# Введение

# Что такое информационная безопасность и почему этот вопрос актуален

Информационная безопасность - это защищенность информации и поддерживающей ее инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести ущерб владельцам или пользователям информации.

В нынешнее время информация является главным фактором в развитии инфраструктуры любого государства, организации или предприятия. Но развитие предполагает и появление новых угроз, от которых нужно предвидеть и от которых нужно уметь защищаться. При создании информационной системы главам организаций нужно учитывать все неблагоприятные факторы, которые могут повлиять на нормальное функционирование предприятия. Безопасность информации становится на первый план.

# Ключевые факторы информационной безопасности

Во всех странах происходит активное развитие инфраструктур, каждый стремится быть первым в информационной гонке. Происходящие преобразования, оказывают сильное влияние на состояние защищённости информации. Появляются новые факторы, которые необходимо учитывать при оценке состояния информационной безопасности.

Всю совокупность факторов можно разделить на 3 категории:

* Политические
* Экономические
* Организационно-технические

Также нельзя забывать про угрозы, которые могут навредить вашей информационной системе. Для того чтобы предотвратить их, необходимо проанализировать источники угроз.

Все источники угроз делятся на 2 категории:

* Внешние
* Внутренние

К внешним угрозам можно отнести политику иностранных государств в области информационных технологий, деятельность иностранных спецслужб, природные катастрофы.

К внутренним угрозам относятся действия со стороны государства, нарушающие права граждан и организаций в информационной сфере, нарушение законов и постановлений по сбору, обработке и передачи данных, преднамеренные или непреднамеренные действия персонала (порча техники, приводящая к сбою и нормальному функционированию информационной системы).

# Для чего нужна информационная безопасность

В связи с высокоразвитыми технологиями люди подвергнуты огромному риску, пострадать от последствий информационных атак.

Под угрозой находятся все сферы деятельности государства.

В политической сфере требуется защищать общественное сознание, политическую ориентацию различных групп регионов, СМИ и т.д.

В экономической сфере под угрозой находятся система государственной статистики, системы сбора обработки финансовой, биржевой, налоговой и таможенной информации и т.д.

В оборонной сфере к наиболее уязвимым аспектам относят информационные ресурсы аппарата Министерства обороны, предприятий оборонного комплекса и т.д.

В нынешнее время появился такой термин как “информационная война”, что означает появление более серьёзных угроз со стороны враждебных лиц, к которым нужно быть готовым и быстро реагировать на них.

Таким образом, проблема обеспечения информационной безопасности является актуальной как никогда в наше время, её можно отнести к ключевому фактору в существовании и развитии любого общества, предприятия или государства.

# Глава 1 Комплексная система защиты

# Почему комплексная система защиты?

Опыт в области защиты информации и построения систем защиты ясно даёт понять, что самой эффективной может быть только комплексная защита, сочетающая в себе правовое, организационное и инженерно–техническое мероприятия.

Нужда в разработке и создании комплексной системы защиты исходит от комплексных действий злоумышленников, которые стремятся любой ценой и любыми средствами добыть необходимую им информацию. В связи с этим защита должна быть выстроена так, чтобы противодействовать всем типам угроз.

# Организационно-правовые мероприятия

Правовое направление предусматривает разработку законодательных актов, нормативно-правовых документов, положений, инструкций и руководств, требования которых являются обязательными в системе защиты информации.

Организационное – это регламент деятельности и взаимоотношений внутри организации на нормативно-правовой основе, таким образом, утечка и несанкционированный доступ к информации становится невозможным или затрудняется за счёт проведения организационных мероприятий.

Организационные мероприятия играют очень важную роль при создании надёжного механизма защиты, так как несанкционированный доступ к информации обуславливается не только техническими аспектами, но и человеческими факторами (небрежностью, халатностью сотрудников организации).

К организационным мероприятиям можно отнести:

* Мероприятия, осуществляемые при проектировании, строительстве и оборудовании служебных и производственных зданий и помещений;
* Мероприятия, касающиеся подбора персонала, включающие знакомство с сотрудниками, их изучение, обучение правилам работы с информацией в зависимости от уровня допуска, ознакомление с мерами ответственности за нарушение правил защиты;
* Организация и поддержание надежного пропускного режима и контроля посетителей;
* Организация надежной охраны помещений и территории;
* Организация хранения и использования документов и носите­лей конфиденциальной информации, включая порядок учета, выдачи, исполнения и возвращения;
* Назначение ответственного лица, отвечающего за защиту информации.

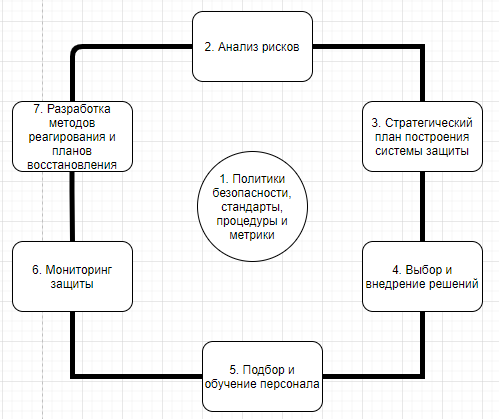


Схема - обобщённая схема построения комплексной защиты предприятия

# Инженерно-технические мероприятия

Инженерно-техническое направление – включает в себя программно-аппаратные средства защиты информации.

К аппаратным средствам относятся механические, электромеха­нические, электронные, оптические, лазерные, радио- и радиотехни­ческие, радиолокационные и другие устройства.

Эти средства применяются для решения следующих задач:

* Препятствие визуальному наблюдению и подслушиванию;
* Защита от ПЭМИН;
* Обнаружение закладных устройств;

По предназначению аппаратные средства можно разделить на две категории: средства выявления и средства защиты.

С закладными устройствами можно бороться при помощи современных технических средств защиты или при помощи визуально-оптического контроля, что на сегодняшний день всё ещё является самым основным методом.

Под визуально-оптическим методом понимается фиксирование:

* Изменений в интерьере и оборудовании помещений;
* Появления свежих царапин;
* Выявление следов чистки и подкраски;
* Состояние мебели, наличие швов, обивки мягкой мебели;
* Содержимое полок и шкафов;
* Проводится осмотр телефонных линий с вскрытием коробов;
* Осмотр труднодоступных мест и подвесных потолков.

Для проведения данных мероприятий используют досмотровые зеркала («Шмель-2М», «КЗ-1-5», «Поиск-2У»), они считаются самым простейшим способом визуального контроля, но не всегда достаточным, поэтому также применяются эндоскопы («ЭТ-10-1,2», «ЭТ-8-1,5» и др., телевизионный видеоскоп «ТВ-10х0,5-5» и др.).

В качестве технического решения, большое распространение получили следующие принципы построения АППК:

* Комплексы с распределённой антенной и единым центром управления;
* Комплексы, состоящие из центра управления, в котором размещаются управляющий компьютер с коммутационным оборудованием, и установленные в контролируемых помещениях дистанционно управляемые сканирующие приёмники.

Ниже приведена таблица с сравнительными характеристики нескольких автоматизированных поисковых комплексов.

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Название** | **Диапазон частот (МГц)** | **Скорость просмотра диапазона (МГц/с)** | **Виды модуляции обнаруживаемых ЗУ** | **Возможность документирования** | **Возможность определения места установки ЗУ в помещении** | **Контроль проводных коммуникаций** | **Питание (В)** | **Возможность модернизации** | **Возможность постановки прицельной помехи** | **Конструктивное оформление** |
| Крона-4 | 0,25-2036 | 4 – 7 | AM, WFM, NFM | + | + | + | 220/12/А | Ограничена | опция | Два кейса |
| Крона-6000 | 0,01-6000 | 40-70 | AM, WFM, NFM | + | + | + | 220 | Ограничена | опция | Кейс |
| RS1000/5 | 0,1-2600 | 4 – 9,8 | Все виды | + | + | + | 220/12/А | + | опция | Кейс |
| RS1000/8 | 0,3-1900 | 7 – 8 | Все виды | + | + | + | 220/12/А | + | опция | Кейс |
| RS1100 | 0,1-2600 | 11 | Все виды | + | + | + | 220/12 | + | есть | Кейс |
| RS1200 | 0,1-2600 | 4 – 9,8 | Все виды | + | + | + | 220/12/А | + | опция | Кейс |
| АРК-Д2 | 0,25 –2036 | - | AM, NFM | + | + | + | 220/А | Ограничена | - | - |
| АРК-Д1Т | 0,01 –6000 | 120 – 140 | Все виды | + | + | + | 220/12/А | + | опция | Кейс |
| АРК-ПК-12 | 0,25 –2600 | 40 –70 | Все виды | + | + | + | 220/12/А | + | опция | Кейс |
| АРК-Д3-12 | 0,1 –2036 | 40 - 70 | Все виды | + | + | + | 220/12 | + | опция | Кейс |
| КРК («Омега») | 0,1 –2600  (с расшир. До18ГГц) | 40 | AM, WFM, NFM | + | + | + | 220 | Нет | опция | Единый корпус |
| Дельта-П05 | 0,25 –2036 | - | Все виды | + | + | + | 220/12/А | Ограничена | нет | Два кейса |
| Дельта-П08 | 0,25 –2036 | - | Все виды | + | + | + | 220/12/А | Ограничена | нет | Два кейса |

Также используются средства для выявления закладочных устройств, которые используют проводные коммуникации. В таких случаях применяются:

* Универсальный прибор «ПКУ-6»;
* Телефонное проверочное устройство «ТПУ-7»;
* Прибор проверки проводных линий «Улан-2».

Для предотвращения утечки информации по акустическому и вибрационному каналу утечки информации используются приборы виброакустической защиты, создающие акустические и вибрационные помехи.

В таких случаях применяется оборудование, включающее в себя генератор шума и комплект акустических и вибрационных излучателей. Качество таких систем оценивают по превышению уровня маскирующего воздействия над уровнем опасных сигналов.

Ниже в таблице приведены технические параметры генераторов шума, используемых в системах виброакустической защиты.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Параметр** | **Шорох-1** | **Шорох-2** | **Соната-АВ, /АВ-квадро** | **ANG-2000** |
| Количество независимых каналов зашумления | 3 | 1 | 2/4 | 1 |
| Полоса частот зашумления (кГц) | 0,2 - 5 | 0,2 – 5 | 0,3 – 5 | 0,25 – 5 |
| Наличие эквалайзера | + | + | - | - |
| Максимальное количество вибродатчиков (шт.) | КВП-2- 72 и  КВП-7 - 48 | КВП-2- 24 и  КВП-7 – 16 | ВИ-45 -12/24,  Акустическ. Изл. - 16/32 | TRN-2000 – 18 |
| Эффективный радиус действия стеновых вибродатчиков (м) | 6 (для КВП-2) | 6 (для КВП-2) | - | 5 (для TRN-2000) |
| Эффективный радиус действия оконных вибродатчиков (м) | 1,5 (для КВП-7) | 1,5 (для КВП-7) | - | - |
| Возможность подключения систем акустического зашумления | + | + | + | + |

Для защиты от подслушивания по телефонным линиям связи и линиям электросетей, выходящих за пределы КЗ, используется зашумление. Принцип работы такой же как и в случае с пространственным зашумлением. Отличие состоит в том, что помехи создаются не в эфире, а в самой линии, где обнаружен опасный сигнал.

Ниже приведена таблица с основными типами систем активной защиты линий.

|  |  |  |  |
| --- | --- | --- | --- |
| **N/N** | **Название** | **Назначение** | **Наличие сертификата ФСТЭК Росии** |
| **Системы активной защиты сети электропитания** | | | |
| 1 | Цикада-с | Генератор шума для сети электропитания 220В | + |
| 2 | Цикада-3С | Генератор шума для трехфазной сети электропитания | - |
| 3 | Соната-С1.1 | Генератор шума для сети электропитания 220В | + |
| 4 | Соната-С1.2 | Генератор шума для сети электропитания 220В на две линии | + |
| 5 | Соната-С2.1 | Генератор шума повышенной мощности для сети электропитания 220В | + |
| 6 | Соната-С2.2 | Генератор шума повышенной мощности для сети электропитания 220В на две линии | + |
| 7 | Соната-С2.3 | Генератор шума повышенной мощности для сети электропитания 220В на три линии | + |
| **Системы активной защиты телефонной сети** | | | |
| 1 | NG-305 (Цикада-М) | Устройство защиты телефонных линий | - |
| 2 | Щит | Односторонний маскиратор телефонных линий | - |
| 3 | НГ-305Т | Устройство защиты телефонных линий | - |
| 4 | МП-1А | Устройство защиты аналоговых телефонных аппаратов | + |
| 5 | МП-1Ц | Устройство защиты цифровых телефонных аппаратов | + |

Под программным обеспечением ИС понимается совокупность программ, включаемых в программное обеспечение ИС, которые реализуют функции защиты и контроля.

Программные средства выполняют:

* Идентификацию технических средств, файлов и аутентификации пользователя;
* Регистрацию и контроль работы технических средств и пользо­вателей;
* Уничтожение информации в ЗУ после использования;
* Cигнализирующие действия при нарушении регламента организации во время использования ресурсов.

На рисунке ниже наглядно продемонстрировано, для чего нужны программные средства, и какую роль они выполняют.

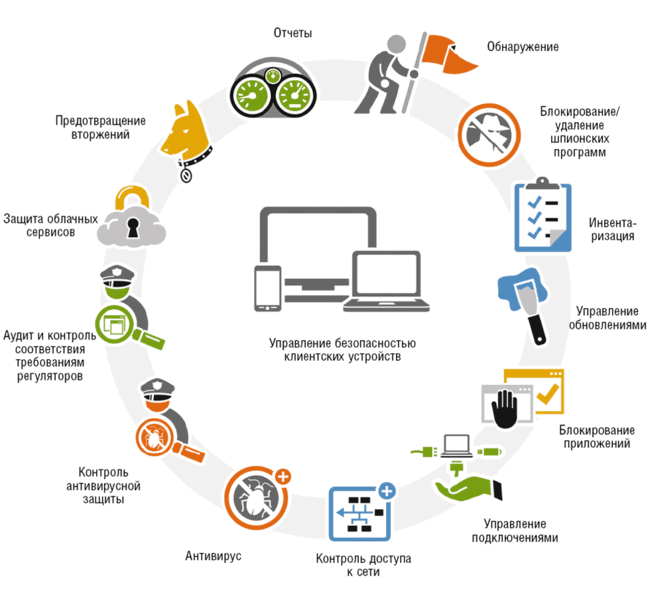


Рисунок - роль программных средств

В настоящий момент самыми популярными решениями среди программных средств защиты информации являются:

* Dallas Lock 8.0-K;
* Secret Net;
* Аппаратно-программный модуль доверенной загрузки «Соболь».

Все вышеперечисленные продукты сертифицированы ФСТЭК и имеют действующие сертификаты. Подробнее о возможностях каждого программного обеспечения можно узнать из таблицы, приведённой ниже.

|  |  |
| --- | --- |
| СЗИ от НСД Secret Net СЗИ от НСД Secret Net | СЗИ Secret Net предназначено для решения следующих типовых задач:   * Защита информации на рабочих станциях и серверах в соответствии с требованиями регулирующих органов * Контроль утечек и каналов распространения защищаемой информации   Основные возможности:   * Разграничение доступа * Контроль утечек * Защита VDI-инфраструктуры * Централизованное управление * Система отчетов * Высокая масштабируемость   Имеет сертификаты соответствия ФСТЭК России и Мин. обороны РФ.  Производитель [ООО «Код Безопасности»](http://www.securitycode.ru/) |
| Dallas Lock 8.0-K  https://www.y-center.ru/netcat_files/userfiles/Dallas-Lock.jpg | СЗИ Dallas Lock 8.0-K представляет собой программный комплекс средств защиты информации в ОС семейства Windows с возможностью подключения аппаратных идентификаторов.  Обеспечивает:   * защиту информации от несанкционированного доступа; * поддержку виртуальных сред; * дискреционный принцип разграничения доступа к информационным ресурсам и подключаемым устройствам в соответствии с матрицей доступа; * аудит действий пользователей; * контроль целостности файловой системы, программно-аппаратной среды и реестра; * объединение защищенных ПЭВМ для централизованного управления механизмами безопасности; * приведение АС, ГИС, АСУ ТП и систем обработки персональных данных в соответствие законодательству РФ по защите информации.   Имеет сертификат соответствия ФСТЭК России № 2720 от 25.09.2012.  Производитель [ЦЗИ «Конфидент»](https://www.dallaslock.ru/). |
| Аппаратно-программный модуль доверенной загрузки «Соболь» Электронный замок Соболь | Электронный замок «Соболь» предназначен для решения следующих типовых задач:   * Защита компьютеров от несанкционированного доступа и обеспечение доверенной загрузки * Создание доверенной программной среды для повышения класса защиты СКЗИ   Основные возможности МДЗ «Соболь»:   * Идентификация и аутентификация * Контроль целостности * Аппаратный ДСЧ * Регистрация попыток доступа * Доверенная загрузка * Сторожевой таймер   Имеет сертификаты соответствия ФСТЭК России и ФСБ в России.  Производитель [ООО «Код Безопасности»](http://www.securitycode.ru/) |

# Реализация защитных мер

Реализацию защитных мероприятий по обеспечению безопасности информационных систем можно разделить на три этапа.

Первый этап – выработка требований:

* Определение состава ИС
* Анализ уязвимостей ИС
* Оценка угроз
* Анализ риска (прогнозирование последствий от угроз)

Второй этап – определение способов защиты:

* Какие угрозы должны быть устранены и в какой мере
* Какие ресурсы должны быть защищены и в какой мере
* С помощью каких средств должна быть реализована защита
* Определение полной стоимости реализации защиты и затрат на эксплуатацию с учётом потенциальных угроз

Третья стадия – определение функций, процедур и средств безопасности, реализуемых в виде механизмов защиты.

# Контролирующие мероприятия

После того как все мероприятия были осуществлены и все меры приняты, систему необходимо тестировать, чтобы убедиться, что рассчитанные приемлемые риски остались на том же уровне.

Независимо от того насколько хорошо были проработаны организационные и технические меры безопасности, они основываются на человеческой деятельности. Ни одна система защиты не сможет предотвратить утечку информации, если человек захочет её обмануть.

В данном случае применяются различные методы проверки. Это регулярные независимые инспекции и ревизии, а также проверочные комиссии.

На предприятиях общий контроль за системой защиты осуществляет лицо или структурное подразделение, назначенное руководством.

Организация и проведение проверок осуществляется с целью выявления нарушений требований соответствующей инструкции по обеспечению режима, который действует на объекте, а также тестирования программных средств защиты, функционирующих в ИС, на предмет соответствия функциям к необходимой степени защиты информации, так как при неправильном определении степени конфиденциальности защищаемой информации защита от НСД может оказаться неэффективной.

Особое внимание при оценке эффективности системы защиты техническими средствами необходимо обратить на их надежность и безотказность.

## Оценка эффективности вариантов построения защиты

После принятия того или иного варианта политики безопасности необходимо оценить уровень безопасности информационной системы. Оценка осуществляется по трём показателям: стоимость, эффективность, реализуемость.

Задача оценки вариантов построения системы зашиты информации достаточно сложная, требующая привлечения современных математических методов многопараметрической оценки эффективности. К таким методам относятся метод анализа иерархий, экспертные методы, метод последовательных уступок и ряд подобных им.

### Тестирование системы защиты

Такая проверка называется тестирование на проникновение. Его целью является предоставление гарантий, что злоумышленник не сможет простыми способами обойти механизм защиты.

Для данной проверки назначается группа из 2-х человек с специальным образованием, которые в течение 1-3 месяцев пытаются найти уязвимые места и разработать на их основе средства для обхода механизма защиты.

Для проведения полного анализа и управления рисками существуют специально разработанные инструментальные средства, построенные с использованием структурных методов системного анализа и проектирования (SSADM — Structured Systems Analysis and Design), которые обеспечивают:

* Построение модели ИС с точки зрения ИБ;
* Методы для оценки ценности ресурсов;
* Инструментарий для составления списка угроз и оценки их вероятностей;
* Выбор контрмер и анализ их эффективности;
* Анализ вариантов построения защиты;
* Документирование (генерация отчётов).

В настоящее время самым популярным средством на рынке является CRAMM.

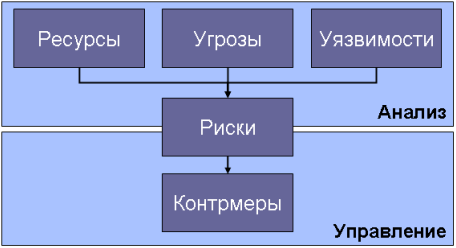


Схема - Анализ рисков и поиск мер противодействия (CRAMM)

# Глава 2 Методика эффективности

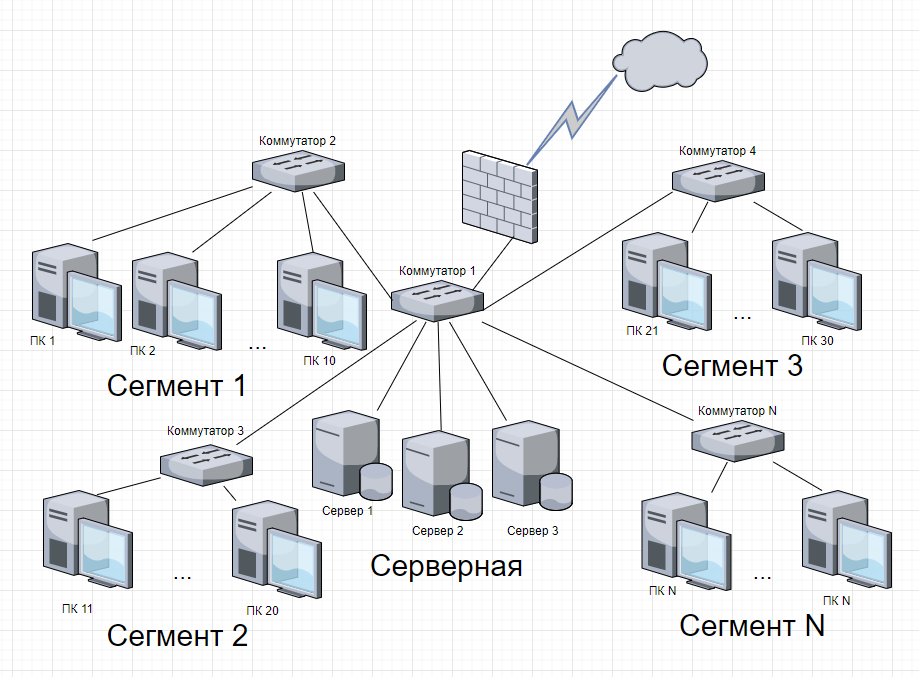
# Цель и задачи

Основной целью данного раздела является проверка методики эффективности принятых мер по защите информации в организации. Для решения данной задачи были решены следующие задачи:

* Анализ законодательной базы России в области защиты конфиденциальных данных, персональных данных, обрабатываемых в государственных информационных системах;
* Исследование существующей информационной системы, изучение её системы защиты и принятых организационных мер;
* Проверка методики проведения оценки концепции системы защиты информации;
* Применение методики к существующей ИС организации и анализ полученных результатов
* Устранение выявленных недостатков, разработка системы защиты.

# Описание существующей информационной системы

ИС «ВУЗ»



* Наличие различного программного обеспечения: Windows Server 2012 R2, Windows XP, Windows 7 Professional, Windows 8.1, Windows 10;
* Наличие многих сегментов сети, в которых обрабатываются различные данные;
* Архитектура клиент-сервер для ведения бухгалтерского учёта, баз данных, контроля за состоянием оборудования и т.д.;
* Наличие выхода в интернет.

# Определение перечня данных, обрабатываемых в информационной системе

* Персональные данные сотрудников
* Конфиденциальные информация
* Коммерческая тайна
* Конфигурация АРМов сегментов сети

## Законодательство

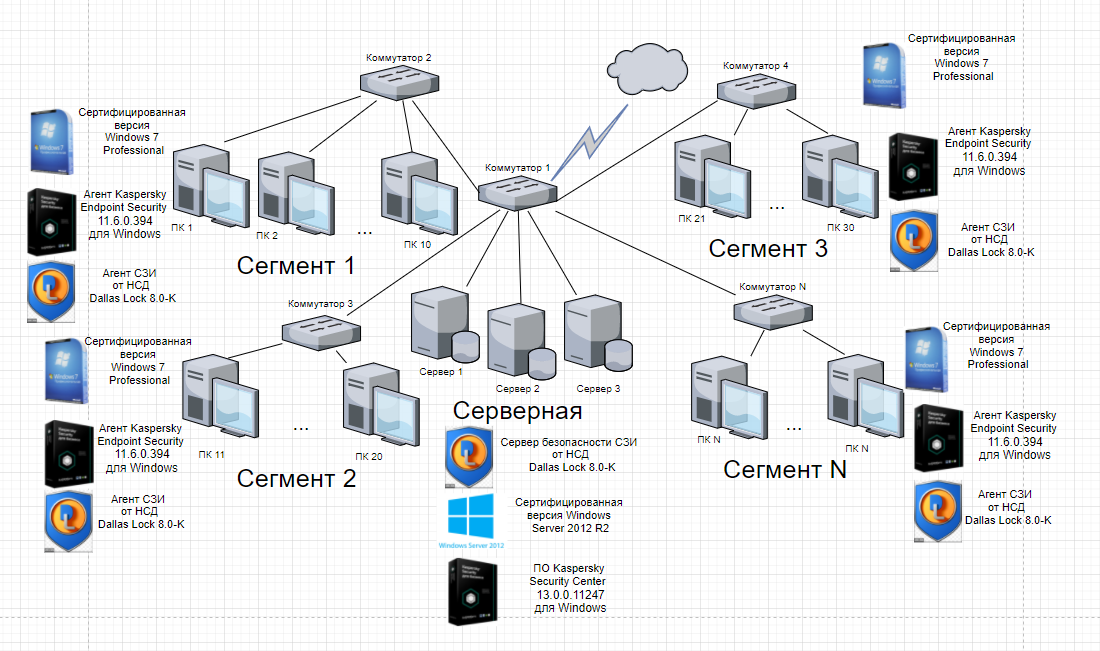
* «Трудовой кодекс РФ»;
* «Налоговый кодекс Российской Федерации (часть вторая)» от 05.08.2000 N 117-ФЗ;
* Приказ ФСТЭК России от 11 февраля 2013 г. N 17;
* Приказ ФСТЭК России от 18 февраля 2013 г. N 21;
* Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 N 149-ФЗ;
* Федеральный закон «О персональных данных» от 27.07.2006 N 152-ФЗ;
* Постановление Правительства Российской Федерации от 1 ноября 2012 г. N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
* Федеральный закон «О коммерческой тайне» от 29.07.2004 N 98-ФЗ.

# Уточнение уровня защищённости информации

1. Информационная система «ВУЗ» является информационной системой, обрабатывающей общедоступные персональные данные и иные категории персональных данных, так как в ней обрабатывается информация, касающаяся ФИО сотрудников, их места регистрации, данные о заработной плате, информация об отпусках и т.д., также в данной ИС обрабатывается конфиденциальная информация и коммерческая тайна.
2. Для ИС «ВУЗ» актуальными являются угрозы 3-го типа, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.
3. ИС «ВУЗ» обрабатывает общедоступные персональные данные и иные категории персональных данных менее чем 100000 субъектов персональных данных, являющихся сотрудниками оператора.
4. В соответствии с приложением N 1 к настоящим требованиям приказа ФСТЭК России от 11 февраля 2013 г. N17, для информации, обрабатываемой в ИС «ВУЗ», установлен низкий уровень значимости (УЗ 3). Масштаб информационной системы равен объектовому. В связи с этими данными для данной ИС был установлен третий класс защищённости (К3).

# Описание выбранных средств защиты

ИС «ВУЗ»



# Проверка общей концепции оценки системы защиты информации



# Проверка этапа оценки организационно-распорядительной документации

1. Оценка документации, связанной с ПДн, конфиденциальной информацией и коммерческой тайной
   1. Проверка целей обработки ПДн, конфиденциальной информации, коммерческой тайны
   2. Проверка законности обработки персональных данных, конфиденциальной информации и коммерческой тайны
   3. Проверка сроков обработки ПДн, конфиденциальной информации и коммерческой тайны
2. Оценка политики информационной безопасности
   1. Обоснованность выбора типа нарушителей
   2. Актуальность определённых угроз
   3. Соответствие мер защиты
   4. Обоснованность выбора состава и классов технических СЗИ
   5. Наличие инструкций и назначение ответственного за организацию процесса обеспечения защиты
   6. Наличие нормативно-правовой и организационно-распорядительной документации
3. Оценка классификации и уровня защищённости ИС
   1. Наличие документа, в котором описывается классификация
   2. Правильность проведённой классификации
   3. Оценка соответствия имеющихся технических средств и средств защиты информации тем, что представлены в документации
   4. Оценка выбранного для ИС типа актуальных угроз
4. Оценка документации на технические средства защиты
   1. Наличие сертификатов ФСТЭК
   2. Наличие паспорта технического средства
   3. Проверка актуальности сертификата
   4. Соответствие классу защищённости
5. Оценка требований к помещениям, где обрабатывается информация
   1. Проверка работы режима доступа в помещения
6. Оценка квалификации сотрудников, которые обеспечивают защиту информации
   1. Проверка на знание инструкций
   2. Проверка документов
   3. Проверка знания ТС и технологий, работы с ПО
7. Оценка анализа информационных потоков
   1. Содержание информационного потока
   2. Соотнесение информационных потоков с внешними ИС
   3. Законное основание передачи данных

# Проверка этапа оценки технической защиты



# Инструментальная оценка подсистемы идентификации и авторизации

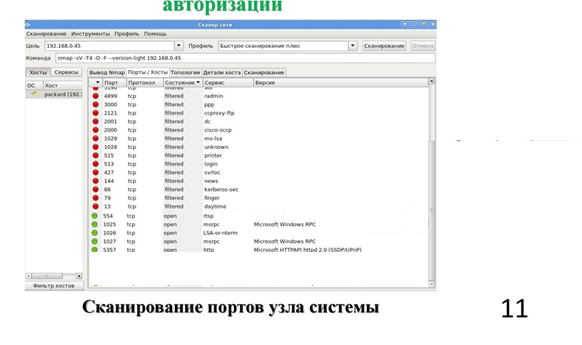


Рисунок - сканирование портов

# Инструментальная оценка подсистемы идентификации и авторизации

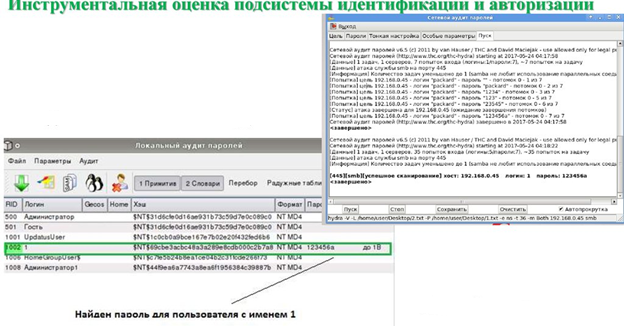


Рисунок - аудит паролей

# Проверка подсистемы антивирусной защиты и межсетевого экрана

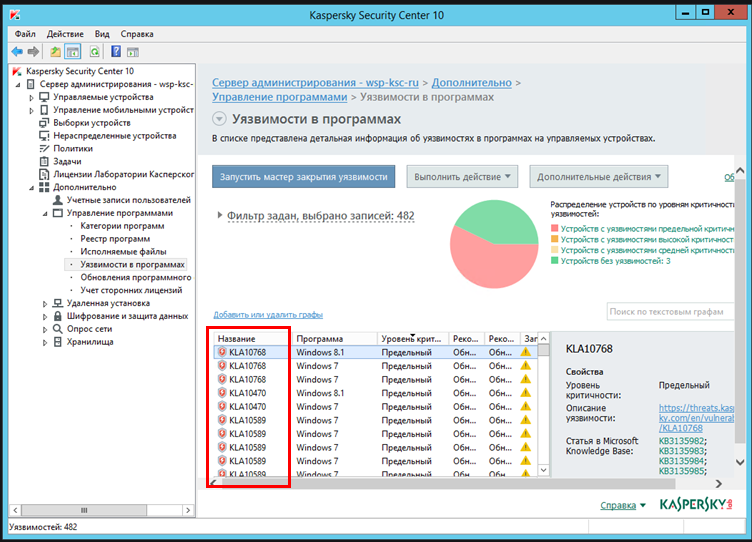


Рисунок - результат сканирования

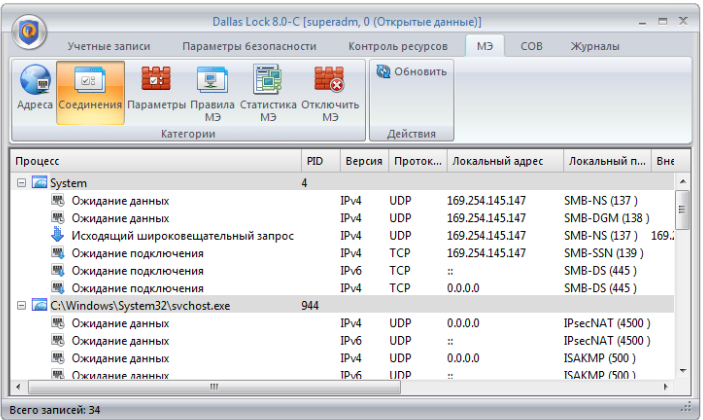


Рисунок - список текущих сетевых подключений компьютера

# Применение разработанной методики на объекте информатизации. Проверка организационно-распорядительной документации

|  |  |  |  |
| --- | --- | --- | --- |
| № | Этапы и пункты проверки согласно методике | Степень соответствия пунктам методики | Разъяснение |
| 1.1 | Проверка целей обработки ПДн, конфиденциальной информации, коммерческой тайны | Частично соответствует | Излишняя обработка ксерокопий документов |
| 1.2 | Проверка законности обработки персональных данных, конфиденциальной информации и коммерческой тайны | Соответствует | Все данные обрабатываются согласно законодательству РФ и нормативно-правовым документам |
| 1.3 | Проверка сроков обработки ПДн, конфиденциальной информации и коммерческой тайны | Частично соответствует | Не определены сроки обработки информации |
| 2.4 | Обоснованность выбора состава и классов технических СЗИ | Соответствует | Все средства защиты информации были подобраны согласно уровню защищённости, все инструменты соответствуют приложению N 1 Приказа ФСТЭК N 17 |
| 2.5 | Наличие инструкций и назначение ответственного за организацию процесса обеспечения защиты | Соответствует | Все инструкции по плану действий в различных ситуациях составлены и находятся на месте. Ответственное лицо, отвечающее за организацию процесса обеспечения защиты, назначено. |
| 3.2 | Правильность проведённой классификации | Соответствует | Классификация проведена корректно, количество субъектов ИС соответствует классу защищённости. |
| 3.3 | Оценка соответствия имеющихся технических средств и средств защиты информации тем, что представлены в документации | Соответствует | Все имеющиеся ТС и СЗИ соответствуют представленным в документации |

# Проверка технической защиты информационной системы

|  |  |  |  |
| --- | --- | --- | --- |
| № | Этапы и пункты проверки согласно методике | Степень соответствия пунктам методики | Разъяснение |
| 1 | Сканирование персональных компьютеров системы | Частично соответствует | Сканирование выявило наличие открытых портов, которые несут угрозу информационной безопасности |
| 2 | Инструментальная оценка подсистемы идентификации и авторизации | Соответствует | Функционал локальной и сетевой идентификации и авторизации организован корректно для получения ресурсов субъектами |
| 3 | Проверка подсистемы разграничения доступа | Соответствует | Разграничение доступа выполняется согласно правам субъектов |
| 4 | Проверка подсистемы регистрации и учёта | Соответствует | - |
| 5 | Проверка подсистемы антивирусной защиты и межсетевого экранирования | Частично соответствует | Правила межсетевого экранирования некорректно настроены |
| 6 | Проверка подсистемы реагирования на события безопасности | Соответствует | - |

# Проверка подсистемы антивирусной защиты и межсетевого экранирования

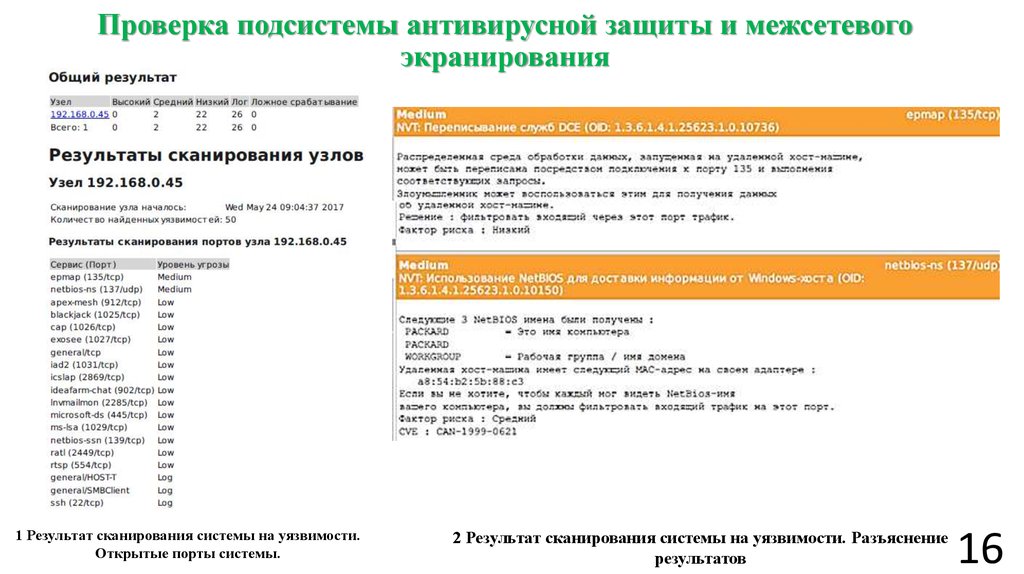


Рисунок - результат сканирования системы на уязвимости. Открытые порты системы.

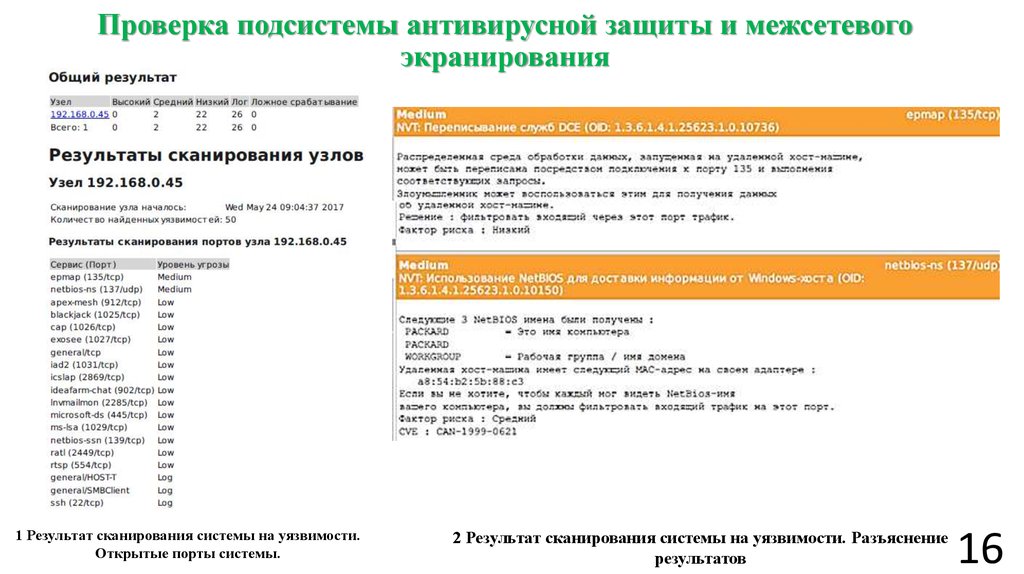


Рисунок - результат сканирования системы на уязвимости. Разъяснение результатов.

# Выработка мер по устранению выявленных недостатков

|  |  |  |  |
| --- | --- | --- | --- |
| Наименование | Кол-во | Цена, руб. | Сумма, руб. |
| Поставка средств защиты информации | | | |
| СЗИ от НСД Dallas Lock 8.0-С | 1 | 194900 | 194900 |
| Средство анализа защищённости «Сканер-ВС (специальная версия)» | 1 | 6000 | 6000 |
| Всего | | | 200900 |

Характеристика политики ИБ:

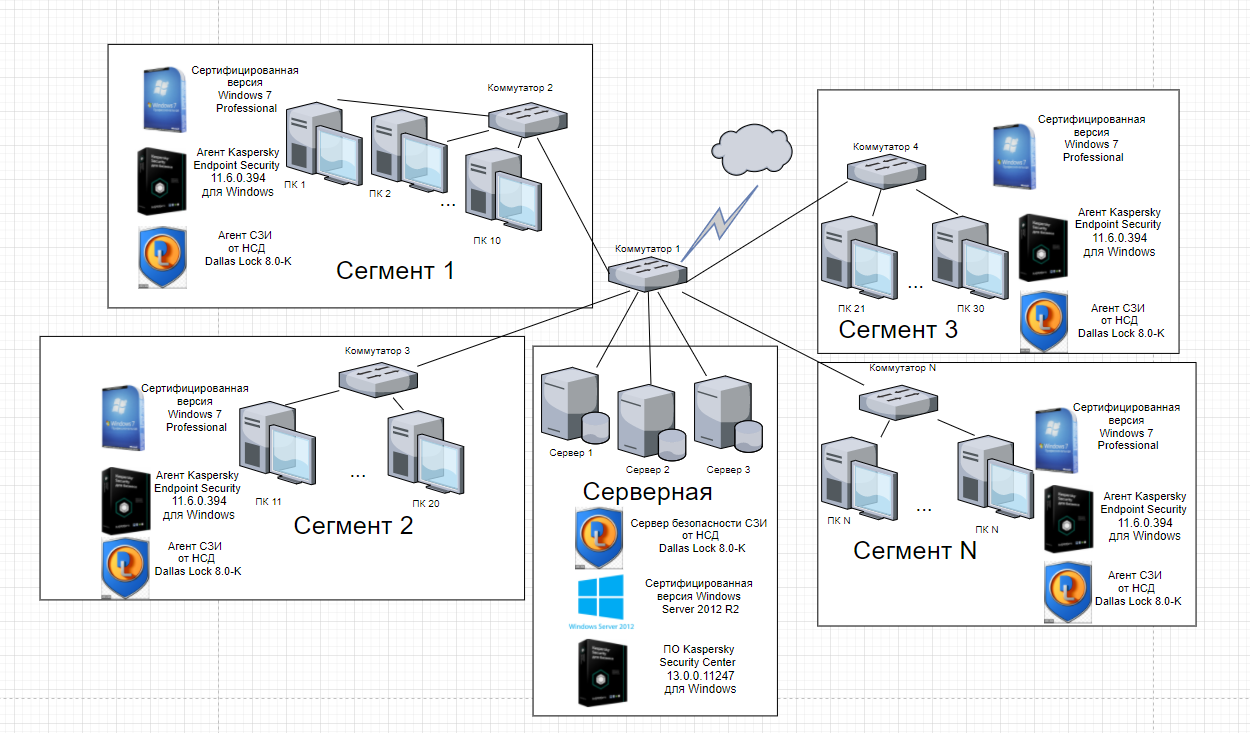
Изменение состава средств защиты информации согласно выявленным недостаткам в системе:

* Системы обнаружения вторжений и средства антивирусной защиты не ниже 4 класса;
* Межсетевые экраны не ниже 3 класса.

Требуется определить перечень сетевых ресурсов, к которым будет ограничен доступ из внутренней сети. Также необходимо настроить работу фильтрации межсетевого экрана для защиты от вредоносного трафика из внешних ресурсов.

# Предложенные меры по организации технической защиты ИС «ВУЗ»

ИС «ВУЗ»



1. В рамках обеспечения функций идентификации и аутентификации ИС имеет:

* Механизм авторизации, позволяющим подключать аппаратные средства ввода пароля (eToken, ruToken и т.д.);
* Механизм контроля корректности идентификации субъекта доступа к ресурсам.

1. Проверка подсистемы разграничения доступа:

* Механизмы разграничения доступа к локальным и сетевым ресурсам;
* Включение в политику разграничения доступа субъекта системы действий, выполняемых внутри ИС для расширения функциональных возможностей, приводящих к расширениям противодействующих действий;
* Механизм управления подключением устройств.

1. Необходимо произвести корректную настройку правил межсетевого экранирования:

* Ограничить доступ по открытым или уязвимым портам устройства из внешней сети;
* Задать правила для доступа из каждого сегмента сети к каждому;
* Реализовать правила межсетевого экранирования согласно политике безопасности.

# Основные полученные результаты

1. В ходе написания данного дипломного проекта была проведена исследовательская работа по изучению структуры информационной системы «ВУЗ». Также были изучены нормативно-правовые акты, инструкции и документы, разработанные внутри организации, которые описывают принятые организационные меры, изучена документация, описывающая процесс создания СЗИ для предотвращения НСД и утечки ПДн и конфиденциальной информации, а также введение режима коммерческой тайны на предприятии.
2. Был проведён анализ действующего законодательства Российской Федерации в области обеспечения безопасности, не относящейся к государственной тайне, обрабатываемой в государственной информационной системе, также был изучен процесс построения организационно-правовых мероприятий при обработке персональных данных, конфиденциальной информации и коммерческой тайны. В процессе изучения были выделены основные моменты, на которые стоит обратить особое внимание при организации работ с информацией данного рода на предприятии.
3. Ключевым моментом дипломного проекта является проверенная и обновлённая методика оценки эффективности принятых мер по обеспечению защиты данных. Главной особенностью является то, что подобную методику нельзя найти в открытом доступе, так как она была разработана внутри организации, и другие предприятия не могут воспользоваться ей в своих целях.
4. Были изучены функциональные возможности ПО «Сканер-ВС».
5. Проведена проверка организации с использованием существующей методики. Данная проверка помогла выявить несколько недостатков в системе защиты информации и устранить их.
6. Для устранения выявленных недостатков были предложены компенсирующие меры, включающие в себя меры для корректировки организационно-технической документации и меры по улучшения отдельных аспектов существующей системы защиты.