МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение

высшего профессионального образования

«Московский государственный лингвистический университет»

Евразийский лингвистический институт

в г. Иркутске (филиал)

МГЛУ ЕАЛИ

Кафедра информационных технологий

**ОТЧЁТ О ПРЕДДИПЛОМНОЙ ПРАКТИКЕ**

Выполнила: студентка группы ЕАЛИ6-10-72

специальности «Организация и технология защиты информации»

Кокарева Валерия Викторовна

Руководитель практики:

А. В. Фрязинов, к. т. н., доцент

К защите допускаю: Зав. кафедрой

информационных технологий

Н. В. Амбросов, к.э.н., профессор

Иркутск 2015

# Оглавление

# ВВЕДЕНИЕ

# 1. ОБЩИЕ СВЕДЕНИЯ ОБ ОТДЕЛЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

# 2. ПРАВОВАЯ ЗАЩИТА ИНФОРМАЦИИ, ОСУЩЕСТВЛЯЕМАЯ НА ПРЕДПРИЯТИИ

# 3. ПРОГРАММНО-АППАРАТНЫЕ МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ, ПРИМЕНЯЕМЫЕ НА ПРЕДПРИЯТИИ

# 3.1 Аппаратные средства

# 3.2 Программные средства

# 4. ИНДИВИДУАЛЬНОЕ ЗАДАНИЕ. ОЦЕНКА ЗАЩИЩЕННОСТИ СЕТИ ПЕРЕДАЧИ ДАННЫХ АДМИНИСТРАЦИИ ГОРОДА ИРКУТСКА

# БИБЛИОГРАФИЧЕСКИЙ СПИСОК

# ВВЕДЕНИЕ

информационный безопасность криптографический администрация

Отчет сформирован по итогам прохождения преддипломной практики в отделе информационной безопасности и криптографической защиты информации департамента информатизации комитета по экономике администрации города Иркутска (далее – отдел), являющемся структурным подразделением отдела программ и проектов департамента информатизации комитета по экономике администрации города Иркутска, расположенному по адресу: город Иркутск, улица Ленина, 14 Б.

***Целями*** преддипломной практики являются:

* сбор материала, необходимого для выполнения ВКР;
* приобретение выпускниками профессионального опыта;
* овладение производственными навыками, необходимыми в экспериментально-исследовательской, проектной, организационно-управленческой и эксплуатационной деятельности;
* проверка готовности будущих специалистов к самостоятельной трудовой деятельности.

***Задачами*** преддипломной практики является практическое применение:

* методов количественного анализа процессов обработки, поиска и передачи информации;
* методов моделирования с учетом их иерархической структуры и оценки пределов применимости полученных результатов;
* методов обработки и анализа экспериментальных данных;
* методики отнесения информации к государственной и другим видам тайны и ее засекречивания;
* методики выявления и анализа потенциально существующих угроз безопасности информации, составляющей государственную и другие виды тайны;
* методов анализа и оценки риска, методов определения размеров возможного ущерба вследствие разглашения сведений, составляющих государственную и другие виды тайны;
* методов организации и моделирования комплексной системы защиты информации, составляющей государственную и другие виды тайны;
* методов управления комплексной системой защиты информации, составляющей государственную или другие виды тайны;
* методов организации и управления службами защиты информации.
1. **ОБЩИЕ СВЕДЕНИЯ ОБ ОТДЕЛЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ**

Отдел информационной безопасности и криптографической защиты информации администрации города Иркутска относится непосредственно к департаменту информатизации.

Структура администрации города Иркутска представлена на рисунке 1.



Рисунок 1 – Структура администрации.

Отдел находится в непосредственном подчинении начальника отдела программ и проектов департамента информатизации комитета по экономике администрации города Иркутска.

Отдел в своей деятельности руководствуется Конституцией Российской Федерации, законодательством Российской Федерации и Иркутской области, Уставом города Иркутска, иными муниципальными правовыми актами города Иркутска, Положением о комитете по экономике администрации города Иркутска, Положением об отделе программ и проектов департамента информатизации комитета по экономике администрации города Иркутска.

Отдел возглавляет заведующий отдела информационной безопасности и криптографической защиты информации администрации города Иркутска.

Основные задачи

Основными задачами отдела являются:

* организация работы программно-технического комплекса, реализующего функции Удостоверяющего центра электронной подписи органов местного самоуправления города Иркутска, муниципальных учреждений и муниципальных унитарных предприятий города Иркутска (далее - НТК УЦ ЭП);
* участие в организации электронного документооборота в органах местного самоуправления города Иркутска, муниципальных учреждениях и муниципальных унитарных предприятиях города Иркутска с использованием электронной подписи;
* участие в формировании информационно-телекоммуникационной среды с целью своевременного обеспечения органов местного самоуправления города Иркутска информацией и данными, необходимыми для подготовки и принятия обоснованных решений, на основе внедрения новых информационных технологий, современной вычислительной техники и телекоммуникаций с использованием электронной подписи;
* участие в формировании и проведении единой политики в сфере эксплуатации электронной подписи в органах местного самоуправления города Иркутска, муниципальных учреждениях и муниципальных унитарных предприятиях города Иркутска. Определение стратегии развития городской информационной системы в сфере применения электронной подписи;
* участие в формировании и проведении единой политики в сфере обеспечения общих требований и правил защиты конфиденциальных сведений, содержащихся в информационных ресурсах ПТК УЦ ЭП, и порядка доступа к ним.

Функции отдела

Для выполнения поставленных задач отдел осуществляет следующие функции:

* проведение работ в ПТК УЦ ЭП по обеспечению средствами электронной подписи в органах местного самоуправления города Иркутска, муниципальных учреждениях и муниципальных унитарных предприятиях города Иркутска;
* создание и ведение единого реестра электронной подписи органов местного самоуправления города Иркутска, муниципальных учреждений и муниципальных унитарных предприятий города Иркутска;
* обеспечение сохранности средств и оборудования ПТК УЦ ЭП;
* формирование и обеспечение выполнения общих требований и правил защиты конфиденциальной информации, содержащейся в муниципальных информационных ресурсах ПТК УЦ ЭП, и порядка доступа к ней;
* оказание консультационных услуг работникам органов местного самоуправления города Иркутска, муниципальных учреждений и муниципальных унитарных предприятий города Иркутска в сфере применения электронной подписи;
* взаимодействие с Федеральным агентством по информационным технологиям в рамках подсистемы удостоверяющих центров общероссийского государственного информационного центра;
* разработка проектов муниципальных правовых актов города Иркутска по вопросам, отнесенным к компетенции отдела;
* участие в проведении технического освидетельствования информационных систем, муниципальных информационных ресурсов в сфере эксплуатации электронной подписи, а также обеспечение контроля за их созданием и применением в подведомственных администрации города Иркутска муниципальных унитарных предприятиях и учреждениях города Иркутска;
* участие в разработке и реализации проектов городских, региональных и федеральных программ в сфере информатизации с использованием электронной подписи;
* участие в организации и работе выставок информационных технологий, средств вычислительной техники и информационных систем, а также совещаний, семинаров и конференций по вопросам использования электронной подписи;
* формирование и обеспечение выполнения общих требований и правил защиты конфиденциальных сведений, содержащихся в информационных ресурсах ПТК УЦ ЭП, и порядка доступа к ним.

1. **ПРАВОВАЯ ЗАЩИТА ИНФОРМАЦИИ, ОСУЩЕСТВЛЯЕМАЯ НА ПРЕДПРИЯТИИ**

Руководство администрации регламентирует правила хранения, передачи и обработки и информации, обрабатываемой на территории предприятия, включая и правила ее защиты, а также устанавливает меру ответственности за нарушение этих правил в соответствии со следующими нормативно-правовыми документами:

* Федеральный закон РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»;
* Федеральный закон от 06.04. 2011 №63-ФЗ «Об электронной подписи»;
* приказ ФСТЭК РФ от 18.02.2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
* приказ ФСТЭК РФ от 11.02.2013 № 17 «Об утверждении требований
* о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;
* приказ Министерства связи и массовых коммуникаций РФ от 23.11.2011 г. № 320 «Об аккредитации УЦ»;
* распоряжение администрации г. Иркутска от 30.12.2010 г. № 031-10-1285/10 «О порядке организации и осуществления обработки и защиты конфиденциальной информации в администрации г. Иркутска»;
* распоряжение администрации г. Иркутска от 07.12.2010 г. № 031-10-1167/10 «Об утверждении положения о порядке организации и проведения работ по обеспечению безопасности персональных данных при их обработке
* в информационной системе персональных данных администрации
* г. Иркутска»;
* распоряжение администрации г. Иркутска от 05.09.2010 г. № 031-10-917/12 «Об обеспечении информационной безопасности в корпоративной информационно-вычислительной сети администрации г. Иркутска»;
* распоряжение администрации г. Иркутска от 10.12.2009 г. № 031-10-1386/9 «О вводе в эксплуатацию автоматизированной системы «Программно-технический комплекс, реализующий функции Удостоверяющего Центра электронно-цифровой подписи органов местного самоуправления
* г. Иркутска, муниципальных учреждений и предприятий»;
* распоряжение администрации г. Иркутска от 12.04.2013 г. № 031-10-263/13 «О предоставлении доступа к муниципальным ИС органов местного самоуправления г. Иркутска»;
* распоряжение администрации города Иркутска от 18.08.2010 № 031-10-718/10-1 «Об утверждении Положений».

1. **ПРОГРАММНО-АППАРАТНЫЕ МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ, ПРИМЕНЯЕМЫЕ НА ПРЕДПРИЯТИИ**

## Аппаратные средства

Аппаратные (технические) средства - это различные по типу устройства (механические, электромеханические, электронные и др.), которые аппаратными средствами решают задачи защиты информации. Они либо препятствуют физическому проникновению, либо, если проникновение все же состоялось, доступу к информации, в том числе с помощью ее маскировки. Преимущества технических средств связаны с их надежностью, независимостью от субъективных факторов, высокой устойчивостью к модификации. Слабые стороны — недостаточная гибкость, относительно большие объем и масса, высокая стоимость.

Аппаратные средства, имеющиеся на предприятии:

1. устройства для ввода идентифицирующей информации: кодовый замок BOLID на входной двери в комплекте с идентифицирующими пластиковыми картами;
2. устройства для шифрования информации: шифрование по ГОСТ;
3. устройства для воспрепятствования несанкционированного включения рабочих станций и серверов: достоверная загрузка системы при помощи ПАК «Соболь».

Электронный замок «Соболь» - это аппаратно-программное средство защиты компьютера от несанкционированного доступа [7]. Электронный замок «Соболь» может применяться как устройство, обеспечивающее защиту автономного компьютера, а также рабочей станции или сервера, входящих в состав локальной вычислительной сети.

Возможности электронного замка «Соболь»:

* аутентификация пользователей;
* блокировка загрузки ОС со съемных носителей;
* контроль целостности программной среды;
* контроль целостности системного реестра Windows;
* контроль конфигурации компьютера;
* сторожевой таймер;
* регистрация попыток доступа к ПЭВМ.

Достоинства электронного замка «Соболь»:

* наличие сертификатов ФСБ и ФСТЭК России;
* защита информации, составляющей государственную тайну;
* помощь в построении прикладных криптографических приложений;
* простота в установке, настройке и эксплуатации;
* поддержка 64-битных операционных систем Windows;
* поддержка идентификаторов iButton, iKey 2032, eToken PRO, eToken PRO (Java) иRutoken S/ RF S;
* гибкий выбор вариантов комплектации.
1. устройства уничтожения информации на магнитных носителях: тройная перезапись информации при помощи SecretNet.

SecretNet является сертифицированным средством защиты информации от несанкционированного доступа и позволяет привести автоматизированные системы в соответствие с требованиями регулирующих документов:

* №98-ФЗ ("О коммерческой тайне");
* №152-ФЗ ("О персональных данных");
* №5485-1-ФЗ ("О государственной тайне");
* СТО БР (Стандарт Банка России).

## Ключевые возможности СЗИ от НСД SecretNet:

* аутентификация пользователей;
* разграничение доступа пользователей к информации и ресурсам автоматизированной системы;
* доверенная информационная среда;
* контроль утечек и каналов распространения конфиденциальной информации;
* контроль устройств компьютера и отчуждаемых носителей информации на основе централизованных политик, исключающих утечки конфиденциальной информации;
* централизованное управление системой защиты, оперативный мониторинг, аудит безопасности;
* масштабируемая система защиты, возможность применения SecretNet (сетевой вариант) в организации с большим количеством филиалов.

5) устройства сигнализации о попытках несанкционированных действий пользователей:

* блокировка системы;
* программно-аппаратный комплекс ALTELL NEO 200

ALTELL NEO — первые российские межсетевые экраны нового поколения. Главная особенность этих устройств — сочетание возможностей межсетевого экранирования с функциями построения защищенных каналов связи, обнаружения и предотвращения вторжений, контент-фильтрации (веб- и спам-фильтры, контроль приложений) и защиты от вредоносных программ, что обеспечивает полное соответствие современной концепции унифицированной защиты от угроз (UnifiedThreatManagement, UTM).

* программно-аппаратный комплекс ViPNetCoordinator HW1000

ViPNetCoordinator HW 100 - это компактный криптошлюз и межсетевой экран, позволяющий безопасно включить любое сетевое оборудование в виртуальную частную сеть, построенную с использованием продуктов ViPNet, и надежно защитить передаваемую информацию от несанкционированного доступа и подмены.

ViPNetCoordinator HW 100 обеспечивает эффективную реализацию множества сценариев защиты информации:

* межсетевые взаимодействия;
* защищенный доступ удаленных и мобильных пользователей;
* защита беспроводных сетей;
* защита мультисервисных сетей (включая IP телефонию и видеоконференцсвязь);
* защита платежных систем и систем управления технологическими процессами в производстве и на транспорте;
* разграничение доступа к информации в локальных сетях.
* программно-аппаратный комплекс "Удостоверяющий Центр "КриптоПроУЦ" версии 1.5R2.

**3.2 Программные средства**

Программные средства – это объективные формы представления совокупности данных и команд, предназначенных для функционирования компьютеров и компьютерных устройств с целью получения определенного результата, а также подготовленные и зафиксированные на физическом носителе материалы, полученные в ходе их разработок, и порождаемые ими аудиовизуальные отображения.

Программными называются средства защиты данных, функционирующие в составе программного обеспечения. Ниже перечислены программные средства защиты информации, имеющиеся на предприятии.

* 1. Антивирусные программы:
	2. Средство антивирусной защиты для компьютеров и серверов SystemCenterEndpointProtection

MicrosoftSystemCenter 2012 EndpointProtection обеспечивает универсальную защиту от вредоносных программ конечных устройств: бизнес компьютеров, ноутбуков и серверных операционных систем.

### Основные особенности Microsoft System Center 2012 Endpoint Protection:

1. простой в использовании:
* создает единый опыт работы администратора для управления и обеспечения устройств;
* улучшает видимость для выявления и ликвидации последствий уязвимых конечных устройств.

2) интеграция средств защиты:

* развертывание более тысячи конечных устройств, используя совместимость с системой SystemCenterConfigurationManager;
* снижает стоимость владения, используя общую инфраструктуру для управления конечными устройствами и безопасности.

3) защита от угроз:

* обновленный антивирусный движок гарантирует более эффективное обнаружение угроз и обеспечивает надежную защиту от новых версий вредоносных программ;
* новые механизмы поведенческого анализа и мониторинга помогут справиться с малоизученными угрозами;
* встроенные средства управления межсетевым экраном WindowsFirewall позволят специалистам убедиться в правильной настройке этого защитного механизма и его корректном функционировании на всех конечных точках сети;
* механизм DynamicCloudUpdate обеспечит своевременное обновление сигнатур для успешной идентификации подозрительных файлов и ранее неизвестных вредоносных программ.

1.2. Антивирус Касперского, сертифицированный ФСТЭК; WindowsDefender – антивирусная программа, разработанная компанией Microsoft самостоятельно, присутствует в последних версиях операционных систем Windows;

1. Программы идентификации и аутентификации пользователей: CryptoProCSP версии 3.6.

Криптопровайдер КриптоПро CSP предназначен для:

* авторизации и обеспечения юридической значимости электронных документов при обмене ими между пользователями, посредством использования процедур формирования и проверки электронной цифровой подписи (ЭЦП) в соответствии с отечественными стандартами ГОСТ Р 34.11-94 и ГОСТ Р 34.10-2001;
* обеспечения конфиденциальности и контроля целостности информации посредством ее шифрования в соответствии с ГОСТ 28147-89;
* контроля целостности системного и прикладного программного обеспечения для его защиты от несанкционированных изменений и нарушений правильности функционирования;
* управления ключевыми элементами системы в соответствии с регламентом средств защиты.

### Реализуемые алгоритмы:

* алгоритм выработки значения хэш-функции реализован в соответствии с требованиями ГОСТ Р 34.11 94 "Информационная технология. Криптографическая защита информации. Функция хэширования";
* алгоритмы формирования и проверки ЭЦП реализованы в соответствии с требованиями ГОСТ Р 34.10-2001 "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи";
* алгоритм зашифрования/расшифрования данных и вычисление имитовставки реализованы в соответствии с требованиями ГОСТ 28147-89 "Системы обработки информации. Защита криптографическая".
1. Программы разграничения доступа пользователей к ресурсам:
	1. ActiveDirectory;
	2. Контроллер доступа С2000-2

Контроллер доступа «С2000-2» предназначен для управления доступом через одну или две точки доступа путем считывания кодов предъявляемых идентификаторов (карт Proximity, ключей TouchMemory и PIN-кодов), проверки прав доступа и замыкания (размыкания) контактов, управляющих запорными устройствами (электромеханическими и электромагнитными замками и защелками, турникетом, шлагбаумом).

Особенности:

* настраиваемый контроль взлома и блокировки двери;
* программируемый временной график доступа;
* встроенные энергонезависимые часы с календарем;
* встроенный звуковой сигнализатор.
1. Программы шифрования информации:
	1. CryptoPro IPsec

IPsec — это набор протоколов по защите информации в сети, который позволяет подтверждать подлинность участников сетевого обмена, контролировать конфиденциальность и целостность сетевых пакетов.

Данный продукт разрабатывается по техническому заданию, согласованному с ФСБ России.

КриптоПро IPsec применяется для:

* защиты подключений удалённых пользователей или малых офисов (VPN);
* защиты соединений между шлюзами корпоративной вычислительной сети (Site-to-Site VPN);
* защиты передачи конфиденциальной информации в ЛВС от нарушителей, не являющихся пользователями автоматизированных систем, но имеющим физический доступ к ЛВС и нарушителей, являющихся пользователями ЛВС, но не имеющих необходимых полномочий.
	1. CryptoProArm

КриптоАРМ – программа, предназначенная для шифрования и расшифрования данных, создания и проверки электронной цифровой подписи (ЭЦП) с использованием сертификатов открытых ключей, для работы с сертификатами и криптопровайдерами. «КриптоАРМ», наряду со стандартными криптопровайдерами (входящими в поставку Windows), использует реализацию криптоалгоритмов в сертифицированных ФСБ РФ криптопровайдерах компании «КРИПТО-ПРО».

### Функциональные возможности программы:

* шифрование и расшифрование файлов произвольного формата (преобразования файлов функциями СКЗИ);
* создание и проверка корректности одной или нескольких ЭЦП;
* выполнение операций подписи и шифрования за одно действие;
* управление цифровыми сертификатами и ключами пользователя, списками отозванных и доверенных сертификатов;
* управление криптопровайдерами;
* совместимость с ключевыми носителями Рутокен, eToken;
* отправка подписанных и зашифрованных файлов по e-mail.
	1. Средство шифрации и аутентификации РУТОКЕН

Электронный идентификатор (токен) Рутокен S — это компактное USB-устройство, предназначенное для безопасной двухфакторной аутентификации пользователей, защищенного хранения ключей шифрования и ключей электронной подписи, а также цифровых сертификатов и иной информации.

Рутокен S обеспечивает двухфакторную аутентификацию в компьютерных системах. Для успешной аутентификации требуется выполнение двух условий: физическое наличие самого USB-токенаРутокен и знание PIN-кода к нему. Это обеспечивает гораздо более высокий уровень безопасности по сравнению с традиционным доступом по паролю. Основу Рутокен S составляют микроконтроллер, который выполняет криптографическое преобразование данных, и защищенная память, в которой в зашифрованном виде хранятся данные пользователя: пароли, сертификаты, ключи шифрования и т.д.

Назначение:

|  |  |
| --- | --- |
| **Аутентификация** | * Двухфакторная аутентификация при доступе к операционным системам, почтовым серверам, серверам баз данных, Web-серверам и файл-серверам.
 |
| **Безопасное хранение ключевой информации** | * Использование ключевой информации для выполнения криптографических операций на самом устройстве, без возможности выдачи наружу закрытой ключевой информации.
* Сгенерированные на токене ключи не могут быть скопированы.
* При утере или краже токена безопасность не нарушается: для доступа к информации требуется PIN-код.
 |
| **Защита персональных данных** | * Защита электронной переписки: шифрование почты, электронная подпись почтовых отправлений.
* Защита доступа к компьютеру и в домен локальной сети.
* Возможность шифрования данных на дисках.
 |
| **Корпоративное использование** | * Используется в корпоративных системах для хранения служебной информации, персональной информации пользователей, паролей, ключей шифрования, цифровых сертификатов и любой другой конфиденциальной информации.
* Может выступать как единое идентификационное устройство для доступа пользователя к разным элементам корпоративной системы и обеспечивать, например, необходимое разграничение доступа, цифровую подпись создаваемых документов, аутентификацию при доступе к компьютерам и приложениям системы.
 |
| **Дополнительные возможности** | * Поддержка национального стандарта шифрования ГОСТ 28147-89.
 |
| **Аутентификация и конфиденциальность** | * Двухфакторная аутентификация: предъявление самого идентификатора и уникального PIN-кода.
* 3 уровня доступа к токену: Гость, Пользователь, Администратор.
* Разграничение доступа к файловым объектам в соответствии с уровнем доступа.
* Ограничение числа попыток ввода PIN-кода.
 |

1. Программы защиты ресурсов от несанкционированного копирования, изменения и использования:
	1. MicrosoftRMS (RightsManagementServices - технология защиты документов MicrosoftActiveDirectory путем шифрования с применением ограничений доступа и лицензий доступа позволяющая сохранять ограничения даже после загрузки и открытия файла пользователем).

# Вспомогательные средства:

– программы уничтожения остаточной информации: деформация носителей, сжигание;

– программы аудита событий: встроенные в рабочие станции локальные программы на базе домена.

# Криптографические методы и средства защиты информации

# Криптографические методы защиты информации — это специальные методы шифрования, кодирования или иного преобразования информации, в результате которого ее содержание становится недоступным без предъявления ключа криптограммы и обратного преобразования. Криптографический метод защиты, безусловно, самый надежный метод защиты, так как охраняется непосредственно сама информация, а не доступ к ней (например, зашифрованный файл нельзя прочесть даже в случае кражи носителя). Данный метод защиты реализуется в виде программ или пакетов программ.

# Методы криптографической защиты, применяемые на предприятии:

* запрет на хранение конфиденциальной информации на открытых носителях;
* обеспечение целостности информации при передаче при помощи единого центра обработки данных.

# Методы и средства инженерно-технической защиты информации

Инженерно-техническая защита информации включает комплекс организационных и технических мер по обеспечению безопасности информации техническими средствами. Она решает следующие задачи:

* предотвращение проникновения злоумышленника к источникам информации с целью ее уничтожения, хищения или изменения;
* защита носителей информации от уничтожения в результате воздействия стихийных сил и прежде всего, пожара и воды (пены) при его тушении;
* предотвращение утечки информации по различным техническим каналам.

Методы и средства инженерно-технической защиты информации, применяемые на предприятии:

1. Защита от проникновения нарушителей: проход строго по пропускам/документам, удостоверяющим личность; контроллер доступа VIZIT в комплекте со считывателем; железная дверь; датчик движения.

2. Защита аппаратных средств и носителей от хищения производится путем опечатывания всех ПК и носителей.

3. Предотвращение возможности удаленного видеонаблюдения/подслушивания за работой персонала и ТС: системы защиты «Гром» и «Шорох».

Система защиты «Гром»

Назначение:

Система защиты «Гром» предназначена для маскировки побочных электромагнитных излучений и наводок (ПЭМИН) средств вычислительной техники.

Особенности:

«Гром» формирует шумовую помеху в широком диапазоне частот и полностью соответствует СМД ФСТЭК по контролю защищенности информации, обрабатываемой СВТ от утечки за счет ПЭМИН.

Система является двухканальной. Первый канал системы формирует магнитную составляющую электромагнитного поля помех в диапазоне частот от 0,01 МГц до 30 МГц. Второй канал формирует электрическую составляющую электромагнитного поля в диапазоне от 0,01 МГц до 2000 МГц.

Система состоит из генератора шумовой помехи «Гром», дисконусной антенны «SI-5002.1» и трёх рамочных антенн.

Система защиты «Шорох»

Назначение**:**

Система «Шорох» предназначена для защиты акустической речевой информации в выделенных помещениях (до второй категории включительно) от утечки по акустическому и вибрационному каналам.

Минимизация ущерба от потерь информации, возникших в результате стихийных бедствий и техногенных аварий на предприятии происходит при помощи следующих средств и выполнения нижеприведенных действий: конфиденциальная информация находится в сейфах; источники бесперебойного питания АРС; также присутствуют ТС охраны;

Доступ сотрудников в защищенное помещение (9 человек) осуществляется только в присутствии ответственных за эксплуатацию УЦ.

**4. ИНДИВИДУАЛЬНОЕ ЗАДАНИЕ. ОЦЕНКА ЗАЩИЩЕННОСТИ СЕТИ ПЕРЕДАЧИ ДАННЫХ АДМИНИСТРАЦИИ ГОРОДА ИРКУТСКА**

Защищенность является одним из важнейших показателей эффективности функционирования сети передачи данных, наряду с такими показателями как надежность, отказоустойчивость, производительность и т. п.

Под защищенностью сети будем понимать степень адекватности реализованных в ней механизмов защиты информации существующим в данной среде функционирования рискам, связанным с осуществлением угроз безопасности информации. Под угрозами безопасности информации традиционно понимается возможность нарушения таких свойств информации, как конфиденциальность, целостность и доступность.

На практике всегда существует большое количество не поддающихся точной оценке возможных путей осуществления угроз безопасности в отношении ресурсов сети. В идеале каждый путь осуществления угрозы должен быть перекрыт соответствующим механизмом защиты. Данное условие является первым фактором, определяющим защищенность сети. Вторым фактором является прочность существующих механизмов защиты, характеризующаяся степенью сопротивляемости этих механизмов попыткам их обхода, либо преодоления. Третьим фактором является величина ущерба, наносимого владельцу сети в случае успешного осуществления угроз безопасности.

На практике получение точных значений приведенных характеристик затруднено, т. к. понятия угрозы, ущерба и сопротивляемости механизма защиты трудноформализуемы. Например, оценку ущерба в результате НСД к информации политического и военного характера точно определить вообще невозможно, а определение вероятности осуществления угрозы не может базироваться на статистическом анализе. Оценка степени сопротивляемости механизмов защиты всегда является субъективной.

Описанный далее подход позволяет получать качественные оценки уровня защищенности сети путем сопоставления свойств и параметров сети с многократно опробованными на практике и стандартизированными критериями оценки защищенности.

Для того, чтобы математически точно определить этот показатель, рассмотрим формальную модель системы защиты сети передачи данных.

Основой формального описания систем защиты традиционно считается модель системы защиты с полным перекрытием, в которой рассматривается взаимодействие "области угроз", "защищаемой области" (ресурсов сети) и "системы защиты" (механизмов безопасности сети).

Таким образом, имеем три множества:

* T = {ti} - множество угроз безопасности,
* O = {oj} - множество объектов (ресурсов) защищенной системы,
* M = {mk} - множество механизмов безопасности.

Элементы этих множеств находятся между собой в определенных отношениях, собственно и описывающих систему защиты.

Для описания системы защиты обычно используется графовая модель, представленная на рисунке 1. Множество отношений угроза-объект образует двухдольный граф {<T, O>}. Цель защиты состоит в том, чтобы перекрыть все возможные ребра в графе. Это достигается введением третьего набора M. В результате получается трехдольный граф {<T, M, O>}.



Рисунок 6.2 — Модель системы защиты

Развитие этой модели предполагает введение еще двух элементов:

V - набор уязвимых мест. Таким образом, под уязвимостью системы защиты будем понимать возможность осуществления угрозы t в отношении объекта o (На практике под уязвимостью системы защиты обычно понимают не саму возможность осуществления угрозы безопасности, а те свойства системы, которые способствуют успешному осуществлению угрозы, либо могут быть использованы злоумышленником для осуществления угрозы);

B - набор барьеров, представляющих собой пути осуществления угроз безопасности, перекрытые средствами защиты.

В результате получаем систему, состоящую из пяти элементов: <T, O, M, V, B>, описывающую систему защиты с учетом наличия в ней уязвимостей, которая представлена на рисунке 2.



Рисунок 2. Модель системы защиты, содержащей уязвимости

Для системы с полным перекрытием выполняется условие: для любой уязвимости имеется соответствующий барьер, устраняющий эту уязвимость.

Таким образом в системе защиты с полным перекрытием для всех возможных угроз безопасности существуют механизмы защиты, препятствующие осуществлению этих угроз. Данное условие является первым фактором, определяющим защищенность сети. Вторым фактором является прочность существующих механизмов защиты.

Нормативная база анализа защищенности

Наиболее значимыми нормативными документами в области информационной безопасности, определяющими критерии для оценки защищенности и требования, предъявляемые к механизмам защиты, являются:

* общие критерии оценки безопасности ИТ (The Common Criteria for Information Technology Security Evaluation/ISO 15408);
* практические правила управления информационной безопасностью (Code of practice for Information security management/ISO 17799).

Кроме этого, в нашей стране первостепенное значение имеют Руководящие документы (РД) Гостехкомиссии России. В других странах их место занимают соответствующие национальные стандарты (там, где они есть).

Методика анализа защищенности

Типовая методика анализа защищенности сети включает использование следующих методов:

* изучение исходных данных;
* оценка рисков, связанных с осуществлением угроз безопасности в отношении ресурсов сети;
* анализ механизмов безопасности организационного уровня, политики безопасности организации и организационно-распорядительной документации по обеспечению режима информационной безопасности и оценка их соответствия требованиям существующих нормативных документов, а также их адекватности существующим рискам;
* ручной анализ конфигурационных файлов маршрутизаторов, межсетевых экранов и прокси-серверов, осуществляющих управление межсетевыми взаимодействиями, почтовых и DNS серверов;
* сканирование ресурсов сети изнутри;
* анализ конфигурации серверов и рабочих станций сети при помощи специализированных программ.

Перечисленные методы исследования предполагают использование как активного, так и пассивного тестирования системы защиты. Активное тестирование системы защиты заключается в эмуляции действий потенциального злоумышленника по преодолению механизмов защиты. Пассивное тестирование предполагает анализ конфигурации ОС и приложений по шаблонам с использованием списков проверки. Тестирование может производиться вручную, либо с использованием специализированных программных средств.

### Исходные данные по обследуемой сети

При проведении работ по оценке защищенности сети передачи данных в администрации города Иркутска были получены следующие данные:

1. полное и точное наименование исследуемого объекта и его назначение;
2. характер и уровень секретности обрабатываемой информации;
3. организационная стpуктуpа объекта информатизации;
4. перечень помещений, состав комплекса технических средств, входящих в объект информатизации, в которых обрабатывается указанная информация;
5. особенности и схема расположения объекта информатизации с указанием границ контpолиpуемой зоны;
6. стpуктуpа пpогpаммного обеспечения, используемого на исследуемом объекте и предназначенного для обработки защищаемой информации;
7. общая функциональная схема объекта информатизации, включая схему информационных потоков и режимы обработки защищаемой информации;
8. наличие и хаpактеp взаимодействия с другими объектами информатизации;
9. состав и стpуктуpа системы защиты информации на аттестуемом объекте информатизации;
10. перечень технических и пpогpаммных средств в защищенном исполнении, средств защиты и контроля, используемых на аттестуемом объекте информатизации и имеющих соответствующий сертификат, предписание на эксплуатацию;
11. сведения о pазpаботчиках системы защиты информации, наличие у сторонних pазpаботчиков лицензий на проведение подобных работ;
12. наличие на объекте службы безопасности информации, службы администpатоpа;
13. наличие и основные хаpактеpистики физической защиты объекта информатизации;
14. наличие и готовность проектной и эксплуатационной документации на объект информатизации и другие исходные данные по аттестуемому объекту информатизации, влияющие на безопасность информации.

Но перечисленных исходных данных недостаточно для выполнения работ по анализу защищенности сети, и приведенный в РД Гостехкомиссии список нуждается в расширении и конкретизации. Пункт 14 приведенного списка предполагает предоставление других исходных данных по объекту информатизации, влияющих на безопасность информации. Как раз эти «дополнительные» данные и являются наиболее значимыми для оценки текущего положения дел с обеспечением безопасности сети. Их список включает следующие виды документов:

Дополнительная документация:

1. нормативно-распорядительная документация по проведению регламентных работ;
2. нормативно-распорядительная документация по обеспечению политики безопасности;
3. должностные инструкции для администраторов, инженеров технической поддержки, службы безопасности;
4. процедуры и планы предотвращения и реагирования на попытки НСД к информационным ресурсам;
5. схема топологии корпоративной сети с указанием IP-адресов и структурная схема;
6. данные по структуре информационных ресурсов с указанием степени критичности или конфиденциальности каждого ресурса;
7. размещение информационных ресурсов в корпоративной сети;
8. схема организационной структуры пользователей;
9. схема организационной структуры обслуживающих подразделений;
10. схемы размещения линий передачи данных.

### Сетевые сканеры

Основным фактором, определяющим защищенность сети от угроз безопасности, является наличие в сети уязвимостей защиты. Уязвимости защиты могут быть обусловлены как ошибками в конфигурации компонентов сети, так и другими причинами, в число которых входят ошибки и программные закладки в коде ПО, отсутствие механизмов безопасности, их неправильное использование, либо их неадекватность существующим рискам, а также уязвимости, обусловленные человеческим фактором. Наличие уязвимостей в системе защиты сети, в конечном счете, приводит к успешному осуществлению атак, использующих эти уязвимости.

Сетевые сканеры являются наиболее доступными и широко используемыми средствами анализа защищенности. Основной принцип их функционирования заключается в эмуляции действий потенциального злоумышленника по осуществлению сетевых атак. Поиск уязвимостей путем имитации возможных атак является одним из наиболее эффективных способов анализа защищенности сети, который дополняет результаты анализа конфигурации по шаблонам, выполняемый локально с использованием шаблонов (списков проверки). Сканер является необходимым инструментом в арсенале любого администратора, либо аудитора безопасности сети.

Современный сетевой сканер выполняет четыре основные задачи:

* идентификация доступных сетевых ресурсов;
* идентификация доступных сетевых сервисов;
* идентификация имеющихся уязвимостей сетевых сервисов;
* выдача рекомендаций по устранению уязвимостей.

В функциональность сетевого сканера не входит выдача рекомендаций по использованию найденных уязвимостей для реализации атак на сетевые ресурсы. Возможности сканера по анализу уязвимостей ограничены той информацией, которую могут предоставить ему доступные сетевые сервисы.

Одним из наиболее продвинутых коммерческих продуктов этого класса является сетевой сканер NetRecon компании Symantec.

Сетевой сканер NetRecon

Сетевой сканер NetRecon является инструментом администратора безопасности, предназначенным для исследования структуры сетей и сетевых сервисов и анализа защищенности сетевых сред. NetRecon позволяет осуществлять поиск уязвимостей в сетевых сервисах, ОС, МЭ, маршрутизаторах и других сетевых компонентов. Для поиска уязвимостей используются как стандартные средства тестирования и сбора информации о конфигурации и функционировании сети, так и специальные средства, которые реализуют алгоритмы, эмулирующие действия злоумышленника по осуществлению сетевых атак.



Рисунок 5. Сетевой сканер NetRecon

Программа работает в среде ОС Windows NT и имеет удобный графический интерфейс, позволяющий определять параметры сканирования, наблюдать за ходом сканирования, генерировать и просматривать отчеты о результатах сканирования. Результаты отображаются в графической и в табличной форме в реальном масштабе времени.



Рисунок 6. Суммарное количество уязвимостей, обнаруженных сканером NetRecon

Создаваемые NetRecon отчеты содержат подробную информацию о найденных уязвимостях, включая слабость паролей пользователей, подверженность определенных сервисов угрозам отказа в обслуживании, уязвимые для сетевых атак конфигурации ОС и многие другие. Наряду с сообщениями о найденных уязвимостях и их описаниями, приводятся рекомендации по их устранению. Отчет о результатах сканирования позволяет наметить план мероприятий по устранению выявленных недостатков.

В NetRecon используется следующий формат описания уязвимости:

* vulnerability name (название уязвимости);
* risk (уровень риска);
* description (описание уязвимости);
* solution (способы ликвидации уязвимости);
* additional information (дополнительная информация);
* links (ссылки на источники информации о данной уязвимости);
* network resources (список сетевых ресурсов, подверженных данной уязвимости).

В ходе прохождения преддипломной практики данный сетевой сканер использовался для проверки общего состояния защищенной сети передачи данных в администрации города Иркутска.

Результатом оценки защищенности сети передачи данных оказалось выявление некоторых проблем в построении ныне действующей сети, которые перечислены ниже.

Структура администрации представляет собой 10 комитетов, 3 управления, аппарат Избирательной комиссии города, приемную мэра города Иркутска. Каждая из составляющих ведет работу не только с защищаемыми персональными данными внутри, но также ведется работа с другими комитетами и управлениями по защищенному каналу. Первой проблемой является то, что при передаче данных по каналам существует ухудшение качества связи и замедление обработки информации из-за несоответствующего качества каналов связи. Причиной данной проблемы является тот факт, что каналов передачи данных несколько, и все они отличаются друг от друга характеристиками, такими как помехоустойчивость, объем канала, модель канала, пропускная способность, диапазон и тип среды распространения. Эта проблема решается созданием канала связи с едиными характеристиками.

Кроме того, связь между составляющими администрации города Иркутска должна осуществляться через шифрованный защищенный канал с использованием такого средства защиты как VipNet.

Еще одним важным пунктом для решения проблемы построения защищенной сети передачи данных в администрации города Иркутска является создание терминального режима, который обеспечит уменьшение трафика и повышение скорости обработки передаваемых защищаемых данных.

Кроме того, были выявлены необходимые условия, при которых будет осуществляться доступ к системам, содержащим персональные данные, находящиеся в защищенном сегменте. Условия таковы:

* установка сертифицированной ОС Windows 7 sp1. Возможна загрузка только тех обновлений, которые сертифицированы ФСТЭК РФ;
* установка программы Net check, контролирующей изменения сертифицированных файлов;
* установка клиента DLP, осуществляющего контроль работы со съемными носителями и печатными устройствами;
* установка сертифицированного антивируса Kaspersky, осуществляющего защиту от вредоносных программ.

Отсутствие, изменение и удаление этих программ повлечет за собой невозможность доступа к информационным системам и переаттестации рабочего места.

Клиенты для информационных систем могут быть расположены следующим образом:

* локально;
* в защищенном сегменте;
* на терминальном сервере.

Также должна быть установлена централизация хранения персональных данных в защищенном сегменте, то есть, кроме того, что пользователю будет разрешено хранить персональные данные на локальном компьютере, он сможет хранить их на отведенном файловом сервере защищенного сегмента с разграничением полномочий доступа. Все действия пользователя и администратора должны контролироваться системами контроля с выявлением всех фактов действий с файлами, содержащими персональные данные.

Рассмотренные выше проблемы и вопросы использования нормативной документации, методов и средств анализа защищенности являются наиболее важными в ходе проведенной оценки защищенной сети и отражают основные направления работы в этой области.

В ходе дальнейшей работы над дипломом результатом будет являться схема построения защищенной сети передачи данных в администрации города Иркутска с учетом исправления всех выявленных проблем.

Подводя итоги, важно отметить, что в настоящее время вопросы анализа защищенности сетей являются уже достаточно хорошо проработанными. Существует богатый арсенал средств и методов для проведения таких работ. Использование различных методов позволяет достаточно точно оценивать защищенность исследуемой сети. Отработанные методики проведения обследования защищенности сети в соответствии с проверенными критериями, утвержденными в качестве международных стандартов, делают возможным получение исчерпывающей информации о свойствах сети, имеющих отношение к безопасности. На практике анализ защищенности сети проводится при помощи мощных программных средств, в достаточном объеме представленных на рынке средств защиты информации.

**БИБЛИОГРАФИЧЕСКИЙ СПИСОК**

1. Таненбаум Э. С. Компьютерные сети [Текст] / Э. С. Таненбаум — СПб.: Питер, 2002. — 848с.
2. Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы. / В.Г. Олифер, Н.А. Олифер. — СПб.: Питер, 2000. — 672 с.
3. Бертсекас Д. Сети передачи данных. / Д. Бертсекас, Р. Галлагер. —
4. М.: Мир, 1989. — 562 c.
5. Олифер В.Г. Новые технологии и оборудование IP-сетей. / В.Г. Олифер, Н.А. Олифер. — СПб.: БХВ Санкт-Петербург, 2000. — 512 с.
6. Хелд Г. Технологии передачи данных. 7-е изд. — СПб.: Питер, 2003. — 720 с.
7. Теренин А. А. Создание защищенного канала в сети. Материалы семинара «Информационная безопасность — юг России», Таганрог, 28–30 июня 2000. / А.А. Теренин, Ю.Н. Мельников.

1. Электронный замок «Соболь» [Электронный ресурс] / ООО «Код Безопасности». — http://www.securitycode.ru/company/contacts (дата обращения: 01.04.2015).

Размещено на Allbest.ru