**Дипломная работа на тему "Разработка мер защиты от несанкционированных воздействий на локальную сеть ООО 'МоРо'**

1. Введение.
2. Обзор литературы и существующих технологий.
3. Описание локальной сети ООО "МоРо".
4. Анализ угроз и оценка рисков.
5. Разработка мер защиты.
6. Тестирование и оценка эффективности предложенных мер.
7. Внедрение и рекомендации.
8. Заключение.

ДЛЯ НАПИСАНИЯ РАБОТЫ НЕОБХОДИМА СЛЕДУЮЩАЯ ИНФОРМАЦИЯ ПО ООО «МоРо»:

- ОПИСАНИЕ ЛВС ОРГАНИЗАЦИИ(ИСПОЛЬЗУЕМЫЕ ТЕХНОЛОГИИ И ОБОРУДОВАНИЕ, СЕТЕВУЮ ТОПОЛОГИЮ И ОСНОВНЫЕ СЛУЖБЫ И СЕРВИСЫ, ПРЕДОСТАВЛЯЕМЫЕ СЕТЬЮ) - АНАЛИТИЧЕСКОЙ ЧАСТИ БЕЗ ДАННОЙ ИНФОРМАЦИИ НЕ СДЕЛАТЬ!;

- ЖЕЛАЕМЫЙ АНАЛИЗ КОНКРЕТНЫХ УГРОЗ БЕЗОПАСНОСТИ ЛВС;

- ВОЗМОЖНЫЕ РЕЗУЛЬТАТЫ ТЕСТОВ БЕЗОПАСНОСТИ ЛВС;

- ИСПОЛЬЗУЕМЫЕ ВИДЫ ТЕХНИЧЕСКОЙ И ПРАВОВОЙ ЗАЩИТЫ ИНФОРМАЦИИ, ВОЗМОЖНОСТЬ ПРИМЕНЕНИЯ КРИПТОГРАФИЧЕСКИХ СРЕДСТВ ЗИ.

ЛИБО ИСПОЛЬЗОВАНИЕ СТРУКТУРЫ И БЕЗОПАСНОСТИ ЛВС АНАЛОГИЧНОЙ ОРГАНИЗАЦИИ?

**Введение**

В современном мире информационные технологии играют важную роль в функционировании и развитии различных отраслей, включая промышленность, науку, образование, медицину и другие. Компании и организации активно интегрируют информационные системы и локальные сети для автоматизации бизнес-процессов, обеспечения коммуникации между сотрудниками и управления доступом к корпоративным ресурсам.

Однако, вместе с ростом зависимости организаций от информационных систем возрастает и риск возникновения угроз безопасности. Злоумышленники могут использовать различные методы атак для получения доступа к конфиденциальной информации, нарушения работоспособности сетевой инфраструктуры или причинения вреда бизнесу. Это может привести к значительным материальным и репутационным потерям, а также нарушению нормального функционирования организации.

ООО "МоРо" является современной компанией, активно использующей информационные технологии для оптимизации своих бизнес-процессов и улучшения качества предоставляемых услуг. Локальная сеть компании представляет собой сложную инфраструктуру, включающую множество устройств, сервисов и приложений, которые взаимодействуют между собой для обеспечения надежной работы и доступа к корпоративным ресурсам.

В связи с этим, одной из ключевых задач ООО "МоРо" является обеспечение безопасности своей локальной сети от несанкционированных воздействий. Необходимо разработать и внедрить комплекс мер, позволяющих минимизировать риски возникновения угроз, обеспечить сохранность конфиденциальной информации и гарантировать надежное функционирование сетевой инфраструктуры.

В рамках данной дипломной работы будет проведен анализ угроз безопасности, связанных с несанкционированными воздействиями на локальную сеть ООО "МоРо", и разработаны меры защиты, которые помогут противостоять возможным атакам на локальную сеть.

**Актуальность темы** "Разработка мер защиты от несанкционированных воздействий на локальную сеть ООО 'МоРо'" обусловлена рядом факторов, связанных с постоянным развитием информационных технологий и увеличением числа киберугроз.

Во-первых, информационные технологии стали неотъемлемой частью функционирования большинства современных компаний. Организации, включая ООО "МоРо", активно используют ИТ для автоматизации бизнес-процессов, обработки и хранения данных, коммуникации с клиентами и партнерами. В связи с этим, надежность и безопасность сетевой инфраструктуры становится критическим фактором, влияющим на успешность деятельности компании и ее конкурентоспособность.

Во-вторых, с расширением использования ИТ растет число потенциальных угроз и атак со стороны злоумышленников. Несанкционированные воздействия на локальную сеть могут привести к утечке конфиденциальной информации, сбоям в работе систем, а также финансовым и репутационным потерям для компании. В этом контексте разработка и внедрение мер защиты от подобных воздействий является актуальной и приоритетной задачей.

В-третьих, с учетом постоянного развития технологий и методов атак, обеспечение информационной безопасности требует системного и комплексного подхода. Это включает в себя не только использование современных средств защиты, но и регулярное мониторинг, анализ рисков, обучение персонала и адаптацию стратегии защиты к изменяющейся ситуации.

Таким образом, актуальность темы "Разработка мер защиты от несанкционированных воздействий на локальную сеть ООО 'МоРо'" определяется важностью обеспечения информационной безопасности для успешного функционирования компании, ростом числа киберугроз и необходимостью разработки комплексного подхода к их противодействию. Решение этой задачи позволит снизить риски, связанные с несанкционированными воздействиями, обеспечить сохранность ценной информации и поддержать надежное функционирование сетевой инфраструктуры компании.

В-четвертых, в условиях регулятивных требований в области информационной безопасности, компании обязаны соблюдать определенные стандарты и нормы, а также предпринимать меры по обеспечению конфиденциальности и целостности данных. Разработка и внедрение мер защиты от несанкционированных воздействий на локальную сеть ООО "МоРо" позволит компании соответствовать данным требованиям и избежать возможных штрафов и санкций со стороны регуляторов.

В-пятых, обеспечение информационной безопасности является важным фактором для поддержания доверия клиентов и партнеров к компании. Утечка данных, сбои в работе сети или другие последствия несанкционированных воздействий могут повлечь за собой потерю доверия и ущерб для имиджа компании. Разработка мер защиты позволит минимизировать такие риски и поддерживать высокий уровень деловой репутации ООО "МоРо".

В заключение, актуальность темы "Разработка мер защиты от несанкционированных воздействий на локальную сеть ООО 'МоРо'" определяется рядом факторов, включая важность информационной безопасности для успешного функционирования компании, рост числа киберугроз, необходимость комплексного подхода к защите, регулятивные требования и поддержание доверия клиентов и партнеров. Решение данной задачи способствует обеспечению стабильности и надежности работы компании в условиях постоянного развития информационных технологий и киберпространства.

**Целью данной дипломной работы** является разработка мер защиты от несанкционированных воздействий на локальную сеть ООО "МоРо", обеспечивающих сохранность информационных ресурсов компании и надежное функционирование сетевой инфраструктуры.

Для достижения поставленной цели разработки мер защиты от несанкционированных воздействий на локальную сеть ООО "МоРо" и обеспечения сохранности информационных ресурсов компании, **в рамках данной дипломной работы будут решены следующие задачи**:

1. Изучение существующих технологий и подходов к защите локальных сетей от несанкционированных воздействий.

Для успешной разработки мер защиты необходимо провести анализ современных технологий и методик, используемых для обеспечения информационной безопасности локальных сетей. Это включает в себя изучение аппаратных и программных средств защиты, протоколов и стандартов, а также методов анализа и мониторинга сетевых активов.

1. Анализ структуры локальной сети ООО "МоРо" и выявление потенциальных угроз безопасности.

На этапе анализа структуры сети необходимо исследовать ее архитектуру, устройства, программное обеспечение и настройки, чтобы определить возможные слабые места и уязвимости. Основываясь на полученных данных, будет составлен список потенциальных угроз безопасности, с которыми может столкнуться компания.

1. Разработка комплекса мер защиты от несанкционированных воздействий.

На основе проведенного анализа и изучения существующих технологий будет разработан комплекс мер защиты, направленных на предотвращение и минимизацию рисков, связанных с несанкционированными воздействиями на локальную сеть. Меры защиты могут включать в себя аппаратные и программные решения, изменение настроек сетевых устройств, усиление политик доступа и регулярное проведение аудита безопасности.

1. Оценка эффективности предложенных мер защиты и корректировка стратегии обеспечения информационной безопасности.

После разработки мер защиты и их внедрения, необходимо провести оценку их эффективности с точки зрения снижения рисков и улучшения безопасности сети. В случае выявления неэффективных или недостаточных мер, следует произвести корректировку стратегии обеспечения информационной безопасности и внести соответствующие изменения в предложенные решения. Оценка эффективности мер защиты должна проводиться на регулярной основе, с учетом возможных изменений в сетевой инфраструктуре и появления новых угроз.

1. Обучение персонала компании ООО "МоРо" принципам информационной безопасности и правилам работы с новыми средствами защиты.

Для обеспечения успешного функционирования разработанных мер защиты важным аспектом является обучение персонала компании. Сотрудники должны быть осведомлены о принципах информационной безопасности, основных угрозах и атаках, а также правилах работы с новыми средствами защиты и процедурами реагирования на инциденты. Это позволит снизить вероятность ошибок и утечек информации из-за человеческого фактора.

1. Разработка плана реагирования на инциденты и процедур восстановления сети после атак.

Даже при наличии мер защиты, существует вероятность возникновения инцидентов безопасности. Важным элементом комплексной стратегии обеспечения информационной безопасности является разработка плана реагирования на инциденты и процедур восстановления сети после атак. Это позволит своевременно обнаружить и локализовать угрозы, минимизировать их воздействие на сеть и быстро восстановить работоспособность системы.

Выполнение указанных задач в рамках дипломной работы позволит разработать комплекс мер защиты от несанкционированных воздействий на локальную сеть ООО "МоРо" и обеспечить сохранность информационных ресурсов компании, что является важным условием успешного функционирования предприятия в современных условиях развития информационных технологий и киберпространства.