СОДЕРЖАНИЕ

[Введение 10](#_Toc167230758)

[1. Описание предприятия 11](#_Toc167230759)

[1.1. Сфера деятельности предприятия 11](#_Toc167230760)

[1.2. Организационная структура предприятия 12](#_Toc167230761)

[1.3. Структура сети, аппаратное и программное обеспечение предприятия 14](#_Toc167230762)

[2. Теоретические аспекты облачных технологий в компьютерной сети предприятия 20](#_Toc167230763)

[2.1. Особенности и приемущества использования облачной инфраструктуры 20](#_Toc167230764)

[2.2. Основные проблемы безопасности при использовании облачной инфраструктуры 24](#_Toc167230765)

[3. Проектирование облачной инфраструктуры и системы защиты информации 28](#_Toc167230766)

[3.1 Требования, предъявляемые к сети предприятия 28](#_Toc167230767)

[3.2 Разработка облачной инфраструктуры. 30](#_Toc167230768)

[3.3 Основные угрозы информационной безопасности в облачной сети предприятия и методы их устранения 30](#_Toc167230769)

[3.4 Затраты на разработку облачной инфраструктуры и ожидаемый экономический эффект 39](#_Toc167230770)

Тема: Разработка проекта облачной инфраструктуры на предприятии ООО НПО «РэйнбовСофт» и организация защиты информации программными средствами.

DCI VPS VDS cервак в облако сделать, защита от ddos, ИБП, в дата центре. SSH сеть нестандартный сертификат. Брэндмауэр. Выделенный сервак у провайдера и туда документы, софт и т.п.

Безопасность OpenVPN, сертификаты. Безопасный доступ между предприятием и облаком.

# Введение

Современные тенденции в информационных технологиях настойчиво подталкивают предприятия к поиску новых решений для эффективного управления информационными ресурсами. В рамках этого контекста облачные технологии приобретают все большее значение, предлагая предприятиям гибкую, масштабируемую и безопасную инфраструктуру для хранения и обработки данных. Одним из таких предприятий, инициирующим развитие в этом направлении, является ООО НПО «РэйнбовСофт».

Целью данного дипломного проекта является разработка проекта облачной инфраструктуры на предприятии ООО НПО «РэйнбовСофт», а также организация защиты информации с использованием программных средств. Этот проект направлен на повышение эффективности работы с информационными ресурсами компании, обеспечение их безопасности и готовности к решению современных бизнес-задач.

В ходе данного проекта будет проведен анализ существующей информационной инфраструктуры предприятия, определены потребности и требования к облачной платформе, разработан проект облачной инфраструктуры с учетом специфики бизнес-процессов компании. Также будет рассмотрено использование программных средств для обеспечения безопасности информации и соблюдения требований законодательства в области информационной безопасности.

В результате успешной реализации проекта ООО НПО «РэйнбовСофт» сможет получить значительные преимущества в виде повышенной гибкости, масштабируемости и безопасности своей информационной инфраструктуры, что способствует улучшению бизнес-процессов и конкурентоспособности компании в целом.

# 1. Описание предприятия

# 1.1. Сфера деятельности предприятия

Компания НПО Rainbowsoft является ведущим разработчиком программного обеспечения и приверженной своей миссии в области социальных и информационных инноваций. Важной составляющей работы компании является отдел тестирования, который играет ключевую роль в обеспечении высокого качества и надежности программных продуктов.

Основные виды деятельности компании:

1. Выпуск одноплатных компьютеров Repka Pi 4: Представляет собой альтернативу западному Raspberry Pi 3, обеспечивая доступность и функциональность для широкого круга пользователей.
2. Обучение образовательной робототехнике: Компания предлагает роботов с программно-электронным управлением для различных уровней образования, включая дошкольное, школьное, среднее специальное образование, а также обучение в ВУЗах и профессиональную переподготовку.
3. Интеллектуальная транспортная система: Разработка инновационного решения для фотовидеофиксации и весогабаритного контроля, включая сбор данных от устройств, ЦАФАП ГИБДД, весовой и габаритный контроль, а также выдачу специальных разрешений и снижение аварийности.
4. Оптимизация обучения ПДД и БДД: Предоставление программного обеспечения и оборудования для автоматизации обучения, проведения экзаменов, тестов и аттестаций, ведения учёта и документооборота, а также сертифицированный экзаменационный класс ПДД.

Эти направления деятельности позволяют компании НПО Rainbowsoft оставаться впереди своих конкурентов и эффективно реагировать на потребности рынка в области информационных технологий и образования.

# 1.2. Организационная структура предприятия

Организационная структура предприятия - это формальная система, определяющая внутреннюю организацию и управление компанией. Она включает в себя разделение обязанностей, функций и ответственности между различными подразделениями и должностными лицами, а также иерархическую структуру и систему управления.

Организационная структура ООО НПО "РэйнбовСофт" изображена на рисунке.1:

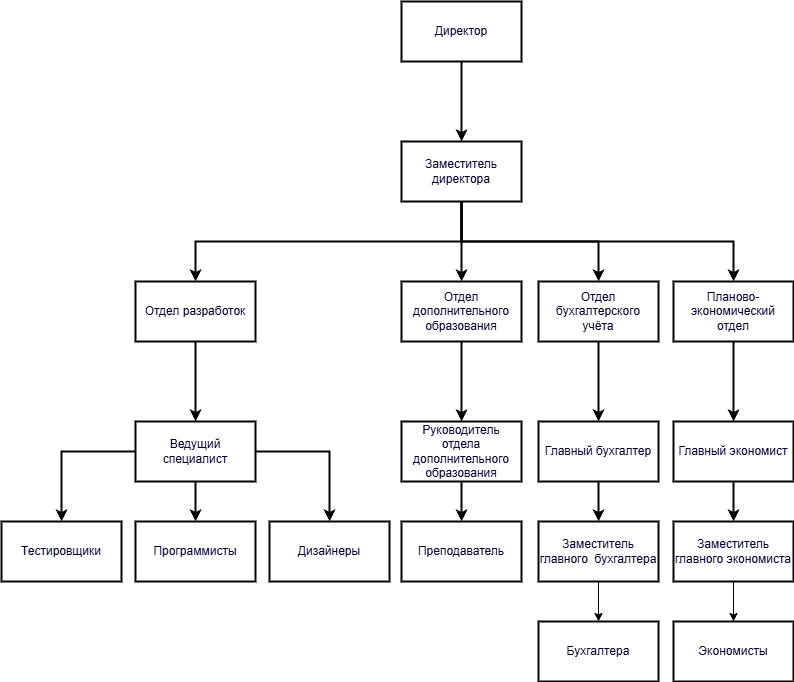


Рисунок 1. Организационная структура предприятия.

Директор - отвечает за общее управление компанией, определяет стратегию развития и принимает стратегические решения, управляет проектами и контролирует выполнение задач, организует работу и эффективное взаимодействие персонала и производственных единиц.

Заместитель директора - при отсутствии выполняет его функции, а также распределяет обязанности между подчиненными, выявляя более продуктивную единицу в отношении конкретной задачи, контролирует соблюдение работниками трудовой и производственной дисциплины, правил и норм охраны труда, требований противопожарной безопасности.

Отдел дополнительного образования - целями образовательного процесса являются теоретическое и практическое повышение профессиональных знаний специалистов, совершенствования их деловых качеств, подготовки их к выполнению новых трудовых функций в области охраны труда, промышленной, экологической, энергетической, пожарной безопасности и смежных отраслей. Практическое обучение производится в офисе №4 в назначенное время, чтобы не создавать помех сотрудникам работающим в этом офисе.

Отдел разработок - разработка программного обеспечения, создание программного обеспечения для клиентов и внутреннего использования компании. Тестирование программного обеспечения, анализ требований, управление проектами.

Планово-экономический отдел - формирование единой экономической

политики предприятия на основе анализа состояния и тенденций развития отраслей.

Отдел бухгалтерского учёта - ведение бухгалтерского и налогового учета, применение утвержденных типовых унифицированных форм, учет основных фондов, обеспечение строгого соблюдения кассовой и расчетной дисциплины, расходование денежных средств по назначению, организация налогового учета, разработка предложений по улучшению организации ведения бухгалтерского учета, контроля и отчетности.

# 1.3. Структура сети, аппаратное и программное обеспечение предприятия

Структура сети предприятия - это организационная и техническая конфигурация сети, которая определяет ее архитектуру, компоненты, топологию, соединения и взаимосвязи между ними. В основе структуры сети лежат различные уровни и типы устройств, такие как серверы, коммутаторы, маршрутизаторы, межсетевые экраны, точки доступа Wi-Fi и т. д.

Кроме того, структура сети предприятия может включать различные сегменты сети, виртуальные частные сети (VPN), облачные ресурсы, защитные барьеры и другие элементы, обеспечивающие безопасность, производительность и доступность сети.

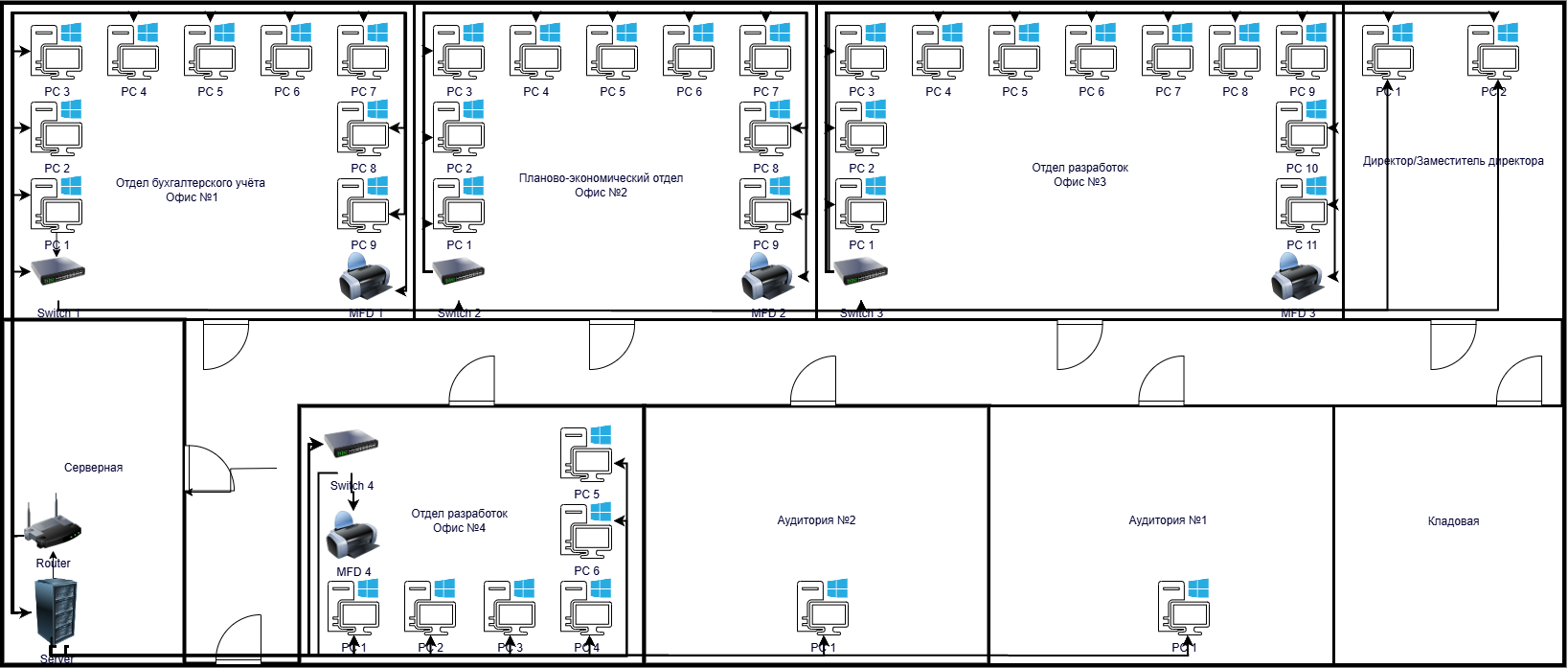
План помещений, а также физическая топология сети, указаны на рисунках 2-3: 

Рисунок 2. План помещения предприятия.

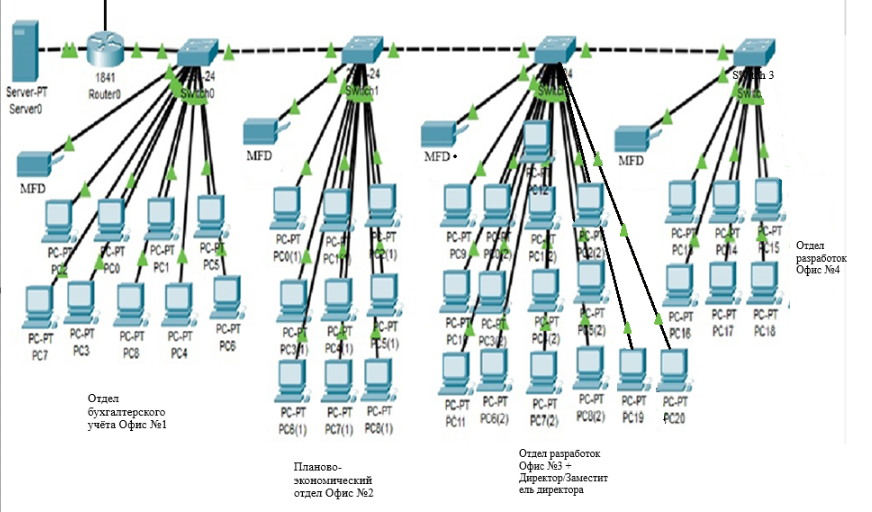


Рисунок 3.Физическая топология компьютерной сети предприятия.

Была составлена таблица 1 имеющегося на предприятии аппаратного обеспечения:

Таблица 1.

Список аппаратного обеспечения предприятия.

|  |  |  |
| --- | --- | --- |
| Наименование | Количество | Описание |
| Маршрутизатор MikroTik RB3011UiAS-RM | 1 шт. | WAN/LAN 10x1000 Мбит/с, SFP 1x1000 Мбит/с, USB 3.0 x1, 3G, 4G/LTE, IPv6 |
| D-Link DGS-3130-30S | 1 шт. | Управляемый L3 стекируемый коммутатор с 24 портами 1000Base-X SFP, 2 портами 10GBase-T и 4 портами 10GBase-X SFP+ |
| D-Link DGS-1520-28 | 3 шт. | Управляемый L3 стекируемый коммутатор с 24 портами 10/100/1000Base-T, 2 портами 10GBase-T |
| Персональный компьютер | 39 шт. | CPU: AMD Ryzen 3 3200G OEM  MB: GIGABYTE A520M H  RAM: Apacer NOX 8 ГБ  HDD: 512 ГБ  БП: DEEPCOOL PF350 350W |
| МФУ лазерное Pantum M6502W | 4 шт. | Черно-белая печать, A4, 1200x1200 dpi, ч/б - 22 стр/мин (А4), USB, Wi-Fi |
| Сервер DELL R630 8SFF | 1 шт. | CPU: 2x Intel Xeon E5-2620 v3 (2.40 GHz)  RAM: 4x 16GB DDR4 RDIMM 2400MHz  БП: 1x Dell 750W  Net: 4 port 1Gb/s  HDD: 4Tb |

После составления списка имеющегося сетевого оборудования, необходимо составить список ПО и ОС, установленного на предприятии.

Для IT компании, такой как ООО НПО "РэйнбовСофт" необходимо различное программное обеспечение в зависимости от ее специализации и потребностей. Ниже показана таблица 2 установленного программного обеспечения и операционной системы предприятия:

Таблица 2.

Программное обеспечение и операционная система предприятия.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № | Программное обеспечение | Кол-во | Минимальные системные требования | Описание |
| 1 | Операционная система Microsoft Windows 11 Pro | 37 шт. | Двухъядерный 64-битный процессор с частотой 1 ГГц;  4 ГБ оперативной памяти;  64 ГБ на жестком диске;  Совместимость с UEFI, Secure Boot и TPM 2.0;  Видеокарта совместимая с DirectX 12 и WWDM 2.x. | Операционная система компании Microsoft |
| 2 | Операционная система Microsoft Windows Server 2019 Standard Edition x64 | 3 шт. | Четырёхъядерный 64-битный процессор с частотой 1,4 ГГц;  512 МБ для основных серверных ядер;  2 ГБ для сервера с рабочим столом | Операционная система корпоративного уровня, которая обеспечивает обработку гибридного облака и данных, а также новый уровень безопасности и инноваций для приложений и инфраструктуры компании. |
| 3 | Программа безопасности Kaspersky Endpoint Security Cloud Plus | 39 шт. | 2 ГБ на жестком диске; 36 и Двухъядерный 64-битный процессор с частотой 1.4 ГГц; поддержка инструкций SSE2. | Это набор эффективных инструментов кибербезопасности. |
| 4 | Приложение Microsoft Visual Studio Professional | 37 шт. | Четырёхъядерный x32/x64 битный с частотой 1 Ггц 1 ГБ оперативной памяти;  3 Гб памяти на жестком диске; Видеокарта совместимая с DirectX10. | Полнофункциональная интегрированная среда разработки с усовершенствованной отладкой. |
| 5 | Пакет Creative Cloud All Apps | 37 шт. | 2 ГБ памяти жестком диске; Четырёхъядерный 36 и 64-битный процессор с частотой 1.4 ГГц; поддержка инструкций SSE2. | Полный набор инструментов Adobe, который включает в себя все приложения для работы с графикой, видео и веб. |
| 6 | Пакет Microsoft Office | 39 шт. | Двухъядерный процессор x32/x64 битный с частотой 1 ГГц 1 ГБ оперативной памяти;  3 Гб памяти а на жестком диске; Видеокарта совместимая с DirectX10. | Набор офисных приложений для работы с документами, таблицами, презентациями, рисунками, бизнес-диаграммами и пр. |
| 7 | 1C:Предприятие | 9 шт. | Четырёхъядерный x32/x64 битный с частотой 1 Ггц 1 ГБ оперативной памяти;  3 Гб памяти на жестком диске; Видеокарта совместимая с DirectX10 | Комплексное программное решение для автоматизации управленческого, финансового и бухгалтерского учета, управления персоналом, складского и торгового учета, а также других бизнес-процессов на предприятии. |
| 8 | 1С:Бухгалтерия | 9 шт. | Четырёхъядерный x32/x64 битный с частотой 1 Ггц 1 ГБ оперативной памяти;  3 Гб памяти на жестком диске; Видеокарта совместимая с DirectX10 | Автоматизация бухгалтерского учета на предприятии. Она включает в себя модули для ведения учета основных средств, документооборота, налогового учета, учета заработной платы, финансового учета и других бухгалтерских операций. |
| 9 | КОМПАС 3D | 17 шт. | 4х ядерный 64-битный процессор с частотой 4 ГГц;  16 ГБ оперативной памяти;  Видеокарта с 4 ГБ видеопамяти;  10 ГБ памяти на жестком диске. | Комплексная система автоматизированного проектирования, направленная не только на машиностроение, но и на разработку чертежей, проектирование кабельных систем и создание документов для инженерных проектов. |

Windows 11 Pro - это операционная система для персональных компьютеров, разработанная корпорацией Microsoft. Она является продвинутой версией операционной системы Windows 11, ориентированной на бизнес-пользователей и профессиональных пользователей.

Microsoft Windows Server 2019 Standard Edition x64 - это операционная система для серверов, разработанная корпорацией Microsoft. Она предназначена для использования в средних и крупных предприятиях, обеспечивает надежное и эффективное функционирование серверных ресурсов, управление сетью, хранение данных, обеспечение безопасности и другие функции, необходимые для работы корпоративных информационных систем.

КОМПАС 3D - это программное обеспечение для трехмерного проектирования и моделирования, разработанное компанией ASCON. Оно предназначено для создания и редактирования трехмерных моделей механических и инженерных конструкций, а также для проектирования изделий различных типов. КОМПАС 3D предоставляет широкий спектр инструментов для создания сложных трехмерных объектов, а также возможности для анализа и визуализации проектов.

Microsoft Visual Studio Professional - это интегрированная среда разработки от Microsoft, предназначенная для создания программного обеспечения на платформе Windows, веб-приложений, мобильных приложений и других типов программ. Она предоставляет разработчикам широкий набор инструментов для написания, отладки, тестирования и развертывания приложений.

Creative Cloud All Apps - это подписка на программное обеспечение от Adobe, которая включает в себя доступ ко всем приложениям Creative Cloud. Это включает в себя широкий спектр программ для дизайна, графики, веб-разработки, видеомонтажа, аудиопроизводства и многого другого.

Microsoft Office - это пакет офисных приложений, разработанный корпорацией Microsoft. Включает в себя программы для работы с текстовыми документами (Word), электронными таблицами (Excel), презентациями (PowerPoint), электронной почтой (Outlook), а также другие инструменты для организации и управления рабочими процессами.

1С Бухгалтерия - это программный продукт, предназначенный для автоматизации бухгалтерского учета и финансовых операций в организации. Он включает в себя модули для ведения бухгалтерского и налогового учета, управления финансами, расчета заработной платы, формирования отчетности и другие функции, необходимые для эффективного ведения бухгалтерии.

1С Предприятие - это программная платформа, разработанная компанией 1С для автоматизации управленческих и бизнес-процессов в различных сферах деятельности предприятий. Она включает в себя различные конфигурации (решения), адаптированные под конкретные отрасли и задачи бизнеса. С помощью 1С Предприятия можно автоматизировать учет, управление персоналом, складской учет, продажи, финансы и другие бизнес-процессы.

# 2. Теоретические аспекты облачных технологий в компьютерной сети предприятия

# 2.1. Особенности и приемущества использования облачной инфраструктуры

Облачная инфраструктура — это совокупность аппаратных и программных компонентов, необходимых для реализации облачных вычислений. Обычно этот термин используется в контексте услуг облачных провайдеров, у которых можно арендовать облако под конкретные задачи бизнеса.

Облачная инфраструктура становится все более популярным выбором для компаний любого размера, благодаря своей гибкости, экономичности и удобству использования.

Для ООО НПО «РэйнбовСофт» облачная инфраструктура представляет собой среду, в которой предприятие может размещать свои ИТ-ресурсы, такие как серверы, хранилища данных, приложения и сервисы, на удаленных облачных серверах и использовать их по мере необходимости. Она позволяет предприятию снизить затраты на оборудование, управление и обслуживание ИТ-инфраструктуры, а также повысить гибкость и масштабируемость своих операций. Вот некоторые ключевые аспекты облачной инфраструктуры для предприятия:

1. Снижение капитальных затрат: Предприятие может избежать затрат на приобретение и обновление физического оборудования, так как все ресурсы предоставляются облачным провайдером.
2. Улучшенная доступность и отказоустойчивость: Облачные провайдеры обычно обеспечивают высокий уровень доступности и резервное копирование данных, что повышает надежность системы.
3. Гибкость и масштабируемость: Предприятие может легко масштабировать свои ресурсы вверх или вниз в зависимости от изменяющихся потребностей, что делает его более гибким и адаптивным.
4. Улучшенная безопасность: Облачные провайдеры обычно обеспечивают высокий уровень безопасности и защиты данных с помощью передовых методов шифрования и многоуровневых механизмов защиты.
5. Быстрое развертывание и обновление: Предприятие может быстро развертывать новые приложения и сервисы, а также обновлять их, без необходимости внедрения нового оборудования или программного обеспечения.
6. Оплата по использованию: Предприятие оплачивает только за использованные ресурсы, что позволяет оптимизировать затраты и бюджетирование.

Облачная инфраструктура для предприятия представляет собой мощный инструмент, который может помочь улучшить эффективность бизнес-процессов, повысить гибкость и ускорить достижение бизнес-целей.

Рассмотрим, из чего состоит облачная инфраструктура в дата-центрах в соответствии с рисунком 4:

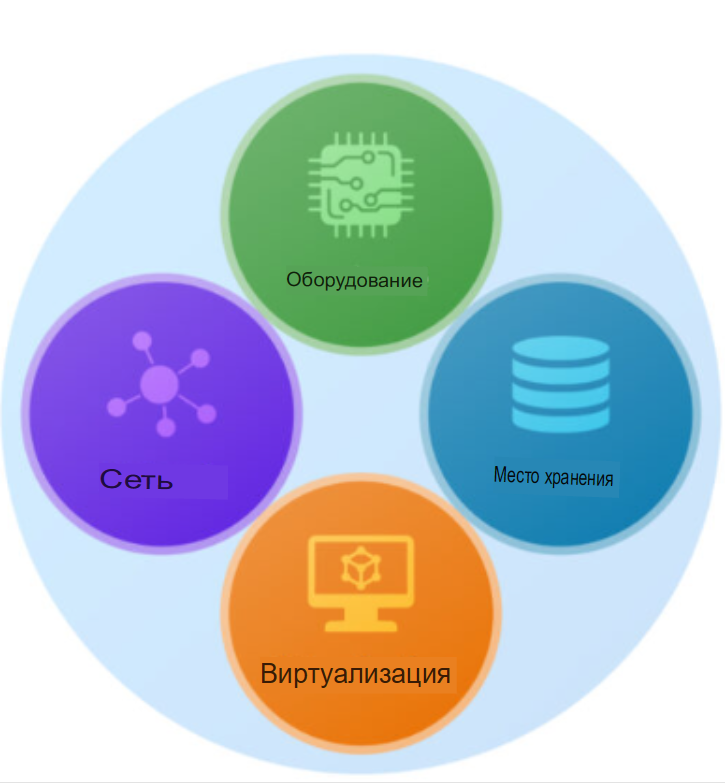
****

Рисунок 4.Состав облачной инфраструктуры.

1. Физическое оборудование: Серверы, коммутаторы, маршрутизаторы, аппаратные фаерволы, балансировщики нагрузки, системы хранения данных.
2. Виртуализация: Технология, которая отделяет вычислительные ресурсы — процессорную мощность, память, место в хранилище — от конкретного физического оборудования. Для этого на сервер или кластер серверов устанавливают специальное ПО, называемое гипервизором. Именно гипервизор и виртуализация отвечают за разделение ресурсов и предоставление их отдельным пользователям в виде полноценных виртуальных машин, работающих на одном физическом оборудовании. Гипервизор – это программное обеспечение, которое можно использовать для запуска нескольких виртуальных машин в одной физической машине. Каждая виртуальная машина имеет свою операционную систему и приложения. Гипервизор по мере необходимости выделяет базовые физические вычислительные ресурсы, такие как ЦП и память, для отдельных виртуальных машин. Таким образом поддерживается оптимальное использование физической ИТ-инфраструктуры.
3. Хранилище: В дата-центрах данные хранятся в массивах, которые объединяют множество дисков, иногда с различными параметрами производительности: например, быстрые NVMe-накопители для «горячих» и традиционные HDD — для «холодных» данных. Их ресурсы благодаря виртуализации также определены от вычислительных мощностей и распределены между множеством различных пользователей. Работа с хранилищем предполагает добавление или удаление отдельных дисков, настройку резервного копирования, индексацию данных и другие операции.
4. Сеть В ее основе лежат коммутаторы, маршрутизаторы и километры проводов. Облачная сеть обычно состоит из нескольких подсетей с различным уровнем видимости. Благодаря сети пользователи могут получать доступ к своим ресурсам в облаке через интернет, если облачная инфраструктура принадлежит локально одной организации.

Так же есть три модели облачных вычислений, каждая из которых определяет принцип выделения ресурсов в облаке в соответствии с рисунком 5.



Рисунок 5. Модели облачных вычислений.

IaaS (Infrastructure as a Service) — «инфраструктура как услуга». Корпоративные клиенты арендуют под свои задачи пул вычислительных ресурсов: процессорную мощность, память, место в хранилище, канал передачи данных. В облако переносят все или часть IT-нагрузок и оплачивают их по мере использования. При этом клиенты не покупают, не занимаются обслуживанием оборудования и могут в любой момент очень быстро масштабировать облако под изменившуюся нагрузку.

PaaS (Platform as a Service) — «платформа как услуга». Компании-разработчики арендуют набор облачных сервисов для разработки, тестирования, доставки и управления новыми программными продуктами.

SaaS (Software as a Service) — «программное обеспечение как услуга». Разработчик ПО размещает его в облаке, откуда с ним работают пользователи. Типичными примерами SaaS-приложений можно назвать сервисы для работы с электронной почтой (всем знакомый Gmail) или хранения.

2.2. Основные проблемы безопасности при использовании облачной инфраструктуры

Использование облачной инфраструктуры предоставляет предприятиям множество преимуществ, включая гибкость, масштабируемость и экономию ресурсов. Однако, переход к облачным технологиям также сопровождается новыми вызовами в области безопасности. С ростом объемов данных и увеличением количества подключенных устройств, обеспечение надежной защиты информации в облаке становится критически важным аспектом для любой организации. В данном разделе будут рассмотрены основные проблемы безопасности, с которыми сталкиваются предприятия при использовании облачной инфраструктуры. Анализ этих проблем позволит глубже понять потенциальные риски и разработать эффективные стратегии их минимизации, что, в свою очередь, обеспечит защиту конфиденциальных данных.

* Угрозы конфиденциальности данных:

Неавторизованный доступ: Злоумышленники могут использовать уязвимости в системе безопасности для получения доступа к данным без разрешения. Это может включать взлом учетных записей пользователей, использование уязвимостей в приложениях или обман администраторов через социальную инженерию.

Нарушение конфиденциальности: Персональные данные, финансовая информация и другие конфиденциальные данные могут быть раскрыты из-за недостатков в безопасности облачных сервисов или неправильного управления доступом. Это может привести к утечкам данных, что негативно сказывается на репутации компании и может привести к юридическим последствиям.

* Целостность данных:

Изменение данных: Данные могут быть изменены злоумышленниками, что приведет к недостоверной информации, нарушению бизнес-процессов и возможным финансовым потерям. Например, изменение финансовых записей может повлиять на отчетность и принятие решений.

Уничтожение данных: Вредоносное ПО или целенаправленные атаки могут привести к удалению важных данных, что может парализовать работу компании и привести к значительным убыткам.

* Доступность данных и сервисов:

DDoS-атаки: Атаки на отказ в обслуживании могут сделать облачные сервисы недоступными для пользователей на продолжительное время, что может привести к остановке бизнес-процессов и финансовым потерям.

Зависимость от провайдера: Если облачный провайдер испытывает технические проблемы или банкротится, компания может потерять доступ к своим данным и сервисам. Это подчеркивает важность выбора надежного провайдера и наличия планов на случай чрезвычайных ситуаций.

Нарушение политики безопасности и комплаенс

Несоответствие требованиям законодательства: Хранение и обработка данных в облаке должны соответствовать локальным и международным требованиям законодательства, таким как GDPR, HIPAA и другие. Нарушение этих требований может привести к штрафам и юридическим последствиям.

Нарушение внутренних политик: Компании должны следить за тем, чтобы использование облачных решений соответствовало их внутренним политикам безопасности и требованиям к защите данных.

* Инсайдерские угрозы:

Внутренние злоумышленники: Сотрудники облачного провайдера или самой компании могут использовать свои права доступа для нанесения вреда. Это могут быть злонамеренные действия, такие как кража данных или саботаж.

Неправильное управление доступом: Ошибки в настройке прав доступа могут привести к утечке данных или их изменению, если доступ предоставлен лицам, не имеющим на это права.

* Управление ключами шифрования:

Потеря контроля над ключами: Передача ключей шифрования облачному провайдеру может снизить уровень контроля над безопасностью данных. Это создает риск, что ключи могут быть скомпрометированы или утрачены.

Уязвимости ключей: Ненадежное хранение или управление ключами шифрования может привести к их компрометации, что поставит под угрозу все зашифрованные данные.

* Виртуальные и физические уязвимости:

Уязвимости виртуальных машин: Виртуальные машины могут быть подвержены атакам, использующим уязвимости гипервизора или других виртуализированных компонентов. Эти атаки могут позволить злоумышленникам получить доступ к данным других виртуальных машин на том же сервере.

Физическая безопасность: Дата-центры облачных провайдеров должны иметь надежные меры физической безопасности для защиты от несанкционированного доступа, кражи, пожаров и других угроз.

* Ошибки конфигурации и управления:

Неправильные настройки безопасности: Ошибки в конфигурации облачной инфраструктуры могут открыть доступ злоумышленникам. Например, открытые порты, неправильные правила брандмауэра или недостаточные настройки аутентификации.

Недостаточное управление изменениями: Несвоевременные обновления и изменения в конфигурации могут привести к уязвимостям. Регулярное управление изменениями и патчами критически важно для поддержания безопасности.

* Вредоносные атаки и программное обеспечение:

Вирусы и трояны: Вредоносное ПО может инфицировать облачные системы и распространяться между пользователями. Облачные провайдеры должны использовать эффективные антивирусные решения и меры по обнаружению и предотвращению таких угроз.

Фишинг и социальная инженерия: Атаки на пользователей для получения их учетных данных и доступа к облачным ресурсам могут быть особенно эффективными. Обучение сотрудников и внедрение многофакторной аутентификации может помочь снизить этот риск.

Эффективная защита облачной инфраструктуры требует комплексного подхода, который включает технические, административные и организационные меры. Это поможет обеспечить безопасность данных и защитить бизнес от разнообразных угроз.

3. Проектирование облачной инфраструктуры и системы защиты информации

3.1 Требования, предъявляемые к сети предприятия

В условиях стремительного развития технологий и растущих объемов данных предприятиям необходимо создавать и поддерживать эффективную и надежную сетевую инфраструктуру. Одним из ключевых требований современной сети предприятия является обеспечение безопасного и надежного хранения данных в облаке. Это требование обусловлено не только необходимостью защищать конфиденциальную информацию, но и потребностью в гибкости и доступности данных для поддержки бизнес-процессов. В данном разделе будут рассмотрены требования, предъявляемые к сети предприятия, с акцентом на аспекты хранения данных в облачной среде. Анализ этих требований поможет сформировать понимание необходимых мер для обеспечения безопасности, доступности и целостности данных, что является основой успешной работы любой организации.

Основные требования к сети предприятия:

* Безопасность данных

Шифрование данных: Все данные, передаваемые и хранящиеся в облаке, должны быть защищены с помощью современных методов шифрования. Это включает в себя как шифрование данных при передаче, так и при хранении.

Аутентификация и авторизация: Использование многофакторной аутентификации и строгих политик доступа для предотвращения несанкционированного доступа к данным.

* Доступность данных

Обеспечение непрерывного доступа: Сеть должна быть спроектирована таким образом, чтобы обеспечить постоянный доступ к данным и приложениям в облаке, минимизируя время простоя.

Резервное копирование и восстановление: Регулярное создание резервных копий данных и наличие планов восстановления в случае сбоя или потери данных.

* Производительность сети

Высокая пропускная способность: Сеть должна обладать достаточной пропускной способностью для обработки большого объема данных, передаваемых между локальными устройствами и облаком.

Минимальная задержка: Оптимизация маршрутов передачи данных для снижения задержек и повышения скорости доступа к данным и приложениям в облаке.

* Гибкость и масштабируемость

Масштабируемость ресурсов: Возможность быстрого масштабирования сетевых и вычислительных ресурсов в зависимости от изменений в объемах данных и нагрузке на систему.

Гибкость конфигурации: Легкость в настройке и управлении сетевой инфраструктурой для адаптации к новым требованиям бизнеса.

* Соответствие стандартам и нормативам

Соответствие законодательству: Убедиться, что все данные и процессы соответствуют действующим законодательным и отраслевым стандартам по защите данных.

Регулярные аудиты и оценки безопасности: Проведение регулярных аудитов и оценки безопасности для выявления и устранения потенциальных уязвимостей.

Следование этим требованиям позволит предприятию эффективно использовать облачную инфраструктуру, обеспечивая при этом высокий уровень защиты и доступности данных, что является критически важным для стабильного и успешного ведения бизнеса.

3.2 Разработка облачной инфраструктуры.

Создание облачной инфраструктуры для безопасного хранения данных и организации электронного документооборота было выполнено мною. Была спроектировано и реализовано облачное хранилище с использованием «Яндекс Диска», а также настроено подключение сетевого диска на все рабочие станции предприятия. Данный подход обеспечил централизованное хранение данных и упростил процесс обмена документами внутри организации.

Для того чтобы подключить сетевой диск необходимо зарегистрировать аккаунт для предприятия в облачном сервисе «Яндекс Диск» с объемом хранилища 10 ГБ в соответствии с рисунком 6, если предприятию потребуется большее пространство для документов и проектов, будет возможность приобрести дополнительное пространство по подписке «Премиум» в соответствии с рисунком 7.

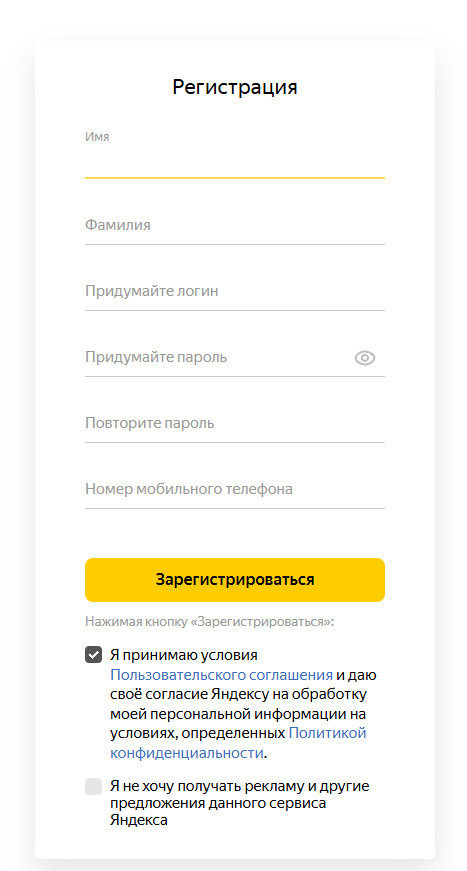


Рисунок 6. Регистрация в облачном сервисе «Яндекс Диск».

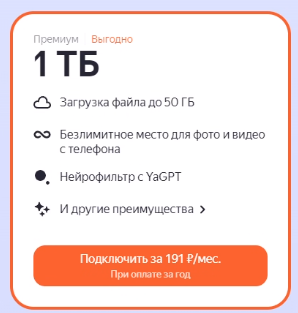


Рисунок 7. Подписка на увеличение объема облачного хранилища.

После вышеупомянутых действий, необходимо установить утилиту Air Live Drive в соответствии с рисунком 8-12.



Рисунок 8. Официальный сайт Air Live Drive.

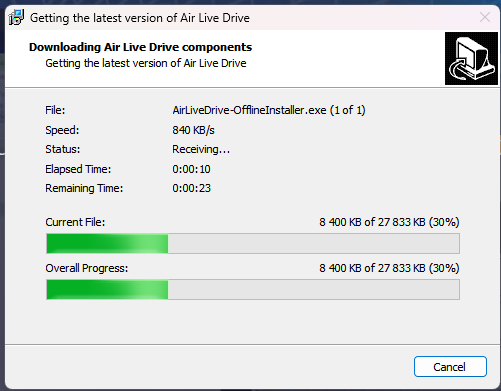


Рисунок 9. Установка Air Live Drive.

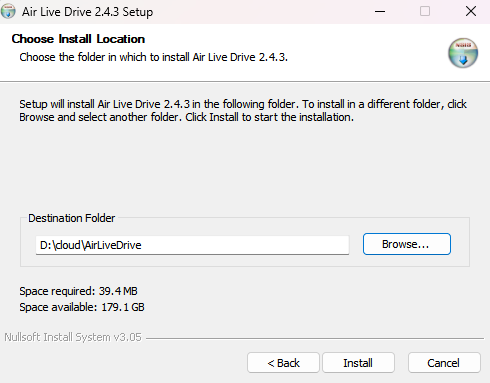


Рисунок 10. Выбор диска для установки Air Live Drive.

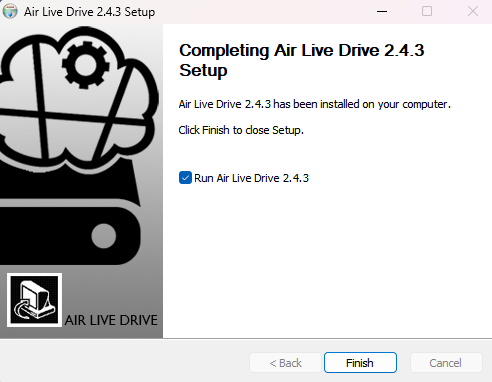


Рисунок 11. Установка Air Live Drive завершена.

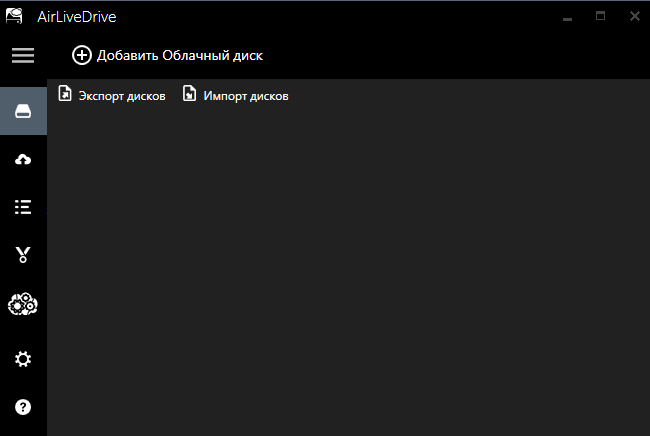


Рисунок 12. Интерфейс программы Air Live Drive.

После установки Air Live Drive, необходимо выбрать облачный диск в облачном сервисе «Яндекс Диск» в соответствии с рисунком 13.

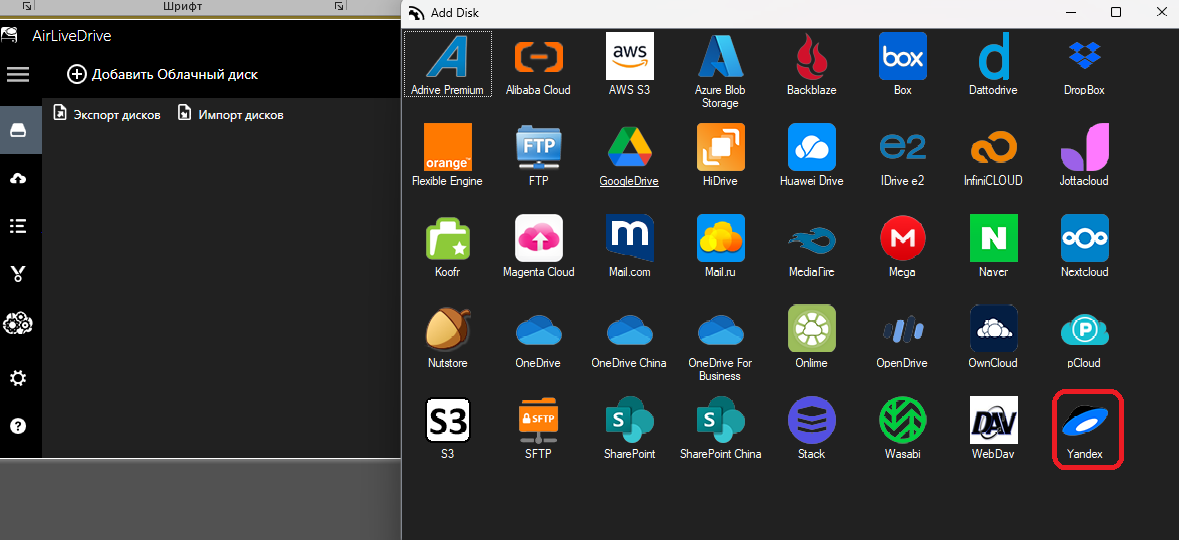


Рисунок 13. Выбор облачного диска.

Далее авторизируемся в созданную учётную запись «Яндекс Диск» в соответствии с рисунком 14.

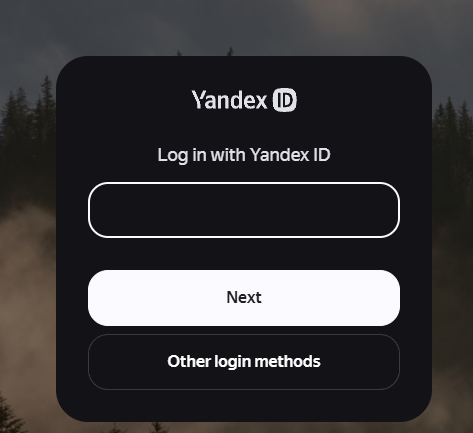


Рисунок 14.Авторизация в «Яндекс Диск».

После авторизации в «Яндекс Диск» в приложении Air Live Drive появляется облачный диск, который необходимо подключить в соответствии с рисунком 15.

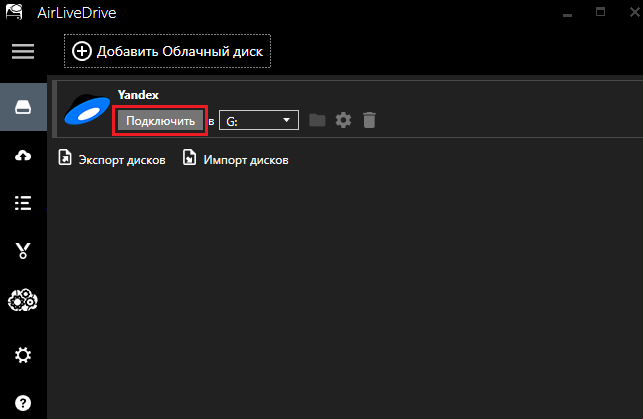


Рисунок 15.Подключение облачного диска в приложении AirLiveDrive.

После подключения облачного диска в проводнике появится облачное хранилище «Яндекс Диск» в соответствии с рисунком 16.

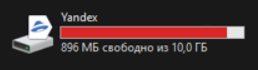


Рисунок 16. Облачное хранилище «Яндекс Диск».

# 3.3 Основные угрозы информационной безопасности в облачной сети предприятия и методы их устранения

Многие компании, согласно законодательству РФ, несут ответственность за сохранность личных данных своих сотрудников и клиентов. И это действительно необходимо. Ведь утечка, например, электронных медицинских карт может нанести моральный ущерб пациентам. А если произойдет утечка персональных данных клиентов какого-либо банка? Это может причинить людям материальный урон. И в той, и в другой ситуации приятного мало.

Есть несколько видов угроз безопасности информации:

1. Потеря конфиденциальных данных – разглашение, несанкционированный доступ, утечка, аудио-, фото- и видеосъемка, неумышленная потеря;
2. Повреждение целостности данных — изменение, трансформация, неприятие достоверности данных, навязывание заведомо ложной информации. Доктрина информационной безопасности подразумевает не просто искажение информации, а внесение новых данных в прежние сведения;
3. Нарушение доступности данных — т. е. блокировка доступа или полное уничтожение.

Организация защиты информации с использованием программных средств - это комплекс мероприятий и инструментов, направленных на обеспечение безопасности данных, приложений и инфраструктуры предприятия. Это включает в себя использование различных программных продуктов и решений для обнаружения и предотвращения угроз, шифрования данных, управления доступом и мониторинга безопасности.

С ростом информатизации общества растет и необходимость в защите персональных данных, а также в противостоянии киберпреступлениям. В связи с этим становятся все более востребованными направления, задействованные в разработках и реализации методов, которые способны обеспечить компьютерную безопасность. Такие решения набирают популярность и еще по нескольким причинам:

1. Программные системы защиты легко интегрировать в оборудование заказчика и разработчика;
2. Использование таких средств не представляет сложностей;
3. Для использования этих методов нет надобности задействовать производство, а реализация осуществляется в сжатые сроки. Но несмотря на это, информация получает необходимую степень защиты.

Была организованна защита информации программными средствами:

1. Антивирусные программы: обеспечивают защиту от вредоносных программ, включая вирусы, троянские программы и шпионские приложения.
2. Настройка групповых политик: настроить групповые политики (ограничение прав пользователей)
3. Средства мониторинга безопасности сети: предоставляют возможность непрерывного мониторинга и анализа событий безопасности для обнаружения инцидентов и реагирования на них.

Эти и другие программные средства используются совместно для создания комплексной защиты информации на предприятии, минимизируя риски утечки данных, нарушений безопасности и других угроз информационной безопасности.

Рассмотрим защиту информации на примере антивирусного ПО:

Для организации защиты информации с помощью Kaspersky Endpoint Security необходимо произвести следующие действия:

1. Установить антивирусное программное обеспечение Kaspersky Endpoint Security на все компьютеры и серверы в сети предприятия в соответствии с рисунками 6 и 7.



Рисунок 17. Установка Kaspersky.

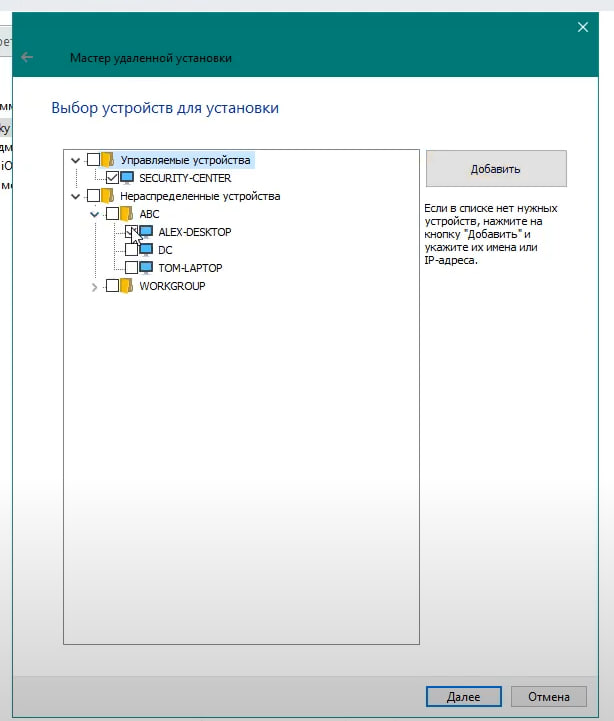


Рисунок 18.Установка Kaspersky Endpoint Security на клиентские ПК и сервера.

1. Настроить параметры защиты в соответствии с рисунком 8 и 9.

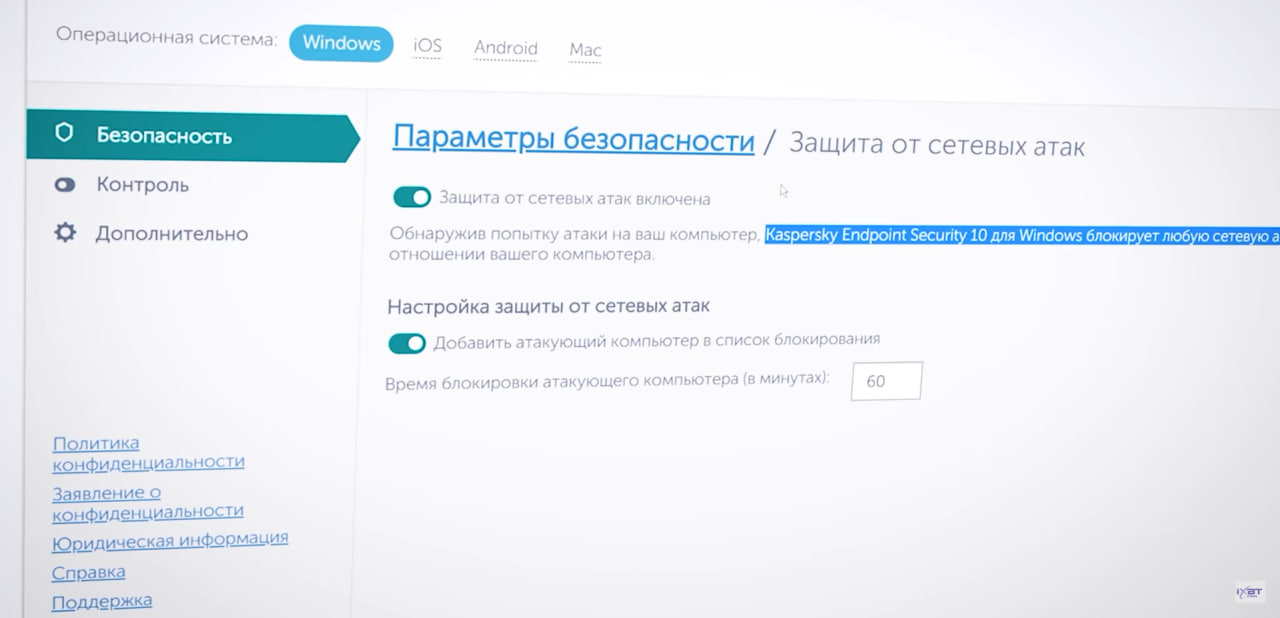


Рисунок 19. Настройка параметров защиты.

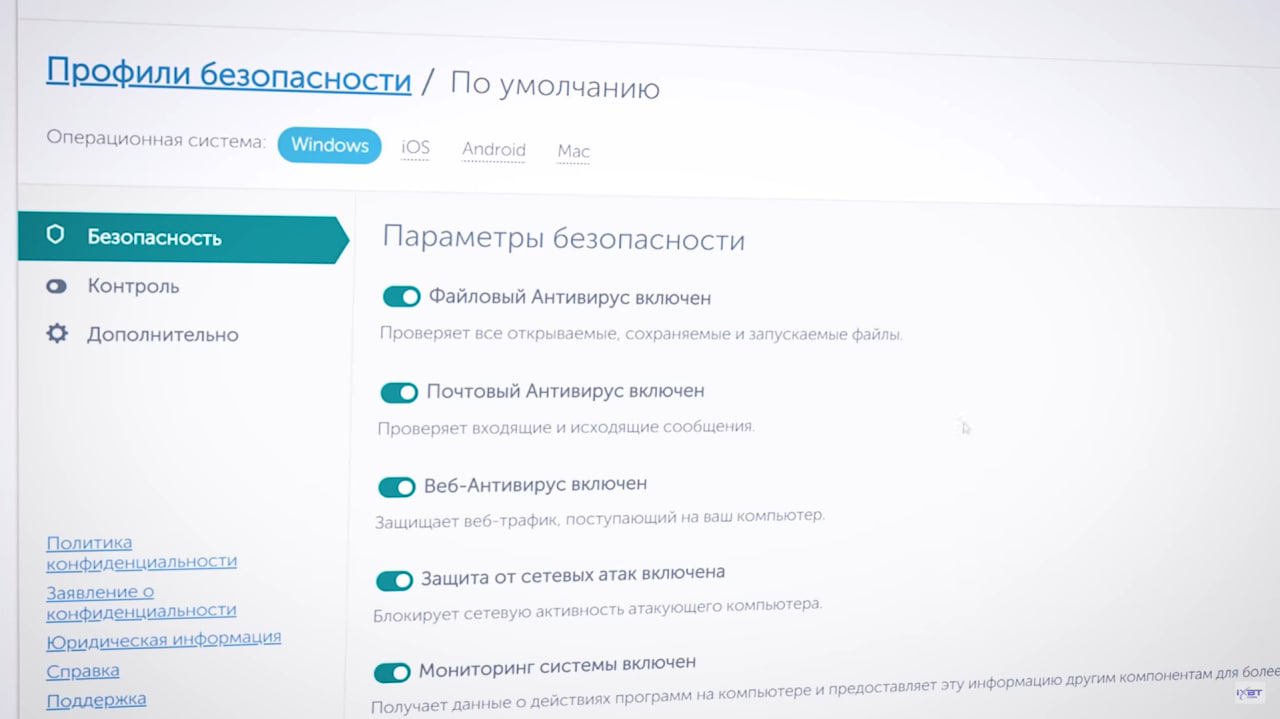


Рисунок 20. Дополнительная настройка параметров защиты.

1. Обеспечить регулярные обновления баз вирусных сигнатур и программного обеспечения Kaspersky Endpoint Security.
2. Проводить мониторинг состояния системы с помощью инструментов мониторинга Kaspersky Endpoint Security и реагируйте на обнаруженные угрозы в соответствии с установленными процедурами реагирования на инциденты безопасности.

Организация защиты информации так же осуществляться Microsoft Defender, функцией Брандмауэра Защитника Windows в которой помимо обычной проверки сети, данных, есть возможность создать необходимые для предприятия правила входящих и исходящих подключений, указать разрешенные и запрещенные правила доступа к портам и адресам в соответствии с рисунком 14 и 15.

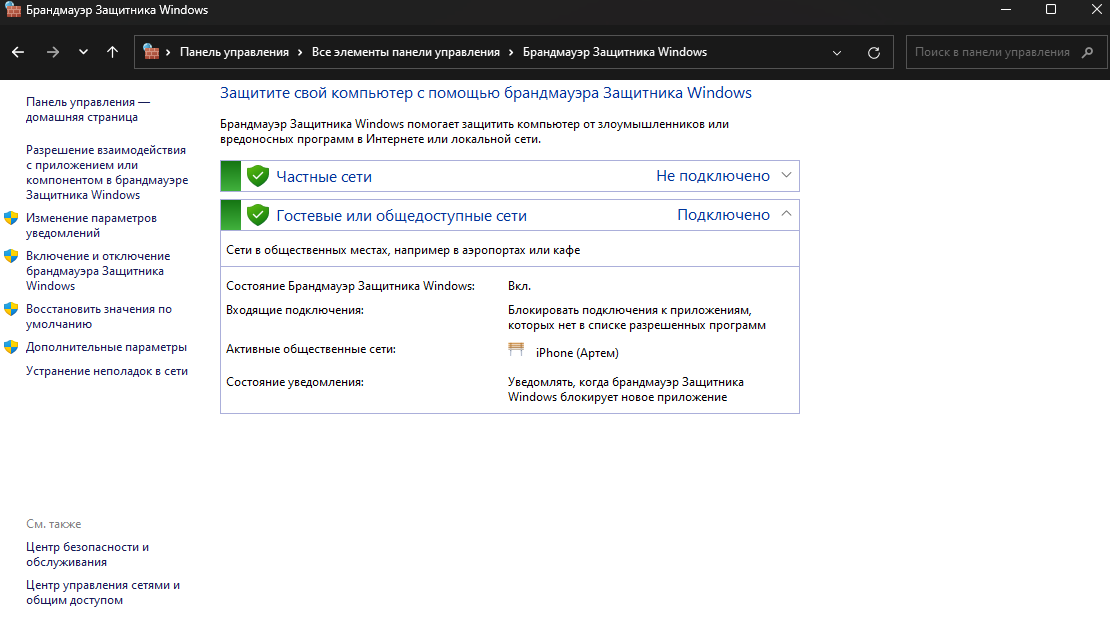


Рисунок 21. Брандмауэр Защитника Windows

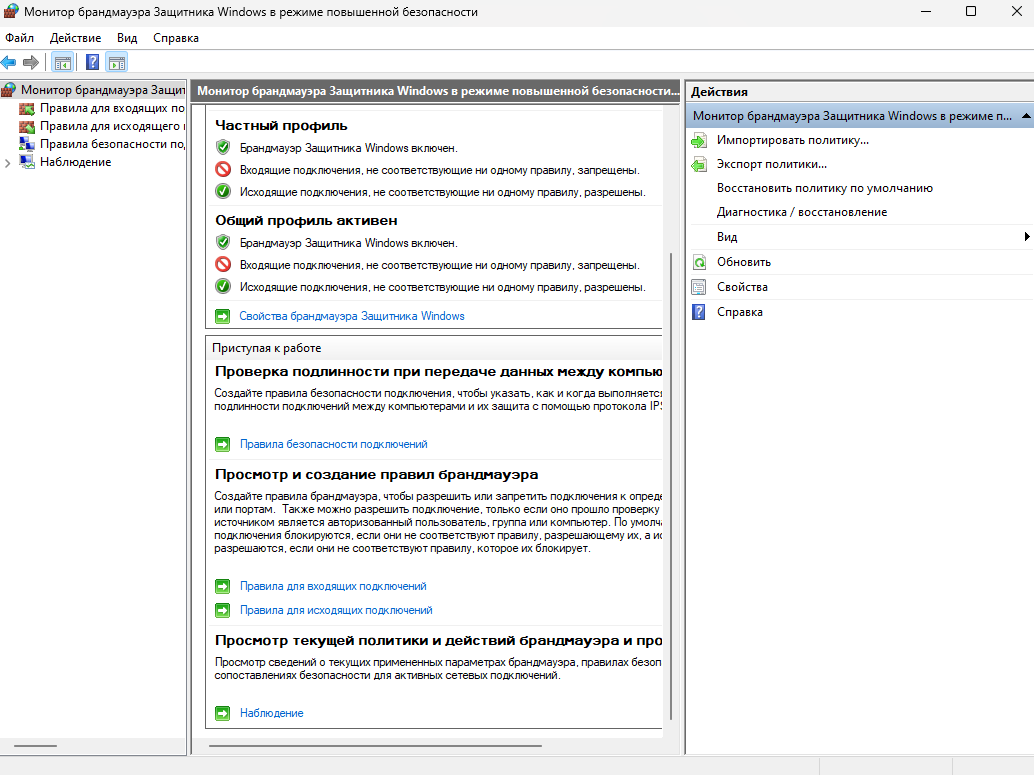


Рисунок 22. Возможность настройки Брандмауэра Защитника Windows.

3.4 Затраты на разработку облачной инфраструктуры и ожидаемый экономический эффект

Многие крупные облачные провайдеры, такие как Amazon Web Services (AWS), Google Cloud Platform (GCP) и Microsoft Azure предлагают бесплатные тарифы своих сервисов. Эти бесплатные уровни позволяют использовать определенные ресурсы без необходимости оплаты в течение ограниченного периода времени или до достижения определенного лимита. Основные преимущества бесплатной инфраструктуры включают:

* Экономия на начальных этапах: Возможность тестирования и разработки приложений без значительных вложений.
* Ознакомление с платформой: Пользователи могут изучить возможности платформы и оценить её функциональность.

Однако, бесплатные уровни имеют свои ограничения, такие как ограниченный объем хранилища, вычислительных мощностей и ограниченное количество транзакций. Например, AWS предлагает 12 месяцев бесплатного доступа к определенным ресурсам, таким как виртуальные машины EC2, хранилище S3 и базы данных RDS, но после превышения установленных лимитов пользователи начинают оплачивать дополнительные ресурсы.

По мере роста потребностей бизнеса и увеличения объема данных, бесплатных ресурсов может оказаться недостаточно. В таком случае требуется расширение инфраструктуры за счет платных услуг. Основные затраты при этом включают:

* Выделенные виртуальные машины: Оплата за использование дополнительных виртуальных машин с различными конфигурациями (CPU, RAM, дисковое пространство).
* Хранение данных: Платные тарифы на хранение данных в облаке, включая архивное и оперативное хранилище.
* Сетевые услуги: Оплата за использование сетевых ресурсов, таких как балансировщики нагрузки, виртуальные частные сети (VPN) и трафик между регионами.
* Базы данных: Использование управляемых баз данных с оплатой за хранилище и вычислительные ресурсы.

Стоимость платных услуг варьируется в зависимости от провайдера и конкретных потребностей бизнеса. Для оптимизации затрат важно тщательно планировать и контролировать использование ресурсов.

Одним из основных преимуществ облачной инфраструктуры является снижение капитальных затрат на покупку и обслуживание собственного оборудования. Использование облачных сервисов позволяет отказаться от дорогостоящих серверов, систем хранения данных и сетевого оборудования, заменяя их арендуемыми облачными ресурсами. Это снижает первоначальные инвестиции и уменьшает риски, связанные с устареванием оборудования.

Облачная инфраструктура предоставляет возможность масштабирования ресурсов в зависимости от текущих потребностей бизнеса. Это позволяет эффективно управлять затратами, оплачивая только те ресурсы, которые действительно используются. В периоды пиковых нагрузок можно быстро увеличить мощность инфраструктуры, а затем сократить её, когда потребность в дополнительных ресурсах снижается. Это особенно важно для стартапов и быстрорастущих компаний, которые могут испытывать значительные колебания в потребностях IT-ресурсов.

Разработка облачной инфраструктуры, начиная с использования бесплатных уровней и постепенного перехода на платные ресурсы, позволяет компаниям значительно снизить капитальные затраты, обеспечить гибкость и масштабируемость, повысить производительность и доступность сервисов, а также оптимизировать операционные расходы. В результате, внедрение облачных технологий способствует не только экономии финансовых средств, но и улучшению общей эффективности и конкурентоспособности бизнеса.

Была спроектирована и организована эффективная, экономичная, масштабируемая инфраструктура с использованием хранилища «Яндекс Диск», безопасности «Kaspersky Endpoint Security» и утилиты «Air Live Drive».