01

Дипломная работа

Разработка организационно-технических решений по обеспечению безопасности в компьютерной сети ООО «ЭСГП»

Выполнил студент гр.СиСАД 19-01
Яненко К. В.

ВВЕДЕНИЕ

Цель темы

Актуальность

Проблема

Гипотеза

Предмет

Практическая значимость

Задачи

Разработка комплекса мер по обеспечению безопасности в компьютерной сети ООО «ЭСГП».

Компьютерные сети становятся все более сложными и масштабными, что усложняет задачу обеспечения их безопасности.

Существование множества угроз, риски нарушений безопасности информации, анализ.

Стратегия информационной безопасности компании.

1. Анализ угроз и уязвимостей сети;
2. Разработка стратегии безопасности;
3. Разработка комплексной стратегии безопасности;
4. Разработка политики безопасности;
5. Внедрение технологий безопасности;
6. Мониторинг и анализ безопасности сети.

АНАЛИЗ СОВРЕМЕННОГО СОСТОЯНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СЕТИ ООО "ЭСГП"

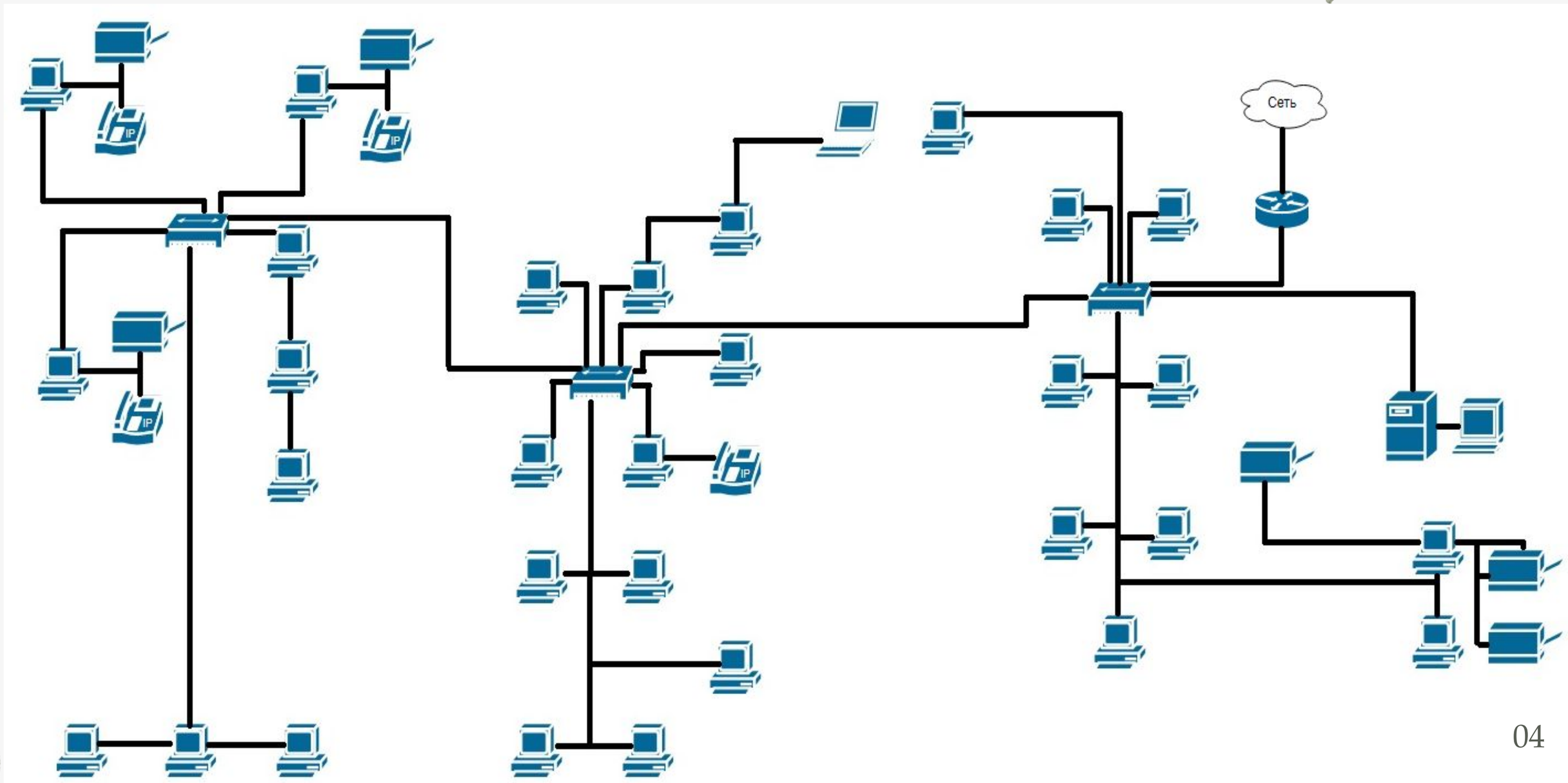
О компании:

ООО «ЭСГП» - архитектурная компания, специализирующаяся на BIM-проектировании, предоставляет услуги по созданию высококачественных проектов зданий и сооружений, используя информационную модель здания (BIM).

Угрозы безопасности. Существующие уязвимости сети ООО «ЭСГП» создают потенциальную угрозу реализации следующих угроз:

- Утечка конфиденциальной информации.
- Внешние атаки.
- Вредоносное ПО (вирусы, трояны, черви и т.п.).
- Атаки на отдельные устройства или системы с целью нарушения их работы.

ТОПОЛОГИЯ **СЕТИ**



ЭШЕЛОНИРОВАННАЯ ЗАЩИТА — КАК СТРАТЕГИЯ БЕЗОПАСНОСТИ КОРПОРАТИВНОЙ КОМПЬЮТЕРНОЙ СЕТИ

1	2	3	4	5
Внешняя сеть	Периметр внутренней сети	Внутренняя сеть	Хост	Данные

РАЗРАБОТКА КОМПЛЕКСНОЙ СИСТЕМЫ ЗАЩИТЫ ЛОКАЛЬНОЙ СЕТИ В ООО "ЭСГП"

Для разработки защиты безопасности локальной сети, использована эшелонированная защита, на основе рубежей защиты системы локальной сети, благодаря чему защита будет разделена на определенные участки безопасности.

Уровень защиты	Возможные угрозы безопасности	Метод предотвращения	Используемая технология
Физическая граница помещения	Несанкционированный доступ в помещение, кража или повреждение оборудования.	Установка системы контроля доступа, видеонаблюдение.	Видеокамеры, организационный регламент для сотрудников.
Внешняя сеть предприятия	Взлом сетевых устройств, DOS/DDOS-атаки.	Программы обнаружения вторжений.	Системы обнаружения вторжений (IDS) и системы предотвращения вторжений (IPS). Специализированное ПО.
Периметр внутренней сети	Несанкционированный доступ к сетевым ресурсам, снижение производительности сети.	Аутентификация и авторизация пользователей.	Системы аутентификации и авторизации, использование групповых политик. Использование VPN.
Внутренняя сеть	Кража данных, вредоносные программы.	Сканирование портов, мониторинг трафика.	Сканирование портов. Системы контроля доступа.
Хост	Вредоносные программы, утечка конфиденциальной информации.	Шифрование данных.	Шифрование данных с использованием BitLocker.

СИСТЕМА ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ И ИХ ПРЕДОТВРАЩЕНИЕ С ПОМОЩЬЮ СИСТЕМЫ SNORT

Использование IDS/IPS позволяет обнаруживать и предотвращать угрозы безопасности, такие как вирусы, трояны, черви и другие типы вредоносного ПО, а также предотвращать несанкционированный доступ к сетевым ресурсам..

Сбор данных: Snort получает входящие данные из сети. Он может прослушивать сетевой интерфейс или использовать файловый поток данных.

Анализ пакетов: Snort анализирует каждый входящий пакет на наличие отклонений от нормального поведения сети.

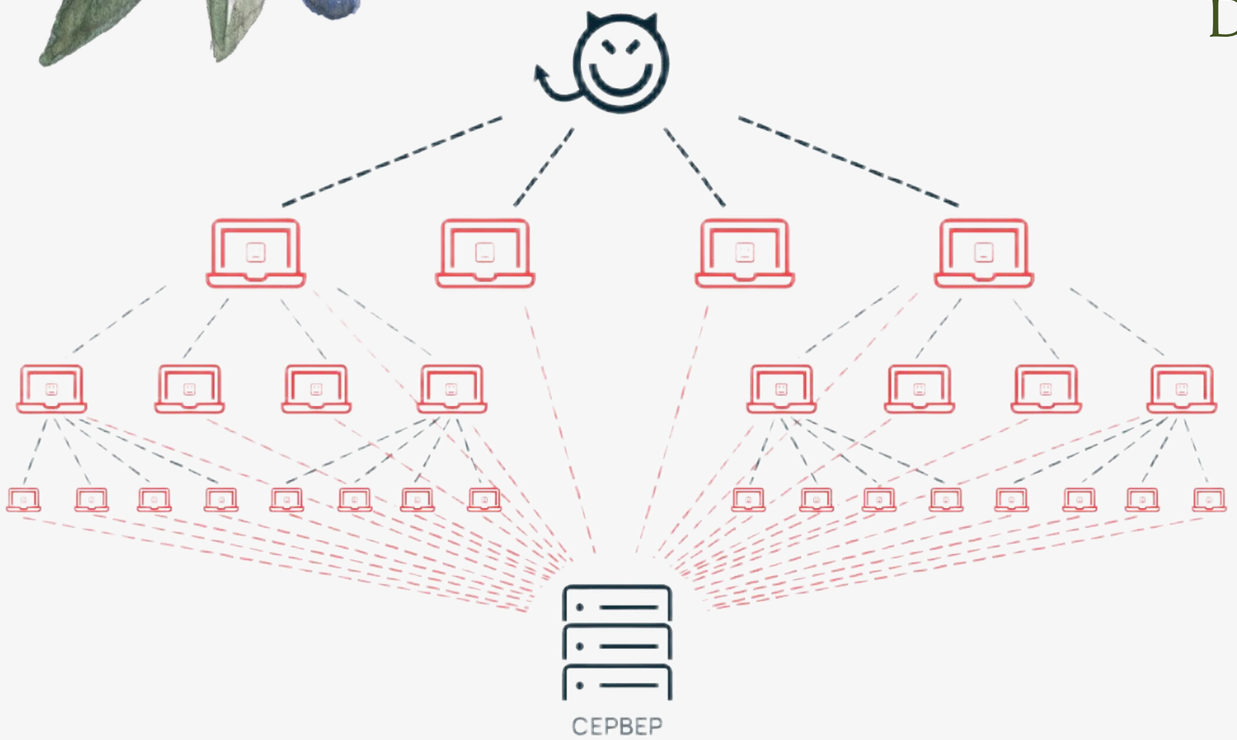
Определение угрозы: Если Snort обнаруживает угрозу, он создает алерт и отправляет его на сервер, который может уведомлять администраторов об уязвимостях и посоветовать по действиям.

Реагирование на такую угрозу: Snort может предотвращать атаки, блокируя пакеты, которые соответствуют определенным правилам.

Анализ угроз: Snort создает журналы, которые содержат информацию о произошедших событиях и дополнительную информацию, необходимую для определения проблем.

Хранение журналов: Snort отправляет журналы на сервер, где они могут быть хранены в течение определенного периода.

ПРОЕКТИРОВАНИЕ И ВНЕДРЕНИЕ СИСТЕМЫ ЗАЩИТЫ ОТ DDOS-АТАК ДЛЯ ОБЕСПЕЧЕНИЯ СТАБИЛЬНОСТИ РАБОТЫ СЕТИ В УСЛОВИЯХ МАССОВОГО НАПАДЕНИЯ



DDoS-атаки (Distributed Denial of Service), или атаки распределенного отказа в обслуживании, являются одним из наиболее распространенных видов кибератак в наши дни..

Kaspersky DDoS Protection

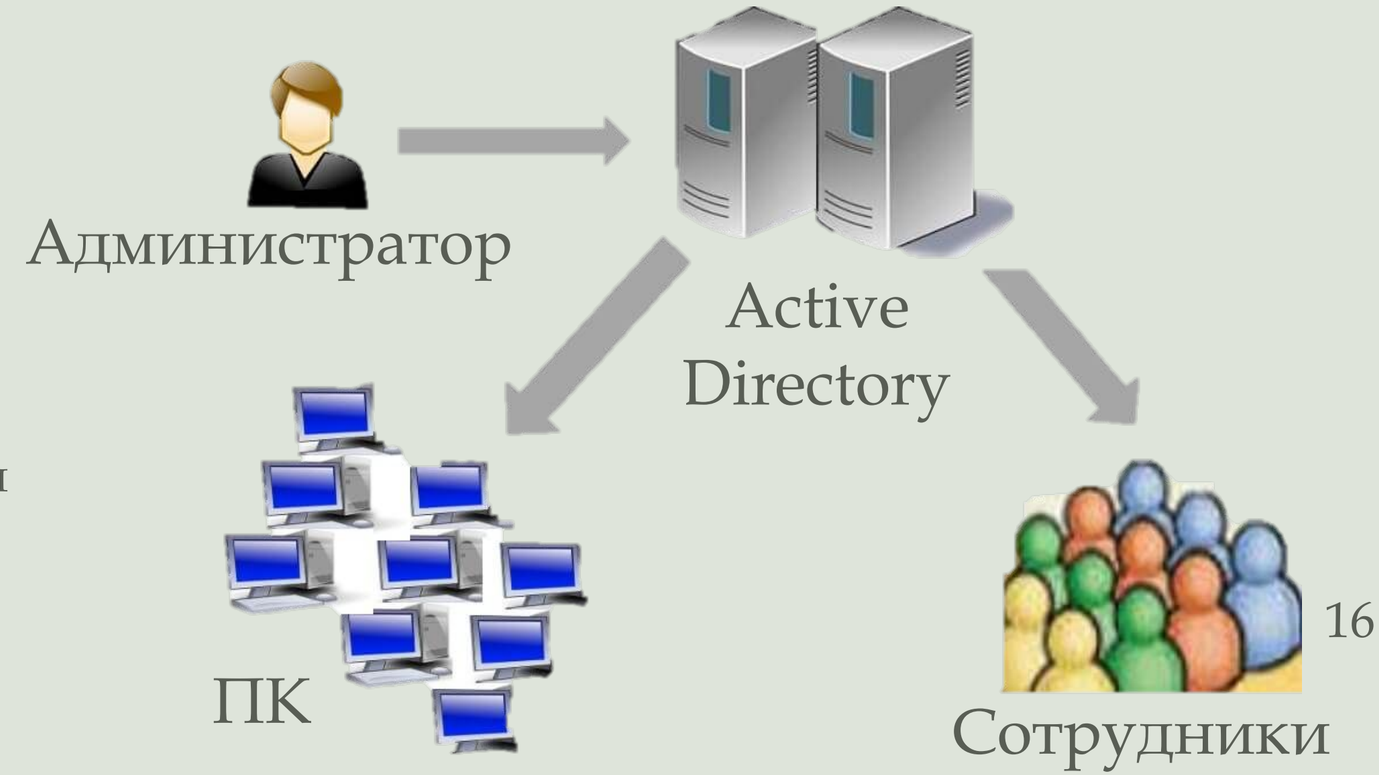
Kaspersky DDoS Protection - это система защиты от DDoS-атак, разработанная компанией Kaspersky Lab.

Методы защиты:

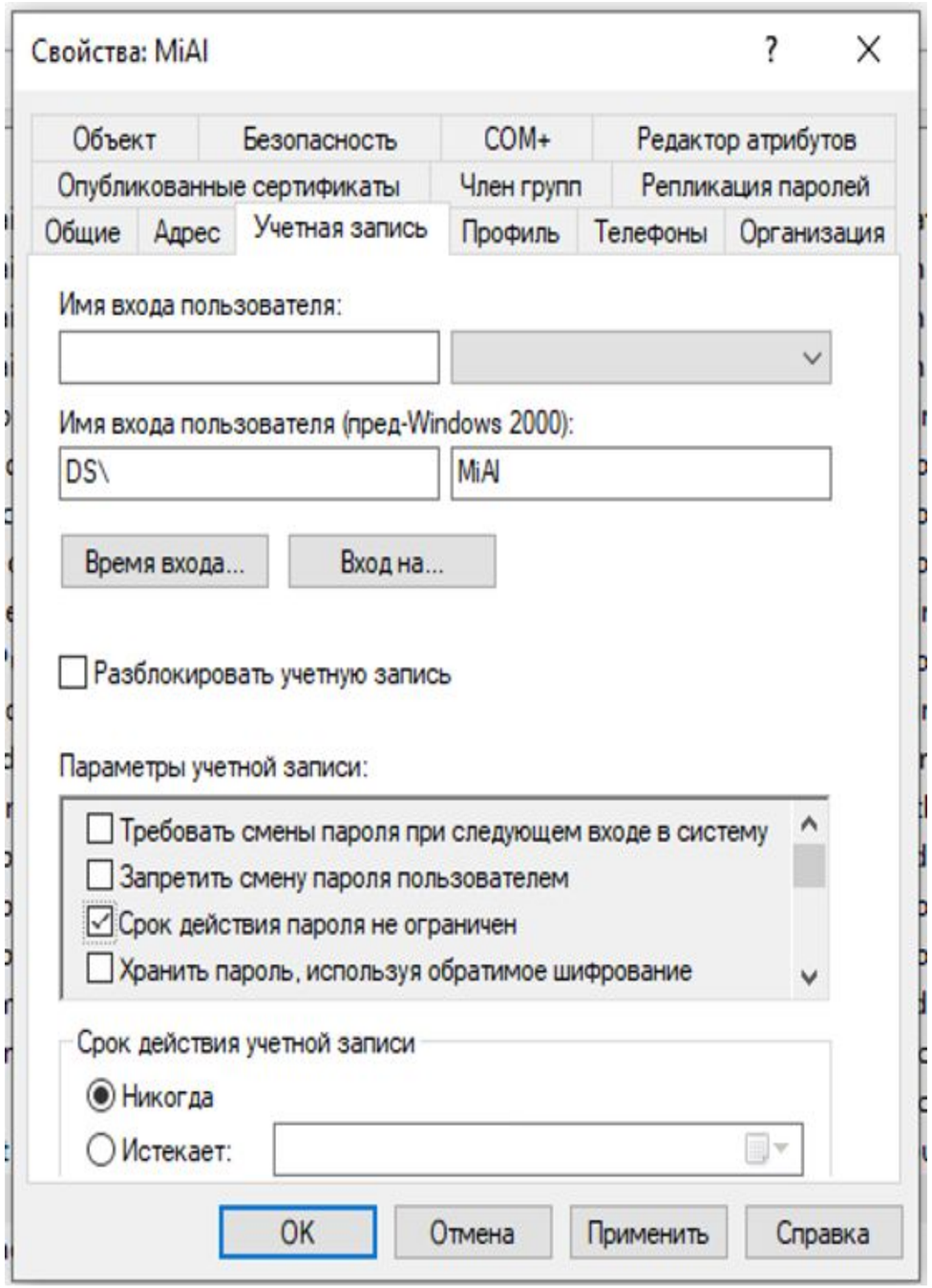
1. Анализ трафика
2. Распознавание атакующих ботов
3. Фильтрация трафика
4. Маскировка защищаемого сервиса
5. Управление трафиком
6. Мониторинг и уведомления

РАЗРАБОТКА ПРАВИЛ С ПОМОЩЬЮ ГРУППОВЫХ ПОЛИТИК ДЛЯ АУТЕНТИФИКАЦИИ И АВТОРИЗАЦИИ ПОЛЬЗОВАТЕЛЕЙ

Групповые политики в Windows - это механизм управления настройками системы, который позволяет администраторам централизованно управлять конфигурацией компьютеров и пользователей в сети.



- Журнал паролей
- Срок действия паролей
- Длина пароля
- Требования сложности
- Блокировка учетной записи

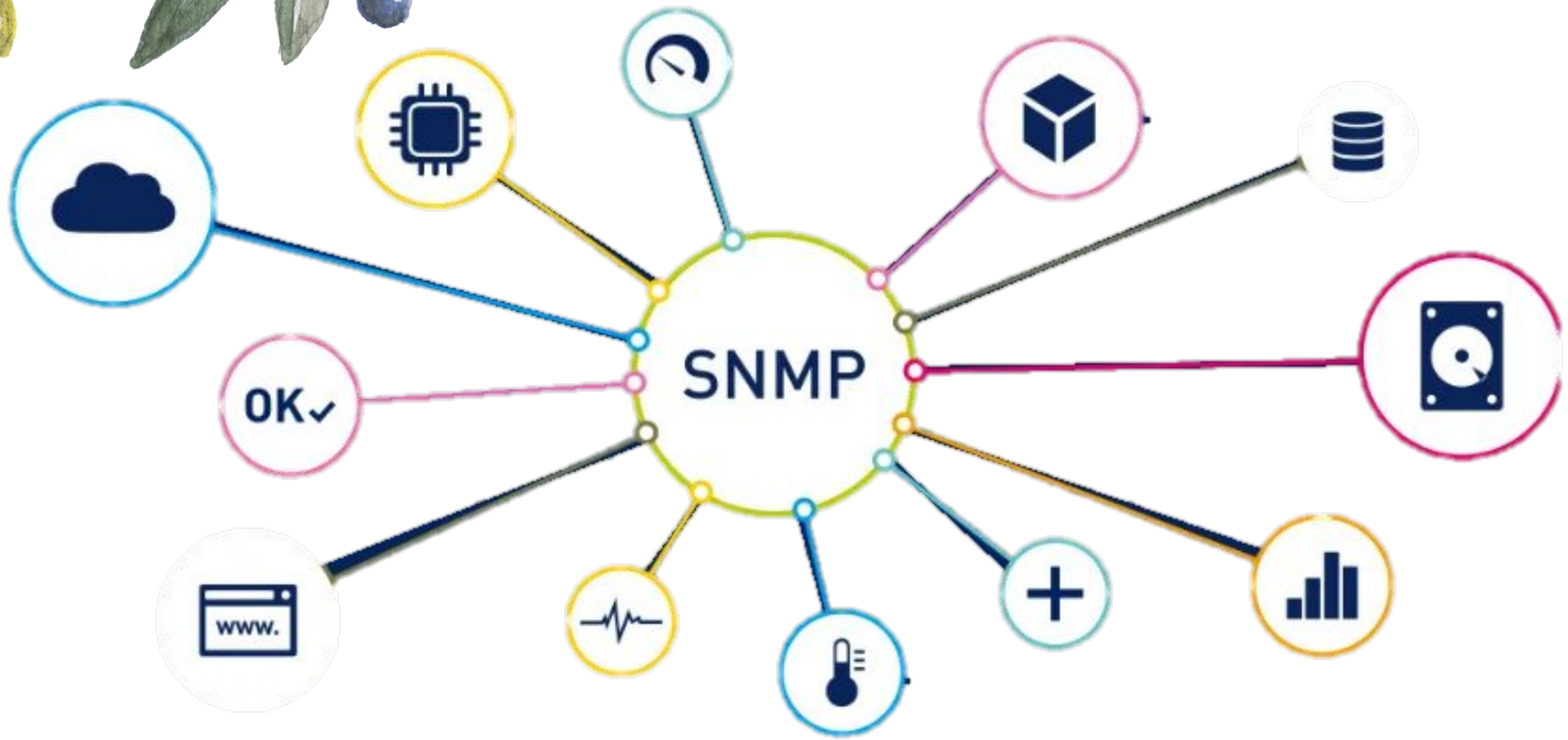


РАЗРАБОТКА И РЕАЛИЗАЦИЯ ТЕХНОЛОГИИ VPN ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРЕДАЧИ ДАННЫХ

VPN (Virtual Private Network) - это технология, которая позволяет создавать защищенные каналы связи через интернет или другую сеть для обеспечения безопасности передачи данных. VPN используется для защиты сетевых соединений путем шифрования трафика.

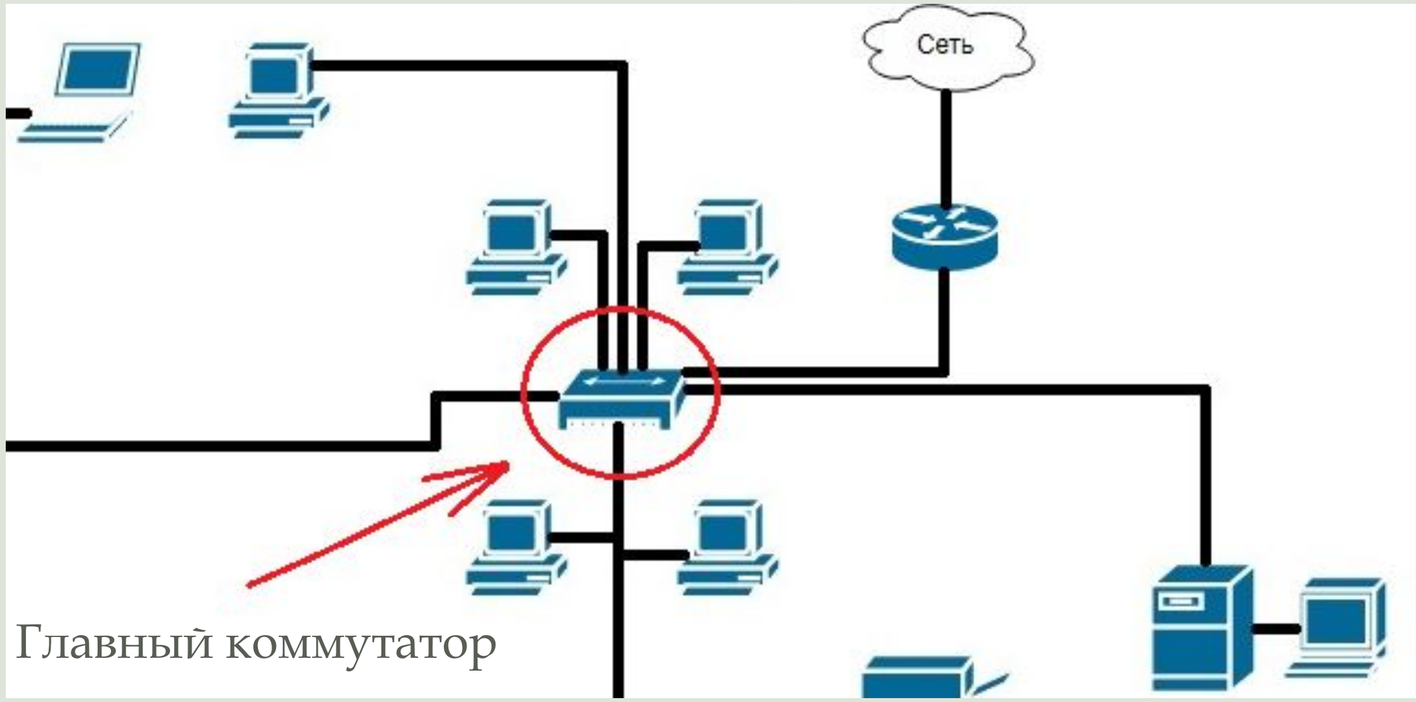
РЕАЛИЗАЦИЯ ПРОТОКОЛА SNMP ДЛЯ МОНИТОРИНГА БЕЗОПАСНОСТИ СЕТИ

Используя SNMP для мониторинга средств и процессов обеспечения безопасности, сетевые администраторы могут эффективно выявлять уязвимости, устранять их и поддерживать высокий уровень защищенности корпоративной сети.

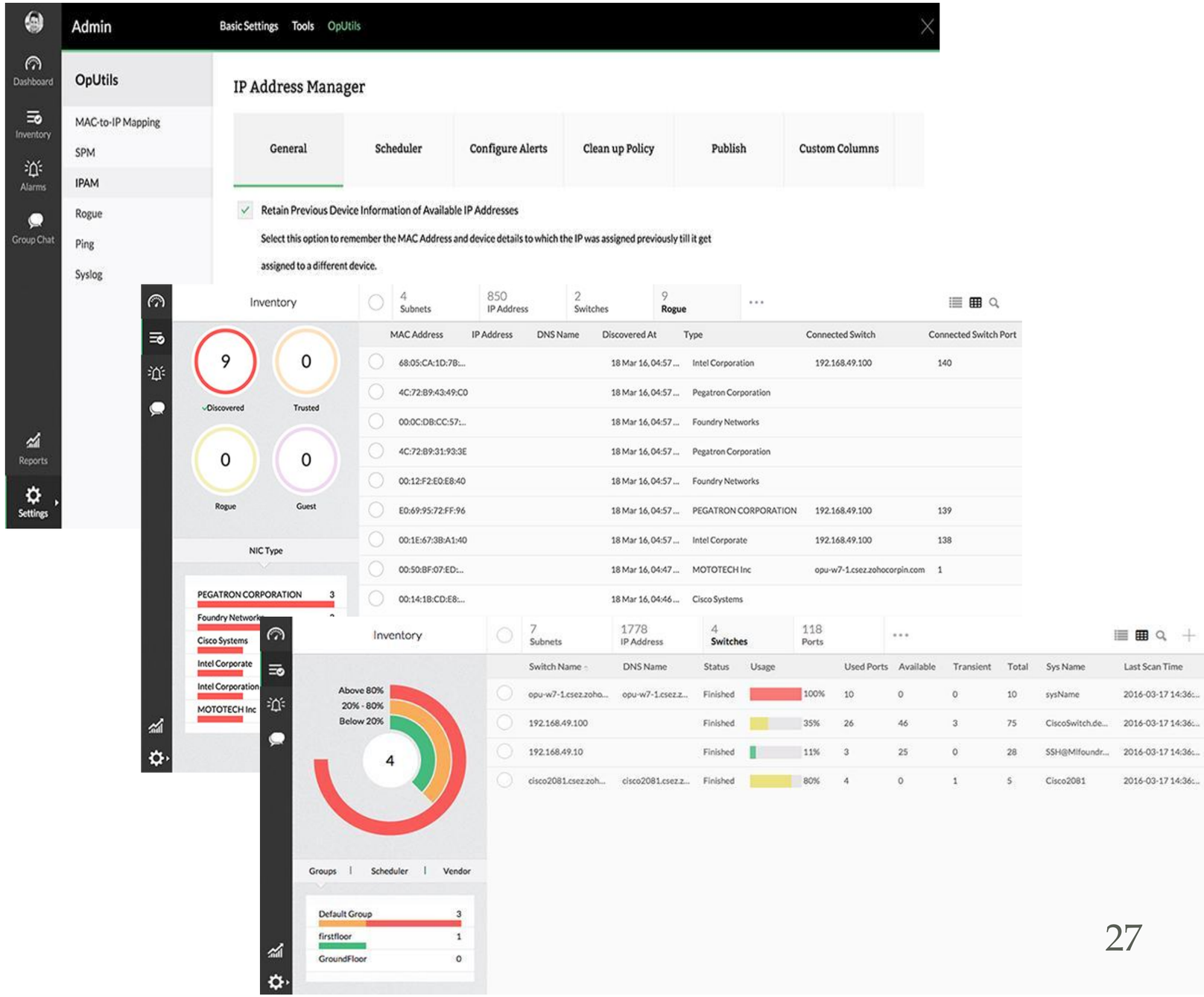


ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ДАННЫХ ЛОКАЛЬНОЙ СЕТИ С ПОМОЩЬЮ СКАНИРОВАНИЯ ПОРТОВ

Сканирование портов - это процесс поиска открытых портов на сетевых устройствах, таких как маршрутизаторы, коммутаторы и серверы, с целью выявления потенциальных уязвимостей и угроз для безопасности сети. Оно позволяет определить, какие порты открыты и какие сервисы работают на них, что помогает администраторам сети принимать меры по укреплению безопасности сети.

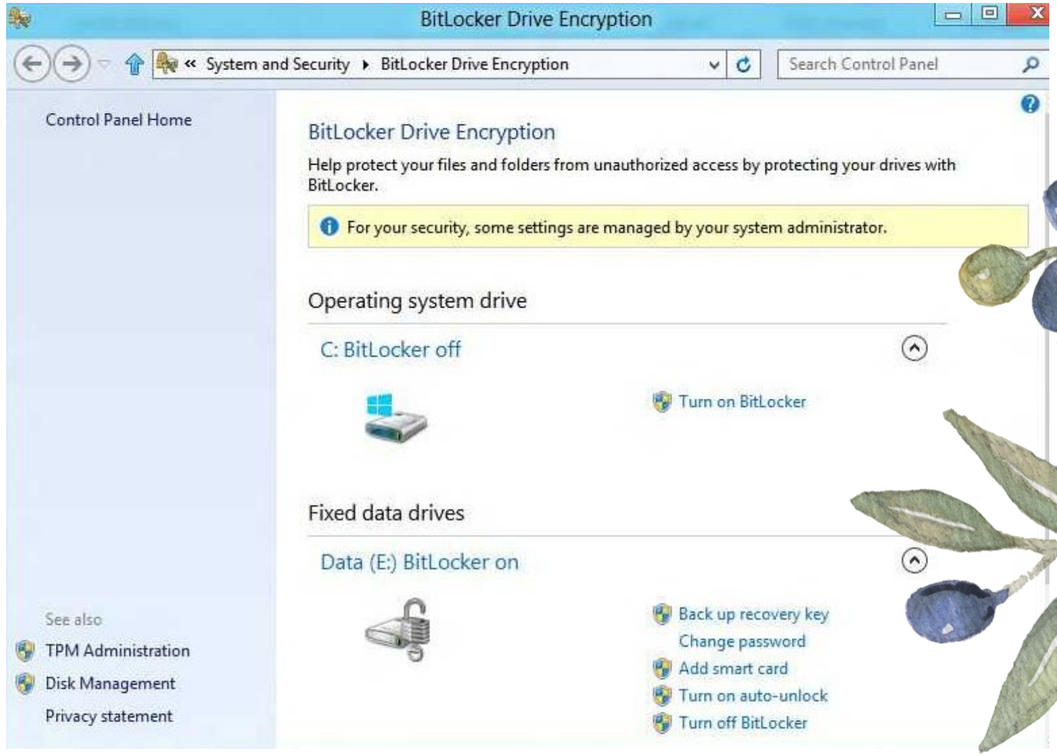


ManageEngine OpManager Plus - это система управления сетями, которая позволяет мониторить и управлять сетевыми устройствами, серверами, приложениями и сервисами. Она обеспечивает простой интерфейс для мониторинга и управления сетевой инфраструктурой.



ШИФРОВАНИЕ ДАННЫХ С ИСПОЛЬЗОВАНИЕМ BITLOCKER

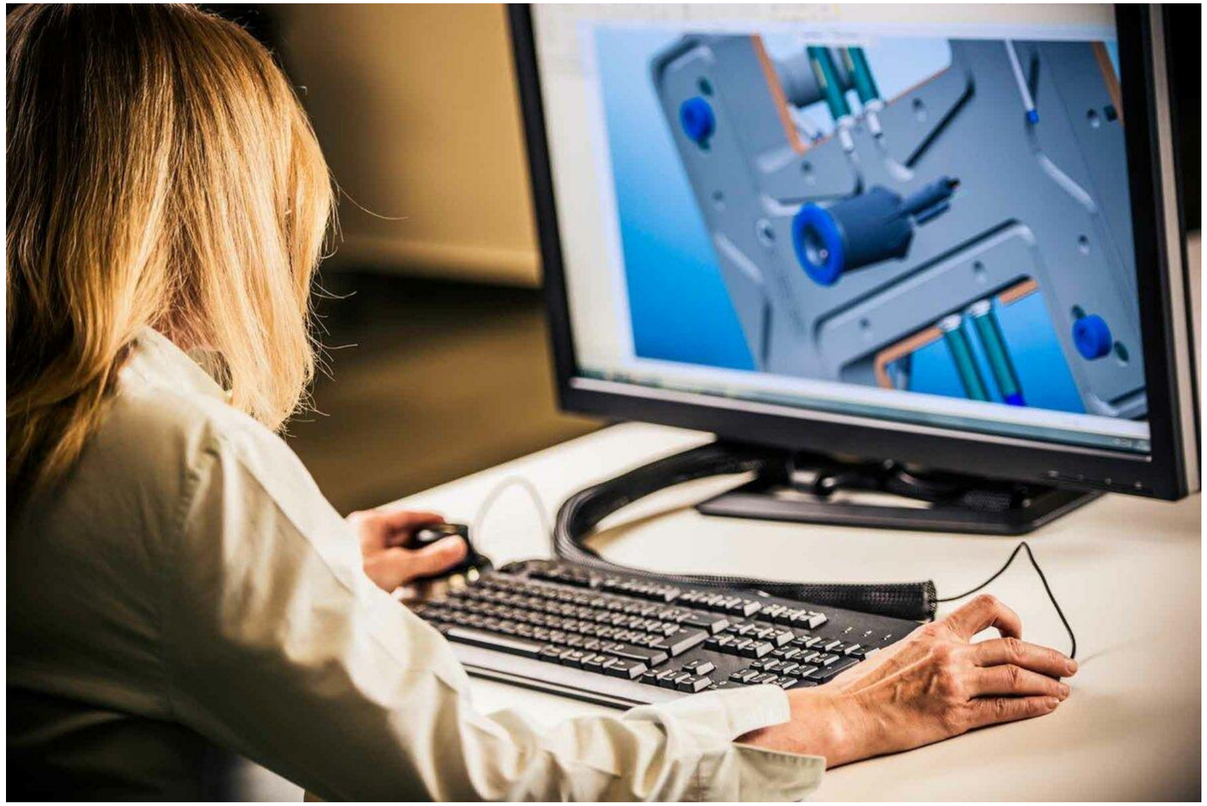
BitLocker – это программное обеспечение, предназначенное для шифрования данных на жестких дисках, USB-накопителях и других устройствах хранения данных. Это средство, разработанное Microsoft, которое используется в операционных системах Windows для защиты конфиденциальных данных от несанкционированного доступа и кражи.



ОРГАНИЗАЦИОННЫЕ ПРОЦЕДУРЫ В ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

Для повышения осведомленности сотрудников в этой области можно предложить следующие меры:

1. Организация обучающих семинаров и тренингов.
2. Разработка и распространение информационных материалов.
3. Проведение тестирования сотрудников на знание информационной безопасности.
4. Повышение ответственности сотрудников за нарушения информационной безопасности.
5. Создание культуры безопасности.



Затраты

№	Мероприятие	Стоимость
1	Приобретение и установка дополнительных средств сетевой защиты	119 000 руб.
2	Приобретение лицензии ПО ManageEngine OpManager для сканирования портов	54 600 руб.
3	Регулярное (ежемесячное) тестирование средств защиты сети на уязвимости и проникновение	200 000 руб.
4	Обучение сотрудников правилам безопасной работы в корпоративной сети и методам защиты от киберугроз	420 000 руб.

Выгоды от реализации мероприятий

№	Выгоды	Стоимость
1	Снижение вероятности инцидентов на 30%	2 100 000 руб.
2	Сокращение риска нарушений на 25%	7 500 000 руб.

ИССЛЕДОВАНИЕ ВОПРОСОВ ПРАВОВОЙ ЗАЩИТЫ ИНФОРМАЦИИ И СОБЛЮДЕНИЯ НОРМ ЗАКОНОДАТЕЛЬСТВА В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Вопросы правовой защиты информации и соблюдения норм законодательства в области информационной безопасности крайне важны для всех организаций, работающих с конфиденциальной информацией. Защита информации является важной составляющей общей системы безопасности, а неправильное использование или утечка конфиденциальной информации может привести к серьезным последствиям, включая финансовые потери, ущерб репутации и нарушение законодательства.

ОБ ИНФОРМАЦИИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЯХ И О ЗАЩИТЕ ИНФОРМАЦИИ

Федеральный закон от 27.07.2006 № 149-ФЗ в редакции Федерального закона от 01.05.2019 № 90-ФЗ

ЗАКЛЮЧЕНИЕ

Разработанные меры по совершенствованию информационной безопасности сети ООО "ЭСГП" позволили повысить защищенность информационных ресурсов, оптимизировать бизнес-процессы и обеспечить соблюдение требований законодательства. Предложенные решения могут быть рекомендованы для внедрения на других предприятиях.

Спасибо за внимание