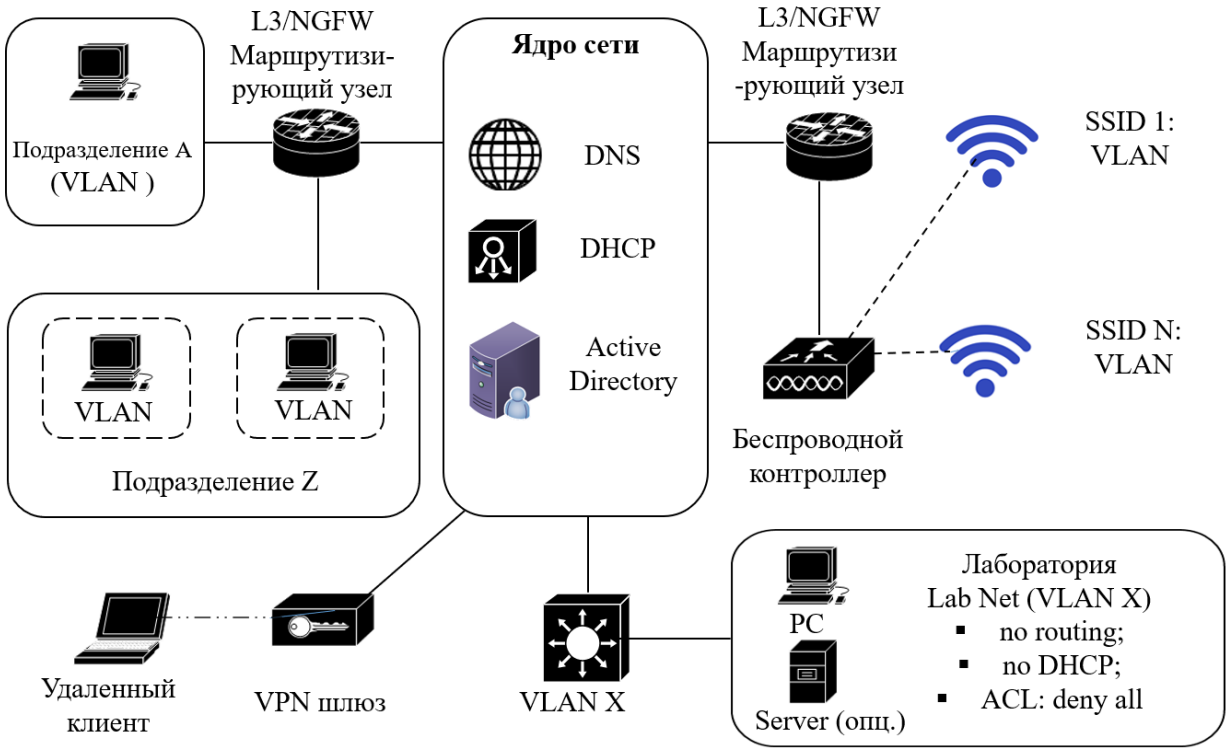

Рисунок 2 — Целевая архитектура защищённой корпоративной сети, объединяющая проводные и беспроводные подключения, VPN-доступ, централизованное управление и изолированные сегменты

Таким образом, в второй главе сформирована модульная архитектура корпоративной сети, которая демонстрирует нормативную совместимость, проектную реализуемость и универсальность для различных типов организаций при наличии аналогичных требований к сегментации, контролю доступа и защищённому беспроводному подключению.

В третьей главе проведена практическая апробация архитектурных решений и разработанной методики оценки защищённости корпоративной сети.

На первом этапе выполнен анализ маршрутизирующих решений, представленных на рынке. Сравнительная таблица 3 демонстрирует, что устройство Check Point 81.10 обладает необходимой глубиной фильтрации, поддержкой Active Directory, расширенными возможностями журналирования и сертификацией по требованиям ОАЦ, что делает его предпочтительным для защищённых сегментов.

Таблица 3 — Сравнительный анализ маршрутизирующих решений

Критерий	**Cisco ISR**	**Fortinet FortiGate**	**MikroTik CCR**	**Check Point 81.10**
Сертификация	Частично (зависит от модели)	Имеется (включая модели, сертифицированные в РБ по требованиям ОАЦ)	Отсутствует	Имеется (ГОСТ Р 50922-2006, рекомендации ОАЦ)
Глубина фильтрации	Средняя (ACL, NAT, базовый IPS)	Глубокая (L7, IPS, Web Filtering)	Поверхностная (L3, NAT, базовый firewall)	Глубокая (L7, IPS, Application Control, Threat Prevention)
Интеграция с Active Directory	Поддерживается	Поддерживается	Ограниченная	Полная поддержка
Централизованное управление	Cisco Prime, CLI, Web GUI	FortiManager, Web GUI	WinBox, CLI	SmartConsole, единая политика
Масштабируемость	Высокая	Высокая	Средняя	Высокая
Журналирование и аналитика	Есть, интеграция с Syslog	Расширенная, с отчётами и визуализацией	Базовая	Расширенная, с экспортом и корреляцией событий

Продолжение таблицы 3

Критерий	Cisco ISR	Fortinet FortiGate	MikroTik CCR	Check Point 81.10
Поддержка VPN	Да (IPSec, SSL)	Да (IPSec, SSL, SSL Inspection)	Да (IPSec, PPTP, L2TP)	Да (IPSec, SSL, Mobile Access)
Применимость в защищённых сетях	Допустима при наличии сертификации	Рекомендовано	Ограничена (тестовые зоны, лаборатории)	Рекомендовано для защищённых сегментов
Стоимость и доступность	Высокая	Средняя–высокая	Низкая	Средняя–высокая (в зависимости от лицензий)

На втором этапе реализована тестовая среда, отражающая ключевые элементы корпоративной сети университета (рисунок 3). В неё включены сегменты кафедр, ядро сети, беспроводной контроллер, VPN шлюз и изолированные лаборатории.

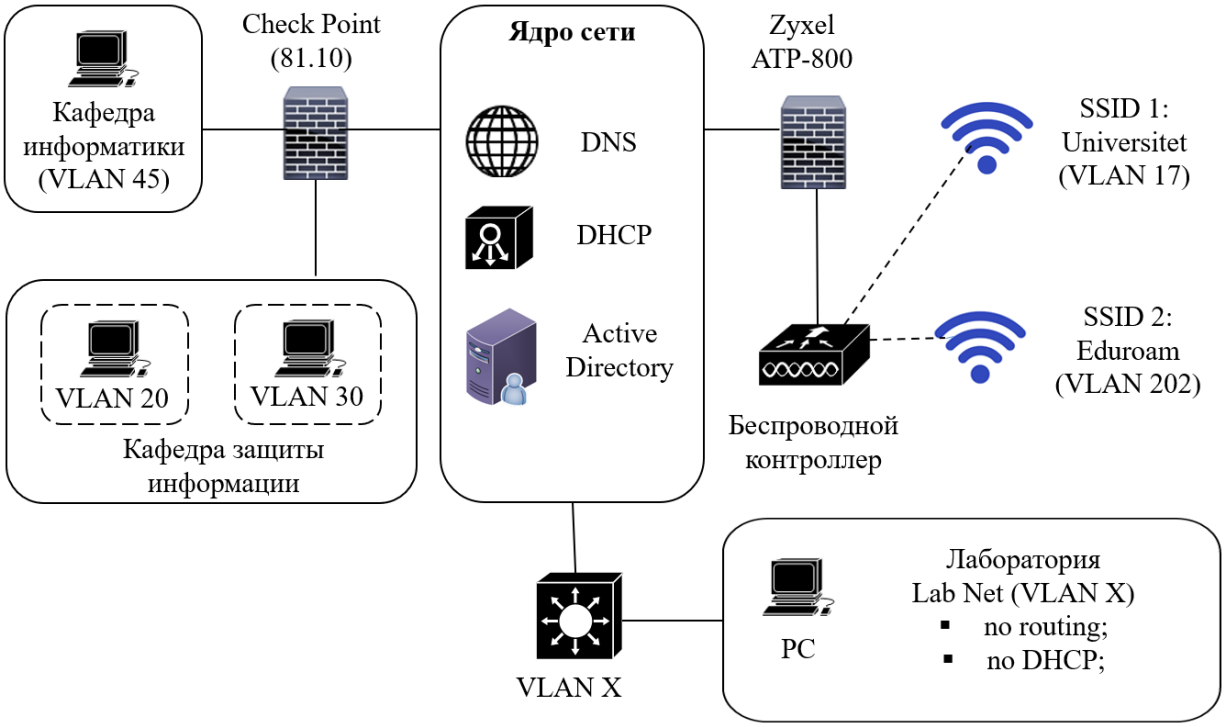

Рисунок 3 – Схема архитектуры защищённой корпоративной сети университета

Предложена методика оценки защищённости, основанная на

количественных и качественных метриках: уровень изоляции, полнота журналирования, количество уязвимостей, соответствие нормативным требованиям. Источниками данных выступают журналы безопасности, результаты сканирования MaxPatrol, показатели нагрузки и активности пользователей.

Практическая апробация показала устойчивость инфраструктуры, эффективность архитектурных решений и выявила направления совершенствования. Проведён анализ сетевой активности, нагрузок на ядро и точки доступа, а также аудит уязвимостей.

На основании результатов сформулированы рекомендации по развитию инфраструктуры, включая:

– использование сертифицированных шлюзов;
– регулярный мониторинг и аудит;
– сохранение сегментации SSID и VLAN;
– применение механизмов защиты на канальном уровне;
– контроль событий через SIEM;
– сопоставление параметров с нормативными требованиями.

Таким образом, предложенная методика оценки защищённости и её практическая апробация демонстрируют универсальность подхода и возможность адаптации к корпоративным сетям различных типов организаций.

ЗАКЛЮЧЕНИЕ

Основные научные результаты диссертации

В ходе работы были систематизированы нормативные требования, архитектурные принципы и технологии, определяющие построение защищённой корпоративной сети образовательного учреждения. На этой основе сформирована методологическая база, обеспечивающая соответствие стандартам информационной безопасности и создающая основу для дальнейшего проектирования. Дополнительно обоснован способ структурирования сетевых сервисов, включая предложенную классификацию по функциональным группам, при этом акцент сделан на их централизованной организации. Это имеет теоретическую значимость и позволяет формировать целостное представление о принципах построения корпоративной сети.

В процессе анализа архитектурных вариантов подключения подразделений к корпоративной сети установлено, что достижение баланса между безопасностью, управляемостью и масштабируемостью возможно лишь при комплексном учёте архитектурных решений и нормативных требований. Обосновано, что предложенная модульная архитектура

корпоративной сети обладает универсальностью и может быть адаптирована к инфраструктурам организаций разных типов.

В ходе изучения практических аспектов была разработана методика количественной оценки защищённости корпоративной сети на основе архитектурных решений. Реализация тестовой среды обеспечила переход от описательного анализа к объективной оценке, дополненной качественными параметрами. Методика обладает универсальностью и может быть масштабирована для применения в образовательных, административных и коммерческих структурах.

Рекомендации, сформулированные в третьей главе, использованы при модернизации архитектуры корпоративной сети учреждения образования «Белорусский государственный университет информатики и радиоэлектроники», включая организацию защищённого беспроводного доступа и развитие механизмов сегментации.

Рекомендации по практическому использованию результатов

1. На основании результатов исследований возможно проведение работ по модернизации архитектуры корпоративных сетей различных типов организаций, включая организацию защищённого беспроводного доступа и развитие механизмов сегментации, которые будут удовлетворять современным стандартам безопасности и требованиям законодательства Республики Беларусь.

СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ

[1-А] Лещенко, Е. А. Методы и специфика защиты компьютерных сетей при работе с Big Data = Methods and specifics of computer network protection when working with Big Data / Е. А. Лещенко, Е. В. Бегляк, В. А. Марцинкевич // BIG DATA и анализ высокого уровня = BIG DATA and Advanced Analytics : сборник научных статей X Международной научно-практической конференции, Минск, 13 марта 2024 г. : в 2 ч. Ч. 2 / Белорусский государственный университет информатики и радиоэлектроники ; редкол.: В. А. Богуш [и др.]. – Минск, 2024. – С. 320–324.

[2-А] Марцинкевич, В. А. Контроль инцидентов информационной безопасности учреждений образования на уровне файерволов = Control of information security incidents of educational institutions at the firewall level / В. А. Марцинкевич, Е. В. Бегляк, С.А. Мигалевич // Инженерное образование в цифровом обществе : материалы Международной научно-методической конференции, Минск, 14 марта 2024 г. : в 2 ч. Ч. 2 / Белорусский государственный университет информатики и радиоэлектроники ; редкол.: Е. Н. Шнейдеров [и др.]. – Минск, 2024. – С. 39–41.

[3-А] Довгун, В. А. Нормативно-правовое регулирование процесса аттестации информационных систем на соответствие требованиям защиты информации / В. А. Довгун, В. А. Марцинкевич // Технические средства защиты информации : тезисы докладов XXII Белорусско-российской научно-технической конференции, Минск, 12 июня 2024 г. / Белорусский государственный университет информатики и радиоэлектроники ; редкол.: Т. В. Борботько [и др.]. – Минск, 2024. – С. 36.

[4-А] Марцинкевич, В. А. Импортозамещение сетевого оборудования и программного обеспечения в разрезе информационной безопасности внутренней инфраструктуры организации = Import substitution of network hardware and software in the context of information security of the organization's internal infrastructure / В. А. Марцинкевич, М. В. Романюк, А. Н. Марков // Информационные технологии обеспечения комплексной безопасности в цифровом обществе : Сборник материалов VII Всероссийской молодежной научно-практической конференции с международным участием, Уфа, 24-25 мая 2024 г. / Уфимский университет науки и технологий. – Уфа, 2024. – С. 38-41

[5-А] Классификация и оценка уязвимостей в беспроводных сетях и методы их устранения = Classification and assessment of vulnerabilities in wireless networks and methods of their elimination / Е. В. Бегляк, В. А. Марцинкевич, М. В. Романюк, Е. И. Шаронова // Eurasian scientific conference : сборник статей II Международной научно-практической конференции, Пенза, 28 февраля 2025 года / Международный центр научного сотрудничества «Наука и просвещение» ; отв. ред. Г. Ю. Гуляев. – Пенза, 2025. – С. 52–55.

[6-А] Сравнительный анализ протоколов безопасности для защищенных беспроводных корпоративных сетей = Comparative analysis of security protocols for secure wireless enterprise networks / В. А. Марцинкевич, Е. В. Бегляк, М. В. Романюк, Е. И. Шаронова // Eurasian scientific conference : сборник статей II Международной научно-практической конференции, Пенза, 28 февраля 2025 года / Международный центр научного сотрудничества «Наука и просвещение» ; отв. ред. Г. Ю. Гуляев. – Пенза, 2025. – С. 56–59.

[7-А] Бегляк, Е. В. Современные протоколы аутентификации и авторизации в беспроводных сетях = Modern authentication and authorization protocols in wireless networks / Е. В. Бегляк, В. А. Марцинкевич // Технологии передачи и обработки информации : материалы Международного научно-технического семинара, Минск, апрель 2025 г. / Белорусский государственный университет информатики и радиоэлектроники ; редкол.: В. Ю. Цветков [и др.]. – Минск, 2025. – С. 168–175.