титульный лист

# Оглавление

I. Аналитическая часть.....4

1.1. Технико-экономическая характеристика предметной области и предприятия ООО «ПК Венткомплекс».....4

1.1.1. Общая характеристика предметной области.....4

1.1.2. Организационно-функциональная структура ООО «ПК Венткомплекс».....5

1.2. Анализ рисков информационной безопасности.....7

1.2.1 Идентификация и оценка информационных активов.....7

1.2.2. Оценка уязвимостей активов.....12

1.2.3 Оценка угроз активам.....17

1.2.4. Оценка существующих и планируемых средств защиты.....38

1.2.5. Оценка рисков.....41

1.3. Характеристика комплекса задач, задачи и обоснование необходимости совершенствования системы обеспечения информационной безопасности и защиты информации ООО «ПК Венткомплекс».....55

1.3.1. Выбор комплекса задач обеспечения информационной безопасности.....55

1.3.2. Определение места проектируемого комплекса задач в комплексе задач ООО «ПК Венткомплекс», детализация задач информационной безопасности и защиты информации.....56

1.4. Выбор защитных мер.....60

1.4.1. Выбор организационных мер.....60

1.4.2. Выбор инженерно-технических мер.....61

II Проектная часть.....73

2.1. Комплекс организационных мер обеспечения информационной безопасности и защиты информации ООО «ПК Венткомплекс».....73

2.1.1. Отечественная и международная нормативно-правовая основа создания системы обеспечения информационной безопасности и защиты информации предприятия.....73

2.1.2. Организационно-административная основа создания системы обеспечения информационной безопасности и защиты информации ООО «ПК Венткомплекс».....77

2.2. Комплекс проектируемых программно-аппаратных средств обеспечения информационной безопасности и защиты информации ООО «ПК Венткомплекс».....81

2.2.1 Структура программно-аппаратного комплекса информационной безопасности и защиты информации ООО «ПК Венткомплекс».....81

2.2.2. Контрольный пример реализации проекта и его описание.....84

III Обоснование экономической эффективности проекта.....88

3.1 Расчёт показателей экономической эффективности проекта.....88

IV Безопасность жизнедеятельности.....91

4.1 Характеристика условий труда на рабочем месте с ПК.....91

4.2 Работоспособность сотрудника и ее динамика.....96

4.3 Пожарная безопасность предприятия.....103

Список литературы.....106

Приложение 1. Горизонтальная СКС.....109

Приложение 2. Телекоммуникационный шкаф.....111

Приложение 3. Схема устройств в сети.....112

# I. Аналитическая часть

## 1.1. Технико-экономическая характеристика предметной области и предприятия ООО «ПК Венткомплекс»

### 1.1.1. Общая характеристика предметной области

Повсеместная компьютеризация, начавшаяся в конце XX века продолжается и в наши дни. Автоматизация процессов в организации повышает производительность труда сотрудников организации. Пользователи информационных систем могут быстро получать данные необходимые для выполнения их должностных обязанностей. Однако вместе с облегчением доступа к данным существует проблемах сохранности этих данных. Обладая доступом к различным информационным системам, злоумышленники могут использовать их в корыстных целях: сбор данных для продажи их на чёрном рынке, кража денежных средств у клиентов организации, кража коммерческой тайны организации.

Поэтому проблема защиты критично важной информации для организаций стоит очень остро. Всё чаще становится известно из СМИ о различных техниках или методиках кражи денежных средств посредством взлома информационных систем финансовых организаций. Получив доступ в информационные системы персональных данных, злоумышленник может своровать данные клиентов финансовых организаций, информацию об их финансовых операциях распространить их, нанеся заказчику как финансовый, так и репутационный вред. Кроме того, узнав данные о клиенте, мошенники могут напрямую позвонить клиенту, представившись сотрудниками организации и обманным путём, используя технику социального инжиниринга узнать пароли от систем дистанционного обслуживания и вывести деньги со счета заказчика.

В нашей стране проблема кражи и незаконного распространения персональных данных стоит очень остро. В сети Интернет существует большое количество ресурсов, на которых содержаться ворованные базы персональных данных, с помощью которых, например, по номеру мобильного телефона, можно найти очень подробную информацию по человеку, включая его паспортные данные, адреса проживания, фотографии и многое другое.

Целью исследования в данной работе является изучение системы защиты персональных данных в ООО «ПК Венткомплекс».

Для реализации поставленной цели необходимо решить ряд задач:

- определить информационные и технические ресурсы, подлежащие защите на объекте информатизации;
- выявить потенциально возможные угрозы и технические каналы утечки информации;
- построить модель вероятного нарушителя;
- провести оценку уязвимости и рисков информации при имеющемся множестве угроз и каналов утечки;
- определить требования к системе защиты.

Объект исследования – сетевая инфраструктура и информационные системы ПАО ООО «ПК Венткомплекс».

Предмет исследования - система защиты персональных данных в ООО «ПК Венткомплекс».

### 1.1.2. Организационно-функциональная структура ООО «ПК Венткомплекс»

Деятельность компании заключается в комплексном оснащении вентиляционно-отопительным оборудованием строящихся зданий и сооружений, промышленных, социальных, спортивных, сельскохозяйственных объектов на территории Российской Федерации и стран СНГ.

Для качественной и бесперебойной работы компании, оказания услуг и поддержки клиентов, компания содержит большой штат сотрудников. В него

входят специалисты разных направлений, большую часть составляют менеджеры по продажам и специалисты удаленной поддержки абонентов.

Ввиду большого количества сотрудников, принята следующая организационная структура (рисунок 1.1). Компания разделена на два департамента и несколько отделов.

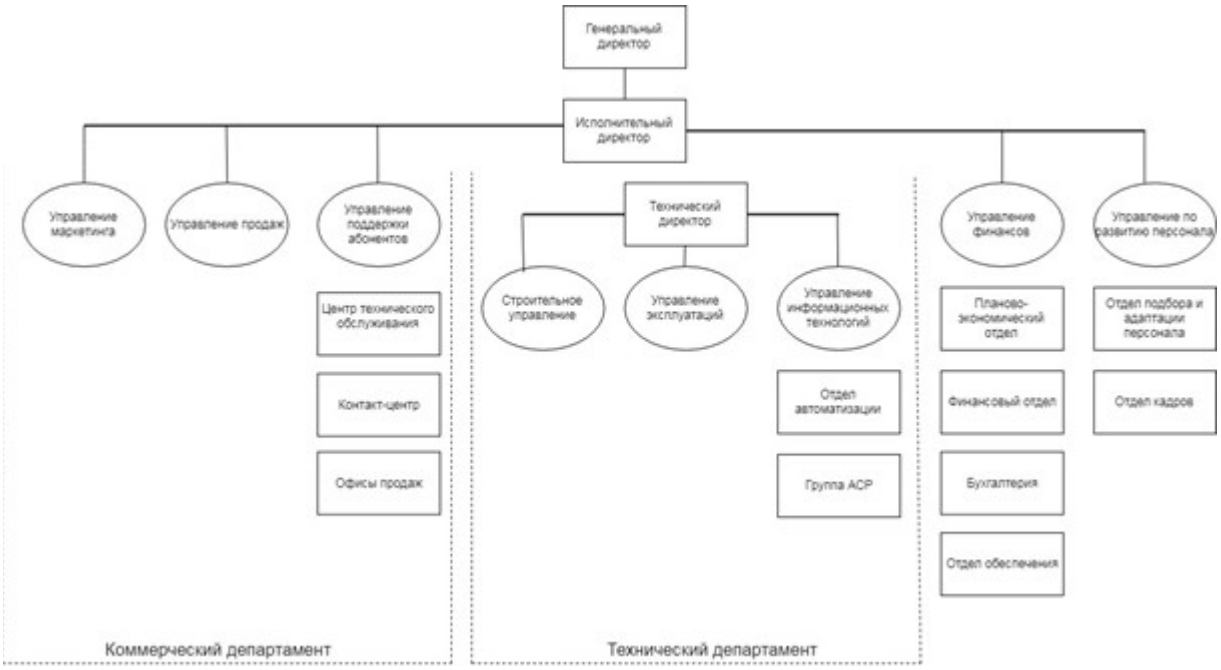



Рисунок 1.1 – Организационная структура ООО «ПК Венткомплекс».

Объект защиты расположен в бизнес – центре. Объект выполнен из кирпичной кладки. На объекте установлены окна с двойным остеклением. Вход на объект расположен в центральной части здания. Так же на въезде на территорию установлен шлагбаум. На первом этаже бизнес – центра установлен пункт пропускного контроля.

На объекте информатизации наиболее важными помещениями с точки зрения обработки конфиденциальной информации являются: отдел информационных технологий (ИТ), бухгалтерия, отдел безопасности, юридический отдел, переговорная (Приложение 1).

В данных помещениях к основным техническим средствам и системам (ОТСС) можно отнести средства вычислительной техники, автоматизированные системы на базе средств вычислительной техники, в том

числе информационно-вычислительные комплексы, сети и системы, средства и системы связи и передачи данных. Используемые системы не имеют сертификатов по требованиям защиты информации от утечки по каналу побочных излучений и наводок.

К вспомогательным техническим средствам и системам (ВТСС) можно отнести различного рода телефонные средства и системы, средства электронной оргтехники, которые располагаются почти во всех помещениях предприятия. ВТСС обладают микрофонным эффектом и возможностью организации на их базе канала утечки информации за счет навязывания.

Также технические каналы утечки информации создают используемые в помещениях средства и системы передачи данных в системе радиосвязи, средства и системы охранной и пожарной сигнализации, средства и системы кондиционирования, средства и системы проводной радиотрансляционной сети и приема программ радиовещания и телевидения. Цепи элект¬роснабжения и заземления могут создавать технические каналы утечки информации.

Специальных звукоизоляционных и вибро - изоляционных средств защиты помещения не имеют, что оказывает влияние на образование технических каналов утечки речевой информации, циркулирующей в этом помещении.

В данном случае контролируемая зона определена охраняемой территорией предприятия. Некоторых ОТСС находятся довольно близко к границе контролируемой зоны и относительно ВТСС и их линий связи, на которые могут наводиться информативные сигналы.

## 1.2. Анализ рисков информационной безопасности

### 1.2.1 Идентификация и оценка информационных активов

В организации необходимо защищать сразу несколько информационных персональныхданных, а именно:

- информационную систему персональных данных сотрудников организации;
- информационную систему персональных данных системы контроля и управления доступом;
- информационную систему персональных данных автоматизированной системы.

ИСПДн сотрудников организации используется для начисления сотрудникам заработной платы, автоматизации работы сотрудников отдела по работе с персоналом, автоматизации работы сотрудников бухгалтерии и решения других кадровых и бухгалтерских вопросов. Состоит из базы данных 1С «Зарплата и управление персоналом», расположено на отдельном автоматизированном рабочем месте с возможностью подключения к рабочему месту по сети. АРМ расположен в кабинете отдела по работе с персоналом. На автоматизированном рабочем месте установлена операционная система Microsoft Windows 7. Подключение к сети Интернет на АРМ отсутствует.

Персональные данные, обрабатываемые в ИСПДн:

- Фамилия, имя, отчество;
- Дата рождения;
- Пол;
- Серия и номер паспорта;
- ИНН;
- СНИЛС;
- Номер телефона;

Право работать с программным обеспечением 1С «Зарплата и управление персоналом» и базой данных персональныхданных имеют:

- Главный бухгалтер;
- Заместитель главного бухгалтера;
- Начальник отдела по работе с персоналом;

- Сотрудник, ответственный за начисление заработной платы сотрудникам.

Доступ к автоматизированному рабочему месту имеют:

- Системные администраторы, для администрирования автоматизированного рабочего места и программного обеспечения 1С «Зарплата и управление персоналом» и базы данных персональныхданных;
- Сотрудники подразделения, ответственного за информационную безопасность организации, для администрирования системы защиты информации АРМ.

В ИСПДн сотрудников могут выполняться следующие функции:

- Автоматизированное удаление персональныхданных;
- Ручное удаление персональныхданных;
- Ручное добавление персональныхданных;
- Ручное изменение данных;
- Автоматизированный поиск персональныхданных.

В информационной системе персональных данных хранятся данные, позволяющие идентифицировать 243 сотрудника.

После достижения целей обработки персональных данных сотрудника, его персональные данные удаляются из ИСПДн.

Информационная система персональных данных системы контроля и управления доступом используется для хранения персональных данных сотрудников и клиентов, имеющих доступ в различные помещения организации. ИСПДН системы контроля и управления доступом используется отделом безопасности. База данных ИСПДн установлена на АРМ, находящимся в комнате охраны отдела безопасности. На АРМ ИСПДн установлена операционная система Microsoft Windows 7, в качестве системы управления базой данных используется СУБД Microsoft SQL Server 2012.

АРМ ИСПДн не имеет доступ в локальную сеть, а также не имеет доступ в сеть Интернет.

В ИСПДн хранятся следующие персональные данные:

- Фамилия, имя, отчество;
- Фотография сотрудника.

Право работать с ИСПДн системы контроля и управления доступом имеют:

- Начальник отдела безопасности;
- Заместитель начальника отдела безопасности;
- Сотрудники отдела безопасности.

Доступ к автоматизированному рабочему месту системы контроля и управления доступом имеют:

- Системные администраторы, для администрирования автоматизированного рабочего места и программного обеспечения 1С «Зарплата и управление персоналом» и базы данных персональныхданных;
- Сотрудники подразделения, ответственного за информационную безопасность, для администрирования системы защиты информации АРМ.

В ИСПДн сотрудников могут выполняться следующие функции:

- Автоматизированное удаление персональныхданных;
- Ручное удаление персональныхданных;
- Ручное изменение данных;
- Ручное добавление персональныхданных;
- Автоматизированный поиск персональныхданных.

В информационной системе персональных данных хранятся данные, позволяющие идентифицировать 243 сотрудника.

После достижения целей обработки персональных данных сотрудника, его персональные данные удаляются из ИСПДн.

Информационная система персональных данных автоматизированной системы предназначена для автоматизации работы большинства работников. Она позволяет повысить производительность труда сотрудников. В качестве автоматизированной системы используется комплекс программных продуктов. В качестве системы управления базой данных используется программное обеспечение компании Oracle. ИСПДн развёрнута на сервере, операционная система установленная на сервере – Microsoft Windows Server 2008 R2. ИСПДн автоматизированной системы подключена к локальной вычислительной сети, но не имеет доступ в сеть Интернет. Подключение пользователей к базе ИСПДн производится с помощью программных продуктов с выделенных виртуальных терминалов. Каждый пользователь имеет в ИСПДн свой логин и пароль.

Персональные данные, обрабатываемые в ИСПДн:

- Фамилия, имя, отчество;
- Дата рождения;
- Пол;
- Серия и номер паспорта;
- ИНН;
- СНИЛС;
- Номер телефона;

Право работать с программным обеспечением и базой данных персональныхданных имеют:

- Сотрудники бухгалтерии;
- Сотрудники кредитного отдела;
- Сотрудники отдела риск-менеджмента;
- Сотрудники отдела залогов;
- Персональные менеджеры;
- Клиентские менеджеры;
- Сотрудники отдела безопасности.

Доступ к автоматизированному рабочему месту имеют:

- Системные администраторы, для администрирования сервера, базы данных персональныхданных и программного обеспечения;
- Сотрудники подразделения, ответственного за информационную безопасность, для администрирования сервера, базы данных персональныхданных и программного обеспечения.

В ИСПДн сотрудников могут выполняться следующие функции:

- Автоматизированное удаление персональныхданных;
- Ручное удаление персональныхданных;
- Ручное добавление персональныхданных;
- Ручное изменение данных;
- Автоматизированный поиск персональныхданных.

В информационной системе персональных данных хранятся данные, позволяющие идентифицировать 243 сотрудника и 9438 клиентов.

После достижения целей обработки персональных данных сотрудника, его персональные данные удаляются из ИСПДн.

### 1.2.2. Оценка уязвимостей активов

Угрозы НСД в ИСПДн с применением программных и программно-аппаратных средств реализуются при осуществлении несанкционированного, в том числе случайного, доступа, в результате которого осуществляется нарушение конфиденциальности, целостности и доступности ПДн, и включают в себя:

- угрозы несанкционированного доступа в операционную среду компьютера с использованием штатного программного обеспечения (средств операционной системы или прикладных программ общего применения);
- угрозы создания нештатных режимов работы программных (программно-аппаратных) средств за счет преднамеренных изменений служебных данных, игнорирования предусмотренных

в штатных условиях ограничений на состав и характеристики обрабатываемой информации, искажения (модификации) самих данных и т.п.;




Рисунок 1.2 Классификация УБПДн, обрабатываемых в информационных системах персональных данных.

- угрозы внедрения вредоносных программ (программно-математического воздействия).

Состав элементов описания угроз НСД к информации в ИСПДн приведен на рисунке 1.3.

Кроме этого, возможны комбинированные угрозы, представляющие собой сочетание указанных угроз. Например, за счет внедрения вредоносных программ могут создаваться условия для НСД в операционную среду компьютера, в том числе путем формирования нетрадиционных информационных каналов доступа.

Угрозы несанкционированного доступа в операционную среду ИСПДн с использованием штатного программного обеспечения разделяются на угрозы непосредственного и удаленного доступа. Угрозы непосредственного доступа осуществляются с использованием программных и программно-аппаратных средств ввода/вывода компьютера. Угрозы удаленного доступа реализуются с использованием протоколов сетевого взаимодействия.

Такие угрозы реализуются относительно ИСПДн как на базе автоматизированного рабочего места, не включенного в сети связи общего пользования, так и применительно ко всем ИСПДн, имеющим подключение к сетям связи общего пользования и сетям международного информационного обмена.

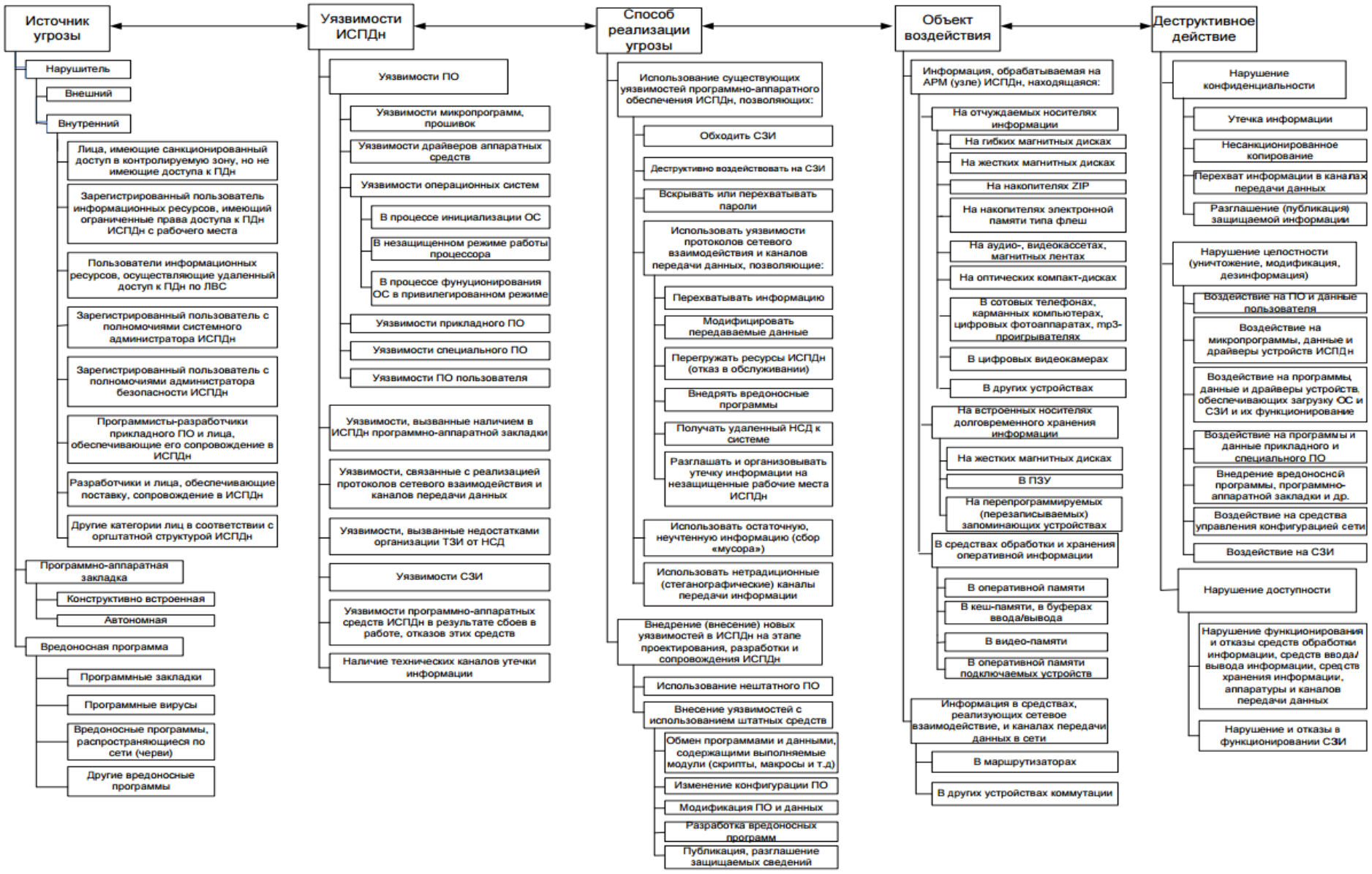



Рисунок 1.3 Классификация УБПДн, обрабатываемых в информационных системах персональных данных.

### 1.2.3 Оценка угроз активам

Источниками угроз в информационной системой персональных данных могут быть:

- нарушитель;
- носитель вредоносной программы;
- аппаратная закладка.

Угрозы безопасности ПДн, связанные с внедрением аппаратных закладок, определяются в соответствии с нормативным документами Федеральной службы безопасности Российской Федерации в установленном ею порядке.

По наличию права постоянного или разового доступа в контролируемую зону ИСПДн нарушители подразделяются на два типа:

- нарушители, не имеющие доступа к ИСПДн, реализующие угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена, – внешние нарушители;
- нарушители, имеющие доступ к ИСПДн, включая пользователей ИСПДн, реализующие угрозы непосредственно в ИСПДн, – внутренние нарушители.

Внешними нарушителями могут быть:

- конкурирующие организации;
- недобросовестные партнеры;
- внешние субъекты (физические лица).

Внешний нарушитель имеет следующие возможности:

- осуществлять несанкционированный доступ к каналам связи, выходящим за пределы служебных помещений;
- осуществлять несанкционированный доступ через автоматизированные рабочие места, подключенные к сетям связи

общего пользования и (или) сетям международного информационного обмена;

- осуществлять несанкционированный доступ к информации с использованием специальных программных воздействий посредством программных вирусов, вредоносных программ, алгоритмических или программных закладок;
- осуществлять несанкционированный доступ через элементы информационной инфраструктуры информационной системой персональных данных, которые в процессе своего жизненного цикла (модернизации, сопровождения, ремонта, утилизации) оказываются за пределами контролируемой зоны;
- осуществлять несанкционированный доступ через информационные системы взаимодействующих ведомств, организаций и учреждений при их подключении к ИСПДн.

Внутренние потенциальные нарушители подразделяются на восемь категорий в зависимости от способа доступа и полномочий доступа к ПДн.

К первой категории относятся лица, имеющие санкционированный доступ к ИСПДн, но не имеющие доступа к ПДн. К этому типу нарушителей относятся должностные лица, обеспечивающие нормальное функционирование ИСПДн.

Лицо этой категории, может:

- иметь доступ к фрагментам информации, содержащей ПДн и распространяющейся по внутренним каналам связи ИСПДн;
- располагать фрагментами информации о топологии ИСПДн и об используемых коммуникационных протоколах и их сервисах;
- располагать именами и вести выявление паролей зарегистрированных пользователей;
- изменять конфигурацию технических средств ИСПДн, вносить в нее программно-аппаратные закладки и обеспечивать съем

информации, используя непосредственное подключение к техническим средствам ИСПДн.

Ко второй категории относятся зарегистрированные пользователи ИСПДн, осуществляющие ограниченный доступ к ресурсам ИСПДн с рабочего места.

Лицо этой категории:

- обладает всеми возможностями лиц первой категории;
- знает, по меньшей мере, одно легальное имя доступа;
- обладает всеми необходимыми атрибутами, обеспечивающими доступ к некоторому подмножеству ПДн;
- располагает конфиденциальными данными, к которым имеет доступ.

Его доступ, аутентификация и права по доступу к некоторому подмножеству ПДн должны регламентироваться соответствующими правилами разграничения доступа.

К третьей категории относятся зарегистрированные пользователи ИСПДн, осуществляющие удаленный доступ к ПДн по локальным и (или) распределенным информационным системам.

Лицо этой категории:

- обладает всеми возможностями лиц первой и второй категорий;
- располагает информацией о топологии ИСПДн на базе локальной и (или) распределенной информационной системы, через которую осуществляется доступ, и о составе технических средств ИСПДн;
- имеет возможность прямого (физического) доступа к фрагментам технических средств ИСПДн.

К четвертой категории относятся зарегистрированные пользователи ИСПДн с полномочиями администратора безопасности сегмента (фрагмента) ИСПДн.

Лицо этой категории:

- обладает всеми возможностями лиц предыдущих категорий;
- обладает полной информацией о системном и прикладном программном обеспечении, используемом в сегменте (фрагменте) ИСПДн;
- обладает полной информацией о технических средствах и конфигурации сегмента (фрагмента) ИСПДн;
- имеет доступ к средствам защиты информации и протоколирования, а также к отдельным элементам, используемым в сегменте (фрагменте) ИСПДн;
- имеет доступ ко всем техническим средствам сегмента (фрагмента) ИСПДн;
- обладает правами конфигурирования и административной настройки некоторого подмножества технических средств сегмента (фрагмента) ИСПДн.

К пятой категории относятся зарегистрированные пользователи с полномочиями системного администратора ИСПДн.

Нарушитель этой категории:

- обладает всеми возможностями лиц предыдущих категорий;
- обладает полной информацией о системном и прикладном программном обеспечении ИСПДн;
- обладает полной информацией о технических средствах и конфигурации ИСПДн;
- имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн;
- обладает правами конфигурирования и административной настройки технических средств ИСПДн.

Системный администратор выполняет конфигурирование и управление программным обеспечением и оборудованием, включая оборудование, отвечающее за безопасность защищаемого объекта: средства

криптографической защиты информации, мониторинга, регистрации, архивации, защиты от НСД.

К шестой категории относятся зарегистрированные пользователи с полномочиями администратора безопасности ИСПДн.

Нарушитель этой категории:

- обладает всеми возможностями лиц предыдущих категорий;
- обладает полной информацией об ИСПДн;
- имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн;
- не имеет прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных).

К седьмой категории относятся разработчики (поставщики) прикладного программного обеспечения и лица, обеспечивающие его сопровождение на защищаемом объекте.

Лицо этой категории:

- обладает информацией об алгоритмах и программах обработки информации на ИСПДн;
- обладает возможностями внесения ошибок, недекларированных возможностей, программных закладок, вредоносных программ в программное обеспечение ИСПДн на стадии ее разработки, внедрения и сопровождения;
- может располагать любыми фрагментами информации о топологии ИСПДн и технических средствах обработки и защиты ПДн, обрабатываемых в ИСПДн.

К восьмой категории относятся разработчики и лица, обеспечивающие поставку, сопровождение и ремонт технических средств на ИСПДн.

Сотрудник этой категории:

- обладает возможностями внесения закладок в технические средства ИСПДн на стадии их разработки, внедрения и сопровождения;

- может располагать любыми фрагментами информации о топологии ИСПДн и технических средствах обработки и защиты информации в ИСПДн.

Указанные категории нарушителей должны учитываться при оценке возможностей реализации УБПДн.

Носителем вредоносной программы может быть аппаратный элемент компьютера или программный контейнер. Если вредоносная программа не ассоциируется с какой-либо прикладной программой, то в качестве ее носителя рассматриваются:

- отчуждаемый носитель, то есть дискета, оптический диск, флэш-память;
- встроенные носители информации (жесткие диски, микросхемы оперативной памяти, процессор, микросхемы системной платы, микросхемы устройств, встраиваемых в системный блок, – видеоадаптера, сетевой платы, звуковой платы, модема, устройств ввода/вывода магнитных жестких и оптических дисков, блока питания и т.п., микросхемы прямого доступа к памяти, шин передачи данных, портов ввода/вывода);
- микросхемы внешних устройств (монитора, клавиатуры, принтера, модема, сканера и т.п.).

Если вредоносная программа ассоциируется с какой-либо прикладной программой, с файлами, имеющими определенные расширения или иные атрибуты, с сообщениями, передаваемыми по сети, то ее носителями являются:

- пакеты передаваемых по компьютерной сети сообщений;
- файлы (текстовые, графические, исполняемые и т.д.).

Угрозы несанкционированного доступа в операционную среду компьютера и несанкционированного доступа к ПДн связаны с доступом:

- к информации и командам, хранящимся в базовой системе ввода/вывода ИСПДн, с возможностью перехвата управления

загрузкой операционной системы и получением прав доверенного пользователя;

- в операционную среду, то есть в среду функционирования локальной операционной системы отдельного технического средства ИСПДн с возможностью выполнения несанкционированного доступа путем вызова штатных программ операционной системы или запуска специально разработанных программ, реализующих такие действия;
- в среду функционирования прикладных программ (например, к локальной системе управления базами данных);
- непосредственно к информации пользователя (к файлам, текстовой, аудио- и графической информации, полям и записям в электронных базах данных) и обусловлены возможностью нарушения ее конфиденциальности, целостности и доступности.

Эти угрозы могут быть реализованы в случае получения физического доступа к ИСПДн или, по крайней мере, к средствам ввода информации в ИСПДн. Их можно объединить по условиям реализации на три группы.

Первая группа включает в себя угрозы, реализуемые в ходе загрузки операционной системы. Эти угрозы безопасности информации направлены на перехват паролей или идентификаторов, модификацию программного обеспечения базовой системы ввода/вывода, перехват управления загрузкой с изменением необходимой технологической информации для получения НСД в операционную среду ИСПДн. Чаще всего такие угрозы реализуются с использованием отчуждаемых носителей информации.

Вторая группа – угрозы, реализуемые после загрузки операционной среды независимо от того, какая прикладная программа запускается пользователем. Эти угрозы, как правило, направлены на выполнение непосредственно несанкционированного доступа к информации. При получении доступа в операционную среду нарушитель может воспользоваться как стандартными функциями операционной системы или

какой-либо прикладной программы общего пользования (например, системы управления базами данных), так и специально созданными для выполнения несанкционированного доступа программами, например:

- программами просмотра и модификации реестра;
- программами поиска текстов в текстовых файлах по ключевым словам и копирования;
- специальными программами просмотра и копирования записей в базах данных;
- программами быстрого просмотра графических файлов, их редактирования или копирования;
- программами поддержки возможностей реконфигурации программной среды (настройки ИСПДн в интересах нарушителя).

Наконец, третья группа включает в себя угрозы, реализация которых определяется тем, какая из прикладных программ запускается пользователем, или фактом запуска любой из прикладных программ. Большая часть таких угроз – это угрозы внедрения вредоносных программ.

Если ИСПДн реализована на базе локальной или распределенной информационной системы, то в ней могут быть реализованы угрозы безопасности информации путем использования протоколов межсетевого взаимодействия. При этом может обеспечиваться НСД к ПДн или реализовываться угроза отказа в обслуживания. Особенно опасны угрозы, когда ИСПДн представляет собой распределенную информационную систему, подключенную к сетям общего пользования и (или) сетям международного информационного обмена. Классификационная схема угроз, реализуемых по сети, приведена на рисунке 1.4. В ее основу положено семь следующих первичных признаков классификации.




Рисунок 1.4 Классификационная схема угроз с использованием протоколов межсетевого взаимодействия.

1. Характер угрозы. По этому признаку угрозы могут быть пассивные и активные. Пассивная угроза – это угроза, при реализации которой не оказывается непосредственное влияние на работу ИСПДн, но могут быть нарушены установленные правила разграничения доступа к ПДн или сетевым ресурсам. Примером таких угроз является угроза «Анализ сетевого трафика», направленная на прослушивание каналов связи и перехват передаваемой информации. Активная угроза – это угроза, связанная с воздействием на ресурсы ИСПДн, при реализации которой оказывается непосредственное влияние на работу системы (изменение конфигурации, нарушение работоспособности и т.д.), и с нарушением установленных правил разграничения доступа к ПДн или сетевым ресурсам. Примером таких угроз является угроза «Отказ в обслуживании», реализуемая как «шторм TCP-запросов».

2. Цель реализации угрозы. По этому признаку угрозы могут быть направлены на нарушение конфиденциальности, целостности и доступности информации (в том числе на нарушение работоспособности ИСПДн или ее элементов).

3. Условие начала осуществления процесса реализации угрозы. По этому признаку может реализовываться угроза:

- по запросу от объекта, относительно которого реализуется угроза. В этом случае нарушитель ожидает передачи запроса определенного типа, который и будет условием начала осуществления несанкционированного доступа;
- по наступлению ожидаемого события на объекте, относительно которого реализуется угроза. В этом случае нарушитель осуществляет постоянное наблюдение за состоянием операционной системы ИСПДн и при возникновении определенного события в этой системе начинает несанкционированный доступ;

- безусловное воздействие. В этом случае начало осуществления несанкционированного доступа безусловно по отношению к цели доступа, то есть угроза реализуется немедленно и безотносительно к состоянию системы.

4. Наличие обратной связи с ИСПДн. По этому признаку процесс реализации угрозы может быть с обратной связью и без обратной связи. Угроза, осуществляемая при наличии обратной связи с информационной системой персональных данных, характеризуется тем, что на некоторые запросы, переданные на ИСПДн, нарушителю требуется получить ответ. Следовательно, между нарушителем и информационной системой персональных данных существует обратная связь, которая позволяет нарушителю адекватно реагировать на все изменения, происходящие в ИСПДн. В отличие от угроз, реализуемых при наличии обратной связи с информационной системой персональных данных, при реализации угроз без обратной связи не требуется реагировать на какие-либо изменения, происходящие в ИСПДн.

5. Расположение нарушителя относительно ИСПДн. В соответствии с этим признаком угроза реализуется как внутрисегментно, так и межсегментно.

Сегмент сети – физическое объединение хостов (технических средств ИСПДн или коммуникационных элементов, имеющих сетевой адрес). Например, сегмент информационной системой персональных данных образует совокупность хостов, подключенных к серверу по схеме «общая шина». В случае, когда имеет место внутрисегментная угроза, нарушитель имеет физический доступ к аппаратным элементам ИСПДн. Если имеет место межсегментная угроза, то нарушитель располагается вне ИСПДн, реализуя угрозу из другой сети или из другого сегмента информационной системой персональныхданных.

6. Уровень эталонной модели взаимодействия открытых систем (ISO/OSI), на котором реализуется угроза. По этому признаку угроза может реализовываться на физическом, канальном, сетевом, транспортном, сеансовом, представительном и прикладном уровне модели ISO/OSI.

7. Соотношение количества нарушителей и элементов ИСПДн, относительно которых реализуется угроза. По этому признаку угроза может быть отнесена к классу угроз, реализуемых одним нарушителем относительно одного технического средства ИСПДн (угроза «один к одному»), сразу относительно нескольких технических средств ИСПДн (угроза «один ко многим») или несколькими нарушителями с разных компьютеров относительно одного или нескольких технических средств ИСПДн (распределенные или комбинированные угрозы).

С учётом проведённой классификации выделим основные типы атак на информационную систему персональныхданных:

1. Анализ сетевого трафика.

Эта угроза реализуется с помощью специального программного обеспечения-анализатора пакетов, перехватывающей все пакеты, передаваемые по сегменту сети, и выделяющей среди них те, в которых передаются идентификатор пользователя и его пароль. В ходе реализации угрозы нарушитель изучает логику работы сети – то есть стремится получить однозначное соответствие событий, происходящих в системе, и команд, пересылаемых при этом хостами, в момент появления данных событий. В дальнейшем это позволяет злоумышленнику на основе задания соответствующих команд получить, привилегированные права на действия в системе или расширить свои полномочия в ней, перехватить поток передаваемых данных, которыми обмениваются компоненты сетевой операционной системы, для извлечения конфиденциальной или идентификационной информации, ее подмены и модификации.

2. Сканирование сети.

Сущность процесса реализации угрозы заключается в передаче запросов сетевым службам хостов ИСПДн и анализе ответов от них. Цель – выявление используемых протоколов, доступных портов сетевых служб, законов формирования идентификаторов соединений, определение активных сетевых сервисов, подбор идентификаторов и паролей пользователей.

3. Угроза выявления пароля.

Цель реализации угрозы состоит в получении НСД путем преодоления парольной защиты. Злоумышленник может реализовывать угрозу с помощью целого ряда методов, таких как простой перебор, перебор с использованием специальных словарей, установка вредоносной программы для перехвата пароля, подмена доверенного объекта сети и перехват пакетов. В основном для реализации угрозы используются специальные программы, которые пытаются получить доступ к хосту путем последовательного подбора паролей. В случае успеха, злоумышленник может создать для себя точку входа для будущего доступа, который будет действовать, даже если на хосте изменить пароль доступа.

4. Подмена доверенного объекта сети и передача по каналам связи сообщений от его имени с присвоением его прав доступа.

Такая угроза эффективно реализуется в системах, где применяются нестойкие алгоритмы идентификации и аутентификации хостов и пользователей. Под доверенным объектом понимается объект сети (компьютер, межсетевой экран, маршрутизатор и т.п.), легально подключенный к серверу. Могут быть выделены две разновидности процесса реализации указанной угрозы: с установлением и без установления виртуального соединения. Процесс реализации с установлением виртуального соединения состоит в присвоении прав доверенного субъекта взаимодействия, что позволяет нарушителю вести сеанс работы с объектом сети от имени доверенного субъекта. Реализацияугрозы данного типа требует преодоления системы идентификации и аутентификации сообщений.

Процесс реализации угрозы без установления виртуального соединения может иметь место в сетях, осуществляющих идентификацию передаваемых сообщений только по сетевому адресу отправителя. Сущность заключается в передаче служебных сообщений от имени сетевых управляющих устройств (например, от имени маршрутизаторов) об изменении маршрутно-адресных данных.

В результате реализации угрозы нарушитель получает права доступа, установленные пользователем для доверенного абонента, к техническому средству ИСПДн .

5. Навязывание ложного маршрута сети.

Данная угроза реализуется одним из двух способов: путем внутрисегментного или межсегментного навязывания. Возможность навязывания ложного маршрута обусловлена недостатками, присущими алгоритмам маршрутизации (в частности, из-за проблемы идентификации сетевых управляющих устройств), в результате чего можно попасть, например, на хост или в сеть злоумышленника, где можно войти в операционную среду технического средства в составе ИСПДн. Реализация угрозы основывается на несанкционированном использовании протоколов маршрутизации и управления сетью для внесения изменений в маршрутно-адресные таблицы. При этом нарушителю необходимо послать от имени сетевого управляющего устройства (например, маршрутизатора) управляющее сообщение.

6. Внедрение ложного объекта сети.

Эта угроза основана на использовании недостатков алгоритмов удаленного поиска. В случае, если объекты сети изначально не имеют адресной информации друг о друге, используются различные протоколы удаленного поиска, заключающиеся в передаче по сети специальных запросов и получении на них ответов с искомой информацией. При этом существует возможность перехвата нарушителем поискового запроса и выдачи на него ложного ответа, использование которого приведет к

требуемому изменению маршрутно-адресных данных. В дальнейшем весь поток информации, ассоциированный с объектом-жертвой, будет проходить через ложный объект сети

7. Отказ в обслуживании.

Эти угрозы основаны на недостатках сетевого программного обеспечения, его уязвимостях, позволяющих нарушителю создавать условия, когда операционная система оказывается не в состоянии обрабатывать поступающие пакеты. Могут быть выделены несколько разновидностей такихугроз:

- скрытый отказ в обслуживании, вызванный привлечением части ресурсов ИСПДн на обработку пакетов, передаваемых злоумышленником со снижением пропускной способности каналов связи, производительности сетевых устройств, нарушением требований ко времени обработки запросов. Примерами реализации угроз подобного рода могут служить: направленный шторм эхо-запросов по протоколу ICMP, шторм запросов на установление TCP-соединений, шторм запросов к FTP-серверу;
- явный отказ в обслуживании, вызванный исчерпанием ресурсов ИСПДн при обработке пакетов, передаваемых злоумышленником (занятие всей полосы пропускания каналов связи, переполнение очередей запросов на обслуживание), при котором легальные запросы не могут быть переданы через сеть из-за недоступности среды передачи либо получают отказ в обслуживании ввиду переполнения очередей запросов, дискового пространства памяти и т.д. Примерами угроз данного типа могут служить шторм широковещательных ICMP-эхо-запросов, направленный шторм, шторм сообщений почтовому серверу;

- явный отказ в обслуживании, вызванный нарушением логической связности между техническими средствами ИСПДн при передаче нарушителем управляющих сообщений от имени сетевых устройств, приводящих к изменению маршрутно-адресных данных или идентификационной и аутентификационной информации;
- явный отказ в обслуживании, вызванный передачей злоумышленником пакетов с нестандартными атрибутами или имеющих длину, превышающую максимально допустимый размер, что может привести к сбою сетевых устройств, участвующих в обработке запросов, при условии наличия ошибок в программах, реализующих протоколы сетевого обмена.

  Результатом реализации данной угрозы может стать нарушение работоспособности соответствующей службы предоставления удаленного доступа к ПДн в ИСПДн, передача с одного адреса такого количества запросов на подключение к техническому средству в составе ИСПДн, какое максимально может обработать трафик, что влечет за собой переполнение очереди запросов и отказ одной из сетевых служб или полную остановку компьютера из-за невозможности системы заниматься ничем другим, кроме обработки запросов.

8. Удалённый запуск приложений.

Угроза заключается в стремлении запустить на хосте ИСПДн различное предварительно внедренное вредоносные программное обеспечение: программы-закладки, вирусы, «сетевые шпионы», основная цель которого – нарушение конфиденциальности, целостности, доступности информации и полный контроль за работой хоста. Кроме того, возможен несанкционированный запуск прикладных программ пользователей для несанкционированного получения необходимых нарушителю данных, для

запуска управляемых прикладной программой процессов и др. Выделяют три подкласса данныхугроз:

- распространение файлов, содержащих несанкционированный исполняемый код;
- удаленный запуск приложения путем переполнения буфера приложений-серверов;
- удаленный запуск приложения путем использования возможностей удаленного управления системой, предоставляемых скрытыми программными и аппаратными закладками либо используемыми штатными средствами.

Типовые угрозы первого из указанных подклассов основываются на активизации распространяемых файлов при случайном обращении к ним. Примерами таких файлов могут служить: файлы, содержащие исполняемый код в виде макрокоманд (документы Microsoft Word, Excel), html-документы, содержащие исполняемый код в виде элементов ActiveX, Java-апплетов, интерпретируемых скриптов (например, вредоносное ПО на JavaScript); файлы, содержащие исполняемые коды программ.

Для распространения файлов могут использоваться службы электронной почты, передачи файлов, сетевой файловой системы.

При угрозах второго подкласса используются недостатки программ, реализующих сетевые сервисы (в частности, отсутствие контроля переполнения буфера). Настройкой системных регистров иногда удается переключить процессор после прерывания, вызванного переполнением буфера, на исполнение кода, содержащегося за границей буфера.

При угрозах третьего подкласса нарушитель использует возможности удаленного управления системой, предоставляемые скрытыми компонентами либо штатными средствами управления и администрирования компьютерных сетей. В результате их использования удается добиться удаленного контроля над станцией в сети. Схематично основные этапы работы этих программ

выглядят следующим образом: инсталляция в памяти; ожидание запроса с удаленного хоста, на котором запущена клиент- программа, и обмен с ней сообщениями о готовности; передача перехваченной информации клиенту или предоставление ему контроля над атакуемым компьютером. Возможные последствия от реализацииугроз различных классов приведены в таблице 1.1.

Таблица 1.1. Возможные последствия реализацииугроз различных классов.

| № п/п | Тип атаки | | Возможные последствия |
|---|---|---|---|
| 1 | Анализ сетевого трафика | | Исследование характеристик сетевого трафика, перехват передаваемых данных, в том числе идентификаторов и паролей пользователей |
| 2 | Сканирование сети | | Определение протоколов, доступных портов сетевых служб, законов формирования идентификаторов соединений, активных сетевых сервисов, идентификаторов и паролей пользователей |
| 3 | «Парольная» атака | | Выполнение любого деструктивного действия, связанного с получением несанкционированного доступа |
| 4 | Подмена доверенного объекта сети | | Изменение трассы прохождения сообщений, несанкционированное изменение маршрутно-адресных данных. Несанкционированный доступ к сетевым ресурсам, навязывание ложной информации |
| 5 | Навязывание ложного маршрута | | Несанкционированное изменение маршрутно-адресных данных, анализ и модификация передаваемых данных, навязывание ложных сообщений |
| 6 | Внедрение ложного объекта сети | | Перехват и просмотр трафика. Несанкционированный доступ к сетевым ресурсам, навязывание ложной информации |
| 7 | Отказ в обслуживании | Частичное исчерпание ресурсов | Снижение пропускной способности каналов связи, производительности сетевых устройств. Снижение производительности серверных приложений. |
| | | Полное исчерпание ресурсов | Невозможность передачи сообщений из-за отсутствия доступа к среде передачи, отказ в установлении соединения. Отказ в предоставлении сервиса. |
| | | Нарушение логической связанности между атрибутами, данными, объектами | Невозможность передачи сообщений из-за отсутствия корректных маршрутно-адресных данных. Невозможность получения услуг ввиду несанкционированной модификации идентификаторов, паролей и т.п. |
| | | Использование ошибок в программах | Нарушение работоспособности сетевых устройств. |

| | | | |
|---|---|---|---|
| 8 | Удалённый запуск приложений | Путём рассылки файлов, содержащих деструктивный исполняемы код, вирусное заражение. | Нарушение конфиденциальности, целостности, доступности информации. |
| | | Путём переполнения буфера серверного приложения | |
| | | Путём использования возможностей удалённого управления системой, предоставляемых скрытыми программными и аппаратными закладками либо используемыми штатными средствами | Скрытое управление системой. |

Процесс реализации угрозы в общем случае состоит из четырех этапов:

- сбора информации;
- вторжения (проникновения в операционную среду);
- осуществления несанкционированного доступа;
- ликвидации следов несанкционированного доступа.

На этапе сбора информации нарушителя могут интересовать различные сведения об ИСПДн, в том числе:

- о топологии сети, в которой функционирует система. При этом может исследоваться область вокруг сети (например, нарушителя могут интересовать адреса доверенных, но менее защищенных хостов). Существуют утилиты, осуществляющие параллельное определение доступности хостов, которые способны просканировать большую область адресного пространства на предмет доступности хостов за короткий промежуток времени.;
- о типе операционной системы (ОС) в ИСПДн. Можно отметить метод определения типа ОС, как простейший запрос на установление соединения по протоколу удаленного доступа Telnet, в результате которого по «внешнему виду» ответа можно определить тип ОС хоста. Наличие определенных сервисов также

может служить дополнительным признаком для определения типа ОС хоста;

- о функционирующих на хостах сервисах. Определение сервисов, исполняемых на хосте, основано на методе выявления «открытых портов», направленном на сбор информации о доступности хоста.

На этапе вторжения исследуется наличие типовых уязвимостей в системных сервисах или ошибок в администрировании системы. Успешным результатом использования уязвимостей обычно является получение процессом нарушителя привилегированного режима выполнения (доступа к привилегированному режиму выполнения процессора), внесение в систему учетной записи незаконного пользователя, получение файла паролей или нарушение работоспособности атакуемого хоста.

Этот этап развития угрозы, как правило, является многофазным. К фазам процесса реализации угрозы могут относиться, например: установление связи с хостом, относительно которого реализуется угроза; выявление уязвимости; внедрение вредоносной программы в интересах расширения прав и др.

Угрозы, реализуемые на этапе вторжения, подразделяются по уровням стека протоколов TCP/IP, поскольку формируются на сетевом, транспортном или прикладном уровне в зависимости от используемого механизма вторжения. К типовым угрозам, реализуемым на сетевом и транспортном уровнях, относятся такие как:

- угроза, направленная на подмену доверенного объекта;
- угроза, направленная на создание в сети ложного маршрута;
- угрозы, направленные на создание ложного объекта с использованием недостатков алгоритмов удаленного поиска;
- угрозы типа «отказ в обслуживании».

К типовым угрозам, реализуемым на прикладном уровне, относятся угрозы, направленные на несанкционированный запуск приложений, угрозы,

реализация которых связана с внедрением программных закладок, с выявлением паролей доступа в сеть или к определенному хосту и т.д. Если реализация угрозы не принесла нарушителю наивысших прав доступа в системе, возможны попытки расширения этих прав до максимально возможного уровня. Для этого могут использоваться уязвимости не только сетевых сервисов, но и уязвимости системного программного обеспечения хостов ИСПдн.

На этапе реализации несанкционированного доступа осуществляется достижение цели реализацииугрозы:

- нарушение конфиденциальности (копирование, неправомерное распространение);
- нарушение целостности (уничтожение, изменение);
- нарушение доступности (блокирование).

На этом же этапе, после указанных действий, как правило, формируется так называемый «черный вход» в виде одного из сервисов, обслуживающих некоторый порт и выполняющих команды нарушителя. «Черный вход» оставляется в системе в интересах обеспечения: возможности получить доступ к хосту, даже если администратор устранит использованную для успешной реализации угрозы уязвимость; возможности получить доступ к хосту как можно более скрытно; возможности получить доступ к хосту быстро (не повторяя заново процесс реализации угрозы). «Черный вход» позволяет нарушителю внедрить в сеть или на определенный хост вредоносную программу, например, «анализатор паролей» – программу, выделяющую пользовательские идентификаторы и пароли из сетевого трафика при работе протоколов высокого уровня). Объектами внедрения вредоносных программ могут быть программы аутентификации и идентификации, сетевые сервисы, ядро операционной системы, файловая система, библиотеки и т.д.

Наконец, на этапе ликвидации следов реализации угрозы осуществляется попытка уничтожения следов действий нарушителя. При этом удаляются соответствующие записи из всех возможных журналов аудита, в том числе записи о факте сбора информации.

### 1.2.4. Оценка существующих и планируемых средств защиты

Анализ показал, что основными составляющими обеспечения безопасности ООО «ПК Венткомплекс» объектов являются:

- система физической защиты (безопасности) материальных объектов и финансовых ресурсов;
- система безопасности информационных ресурсов.

К защищаемым объектам ООО «ПК Венткомплекс» относят:

- финансовые средства, материальные ценности (здания, сооружения, хранилища, техническое оборудование, транспорт и иные средства);
- информационные ресурсы (информация с ограниченным доступом, составляющая коммерческую тайну, иная конфиденциальная информация, предоставленная в виде документов независимо от формы и вида их представления).

Каждому объекту защиты соответствует некоторые виды угроз безопасности. Целью угроз финансовым средствам и материальным ценностям является нанесение серьезного материального ущерба и срыв на длительное время нормального функционирования. Основная угроза финансовым средствам и материальным ценностям - хищение, повреждение, уничтожение.

В отношении зданий и помещений угрозы проявляются в виде:

- пожаров, поджогов, затоплений;
- технологических аварий и повреждений;
- повреждения входных дверей, решеток, ограждений, личных и служебных транспортных средств.

Угрозы информационным ресурсам:

- разглашения конфиденциальной информации;
- несанкционированного доступа к охраняемым сведениям;
- утечки конфиденциальной информации через технические средства обеспечения производственной деятельности различного характера и исполнения.

Далее проанализируем риски и составим модель нарушителя ООО «ПК Венткомплекс».

В качестве исходных данных для разработки модели нарушителя ООО «ПК Венткомплекс» определим:

- предположения о категориях лиц, к которым может принадлежать нарушитель;
- предположения о мотивах действий нарушителя;
- предположения о квалификации нарушителя и его технической оснащенности;
- ограничения и предположения о характере возможных действий нарушителей.

Построим модель предполагаемого нарушителя (таблица 1.2).

Таблица 1.2 - Модель нарушителя ООО «ПК Венткомплекс».

| Уровень | Положение | Возможности нарушителя | Потенциальная группа нарушителей |
|---|---|---|---|
| 1 | внутренний | Не имеет физического доступа к финансовым ценностям, материальным носителям с конфиденциальной информацией, имеет доступ к материальным ценностям | Рабочие ремонтного, механического, транспортного участка, вспомогательный персонал (например, грузчики) и т.п. |

| Уровень | Положение | Возможности нарушителя | Потенциальная группа нарушителей |
|---|---|---|---|
| 2 | внутренний | Имеет физический доступ к материальным носителям с конфиденциальной информацией и материальным ценностям | Конструкторы, технологи, и т.п. |
| 3 | внутренний | Имеет физический доступ к финансовым ценностям, материальным носителям с конфиденциальной информацией и материальным ценностям | Руководство, финансово-экономический отдел, отдел снабжения |
| 4 | внешний | Не имеет физического доступа на территорию предприятия, но оснащен средствами и для его осуществления, профессиональными знаниями в области охранной сигнализации не обладает | Преступник – дилетант |

| Уровень | Положение | Возможности нарушителя | Потенциальная группа нарушителей |
|---|---|---|---|
| 5 | внешний | Не имеет физического доступа на территорию предприятия, но оснащен средствами для его осуществления, обладает профессиональными знаниями в области физической защиты | Преступные организации, конкуренты |

Итак, в соответствии с данными таблицы 1.2, на безопасность предприятия ООО «ПК Венткомплекс» могут посягать нарушители пяти уровней.

Учитывая модель нарушителя при анализе рисков будем рассматривать следующие угрозы:

- техногенные:
  - пожар/поджег;
  - взрыв;
  - затопление помещений;
- технологические:
  - вывод из строя производственной техники;
- по отношению к информационным ресурсам:
  - хищение;
  - искажение;
  - уничтожение;
- по отношению к готовой продукции:
  - хищение;

- повреждение;
- уничтожение;

- по отношению к материалам:
  - хищение;
  - повреждение;
  - уничтожение.

Данные типы угроз являются основными в рамках темы диплома.

### 1.2.5. Оценка рисков

Под угрозой информационной безопасности понимается угроза нарушения свойств информационной безопасности – доступности, целостности или конфиденциальности информационных активов организации.

Перечень угроз, оценка вероятности их реализации, а также модель нарушителя служат основой для анализа риска реализации угроз и формулирования требований к системе защиты автоматизированной системы. Кроме выявления возможных угроз, необходимо провести анализ выявленных угроз на основе их классификации по ряду признаков. Угрозы, соответствующие каждому признаку классификации, позволяют детализировать отражаемое этим признаком требование.

Так как хранимая и обрабатываемая информация в современных АС подвержена воздействию чрезвычайно большого числа факторов, то становится невозможным формализовать задачу описания полного множества угроз. Поэтому для защищаемой системы обычно определяется не перечень угроз, а перечень классов угроз.

Классификация возможных угроз информационной безопасности АС может быть проведена по следующим базовым признакам:

- По природе возникновения:

1. естественные угрозы, вызванные воздействиями на АС объективных физических процессов или стихийных природных явлений;
2. искусственные угрозы безопасности АС, вызванные деятельностью человека.

- По степени преднамеренности проявления:

1. угрозы, вызванные ошибками или халатностью персонала, например неправильное использование средств защиты, халатность при работе с данными;
2. угрозы преднамеренного действия, например взлом автоматизированной системы злоумышленниками, уничтожение данных работниками организации с целью мести работодателю.

- По непосредственному источнику угроз:

1. естественные угрозы, например стихийные бедствия, техногенные катастрофы;
2. человеческие угрозы, например: уничтожение информации, разглашение конфиденциальных данных;
3. разрешенные программно-аппаратные средства, например физическая поломка аппаратуры, ошибки программного обеспечения, конфликты программного обеспечения;
4. неразрешённые программно-аппаратные средства, например внедрение аппаратных закладок, программных закладок.

- По положению источника угроз:

1. вне контролируемой зоны, например перехват данных, передаваемых по каналам связи;
2. в пределах контролируемой зоны, например несанкционированное копирование информации, несанкционированный доступ в защищаемую зону;
3. непосредственно в автоматизированной системе, например некорректное использование ресурсовАС.

- По степени зависимости от активностиАС:

1. независимо от активности АС, например физическая кража носителей информации;
2. только в процессе обработки данных, например заражение вредоносным ПО.

- По степени воздействия наАС:

1. пассивные угрозы, которые при реализации ничего не меняют в структуре и содержании АС, например угроза копирования секретных данных;
2. активные угрозы, которые при воздействии вносят изменения в структуру и содержание АС, например удаление данных, их модификация.

- По этапам доступа пользователей или программ к ресурсам:

1. угрозы, проявляющиеся на этапе доступа к ресурсам АС, например: угрозы несанкционированного доступа вАС;
2. угрозы, проявляющиеся после разрешения доступа к ресурсам АС, например некорректное использование ресурсовАС.

- По способу доступа к ресурсамАС:

1. угрозы, осуществляемые с использованием стандартного пути доступа к ресурсамАС
2. угрозы, осуществляемые с использованием скрытого нестандартного пути доступа к ресурсам АС, например: несанкционированный доступ к ресурсам АС путем использования недокументированных возможностей установленного ПО.

- По текущему месту расположения информации, хранимой и обрабатываемой вАС:

1. угрозы доступа к информации, находящейся на внешних запоминающих устройствах, например: копирование конфиденциальной информации с носителей информации;
2. угрозы доступа к информации, находящейся в оперативной памяти, например: чтение остаточной информации из оперативной памяти, доступ к системной области оперативной памяти со стороны прикладных программ;
3. угрозы доступа к информации, циркулирующей в линиях связи, например: незаконное подключение к линиям связи с целью снятия информации, отправка модифицированных данных;

Опасные воздействия на автоматизированную систему подразделяются на случайные и преднамеренные.

Причинами случайных воздействий при эксплуатацииАС могут быть:

- аварийные ситуации из-за стихийных бедствий и отключений электропитания;
- отказы в обслуживании;
- ошибки в программном обеспечении;
- ошибки в работе обслуживающего персонала и пользователей;
- помехи в линиях связи из-за воздействий внешней среды.

Использование ошибок в программном обеспечении является самым распространённым способом нарушения информационной безопасности информационных систем. В зависимости от сложности ПО, количество ошибок возрастает. Злоумышленники могут находить эти уязвимости и через них получать доступ в информационную систему организации. Чтобы минимизировать эти угрозы необходимо постоянно поддерживать актуальность версий программного обеспечения.

Преднамеренные угрозы связаны с целенаправленными действиями злоумышленников. Злоумышленники разделяются на два типа: внутренний злоумышленник и внешний злоумышленник. Внутренний злоумышленник совершает противоправные действия находясь в пределах контролируемой

зоны автоматизированной системы и может пользоваться должностными полномочиями для санкционированного доступа к автоматизированной системе. Внешний злоумышленник не имеет доступа в пределы контролируемой зоны, но может действовать одновременно с внутренним злоумышленником для достижения своих целей.

Существует три основных угрозы безопасности информации, направленных непосредственно на защищаемую информацию:

Нарушение конфиденциальности – конфиденциальная информация не изменяется, но становится доступна третьим лицам, не допущенным к это информации. При реализации этой угрозы существует большая вероятность разглашения злоумышленником украденной информации, что может повлечь за собой финансовый или репутационный вред. Нарушение целостности защищаемой информации – искажение, изменение или уничтожение информации. Целостность информации может быть нарушена не умышленно, а в следствии некомпетентности или халатности сотрудника предприятия. Так же целостность может быть нарушена злоумышленником для достижения собственных целей. Например, изменение реквизитов счетов в автоматизированной системе с целью перевода денежных средств на счёт злоумышленника или подмена персональных данных клиента организации для получения информации о сотрудничестве клиента с организацией.

Нарушение доступности защищаемой информации или отказ в обслуживании – действия, при которых авторизованный пользователь не может получить доступ к защищаемой информации в следствии таких причин как: отказ аппаратуры, программного обеспечения, выхода из строя локальной вычислительной сети.

После рассмотрения угроз автоматизированных систем можно перейти к анализу угроз информационной системы персональныхданных.

Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Информационные системы персональных данных представляют собой совокупность информационных и программно-аппаратных элементов, а также информационных технологий, применяемых при обработке персональныхданных.

Основными элементами ИСПДн являются:

- персональные данные, содержащиеся в базах данных;
- информационные технологии, применяемые при обработке ПДн;
- технические средства, осуществляющие обработку персональных данных (средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных, средства и системы звукозаписи, звукоусиления, звуковоспроизведения, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации);
- программные средства (операционные системы, системы управле-ния базами данных и т.п.);
- средства защиты информации ИСПДн;
- вспомогательные технические средства и системы – технические средства и системы, их коммуникации, не предназначенные для обработки персональныхданных, но размещенные в помещениях, в которых расположены ИСПДн.

Угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение

персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

Состав и содержание УБПДн определяется совокупностью условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к ПДн. Совокупность таких условий и факторов формируется с учетом характеристик ИСПДн, свойств среды (пути) распространения информативных сигналов, содержащих защищаемую информацию, и возможностей источников угрозы.

К характеристикам информационной системы персональных данных, обусловливающим возникновение УБПДн, можно отнести категорию и объем обрабатываемых в информационной системе персональных данных персональных данных, структуру информационной системы персональных данных, наличие подключений ИСПДн к сетям связи общего пользования и (или) сетям международного информационного обмена, характеристики подсистемы безопасности персональных данных, обрабатываемых в ИСПДн, режимы обработки персональных данных, режимы разграничения прав доступа пользователей ИСПДн, местонахождение и условия размещения технических средств ИСПДн.

Свойства среды распространения информативных сигналов, содержащих защищаемую информацию, характеризуются видом физической среды, в которой распространяются ПДн, и определяются при оценке возможности реализации УБПДн. Возможности источников УБПДн обусловлены совокупностью способов несанкционированного и (или) случайного доступа к ПДн, в результате которого возможно нарушение конфиденциальности (копирование, неправомерное распространение), целостности (уничтожение, изменение) и доступности (блокирование) ПДн.

Угроза безопасности персональных данных реализуется в результате образования канала реализации УБПДн между источником угрозы и

носителем (источником) ПДн, что создает условия для нарушения безопасности ПДн.

Основными элементами канала реализации УБПДн (рисунок 1) являются:

- источник УБПДн – субъект, материальный объект или физическое явление, создающие УБПДн;
- среда распространения ПДн или воздействий, в которой физическое поле, сигнал, данные или программы могут распространяться и воздействовать на защищаемые свойства персональныхданных;
- носитель персональных данных – физическое лицо или материальный объект, в том числе физическое поле, в котором ПДн находят свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.




Рисунок 1.5 Обобщенная схема канала реализации угроз безопасности персональныхданных.

Носители ПДн могут содержать информацию, представленную в следующих видах:

- акустическая (речевая) информация, содержащаяся непосредственно в произносимой речи пользователя ИСПДн при осуществлении им функции голосового ввода ПДн в

информационной системе персональных данных, либо воспроизводимая акустическими средствами ИСПДн (если такие функции предусмотрены технологией обработки ПДн), а также содержащаяся в электромагнитных полях и электрических сигналах, которые возникают за счет преобразований акустической информации;

- видовая информация (ВИ), представленная в виде текста и изображений различных устройств отображения информации средств вычислительной техники, информационно-вычислительных комплексов, технических средств обработки графической, видео- и буквенно-цифровой информации, входящих в состав ИСПДн;
- информация, обрабатываемая (циркулирующая) в ИСПДн, в виде электрических, электромагнитных, оптических сигналов;
- информация, обрабатываемая в ИСПДн, представленная в виде бит, байт, файлов и других логических структур.

В целях формирования систематизированного перечня УБПДн при их обработке в ИСПДн и разработке на их основе частных моделей применительно к конкретному виду ИСПДн угрозы классифицируются в соответствии со следующими признаками (рисунок 2):

- по виду защищаемой от УБПДн информации, содержащей ПДн;
- по видам возможных источников УБПДн;
- по типу ИСПДн, на которые направлена реализация УБПДн;
- по способу реализации УБПДн;
- по виду нарушаемого свойства информации (виду несанкционированных действий, осуществляемых с ПДн);
- по используемой уязвимости;
- по объекту воздействия.

По видам возможных источников УБПДн выделяются следующие классы угроз:

- угрозы, связанные с преднамеренными или непреднамеренными действиями лиц, имеющих доступ к ИСПДн, включая пользователей информационной системы персональных данных, реализующих угрозы непосредственно в ИСПДн (внутренний нарушитель);
- угрозы, связанные с преднамеренными или непреднамеренными действиями лиц, не имеющих доступа к ИСПДн, реализующих угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена (внешний нарушитель).

Кроме того, угрозы могут возникать в результате внедрения аппаратных закладок и вредоносных программ.

По типу ИСПДн, на которые направлена реализация УБПДн, выделяются следующие классы угроз:

- УБПДн, обрабатываемых в ИСПДн на базе автономного автоматизированного рабочего места (АРМ);
- УБПДн, обрабатываемых в ИСПДн на базе АРМ, подключенного к сети общего пользования (к сети международного информационного обмена);
- УБПДн, обрабатываемых в ИСПДн на базе локальных информационных систем без подключения к сети общего пользования (к сети международного информационного обмена);
- УБПДн, обрабатываемых в ИСПДн на базе локальных информационных систем с подключением к сети общего пользования (к сети международного информационного обмена);
- УБПДн, обрабатываемых в ИСПДн на базе распределенных информационных систем без подключения к сети общего пользования (к сети международного информационного обмена);

- УБПДн, обрабатываемых в ИСПДн на базе распределенных информационных систем с подключением к сети общего пользования (к сети международного информационного обмена).

По способам реализации УБПДн выделяются следующие классы угроз:

- угрозы, связанные с НСД к ПДн (в том числе угрозы внедрения вредоносных программ);
- угрозы утечки персональных данных по техническим каналам утечки информации;
- угрозы специальных воздействий на ИСПДн.

По виду несанкционированных действий, осуществляемых с ПДн, выделяются следующие классы угроз:

- угрозы, приводящие к нарушению конфиденциальности ПДн (копированию или несанкционированному распространению), при реализации которых не осуществляется непосредственного воздействия на содержание информации;
- угрозы, приводящие к несанкционированному, в том числе случайному, воздействию на содержание информации, в результате которого осуществляется изменение ПДн или их уничтожение;
- угрозы, приводящие к несанкционированному, в том числе случайному, воздействию на программные или программно-аппаратные элементы ИСПДн, в результате которого осуществляется блокирование ПДн.
- По используемой уязвимости выделяются следующие классы угроз:
- угрозы, реализуемые с использованием уязвимости системного ПО;
- угрозы, реализуемые с использованием уязвимости прикладного ПО;

- угрозы, возникающие в результате использования уязвимости, вызванной наличием вАС аппаратной закладки;
- угрозы, реализуемые с использованием уязвимостей протоколов сетевого взаимодействия и каналов передачи данных;
- угрозы, возникающие в результате использования уязвимости, вызванной недостатками организации ТЗИ от НСД;
- угрозы, реализуемые с использованием уязвимостей, обусловливающих наличие технических каналов утечки информации;
- угрозы, реализуемые с использованием уязвимостей СЗИ.

По объекту воздействия выделяются следующие классы угроз:

- угрозы безопасности ПДн, обрабатываемых на АРМ;
- угрозы безопасности ПДн, обрабатываемых в выделенных средствах обработки (принтерах, плоттерах, графопостроителях, вынесенных мониторах, видеопроекторах, средствах звуковоспроизведения и т.п.);
- угрозы безопасности ПДн, передаваемых по сетям связи;
- угрозы прикладным программам, с помощью которых обрабатываются ПДн;
- угрозы системному ПО, обеспечивающему функционирование ИСПДн.

Реализация одной из УБПДн перечисленных классов или их совокупности может привести к следующим типам последствий для субъектов ПДн:

- значительным негативным последствиям для субъектов ПДн;
- негативным последствиям для субъектов ПДн;
- незначительным негативным последствиям для субъектов ПДн.

Угрозы утечки персональных данных по техническим каналам однозначно описываются характеристиками источника информации, среды

распространения и приемника информативного сигнала, то есть определяются характеристиками технического канала утечки ПДн.

Угрозы, связанные с несанкционированным доступом (НСД), представляются в виде совокупности обобщенных классов возможных источников угроз НСД, уязвимостей программного и аппаратного обеспечения ИСПДн, способов реализации угроз, объектов воздействия (носителей защищаемой информации, директориев, каталогов, файлов с ПДн или самих ПДн) и возможных деструктивных действий. Такое представление описывается следующей формализованной записью (рис. 1.3).

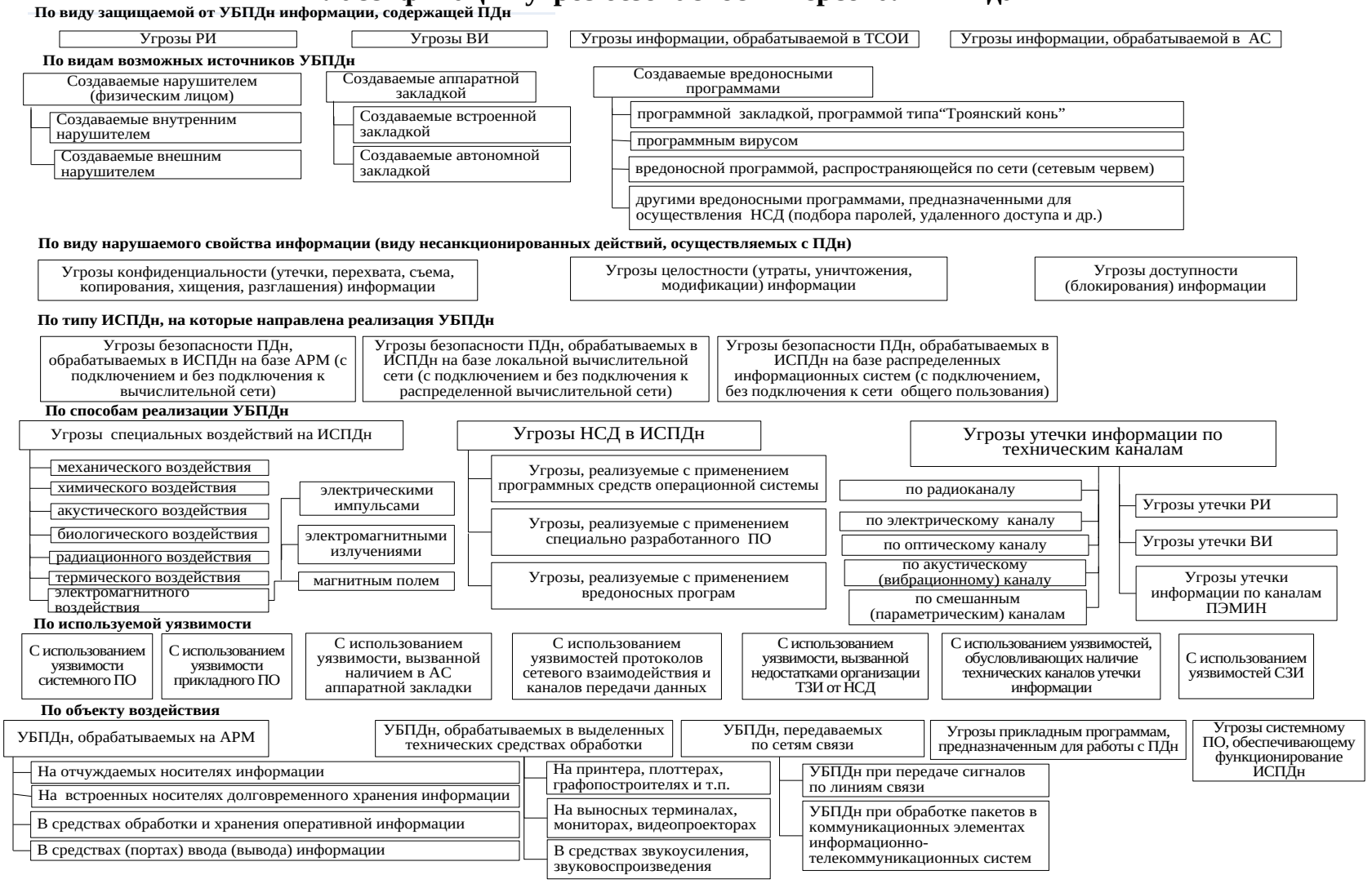



Рисунок 1.6. Классификация УБПДн, обрабатываемых в информационных системах персональных данных.

## 1.3. Характеристика комплекса задач, задачи и обоснование необходимости совершенствования системы обеспечения информационной безопасности и защиты информации ООО «ПК Венткомплекс»

### 1.3.1. Выбор комплекса задач обеспечения информационной безопасности.

После рассмотрения особенностей построения локальной сети ООО «ПК Венткомплекс», средств защиты персональных данных, организационных мер защиты персональных данных и самих информационных систем персональных данных была составлена базовая политика безопасности ООО «ПК Венткомплекс».

Политика безопасности в организации регламентирует:

- Систему повышения осведомленности сотрудников в вопросах информационной безопасности;
- Порядок доступа сотрудников к ресурсам сети Интернет;
- Порядок доступа сотрудников к внутренним ресурсам;
- Порядок работы сотрудников с электронной почтой;
- Парольную политику организации;
- Правила доступа сотрудников к персональным данным.

Система повышения осведомлённости сотрудников в вопросах информационной безопасности состоит из:

- Обучения сотрудников;
- Регулярном информировании сотрудников о новых угрозах информационной безопасности организации.

Обучение сотрудников проводится специалистом отдела информационной безопасности.

Сотрудник отдела информационной безопасности проводит обучение в определённом планом подразделении организации. После проведённого обучения, сотрудники подразделения проходят тесты, в которых подтверждают полученные на обучении знания.

Базовой политикой безопасности регламентируется проведение обучения в каждом подразделении не реже четырёх раз в год.

Так же параллельно с обучением сотрудников, сотрудники отдела информационной безопасности обязаны не реже раза в месяц рассылать всем сотрудникам информационные письма, в которых описываются основные правила безопасности, новые угрозы информационной безопасности, если такие обнаружены.

### 1.3.2. Определение места проектируемого комплекса задач в комплексе задач ООО «ПК Венткомплекс», детализация задач информационной безопасности и защиты информации.

В организации созданы 3 группы доступа в сеть Интернет, но такое разделение доступа неэффективно, поскольку у сотрудника, для выполнения его должностных обязанностей, может возникнуть потребность получить информацию с сетевого ресурса, входящего в группу полного доступа, тогда ему придётся давать полный доступ к сети Интернет, что небезопасно.

Для того, чтобы этого не происходило, было создано восемь групп доступа в сеть Интернет:

- Группа 1: минимальный доступ – доступ только к внешнему сайту ООО «ПК Венткомплекс». Все новые сотрудники по умолчанию добавляются в эту группу;
- Группа 2: федеральные службы – доступ к ресурсам группы 1 с добавлением ресурсов Федеральных служб Российской Федерации;
- Группа 3:расширенный доступ – доступ к ресурсом групп 1 и 2 и ресурсы не запрещённые в следующих группах;
- Группа 4: Социальные сети – доступ к социальным сетям;

- Группа 5: Мультимедийный контент – предоставление доступа к сайтам, содержащим мультимедийный контент, без этой группы весь мультимедийный контент даже на разрешённых ресурсах блокируется;
- Группа 6: скачивание архивов – группа не предоставляет какой-либо доступ к ресурсам сети Интернет;
- Группа 7: скачивание исполняемых файлов – группа не предоставляет какой-либо доступ к ресурсам сети Интернет;
- Группа 8: полный доступ в сеть Интернет – полный доступ к ресурсам сети Интернет, загрузка любых файлов.

Для получения доступа к ресурсам сети Интернет сотрудник создаёт заявку через систему ServiceDesk и после одобрения руководителем отдела или управления и сотрудником отдела информационной безопасности сотруднику предоставляется доступ к ресурсам сети Интернет согласно запрошенной группы.

Основные документы по работе сотрудника находятся на локальном рабочем месте или в автоматизированной системе, в которой он работает. Так же у каждого подразделения на файловом сервере организации существует раздел, в котором хранится информация, необходимая нескольким сотрудникам подразделения и которая велика по размеру для передачи по электронной почте.

Когда новый сотрудник устраивается на работу в в организацию, его прямой руководитель направляет заявку через систему ServiceDesk в отдел системного администрирования о предоставлении доступа к внутреннему ресурсу и после одобрения заявки сотрудником отдела информационной безопасности сотрудник отдела системного администрирования открывает новому сотруднику доступ к запрошенному ресурсу.

Нередко возникают ситуации, в которых работа нескольких подразделений пересекается и для обмена информацией этим подразделениям нужен отдельный на файловом сервере.

Для создания этого раздела руководитель проекта, начальник одного из отделов, задействованных в процессе работы над проектом создаёт заявку через систему ServiceDesk на создание общего ресурса и доступа к этому ресурсу определённых сотрудников своего подразделения, работающих над совместным проектом и начальника подразделения с которым сотрудничает в рамках проекта. После одобрения сотрудником отдела информации сотрудник отдела системного администрирования создаёт запрошенный ресурс и предоставляет к нему доступ заявленных сотрудников. Каждый начальник подразделения, участвующего в проекте запрашивает доступ только для тех сотрудников, которые находятся у него в подчинении.

Ранее, до создания базовой политики безопасности, каждый сотрудник сам определял степень опасности писем и файлов, пришедших по электронной почте с внешних почтовых серверов.

После создания базовой политики безопасности, каждому пользователю вменяется в обязанности каждый файл, полученный по электронной почте от внешних почтовых серверов пересылать в отдел информационной безопасности для проверки его на наличие вредоносного программного обеспечения, степень опасности писем сотрудник определяет самостоятельно. Если сотрудник подозревает, что во входящем сообщении содержится спам или фишинг, он обязан отправить письмо полностью, то есть содержащее в себе всю служебную информацию об отправителе, его почтовый ящик и IP-адрес, в отдел информационной безопасности. После анализа подозрительного письма и при подтверждении угрозы этого письма отдели информационной безопасности направляет адрес отправителя письма в отдел системного администрирования, и сотрудник отдела системного администрирования заносит адрес отправителя письма в чёрный список.

Для предотвращения несанкционированного доступа к информационным ресурсам организации, а также к информационным системам персональных данных, в организации установлена следующая парольная политика:

- Длина пароля – не менее 8 символов;
- Сложность пароля – латинские и /или кириллические символы, верхний и нижний регистр, специальные символы;
- Срок действия пароля – 1 месяц;
- Невозможность повторения пароля в течении трёх месяцев.

При обучении сотрудников им разъясняются правила хранения паролей:

- Не записывать пароли на бумажный или цифровой носитель;
- Вводить пароль от рабочего места или при входе в систему без посторонних лиц, которые могут запомнить или записать, не заметно для пользователя, пароль;
- Всегда блокировать рабочее место, при отлучении от него.

Согласно статьи 89 главы 14 Трудового Кодекса Российской Федерации, сотрудник имеет право на доступ к своим персональным данным, но допускается к обработке персональных данных других сотрудников или клиентов только для исполнения своих должностных обязанностей.

Для обеспечения контроля за доступом в информационным системам персональных данных, в организации установлены следующие правила доступа к информационным системам персональныхданных:

- Только сотрудники, в чьи должностные обязанности входит обработка персональныхданных имеют доступ к ИСПДн;
- Доступ к ИСПДн разрешён только с локального рабочего места сотрудника, работающего с персональными данными;
- В организации создан документ, определяющий пофамильно сотрудников, которым разрешен доступ к персональным данным сотрудников и клиентов с указанием информационной системы персональных данных и перечнем персональных данных, разрешённых для обработки сотрудником.

## 1.4. Выбор защитных мер

### 1.4.1. Выбор организационных мер.

Согласно исследованию, проведённому британской аудиторско-консалтинговой компанией Ernst&Yong в 2014 году, 69 процентов компаний, участвовавших в исследовании, считают сотрудников компании основным источникомугроз информационной безопасности.

Сотрудники компании могут по незнанию или своей некомпетентности в сфере информационной безопасности разгласить критическую информацию, необходимую для совершения целенаправленных атак на организацию. Так же злоумышленники рассылают фишинговые сообщения с вложенным вредоносным программным обеспечением, позволяющим злоумышленникам получить контроль над рабочим местом сотрудника и с этого рабочего места провести атаку на информационные системы организации.

Поэтому отдел информационной безопасности обязан проводить работу по обучению сотрудников основополагающим принципам информационной безопасности, осуществлять контроль за соблюдением требований безопасности при работе на рабочих местах, информировать сотрудников о новыхугрозах информационной безопасности с которыми они могут столкнуться.

В ООО «ПК Венткомплекс» все сотрудники проходят вводный инструктаж при устройстве на работу. Так же новые сотрудники, сотрудники переведённые из других структурных подразделений проходят первичный инструктаж в отделе информационной безопасности, в ходе которого сотрудникам разъясняются основные правила информационной безопасности при работе с информационными системами, правила безопасности при работе в сети Интернет, правила безопасности при работе с электронной почтой, парольная политика организации.

Сотрудники отдела информационной безопасности участвуют при разработке и внедрении новых информационных систем на всех уровнях разработки систем.

На этапе проектирования системы и составления технического задания на разработки информационной системы отдел информационной безопасности предъявляет требования по безопасности к системе.

На этапе разработки информационной системы сотрудники отдела информационной безопасности изучают текущую документацию, тестируют программное обеспечение на возможные уязвимости в программном коде.

На этапе тестирования и ввода в эксплуатацию информационной системы отдел информационной безопасности активно участвует в тестировании информационной системы, проводит тесты на проникновение в информационную систему и тесты отказа в обслуживании, так же распределяет права доступа к информационной системе.

На этапе функционирования уже введённой в эксплуатацию информационной системы отдел информационной безопасности проводит мониторинг, выявляет подозрительную активность.

На этапе доработки информационной системы отдел информационной безопасности, основываясь на данных, полученных при эксплуатации информационной системы, выстраивает новые требования к информационной системе.

Отдел информационной безопасности в ООО «ПК Венткомплекс» согласовывает все заявки на доступ к ресурсам в сети Интернет, а также ко внутренним ресурсам организации.

### 1.4.2. Выбор инженерно-технических мер.

В сети ООО «ПК Венткомплекс» есть ярко выраженные слабые места, используя которые злоумышленники могут получить полный доступ к сети и перехватить над ней контроль, после чего смогут беспрепятственно украсть, изменить или удалить персональные данные клиентов или сотрудников организации.

Так как сеть организации представляет собой один единственный сегмент, то для минимизации рисков проникновения злоумышленников в сеть организации, её необходимо разделить на несколько сегментов с использованием технологии виртуальных сетей.

Концепция технологии построения виртуальных сетей (VLAN) заключается в том, что администратор сети может создавать в ней логические группы пользователей независимо от того, к какому участку сети они подключены. Объединять пользователей в логические рабочие группы можно, например, по признакам общности выполняемой работы или совместно решаемой задачи. При этом группы пользователей могут взаимодействовать между собой или быть совершенно невидимыми друг для друга. Членство в группе можно изменять, и пользователь может быть членом нескольких логических групп. Виртуальные сети формируют логические широковещательные домены, ограничивая прохождение широковещательных пакетов по сети, так же, как и маршрутизаторы, изолирующие широковещательный трафик между сегментами сети. Таким образом, виртуальная сеть предотвращает возникновение широковещательных штормов, так как широковещательные сообщения ограничены членами виртуальной сети и не могут быть получены членами других виртуальных сетей. Виртуальные сети могут разрешать доступ членам другой виртуальной сети в случаях, где это необходимо для доступа в общие ресурсы, типа файловых серверов или серверов приложений, или где общая задача, требует взаимодействия различных служб, например кредитных и расчетных подразделений. Виртуальные сети могут создаваться по признакам портов коммутатора, физических адресов устройств, включаемых в сеть и логических адресов протоколов третьего уровня модели OSI. Преимущество виртуальных сетей состоит в высокой скорости работы коммутаторов, так как современные коммутаторы содержат специализированный набор интегральных схем специально разработанных для решения задач коммутации на втором уровне модели OSI. Виртуальные

сети третьего уровня наиболее просты в установке, если не требуется переконфигурация клиентов сети, наиболее сложны в администрировании, т.к. любое действие с клиентом сети требует либо переконфигурации самого клиента либо маршрутизатора, и наименее гибки, так как для связи виртуальных сетей требуется маршрутизация, что увеличивает стоимость системы и снижает ее производительность.

Таким образом, создание виртуальных сетей предотвратит атаки типа ARP-spoofing. Злоумышленники не смогут перехватить информацию, проходящую между сервером и клиентом. При проникновении в сеть злоумышленники смогут просканировать не всю сеть, а только сегмент сети в который они получили доступ.

При проникновении в сеть организации злоумышленники в первую очередь будут сканировать сеть для поиска критически важных узлов сети. Этими узлами являются:

- Контроллер домена;
- Proxy сервер;
- Почтовый сервер;
- Файловый сервер;
- Сервер приложений.

Так как в ООО «ПК Венткомплекс» локальная сеть организована с использованием технологии виртуальных сетей, злоумышленники не смогут без дополнительных действий обнаружить эти узлы. Для того чтобы усложнить злоумышленникам поиск критически важных узлов локальной сети и запутать их, а в дальнейшем изучить стратегию злоумышленников при проведении атаки в сети нужно использовать ложные объекты, которые будут привлекать злоумышленников. Эти объекты называются Honeypot.

Задача Honeypot – подвергнуться атаке или несанкционированному исследованию, что впоследствии позволит изучить стратегию злоумышленников и определить перечень средств, с помощью которых могут быть нанесены удары по реально существующим объектам безопасности.

Реализация Honeypot может представлять собой как специальный выделенный сервер, так и один сетевой сервис, задача которого – привлечь внимание взломщиков.

Honeypot представляет собой ресурс, который без какого-либо воздействия на него ничего не делает. Honeypot собирает небольшое количество информации, после анализа которой строится статистика методов, которыми пользуются взломщики, а также определяется наличие каких-либо новых решений, которые впоследствии будут применяться в борьбе с ними.

Например, веб-сервер, который не имеет имени и фактически никому не известен, не должен, соответственно, иметь и гостей, заходящих на него, поэтому все лица, которые пытаются на него проникнуть, являются потенциальными взломщиками. Honeypot собирает информацию о характере поведения этих взломщиков и об их способах воздействия на сервер. После чего специалисты отдела информационной безопасности собирают информацию об атаке злоумышленников на ресурс и разрабатывают стратегии отражения атак в будущем.

Для контроля входящей из сети Интернет информации и обнаружения угроз информационной безопасности на этапе их передачи по сети, а также обнаружения активности злоумышленников, проникнувших в локальную сеть необходимо на границе сети установить систему предотвращения вторжений.

Система предотвращения вторжений – программная или аппаратная система сетевой и компьютерной безопасности, обнаруживающая вторжения или нарушения безопасности и автоматически защищающая от них.

Системы предотвращения вторжений можно рассматривать как продолжение Систем обнаружения вторжений, так как задача отслеживания атак остается одинаковой. Однако, они отличаются в том, что система предотвращения вторжений отслеживает активность в реальном времени и быстро реализует действия по предотвращению атак.

Системы обнаружения и предотвращения вторжений подразделяются на:

- Сетевые системы предотвращения вторжений – анализируют трафик, направленный в сеть организации, проходящий в самой сети или направленный к конкретному компьютеру. Системы обнаружения и предотвращения вторжений могут быть реализованы программными или программно-аппаратными методами, устанавливаются на периметре корпоративной сети и иногда внутри нее.
- Персональные системы предотвращения вторжений – это программное обеспечение, которое устанавливается на рабочие станции или серверы и позволяет контролировать деятельность приложений, а также отслеживать сетевую активность на наличие возможных атак.

Для развёртывания в сети организации была выбрана сетевая система предотвращения вторжений.

Рассматривались сетевые системы вторжений компаний IBM, Check Point, Fortinet, Palo Alto, так как заявленный функционал производителей этих систем подходил под требования отдела информационной безопасности организации.

После развёртывания тестовых стендов и проведения тестирования систем предотвращения вторжений была выбрана система производства компании Check Point, так как она показала наилучшее быстродействие, лучшую подсистему обнаружения вирусного программного обеспечения, передаваемого по локальной сети, лучший инструментарий по протоколированию и журналированию важных событий и цене приобретения.

Система предотвращения вторжений компании IBM была отвержена из-за стоимости устройств, превышающей бюджет отдела информационной безопасности на покупку системы предотвращения вторжений.

Система предотвращения вторжений компании Fortinet была отвержена из-за неполного срабатывания при выполнении сотрудниками отдела информационной безопасности тестов по передаче заражённых файлов и недостаточно информативного инструментария журналирования важных событий.

Система предотвращения вторжений компании Palo Alto была отвержена из-за недостаточно информативного инструментария журналирования важных событий, чрезмерной сложности работы с системой и работе в большей степени как маршрутизатор.

Для внедрения в локальную сеть была выбрана система предотвращения вторжений компании Check Point. Эта система показала высокий уровень обнаружения угроз информационной безопасности, гибкие настройки, возможность расширения функционала за счёт приобретения дополнительных программных модулей, имеет мощную систему журналирования важных событий и мощный инструментарий по предоставлению отчётов о происшествиях, с помощью которого можно гораздо проще расследовать произошедшие инциденты информационной безопасности.

Для внедрения в локальную сеть ООО «ПК Венткомплекс» выбрана модель Check Point 4600.

Характеристики модели системы предотвращения вторжений Check Point 4600 представлены в таблице 1.3.

Таблица 1.3 Характеристики модели системы предотвращения вторжений Check Point 4600.

| **Устройство** | **Check Point 4600** |
|---|---|
| **Производительность** | |
| SecurityPower | 405 |
| Пропускная способность файрволла (Гб/с) | |
| Тестовая | 9 |

| **Устройство** | **Check Point 4600** |
|---|---|
| Производительная | 3.4 |
| Пропускная способность VPN AES-128 (Гб/с) | 1.5 |
| Пропускная способность IPS (Гб/с) | |
| Рекомендованная | 1 |
| Производительная | 0.63 |
| Число одновременных соединений | 1.2 млн |
| Соединений в секунду | 50,000 |
| **Виртуальные системы** | |
| Поддержка виртуальных систем | Да |
| Максимальное/поддерживаемое число | 10 / 10 |
| **Аппаратные спецификации** | |
| 10/100/1000Base-T портов | 8-12 |
| 1000Base-F SFP портов | 0-4 |
| 10GBase-F SFP+ портов | -- |
| Память | 4 Гб |
| Хранилище | 250 Гб на жестком диске |
| Слоты расширения I/O | 1 |
| Плата LOM | -- |
| **Физические характеристики** | |
| Корпус | 1U |
| Размеры | 438×410×44 мм |
| Вес | 4 кг |
| **Электропитание** | |
| Входное питание | 100~240VAC, 50~60Hz |
| Максимальная мощность одного источника питания | 250 Вт |
| Максимальная потребляемая мощность | 90 Вт |

Систему предотвращения вторжений было решено установить на границе сети за межсетевым экраном, заменяя при этом proxy-сервер системой предотвращения вторжений, так как она может работать одновременно и как proxy-сервер.

Схема сети ООО «ПК Венткомплекс» с изменённой архитектурой представлена на рисунке 1.7.

Так как безопасность персональных данных не может быть обеспечена только защитой сети, потому что злоумышленники, не смотря на все предпринятые меры для защиты сети, могут получить доступ в сеть организации.

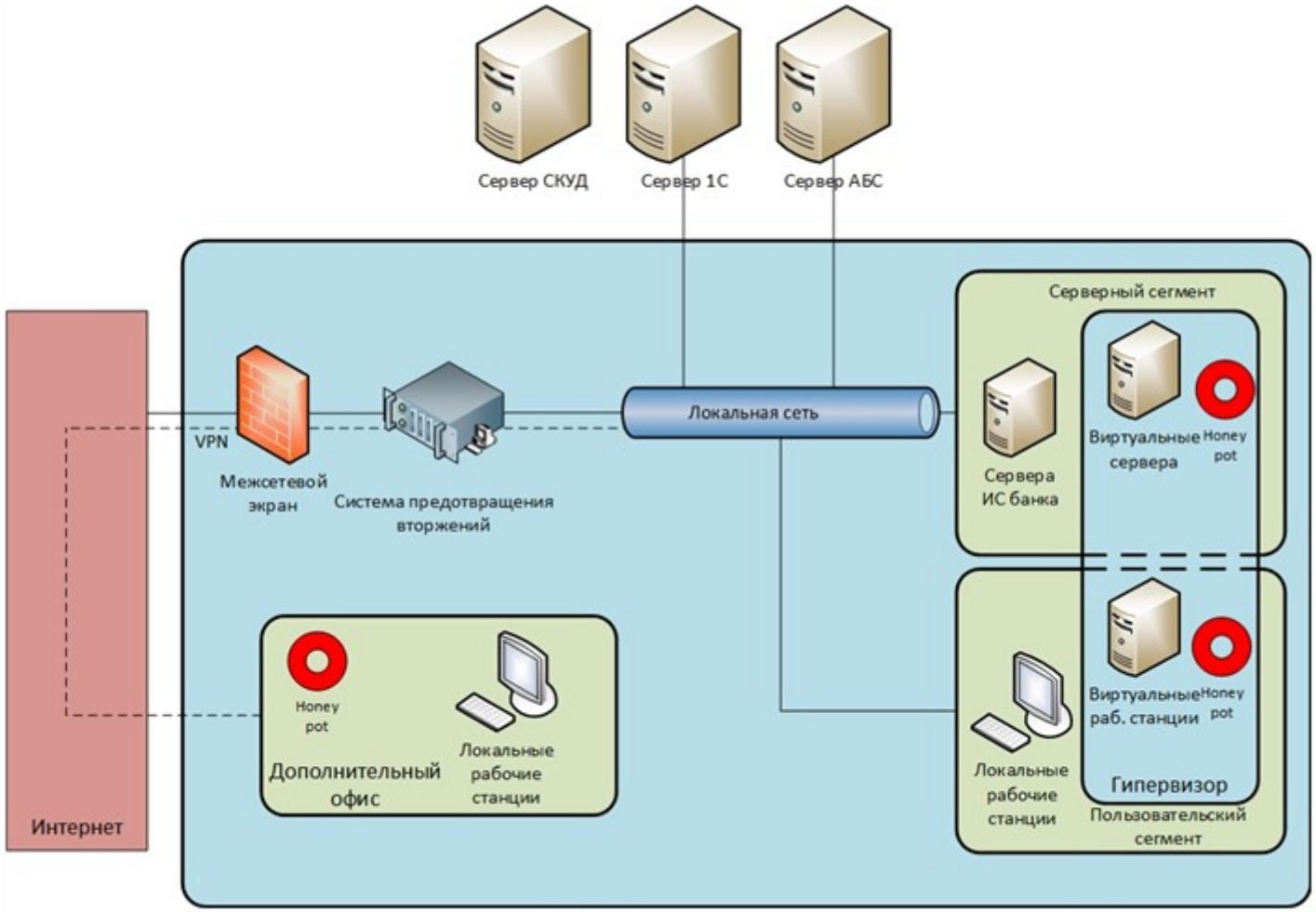



Рисунок 1.7 Схема ООО «ПК Венткомплекс» с дополнительными системами защиты.

Для более устойчивой к атакам защите необходимо добавить к устройствам, предназначенным для защиты сети, программные и аппаратные устройства защиты локальных рабочих станций, виртуальных рабочих станций, виртуальных и обычных серверов.

Как известно антивирусные программы не дают полной защиты от вредоносного программного обеспечения, так как работают по принципу сигнатурного анализа. Компания-разработчик антивирусного программного обеспечения имеет в своём штате экспертов, которые отслеживают вирусную активность в сети Интернет, изучают поведение вирусного программного обеспечения на тестовых станциях и создают сигнатуры, которые в последствии рассылаются на компьютеры пользователей посредством обновления баз данных сигнатур антивирусного программного обеспечения.

Антивирус, получив обновлённую базу данных сигнатур антивирусного программного обеспечения проверяет файлы на рабочей станции пользователя и ищет признаки вредоносного программного обеспечения, если в процессе проверки такие признаки обнаруживаются, то антивирус сигнализирует об этом и действует в соответствии с настройками, которые установлены пользователем или администратором антивируса. Таким образом, если вредоносное программное обеспечение не обнаружено и не проанализировано экспертами компании-разработчика антивирусного программного обеспечения, то антивирус будет не в состоянии выявить вредоносное программное обеспечение и не предпримет никаких действий, считая проверенный файл безопасным. Поэтому в организации, для снижения вероятности пропуска в сеть и запуска вредоносного программного обеспечения, был установлен второй контур антивирусной защиты.

Так как компании-разработчики антивирусного программного обеспечения в большинстве своём работают отдельно друг от друга, то вредоносное программное обеспечение, пока не обнаруженное одной компанией-разработчиком антивирусного обеспечения, может быть

обнаружено другой компанией-разработчиком и на обнаруженнуюугрозу уже могут быть созданы сигнатуры.

Для реализации такой схемы была создана виртуальная рабочая станция, на которой был установлен антивирус Doctor WEB Enterprise security suit, имеющий сертификат соответствия ФСТЭК России № 2446, действительный до 20 сентября 2019 года. Все файлы, которые сотрудники загружали во время своей работы, попадают на эту станцию и проверяются антивирусом. В случае обнаружения вредоносного программного обеспечения антивирус отправляет сотрудникам отдела информационной безопасности письмо с названием угрозы и путём, где хранится зараженный файл. Сотрудники отдела информационной безопасности предпринимают меры по удалению вредоносного программного обеспечения. Если загруженные пользователями файлы проходят проверку антивирусного программного обеспечения, пользователь, загрузивший файл делает заявку в отдел информационной безопасности и сотрудники отдела переносят загруженный файл пользователю.

Также большое количество вредоносного программного обеспечения приходит сотрудникам организации по электронной почте. Это могут быть и обычные вирусы-шифровальщики, так и вредоносное программное обеспечения, позволяющее злоумышленникам проникнуть на заражённый компьютер сотрудника с помощью удалённого подключения.

Для минимизации рисков таких угроз на почтовый сервер было установлено антивирусное программное обеспечения ClamAW, предназначенное для защиты почтовых серверов.

Для защиты от несанкционированного доступа внутренних злоумышленников, каким-либо образом узнавших пароль пользователя локальной станции, имеющей доступ к информационным системам персональныхданных, необходимо установить на локальные рабочие станции

пользователей, работающих с информационными системами персональных данных систему защиты информации от несанкционированного доступа.

Для целей защиты персональных данных в ИСПДн было выбрано семейство система защиты информации, подключаемых к слотам расширения локальных рабочих станций.

Рассматривалось 2 вида программно-аппаратных комплексов от разных производителей:

- ПАК Соболь, производства НИП Информзащита;
- ПАК СЗИ НСД Аккорд, производства ОКБ САПР.

После проведённых испытаний, ПАК СЗИ НСД Аккорд, показал лучшие результаты по сравнению с ПАК Соболь по ряду причин:

- Количество отказов в срабатывании;
- Меньшее количество ошибок при подсчёте контрольных сумм устройств.

Так же ПАК СЗИ НСД Аккорд имеет сертификат ФСТЭК России №246/7, действительный до 13 августа 2019 года.

ПАК СЗИ НСД Аккорд был установлен на следующие локальные рабочие станции:

- Главного бухгалтера;
- Заместителя главного бухгалтера;
- Начальника отдела по работе с персоналом;
- Сотрудника, ответственного за начисление заработной платы сотрудникам;
- На локальной рабочей станции в центральном пункте охраны;
- На локальных рабочих станциях сотрудников, имеющих право работать с информационной системой персональных данных автоматизированной системы персональныхданных.

# II Проектная часть

## 2.1. Комплекс организационных мер обеспечения информационной безопасности и защиты информации ООО «ПК Венткомплекс».

### 2.1.1. Отечественная и международная нормативно-правовая основа создания системы обеспечения информационной безопасности и защиты информации предприятия.

В настоящее время в Российской Федерации осуществляется государственное регулирование в области обеспечения безопасности персональных данных. Основными нормативно-правовыми актами, регулирующими систему защиты персональных данных в Российской Федерации являются Конституция Российской Федерации и Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ. Эти два основных правовых акта устанавливают основные тезисы о персональных данных в Российской Федерации:

- Каждый гражданин имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени;
- Каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права допускается только на основании судебного решения;
- Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются;
- Обработка персональных данных должна осуществляться на законной и справедливой основе;
- Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

- Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.
- Обработке подлежат только персональные данные, которые отвечают целям их обработки.
- Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.
- При обработке персональных данных должны быть обеспечены точность персональныхданных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных.
- Хранение персональныхданных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

Другими нормативными актами, оказывающие правовое регулирование в области защиты персональных данных в организациях Российской Федерации являются:

- Федеральный закон Российской Федерации от 27 июля 2006 г. №149 ФЗ «Об информации, информационных технологиях и о защите информации»;
- Трудовой кодекс Российской Федерации (глава 14);
- Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональныхданных»;
- Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональныхданных».

Рассмотрим основные определения, используемые в законодательстве.

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональныхданных).

Оператор персональных данных – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональныхданных;

Автоматизированная обработка персональных данных – обработка персональныхданных с помощью средств вычислительной техники;

Распространение персональных данных – действия, направленные на раскрытие персональныхданных неопределенному кругу лиц;

Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональныхданных);

Уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональныхданных и (или) в результате которых уничтожаются материальные носители персональныхданных;

Обезличивание персональныхданных – действия, в результате кото-рых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональныхданных;

Информационная система персональных данных – совокупность со-держащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

Трансграничная передача персональных данных – передача персо-нальных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

Биометрические персональные данные – сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические персональные данные) и которые используются оператором для установления личности субъекта персональныхданных.

Безопасность персональных данных – состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональныхданных

### 2.1.2. Организационно-административная основа создания системы обеспечения информационной безопасности и защиты информации ООО «ПК Венткомплекс»

Аудит информационной безопасности объекта защиты показал, что на предприятии циркулирует большой объём информации, имеющей высокую степень важности.

В положениях о подразделениях и должностных инструкциях руководителей и работников никакой ответственности за уничтожение, искажение или утерю информации не предусмотрено, упоминания об информационной безопасности отсутствуют. Никаких инструкций и правил, регламентирующих информационную безопасность, не предусмотрено.

Среди установленных организационных мер по обращению с техническими средствами особо выделены следующие:

1) На входе организован контрольно-пропускной пункт для предотвращения бесконтрольного перемещения по зданию.

2) Конфиденциальные документы хранятся в сейфах.

Дополнительных мероприятий по отношению обеспечения информационной безопасности IT-специалистами, работающими на предприятии не выявлено.

С целью совершенствования защищенного документооборота дополнению подлежат существующие на данном предприятии нормативно-правовые документы:

- Инструкция по конфиденциальному делопроизводству;
- Положение о конфиденциальной информации предприятия;
- Обязательства работника о сохранении коммерческой тайны.

С учетом Закона РСФСР "О предприятиях и предпринимательской деятельности" руководитель предприятия (фирмы) вне зависимости от форм собственности может устанавливать специальные правила доступа к сведениям, составляющим коммерческую тайну, и ее носителям, тем самым обеспечивая их сохранность.

Под доступом понимается получение письменного разрешения руководителя фирмы (или, с его санкции, других руководящих лиц) на выдачу тому или иному сотруднику конкретных (или в полном объеме) закрытых сведений с учетом его служебных обязанностей (должностных полномочий).

Руководитель организации может разрешить пользование любой охраняемой информацией любому работнику данного предприятия или лицу, прибывшему на объект из другой организации для решения каких-либо вопросов, если в отношении этих сведений не установлены ограничения на ознакомление со стороны производственно-коммерческих партнеров по совместному производству и т.п.

Санкцию на доступ к информации другим сотрудникам должны давать только учредитель и директор фирмы.

Для эффективной работы разрешительной системы необходимо соблюдение определенных правил:

1. Необходимо документальное отражение выданного разрешения на право пользования теми или иными защищаемыми сведениями. Это означает, что руководитель, давший разрешения на право пользования, должен его в обязательном порядке зафиксировать в письменном виде на соответствующем документе или в действующей на предприятии

учетной форме. Никакие устные указания и просьбы о доступе кого бы то ни было (за исключением руководителя предприятия) не имеют юридической силы.

2. Следует строго соблюдать принцип контроля. Каждое разрешение должно иметь дату его оформления и выдачи.

Вся классифицированная документация и изделия, поступившие на предприятие и разработанные на нем, должны приниматься и учитываться руководством среднего звена. После регистрации документация должна передаваться на рассмотрение директору предприятия под расписку.

Важно подчеркнуть, что установление на фирме определенного порядка обращения с закрытой информацией и изделиями существенным образом повышает надежность защиты коммерческой тайны, снижает вероятность разглашения, утраты носителей этих сведений.

Для обеспечения сохранности документации предлагается закупить соответствующую мебель, которая позволяет надежно запирать документы. Так же необходимо каждый день, перед уходом, опечатывать шкафы.

Особое внимание следует уделить безопасности компьютерной информации. В ООО «ПК Венткомплекс» сегодня создано несколько баз данных: клиенты фирмы (с указанием не только их рабочих адресов и телефонов, но и домашних, а также сведений носящих личный характер); база данных, содержащая цены и характеристику поставляемого товара; база данных сотрудников организации. Так же в компьютере хранятся различные договора, соглашения и т.п.

В любом случае, попадание этой информации в руки конкурентов крайне нежелательно. Для предотвращения такого развития событий рекомендуется создание паролей для доступа в каждую базу данных (а программные средства позволяют это реализовать). При загрузке компьютера так же рекомендуется ставить двухуровневую защиту. Естественно, пароли так же должны быть доступны только тем сотрудникам фирмы, которые

непосредственно работают с этими базами данных (директор, заместитель директора, операторы).

В случае возникновения каких-либо проблем, связанных с компьютером и необходимости обращения в постороннюю фирму, необходимо полностью контролировать процесс ремонта техники. Так как именно в такой момент, когда сняты все пароли, когда программист «со стороны» имеет свободный и беспрепятственный доступ к содержимому жесткого диска, возможно изъятие им информации и дальнейшее ее использование в различных целях.

Необходимо постоянно обновлять антивирусные программы с целью препятствования попадания и распространения вирусов в компьютерах.

Наряду с приведенными средствами защиты информации компании ООО «ПК Венткомплекс» рекомендуется применение средств криптографической защиты информации (СКЗИ). В применении СКЗИ заинтересовано руководство самой компании. С помощью средства шифрования компания получает возможность защитить свою корпоративную информацию – сведения, представляющие коммерческую тайну, интеллектуальную собственность, оперативную и техническую информацию и др.

На сегодняшний день для эффективного применения в корпоративной среде, программа для шифрования должна обеспечивать:

- шифрование данных на удаленном сервере;
- поддержку асимметричной криптографии;
- прозрачное шифрование;
- шифрование сетевых папок;
- возможность разграничения прав доступа к конфиденциальной информации между сотрудниками компании;
- возможность хранения сотрудниками закрытых ключей на внешних носителях информации (токенах).

Итак, второе применение СКЗИ – это защита конфиденциальной информации компании. Средство шифрования, поддерживающее вышеперечисленные возможности, способно обеспечить достаточно надежную защиту, однако непременно должно использоваться как составляющая комплексного подхода к защите информации. Такой подход дополнительно подразумевает использование межсетевых экранов, антивирусов и файерволлов, а также включает разработку модели угроз информационной безопасности, выработку необходимых политик ИБ, назначение ответственных за информационную безопасность, контроль электронного документооборота, контроль и мониторинг деятельности сотрудников и др.

## 2.2. Комплекс проектируемых программно-аппаратных средств обеспечения информационной безопасности и защиты информации ООО «ПК Венткомплекс».

### 2.2.1 Структура программно-аппаратного комплекса информационной безопасности и защиты информации ООО «ПК Венткомплекс».

Оборудование технической части средств защиты информации (СЗИ) на объекте можно разделить на две большие группы: средства обнаружения устройств съема информации и средства защиты. Ниже рассмотрим рынок изделий и систем технической защиты информации. Заметим, что для защиты информации рекомендуется использовать сертифицированные по требованиям безопасности информации технические средства обработки и передачи информации, технические и программные средства защиты информации.

Анализ ООО «ПК Венткомплекс» показал составить перечень программно-аппаратных СЗИ (таблица 2.1) и других СЗИ (таблица 2.2).

Таблица 2.1 Программно-аппаратные средства защиты ООО «ПК Венткомплекс».

| Вид аппаратуры | Назначение | Тип аппаратуры |
|---|---|---|
| Индикаторы поля | Для обнаружения активных радиопередающих устройств | D-006, Ekostate, RM-10, RFD-2, R-Finder, ДИ-К, «Комар», «Сириус», «Луч», «Пирамида», «Панно», Protect 1203, АПП-7, D-008 |
| Частотомеры | Для обнаружения активных радиопередающих устройств и измерения частоты сигнала | SCOUT, CUB, M1, РИЧ-3, SEL SP-71M, XPLORER |
| Средства контроля проводных линий | Для обнаружения радиопередающих устройств | «Вектор», ТПУ-7, PPL-2, КТЛ-400, «Сканер-3М», D-008, «Улан», LBD-50, TRTD-061, «Бор-1» |
| Универсальные поисковые устройства | Для обнаружения активных радиопередающих устройств в нескольких каналах утечки | ST-031 «Пиранья», ST-032, ST-007, СРМ-700, ПКУ-6М, OSK-500 Basic |
| Приемная аппаратура, анализаторы спектра | Для обнаружения активных радиопередающих устройств | MRA-3, «Скорпион», REL RF-2400, IRIS VCF-200, SP-81 «Оракул», сканирующие приемники, анализаторы спектра Agilent Technologies |
| Автоматизированные поисковые комплексы | Для обнаружения активных радиомикрофонов и контроля проводных сетей | «Омега», «Крона», серия комплексов RS, серия комплексов АРК |
| | Для обнаружения диктофонов | ST-0110 https://hardbroker.ru |
| Специальное программное обеспечение | Для автоматизации процессов обнаружения средств негласного съема информации с передачей сигнала на радиочастоте | Sedif, «Филин», «Корунд», «Патруль» http://www.sis-tss.ru |
| Нелинейные локаторы | Для поиска несанкционированных устройств, в том числе находящихся в выключенном состоянии | «Орион» NGE-400, NR-900 EM, NR-m, «Катран», «Обь», «Родник-2к», «Родник-23М», «Мастер» http://www.infosecur.ru |

Таблица 2.2 Средства защиты информации ООО «ПК Венткомплекс».

| Канал утечки | Решаемая задача | Метод защиты | Тип аппаратуры |
|---|---|---|---|
| Виброакустический | Защита от лазерных микрофонов, стетоскопов, микрофонов в вент.каналах | Создание шумовой помехи на элементах строительных конструкций и инженерных коммуникаций | Системы виброакустической защиты: «Соната-АВ», SEL SP-51/A, ANG-2000, серия «Шорох», серия «Барон», «Заслон-2М», серия SI, «Шелест-4К», «Фон-В», VNG-006 |

| Канал утечки | Решаемая задача | Метод защиты | Тип аппаратуры |
|---|---|---|---|
| | | | https://www.detsys.ru |
| Электро-магнитный | Частичное или полное подавление сигналов радиомикрофонов | Создание широкополосной электромагнитной шумовой помехи | «Штора», SEL SP-21B2 «Спектр», «Вето» http://nposi.ru |
| | Защита от утечки за счет ПЭМИН | 1. Установка сертифицированных ПЭВМ с уменьшенной зоной R2.<br>2. Создание широкополосной электромагнитной шумовой помехи | ПЭВМ типа «Флагман-Z», HighScreen Sekret ГШ-1000М, «Гном-3», «Бриз», «Гром-ЗИ- 4», SEL SP-21B1 |
| | Предотвращение несанкционированного использования сотовых телефонов | 1. Переход на доработанные модели мобильных телефонов с исключенной функцией несанкционированного включения.<br>2. Размещение телефона в чехол с встроенным шумогенератором<br>3. Блокировка сотовых телефонов | Модели телефонов от МВП «СВЕМЕЛ»<br>Чехол типа «Кокон», «Ладья»<br>«Москит GSM», C-Gard, Hammer, «Мозаика» RSJammer, SELSP-23 http://www.swemel.ru |
| Проводной 220 В | Ограничение информационных сигналов в сети | Фильтрация ВЧ-сигналов | Сетевые фильтры типа: ФСП, ФСПК, «Фаза» |
| | Подавление сигналов сетевых передатчиков | Создание широкополосной электромагнитной шумовой помехи | Генераторы типа: «Соната -С1», SEL SP-41/C, «Гром-ЗИ-4», «Цикада-С» http://www.bnti.ru |
| Акустоэле-ктрический | Защита телефонных аппаратов, громкоговорителей системы радиовещания от микрофонного эффекта | Фильтрация малых сигналов | «Корунд», МП-1 - МП-5, «Грань -300» https://www.tinko.ru |
| Телефонные линии | Снижение эффективности работы различных устройств несанкционирован-ного съема информации на участке от аппарата до АТС | Воздействие на устройства несанкционированного съема информации различными видами помех | «Гром-ЗИ-4», «Прокруст-2000», «Акцент», SI-2002, SEL SP-17/D, «Цикада» http://www.sinf.ru |

| Канал утечки | Решаемая задача | Метод защиты | Тип аппаратуры |
|---|---|---|---|
| | Защита от прослушивания на участке «абонент-абонент» | 1. Использование скремблеров, маскираторов 2. Передача информации с преобразованием ее в цифровой вид | SCR-M 1.2, «Грот», «Щит» «Референт», SEL SP-19DT http://kunegin.com |
| Несанкцио-нированная запись | Подавление средств магнитной записи | Создание электромагнитной помехи, наводимой на средства магнитной записи | «Сапфир», «Барсетка», «Буран-4», «Шумотрон-3,4», «Шторм», «Бастион» http://www.bnti.ru |
| Все виды | Защита от перехвата акустической информации средствами акустического контроля | Создание шумовой помехи в речевом диапазоне частот | Генераторы акустического шума: «Эхо», «Хаос», TF-012, WNG-023, ЛГШ-301 http://www.bnti.ru |

### 2.2.2. Контрольный пример реализации проекта и его описание.

С целью блокирования утечки речевой информации по акустическому и виброакустическому каналам в помещениях ООО «ПК Венткомплекс» необходимо произвести доработку защищаемых помещений на предмет улучшения звукоизоляционных и виброизоляционных свойств (установка двойных дверей с тамбурами, выполнение дополнительного остекления окон, установка в инженерно-технические коммуникации шумопоглотителей, установка в воздухопроводы глушителей, устранение щелей и трещин).

В целях блокирования каналов утечки информации за счет возникающих при работе ОТСС информативных наводок на оконечные устройства и линии связи ВТСС, последние удаляются на безопасное расстояние от ОТСС, а линии связи ОТСС - экранируются. Кроме того, устраняются выходы линий ВТСС за пределы контролируемой зоны, параллельные пробеги линий ВТСС с линиями ОТСС. Источники ПЭМИН размещаются на максимально возможном удалении от границы КЗ. Отходящие цепи, в частности ввод телефонной линии, должны быть максимально удалены от аппаратуры обработки информации.

ОТС должны размещаться, по возможности, ближе к центру здания или в сторону наибольшей части контролируемой территории. Составные элементы ОТС должны размещаться в одном помещении либо в смежных.

Предотвращение утечки информации через системы пожарной и охранной сигнализаций осуществляется отключением датчиков пожарной и охранной сигнализации на период проведения важных мероприятий или применением датчиков, не требующих специальных мер защиты.

Для защиты от наблюдения и фотографирования необходимо произвести выбор оптимального расположения средств документирования, размножения и отображения информации (рабочие места, экраны компьютеров, экраны общего пользования) с целью исключения прямого или дистанционного наблюдения; использовать занавески, шторы, жалюзи; использовать средства гашения экрана после определенного времени работы.

Следует отметить, что при использовании исключительно пассивной защиты приходится проводить круглосуточный мониторинг, так как неизвестно, когда включаются средства съема, или теряется возможность использовать оборудование обнаружения при проведении деловой встречи. Поэтому комбинированная защита (пассивная и активная с помощью средств защиты) позволяет устранить эти недостатки.

Рассмотрим рекомендации по установке выбранных устройств и произведем их размещение в помещениях ООО «ПК Венткомплекс».

Стационарный индикатор поля «ДИ-Ч» [http://www.alt-1c.ru] обычно располагается как настольные часы.

Устройство защиты телефонных переговоров «Референт basic» устанавливается как обычный телефонный аппарат.

При использовании «ГРОМ-ЗИ-4» для зашумления малогабаритных, локально размещенных объектов, антенная система может не ориентироваться в пространстве. При зашумлении крупногабаритных объектов (вычислительных центров, терминальных залов, мощных вычислительных комплексов) рекомендуется использовать несколько

комплектов «ГРОМ-ЗИ-4», размещая антенные системы в трех перпендикулярных плоскостях.

Генератор шума ГШ-1000М устанавливается вблизи защищаемого компьютера. Один генератор обеспечивает маскировку (защиту) информации устройств вычислительной техники, размещенной в помещении площадью порядка 40 кв.м. Для защиты информации от утечки по ПЭМИН на больших вычислительных центрах, мощных вычислительных комплексах рекомендуется использовать несколько комплектов ГШ-1000М, размещая их по внешней границе объекта.

Устройство защиты электросети SEL SP – 41/C [http://www.profinfo.ru] устанавливается также как другие генераторы шума.

Функции включения и выключения технических средств защиты, а также контроля их работоспособности возлагаются на работающий в помещении персонал или специалистов отдела информационной безопасности предприятия.

Как было отмечено, помещения с установленными средствами активной защиты на рассматриваемом объекте информатизации можно разделить на два типа. К помещениям первого типа отнесем отдел безопасности, к помещениям второго типа – отдел ИТ, бухгалтерию, юридический отдел и переговорную.

На рисунках 2.1 и 2.2 приведем два варианта установки технических средств защиты информации.

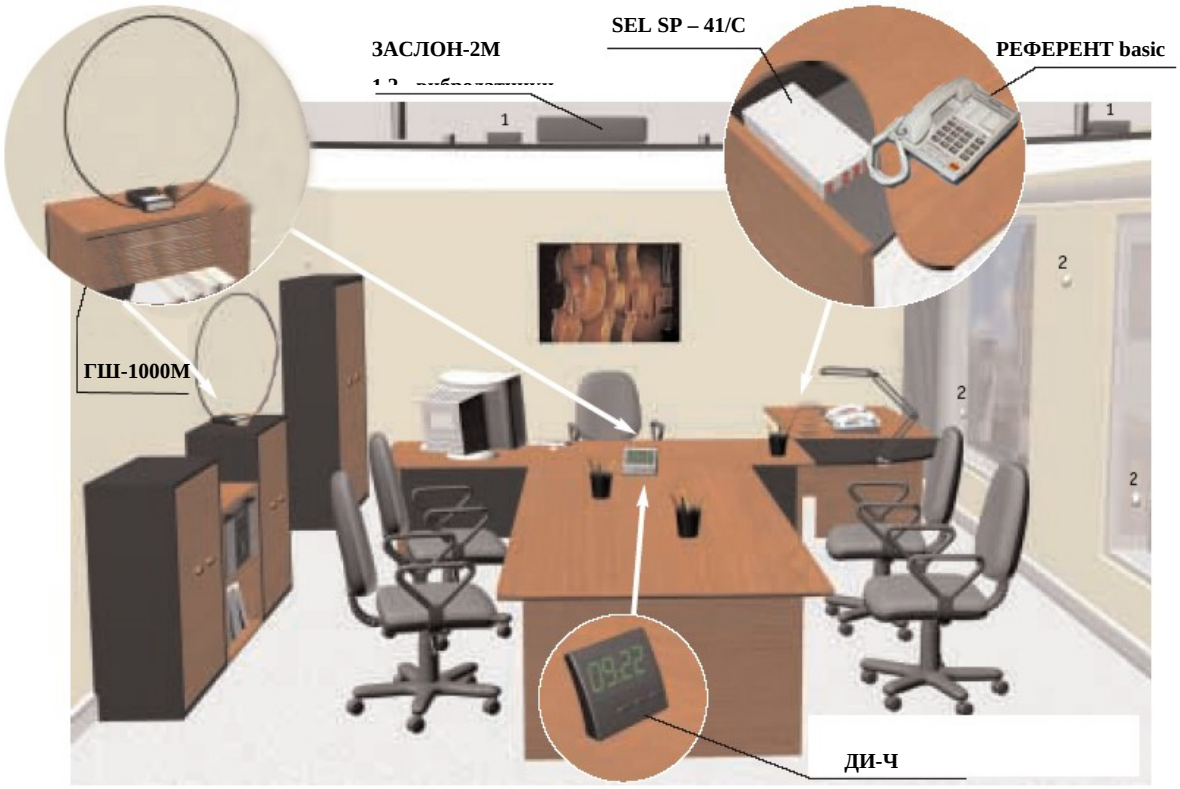



Рисунок 2.1 Установка средств защиты в помещениях первого типа.

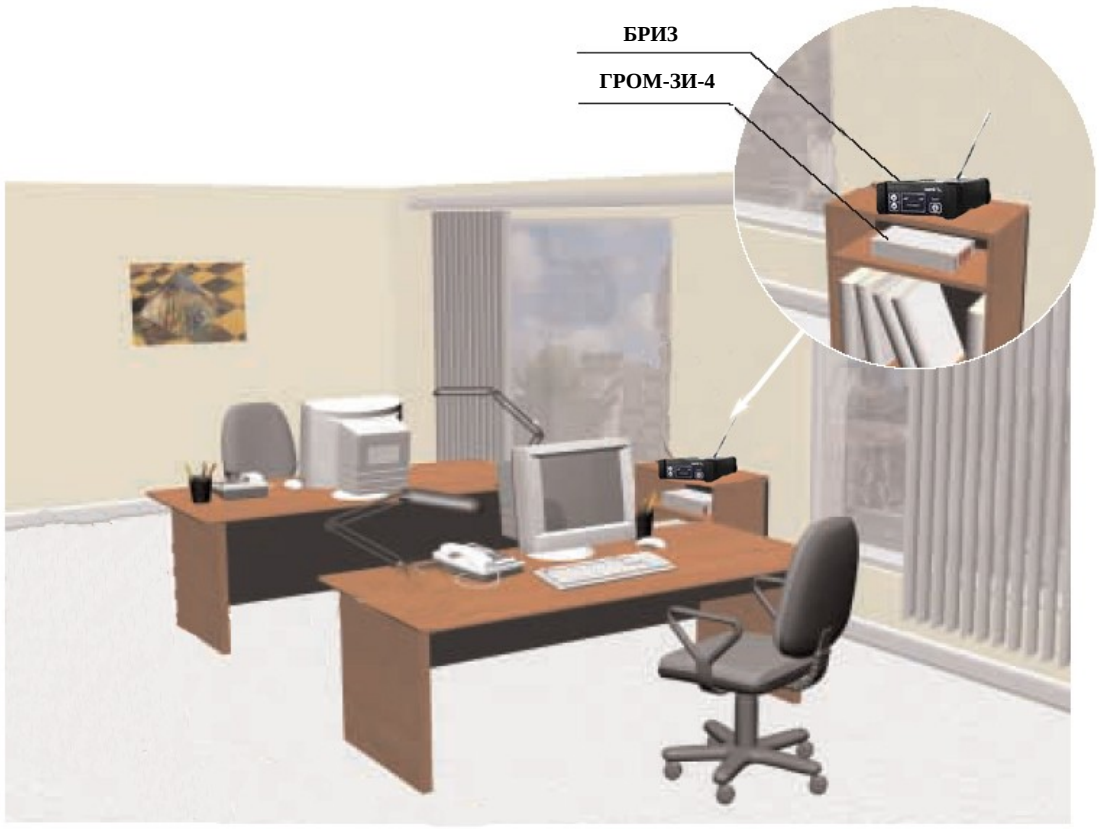



Рисунок 2.2 - Установка средств защиты в помещениях второго типа.

# III Обоснование экономической эффективности проекта

## 3.1 Расчёт показателей экономической эффективности проекта

Для реализации системы защиты персональных данных необходимо произвести закупку:

- Оборудования для защиты сети организации;
- Аппаратные средства защиты информации;
- Программные средства защиты информации.

Для перестроения сети организации необходимо закупить коммутаторы Cisco Catalyst 2960 в количестве 3-х экземпляров. Один коммутатор необходим для работы на уровне ядра сети Банка, 2 других для работы на уровне распределения. Сетевое оборудование, работавшее в организации до перестройки сети тоже будет задействовано.

Для защиты сети организации от вторжений необходимо закупить систему предупреждения вторжений Check Point 4600.

В таблице представлена суммарная стоимость оборудования, закупаемого для перестроения локальной сети (таблица 3.1):

Таблица 3.1 Стоимость оборудования, закупаемая для перестроения локальной сети.

| Наименование устройства | Количество (шт.) | Стоимость одного экземпляра (руб.) | Общая стоимость (руб.) |
|---|---|---|---|
| Cisco Catalyst 2960 | 3 | 137 054 | 411 162 |
| Check Point 4600 | 1 | 795 340 | 795 34 |
| Общая стоимость | | | 1 206 502 |

Для защиты локальных рабочих станций пользователей, работающих с ИСПДн необходимо закупить ПАК СЗИ НСД Аккорд в количестве 16 экземпляров (таблица 3.2):

Таблица 3.2 Стоимость ПАК СЗИ НСД Аккорд.

| Наименование устройства | Количество (шт.) | Стоимость одного экземпляра (руб.) | Общая стоимость (руб.) |
|---|---|---|---|
| ПАК СЗИ НСД Аккорд MX | 17 | 9389 | 159 613 |
| Общая стоимость | | | 159 613 |

Дополнительно запланирована покупка аппаратных средств защиты, а именно антивирусное программное обеспечение Doctor WEB Enterprise security suit. Планируется установка на отдельную рабочую станцию, предназначенную для проверки скачиваемых пользователями файлов. Стоимость покупки антивируса Doctor WEB Enterprise security suit представлена в таблице 3.3.

Таблица 3.3 Стоимость Doctor WEB Enterprise security suit.

| Наименование устройства | Количество (шт.) | Стоимость одного экземпляра (руб.) | Общая стоимость (руб.) |
|---|---|---|---|
| Doctor WEB Enterprise security suit | 1 | 5500 | 5500 |
| Общая стоимость | | | 5500 |

Мною были рассмотрены затраты на организацию системы защиты персональных данных по группам инструментов защиты. Общая стоимость всех закупаемых устройств и программного обеспечения – 1 371 615 рублей (таблица 3.4).

Таблица 3.4 Общая стоимость всех закупаемых устройств и программного обеспечения.

| Наименование устройства | Количество (шт.) | Стоимость одного | Общая стоимость |
|---|---|---|---|

| | | | |
|---|---|---|---|
| | | экземпляра (руб.) | (руб.) |
| Cisco Catalyst 2960 | 3 | 137 054 | 411 162 |
| Check Point 4600 | 1 | 795 340 | 795 340 |
| ПАК СЗИ НСД Акорд MX | 17 | 9389 | 159 613 |
| Doctor WEB Enterprise security suit | 1 | 5500 | 5500 |
| Общая стоимость | | | 1 371 615 |

# IV Безопасность жизнедеятельности

## 4.1 Характеристика условий труда на рабочем месте с ПК

Работа сотрудников ООО «ПК Венткомплекс» непосредственно связана компьютером и другой офисной техникой, а соответственно с дополнительным вредным воздействием целой группы факторов, что отрицательно влияет на их здоровье и существенно снижает производительность труда.

Далее описаны основные факторы вредного и опасного влияния компьютера и другой офисной техники на организм человека. В помещении, где работают операторы ПЭВМ, могут негативно действовать определенные физические факторы.

1. Микроклимат рабочей зоны оператора ПЭВМ.

Не во всех помещениях удается поддерживать благоприятный микроклимат при жаркой погоде: температурный режим, вентиляцию. Непрерывно работающие компьютеры, имеющие систему охлаждения, постоянно отдают тепло в окружающую среду. Ежедневное пребывание в неблагоприятном (допустимом, вредном) микроклимате приводит к ухудшению самочувствия, простудным заболеваниям, обострению хронических заболеваний.

Микроклимат производственных помещений - это климат внутренней среды этих помещений, который определяется действующими на организм человека сочетаниями температуры, влажности и скорости движения воздуха. Кабинет помощника по безопасности - помещение I категории (выполняются легкие физические работы), поэтому должны соблюдаться следующие требования (по СанПиН 2.2.2/2.4.1340-03): оптимальная температура воздуха- 22°С (допустимая - 20-24°С), оптимальная относительная влажность- 40-60% (допустимая - не более 75%), скорость движения воздуха не более 0.1м/с.

Для создания и поддержания в помещении независимо от наружных условий оптимальных значений температуры, влажности, чистоты и скорости движения воздуха, в холодное время года используется водяное отопление, в теплое время года помещение проветривается.

ЭВМ не содержит источников образования пыли и газа. Нормами банка установлена ежедневная влажная уборка и проветривание помещения.

2. Освещение рабочего места.

Глаза человека меньше утомляются, если рабочее место освещено равномерно, т.е. когда возможно избежать тенеобразования и слепящего действия бликов от осветительных приборов на различных поверхностях. Все это ведет к ухудшению зрительной способности и самочувствия. Мерцание люминесцентных ламп оказывает раздражающее действие на нервные клетки головного мозга, и складывается с мерцанием монитора на частоте обновления изображения, что приводит к сильной утомляемости глаз.

Работа, выполняемая с использованием вычислительной техники, в нашем случае, имеет следующие недостатки:

- вероятность появления прямой блёскости;
- ухудшенная контрастность между изображением и фоном;
- отражение экрана.

Окна кабинета помощника по безопасности выходят на северо-восток. Естественный свет падает на экраны мониторов со стороны и практически не создает бликов. В связи с тем, что естественное освещение слабое (северная сторона), на рабочем месте должно применяться также искусственное освещение.

Помещения с ПЭВМ должны иметь естественное и искусственное освещение в соответствии с «Санитарными правилами и нормами».

Далее будет произведен расчет искусственного освещения.

Воздействие шума на оператора ПЭВМ. Защита от шума.

1) Основным источником шума являются печатающие устройства, множительная техника и установки для кондиционирования воздуха, а в самих

ПЭВМ - вентиляторы систем охлаждения и трансформаторы. По «Санитарным правилам и нормам» уровень шума не должен превышать 50 дБ. В помещении, где расположены сервера и коммуникационное оборудование уровень шума максимальный среди других помещений организации.

2) В нашем случае, основным источником шума является системный блок, так как система кондиционирования отсутствует. Уровень шума, создаваемый вентиляторами блока питания и процессора не превышает 40 дБА и постоянен в течение всего рабочего дня (колебания незначительны). Также источником шума является лазерный принтер, но уровень шума, возникающий при его работе, также соответствует нормам.

Согласно СанПиН 2.2.2/2.4.1340-03 [http://www.rosteplo.ru/Npb_files/npb_shablon.php?id=707], эквивалентный уровень звука не должен превышать 50 дБА, что в нашем случае выполняется.

3. Опасность повышенного уровня напряженности электромагнитного поля.

Электромагнитные поля, характеризующиеся напряженностями электрических и магнитных полей, наиболее вредны для организма человека. Основным источником этих проблем являются мониторы с электронно-лучевыми трубками. У сотрудников используются мониторы Siemens Nixdorf MCM 1506 NTD, соответствующие стандарту безопасности TCO’99 и поддерживающие частоту кадровой развертки 100 Гц при разрешении экрана 1024x768 точек.

На настоящий момент в России действуют законодательные акты, гарантирующие соответствие мониторов нормам безопасности, гармонизированным с международными нормативами: ГОСТ Р 50948-96 «Дисплеи. Средства отображения информации индивидуального пользования. Общие эргономические требования и требования безопасности» [http://docs.cntd.ru/document/1200025976] и СанПиН 2.2.2/2.4.1340-03. В помещении, где расположены сервера и коммуникационное оборудование

уровень излучения максимальный для организации, в помещении одного из отделов на небольшой площади находится 7-8 одновременно работающих компьютеров, служащие данного отдела подвергаются воздействию электромагнитных полей от системных блоков и источника бесперебойного питания.

При повышенном уровне напряженности электромагнитных полей следует сократить время работы за компьютером, делать пятнадцатиминутные перерывы в течение полутора-двух часов работы.

В современных мониторах, каковым является наша модель, применяются кинескопы с токопроводящим покрытием на поверхности экрана, поэтому для снятия электростатического заряда с поверхности экрана необходимо заземлить монитор.

Предельно допустимые значения характеристик ЭМП указаны в таблице 23 (СанПиН 2.2.2/2.4.1340-03).

Таблица 3.1 - Временные допустимые уровни ЭМП, создаваемых ПЭВМ

| Наименование параметров | | ВДУ ЭМП |
|---|---|---|
| Напряженность электрического поля | в диапазоне частот 5 Гц - 2 кГц | 25 В/м |
| | в диапазоне частот 2 кГц - 400 кГц | 2,5 В/м |
| Плотность магнитного потока | в диапазоне частот 5 Гц - 2 кГц | 250 нТл |
| | в диапазоне частот 2 кГц - 400 кГц | 25 нТл |
| Электростатический потенциал экрана видеомонитора | | 500 В |
| Напряженность электростатического поля | | 15 кВ/м |

Для предупреждения внедрения опасной техники все дисплеи должны проходить испытания на соответствие требованиям безопасности (например международные стандарты MRP 2, TCO’95, TCO'99), что в нашем случае выполняется (монитор соответствует стандарту TCO’99).

Ионизирующее излучение (рентгеновское).

Опасность этого вида излучения связана с его способностью проникать в тело человека на глубину 1-2 см и поражать поверхностный кожный покров.

По СанПиН 2.2.2/2.4.1340-03 мощность экспозиционной дозы рентгеновского излучения в любой точке на расстоянии 0.05 м от экрана и корпуса при любых положениях регулировочных устройств не должна превышать 100мкР/час. Мониторы, соответствующий стандарту ТСО-99 безопасны в этом отношении.

Видимое излучение экрана.

Видимое излучение способствует возникновению близорукости и переутомлению глаз, мигрени и головной боли, компьютерного зрительного синдрома, раздражительности, нервному напряжению и стрессу. Основное негативное влияние на оператора оказывает зрительно-напряженная работа с монитором. Большое число пользователей (до 60%) жалуется на усталость, резь и боль в глазах. Практически у всех пользователей при непрерывной работе за компьютером в течение шести часов наступает компьютерный зрительный синдром: жжения в глазах, чувство «песка» под веками, боли в области глазниц и лба и т.д.

Электробезопасность.

На расстоянии 50 см влияние электростатического поля уменьшается до безопасного для человека уровня. Но при работе монитора электризуется - приобретает положительный заряд - не только его экран, но и воздух в помещении. Положительно наэлектризованные молекулы кислорода не воспринимается организмом как кислород, приносят в легкие микрочастицы пыли.

Помещение по опасности поражения электрическим током можно отнести к 1 классу, т.е. это помещение без повышенной опасности (сухое, беспыльное, с нормальной температурой воздуха, изолированными полами и малым числом заземленных приборов).

На рабочем месте оператора ПЭВМ из всего оборудования металлическим является лишь корпус системного блока компьютера, но здесь используются системные блоки, отвечающие стандарту фирмы IBM, в которых кроме рабочей изоляции предусмотрен элемент для заземления и провод с заземляющей жилой для присоединения к источнику питания. Таким образом, оборудование кабинета помощника по безопасности выполнено по классу 1 (ПУЭ). [https://www.elec.ru/library/direction/pue.html]

Электробезопасность обеспечивается в соответствии с ГОСТ 12.1. 030.-81.[ http://docs.cntd.ru/document/5200289] Так как все токоведущие части ЭВМ изолированы, то случайное прикосновение к токоведущим частям исключено.

Напряжение сети переменного тока 220 В опасно для жизни человека. Помещения, где размещаются рабочие места с ПЭВМ, должны быть оборудованы защитным заземлением (занулением) в соответствии с техническими требованиями по эксплуатации.

Для обеспечения защиты от поражения электрическим током при прикосновении к металлическим нетоковедущим частям, которые могут оказаться под напряжением в результате повреждения изоляции, применяется защитное заземление. Заземление корпуса ЭВМ обеспечено подведением заземляющей жилы к питающим розеткам. Сопротивление заземления 4 Ом, согласно (ПУЭ) для электроустановок с напряжением до 1000 В.

Основным организационным мероприятием является инструктаж и обучение безопасным методам труда, а также проверка знаний правил безопасности и инструкций в соответствии с занимаемой должностью применительно к выполняемой работе.

## 4.2 Работоспособность сотрудника и ее динамика

Существует целый ряд мероприятий, направленных на предотвращение неблагоприятного влияния на здоровье человека вредных факторов при работе с ЭВМ: характеристики помещения; микроклимат в помещении; уровень шума и вибраций; освещение рабочего места; электромагнитные поля; организация рабочего места; нервное напряжение и нагрузка;

Рассмотрим эти факторы немного подробнее (все ниже перечисленные требования, параметры значения соответствуют СанПиН 2.2.2/2.4.1340-03), с учетом специфики работ.

1. Требования к помещениям:

a) Площадь рабочего места – 6 $м^2$;

b) При отделке интерьера должны использоваться материалы с диффузно-отражающей поверхностью и коэффициентом отражения: для потолка – 0,7÷0,8; для стен - 0,5÷0,6; для пола - 0,3÷0,5;

2. Требования предъявляемые к микроклимату в помещениях для работы с ЭВМ:

a) Ежедневная влажная уборка и ежечасное проветривание.

b) Содержание вредных химических веществ в помещениях не должно превышать предельно допустимых концентраций загрязняющих веществ в атмосферном воздухе населенных мест в соответствии с действующими гигиеническими нормативами (согласно СанПиН 2.2.2/2.4.1340-03, п4.7).

Также уровни шума и вибраций не должны превышать предельно допустимых значений, установленных для данных видов работ в соответствии с действующими санитарно-эпидемиологическими нормативами (согласно СанПиН 2.2.2/2.4.1340-03 п.5.1).

Согласно п.6 СанПиН 2.2.2/2.4.1340-03 - освещенность на поверхности стола в зоне размещения рабочего документа должна быть 300 - 500 лк. Освещение не должно создавать бликов на поверхности экрана. Освещенность поверхности экрана не должна быть более 300 лк. Яркость светильников общего освещения в зоне углов излучения от 50 до 90 градусов

с вертикалью в продольной и поперечной плоскостях должна составлять не более 200 кд/м$^2$, защитный угол светильников должен быть не менее 40 градусов.

В качестве источников света при искусственном освещении следует применять преимущественно люминесцентные лампы типа ЛБ и компактные люминесцентные лампы (КЛЛ). При устройстве отраженного освещения в производственных и административно-общественных помещениях допускается применение металлогалогенных ламп. В светильниках местного освещения допускается применение ламп накаливания, в том числе галогенные.

Для предотвращения болезней связанных с заболеваниями кистей рук, болезнями нервов, мышц, сухожилий рук, которые принято объединять в один комплекс – травмы повторяющихся нагрузок; следует использовать правильно оборудованные рабочие места.

Рабочий стол должен иметь пространство для ног высотой не менее 600 мм, шириной - не менее 500 мм, глубиной на уровне колен - не менее 450 мм и на уровне вытянутых ног - не менее 650 мм. Конструкция рабочего стула должна обеспечивать (согласно СанПиН 2.2.2/2.4.1340-03): ширину и глубину поверхности сиденья не менее 400 мм; поверхность сиденья с закругленным передним краем; регулировку высоты поверхности сиденья в пределах 400 - 550 мм и углам наклона вперед до 15 град, и назад до 5 град; высоту опорной поверхности спинки 300±20 мм, ширину - не менее 380 мм и радиус кривизны горизонтальной плоскости - 400 мм; угол наклона спинки в вертикальной плоскости в пределах ±30 градусов; регулировку расстояния спинки от переднего края сиденья в пределах 260 - 400 мм; стационарные или съемные подлокотники длиной не менее 250 мм и шириной - 50 - 70 мм; регулировку подлокотников по высоте над сиденьем в пределах 230±30 мм и внутреннего расстояния между подлокотниками в пределах 350 - 500 мм.

Для операторов ЭВМ характерны заболевания, связанные с высокими нагрузками на зрительный анализатор, а также с необходимостью постоянно

поддерживать высокую степень готовности, концентрацию внимания. Нагрузка на зрительный анализатор и, как следствие – возникновение психоэмоционального дискомфорта и напряжения, обусловлена следующими факторами:

- пониженным контрастом изображения монитора. Яркость изображения складывается из свечения символа и отраженного света. Контраст можно увеличить применением тонированных фильтров.
- низкая четкость контуров изображения – падает при повышении яркости свечения экрана;
- зеркальные блики от экрана – устраняются применением специальных фильтров с антибликовым покрытием;
- мерцание экрана – устранимо повышением частоты кадровой развертки.

Утомляемость сотрудников, работающих за дисплейным терминалом, представляет собой серьезную проблему. Известно, что наиболее вредны именно повторяющиеся однообразные нагрузки. Через усталость они могут вести к физическому повреждению суставов и сухожилий. Поэтому даже при наличии современной, относительно безопасной офисной техники остается актуальной задача сконструировать рабочее место оператора и организовать режим работы так, чтобы взаимосвязи в системе «человек-машина» были оптимальными со всех точек зрения. На основании проведенного анализа вредных факторов можно сделать вывод, что большое значение для охраны труда сотрудников банка имеет именно правильная организация рабочего места и режим труда.

Правила работы за дисплейными терминалами определяются гигиеническими требованиями к персональным электронно-вычислительным машинам и организации работы (СанПиН 2.2.2/2.4.1340-03). Соответствие рабочих мест нормативным документам обеспечивает администрация, однако, необходимо отметить, что контроль собственного рабочего места и режима труда во многом зависит от самих сотрудников, поэтому

организационные меры по охране труда должны включать также мероприятия по работе с персоналом.

Ниже приводятся рекомендации по организации рабочего места:

1. Использование видеомониторов.

Экран должен находится от глаз на расстоянии 600 - 700 мм, но не ближе 500 мм. Угол считывания, т.е. направление взгляда должно быть на 10-20 градусов ниже горизонтали к центру экрана. Положение экрана – на уровне глаз или немного ниже, таким образом, чтобы шейные мышцы не напрягались. Должна предусматриваться возможность регулирования экрана по высоте, по наклону и в левом и правом направлениях. Для монитора 15" оптимально разрешение 800*600, для 17" - 1024*768 при указанных выше расстояниях, для 19”, 21” - 1280x1024 при 0,8-1,5 м до экрана.

Допустимыми визуальными параметрами устройств отображения информации являются (таблица 3.2):

Таблица 3.2 – Допустимые визуальные параметры устройств отображения информации

| №п/п | Параметры | Допустимые значения |
|---|---|---|
| 1 | Яркость белого поля | Не менее 35 кд/кв. м |
| 2 | Неравномерность яркости рабочего поля | Не более +/- 20% |
| 3 | Контрастность (для монохромного режима) | Не менее 3:1 |
| 4 | Временная нестабильность изображения (непреднамеренное изменение во времени яркости изображения на экране дисплея) | Не должна фиксироваться |
| 5 | Пространственная нестабильность изображения (непреднамеренные изменения положения фрагментов изображения на экране) | Не более 2 x 1E(-4L), где L - проектное расстояние наблюдения, мм |

Плоский монитор более предпочтителен для применения. При использовании выпуклых мониторов вредное воздействие на зрение может компенсироваться гимнастикой для глаз. Согласно СанПиН 2.2.2/2.4.1340-03 частота развертки монитора должна быть не менее 75 Гц при всех режимах разрешения экрана и не менее 60 Гц для LCD мониторов.

Время послесвечения люминофора. Настоятельно рекомендуется выбирать плоскоэкранный монитор с частотой развертки не менее 100 Гц (либо TFT панель) и хорошую видеокарту, поддерживающую оптимальный режим работы монитора.

Цветовая гамма изображения на экране. Общие рекомендации: фоновые цвета должны быть неяркими и в приятной для пользователя цветовой гамме, шрифты контрастными и достаточного размера.

Не рекомендуется устанавливать вплотную к монитору аудиоколонки и источники бесперебойного питания, т.к. эти устройства являются источником наводок и портят качество изображения, иногда это проявляется заметным для глаз дрожанием картинки.

2. Схема размещения рабочих мест.

Расстояние между рабочими столами с видеомониторами (от тыла одного видеомонитора до экрана другого) должно быть не менее 2.0 м, а расстояние между боковыми поверхностями видеомониторов - не менее 1.2 м.

3. Конструкция рабочего стула.

Рабочий стул (кресло) должен быть подъемно-поворотным и регулируемым по высоте и углам наклона сиденья и спинки, а также расстоянию спинки от переднего края сиденья, регулировка каждого параметра должна быть независимой, легко осуществляемой и иметь надежную фиксацию. Правильная высота сиденья: площадь сиденья на 3 см ниже, чем подколенная впадина. Рекомендуемая высота сиденья над уровнем пола должна быть в пределах 400-550 мм. Поверхность сиденья рекомендуется делать мягкой, а передний край закругленным.

Правильная установка рабочего стола:

- при фиксированной высоте - лучшая высота - 72 см;
- рекомендуется возможность регулирования высоты рабочей поверхности в пределах 680-760 мм;

- стол должен обеспечиваться необходимый простор для рук по высоте, ширине и глубине; предпочтительно применение специализированного компьютерного стола;
- в области сиденья не должно быть ящиков стола.

4. Расположение клавиатуры.

Расположение клавиатуры не должно приводить к напряжению рук. Уровень клавиатуры - чуть выше колен, таким образом, чтобы предплечья были параллельны полу. Из современных моделей клавиатур рекомендуется выбрать клавиатуру с разворотом 2х блоков относительно друг друга, и с «горбом». Для избежания неблагоприятных воздействий на суставы кистей рук целесообразно применять подставки для рук и клавиатуры. Если клавиатура выше 1.5 см желательно использовать подлокотники.

5. Расположение документа для чтения.

Документ для чтения должен находиться на одном уровне с дисплеем, сбоку от видеотерминала или между монитором и клавиатурой, клавиатурой и пользователем и т.п. Когда видеотерминал имеет низкое качество изображения, расстояние от глаз до экрана делают больше (около 700 мм), чем расстояние от глаза до документа (300-450 мм). При высоком качестве изображения на видеотерминале расстояние от глаз пользователя до экрана, документа и клавиатуры может быть равным.

6. Рабочая поза пользователя.

Нога должна стоять большую часть времени на полу полной ступней. Благоприятно использование опоры для ног. Рука должна и локтем, и запястьем лежать на чем-нибудь. В том случае, если пользователь сидит за двумя столами, составленными углом, положение рук при печати на клавиатуре наиболее хорошее. При работе мышью, рука всегда должна касаться стола и локтем, и запястьем, и предплечьем. Требования к правильной рабочей позе пользователя видеотерминала следующие:

- шея не должна быть наклонена более чем на 20 градусов;

- плечи должны быть расслаблены, локти - находиться под углом 80–100 градусов, а предплечья и кисти рук - в горизонтальном положении;
- положение туловища и головы прямое;
- руки и ноги - согнуты чуть больше, чем под прямым углом;
- клавиатура и дисплей примерно на одинаковом расстоянии для глаз: при постоянных работах - 50 см, при случайных работах - до 70 см.

7. Режим работы должен соответствовать следующим правилам:

- необходимо предусматривать по возможности перемену задач и нагрузок;
- соблюдать перерывы: 5 минут через 1 час работы на дисплее или 10 минут после 2-х часов работы на дисплее. В перерыве рекомендуется делать физические упражнения с растяжением мышц спины и рук;
- периодически расслаблять глаза, делать гимнастику для глаз, массировать глазные яблоки и переводить взгляд с близко расположенных объектов на объекты за окном.

### 4.3 Пожарная безопасность предприятия

Среди чрезвычайных ситуаций наиболее вероятной является пожар. Общие требования к пожарной безопасности нормируются ГОСТ 12.1.004–91. [http://docs.cntd.ru/document/9051953]

Пожарная безопасность – состояние объекта, при котором исключается возможность пожара, а в случае его возникновения предотвращается воздействие на людей опасных факторов пожара и обеспечивается защита материальных ценностей. Пожарная безопасность обеспечивается системой предотвращения пожара и системой пожарной защиты. Во всех служебных помещениях имеются детекторы системы оповещения о пожаре (детекторы дыма, температурные датчики), а также «План эвакуации людей при пожаре», регламентирующий действия персонала в случае возникновения очага возгорания и указывающий места расположения пожарной техники.

Пожар в кабинете сотрудников подразделения безопасности представляет особую опасность, так как сопряжен с большими материальными и документальными потерями. Характерной особенностью данного помещения является небольшая площадь помещения. Как известно пожар может возникнуть при взаимодействии горючих веществ, окисления и источников зажигания.

Горючими компонентами являются: бумажные документы, строительные материалы для акустической и эстетической отделки помещений, перегородки, двери, полы, изоляция кабелей и др.

Источниками зажигания могут быть электронные схемы от ПЭВМ, приборы, применяемые для технического обслуживания, устройства электропитания, где в результате различных нарушений образуются перегретые элементы, электрические искры и дуги, способные вызвать загорания горючих материалов.

В современных ПЭВМ очень высокая плотность размещения элементов электронных схем. В непосредственной близости друг от друга располагаются соединительные провода, кабели. При протекании по ним электрического тока выделяется значительное количество теплоты. При этом возможно оплавление изоляции. Для отвода избыточной теплоты от ПЭВМ служат системы вентиляции и кондиционирования воздуха. При постоянном действии эти системы представляют собой дополнительную пожарную опасность.

Во всех служебных помещениях установлены дымовые пожарные извещатели системы оповещения о пожаре. В коридорах имеются шкафы с пожарными кранами, противопожарное оборудование присутствует [16].

К средствам тушения пожара, имеющимся на предприятии, относится углекислотный огнетушитель (ОУ-8), достоинством которого является высокая эффективность тушения пожара, сохранность электронного оборудования, диэлектрические свойства углекислого газа, что позволяет

использовать огнетушители даже в том случае, когда не удается обесточить электроустановку сразу.

Общие требования к пожарной безопасности нормируются ГОСТ 12.1.004–91. Оборудование помещений пожарной сигнализацией соответствует нормам.

## Список литературы


1. Постановление Правительства РФ от 01.11.2012 N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» // «Российская газета», N 256, 07.11.2012.
2. Приказ ФСТЭК России от 18.02.2013 N 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (Зарегистрировано в Минюсте России 14.05.2013 N 28375) // «Российская газета», N 107, 22.05.2013.
3. «Стандарт Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» СТО БР ИББС-1.0-2014» (принят и введен в действие Распоряжением Банка России от 17.05.2014 N Р-399) // «Вестник Банка России», N 48-49, 30.05.2014.
4. «Положение о требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств» (утв. Банком России 09.06.2012 N 382-П) (ред. от 14.08.2014) (Зарегистрировано в Минюсте России 14.06.2012 N 24575) // В данном виде документ опубликован не был, первоначальный текст документа опубликован в «Вестник Банка России», N 32, 22.06.2012.
5. «Положение о порядке представления кредитными организациями в уполномоченный орган сведений, предусмотренных Федеральным законом «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» (утв. Банком России 29.08.2008 N 321-П) (ред. от 15.10.2015) (вместе с «Порядком обеспечения информационной безопасности при передаче-приеме ОЭС», «Правилами формирования ОЭС и заполнения отдельных

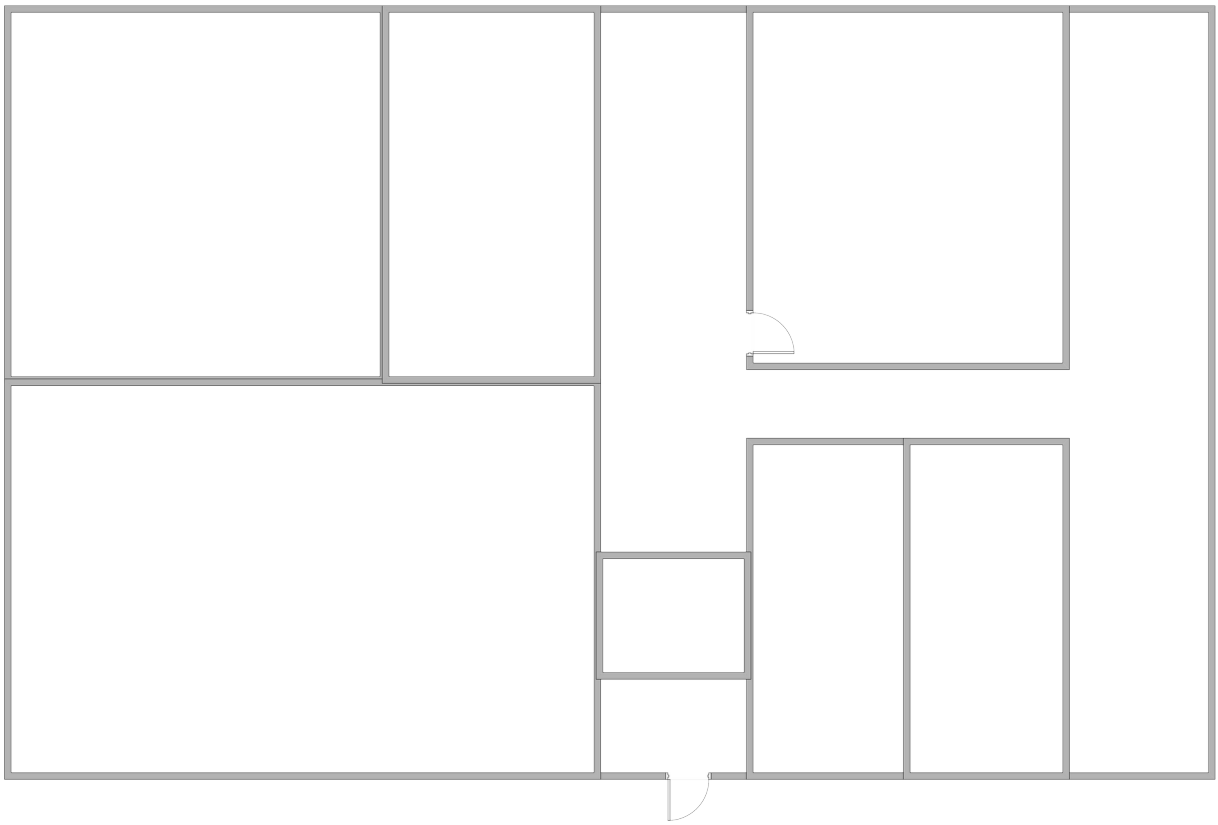
полей записей ОЭС») (Зарегистрировано в Минюсте России 16.09.2008 N 12296) // В данном виде документ опубликован не был, Первоначальный текст документа опубликован в «Вестник Банка России», N 54, 26.09.2008.

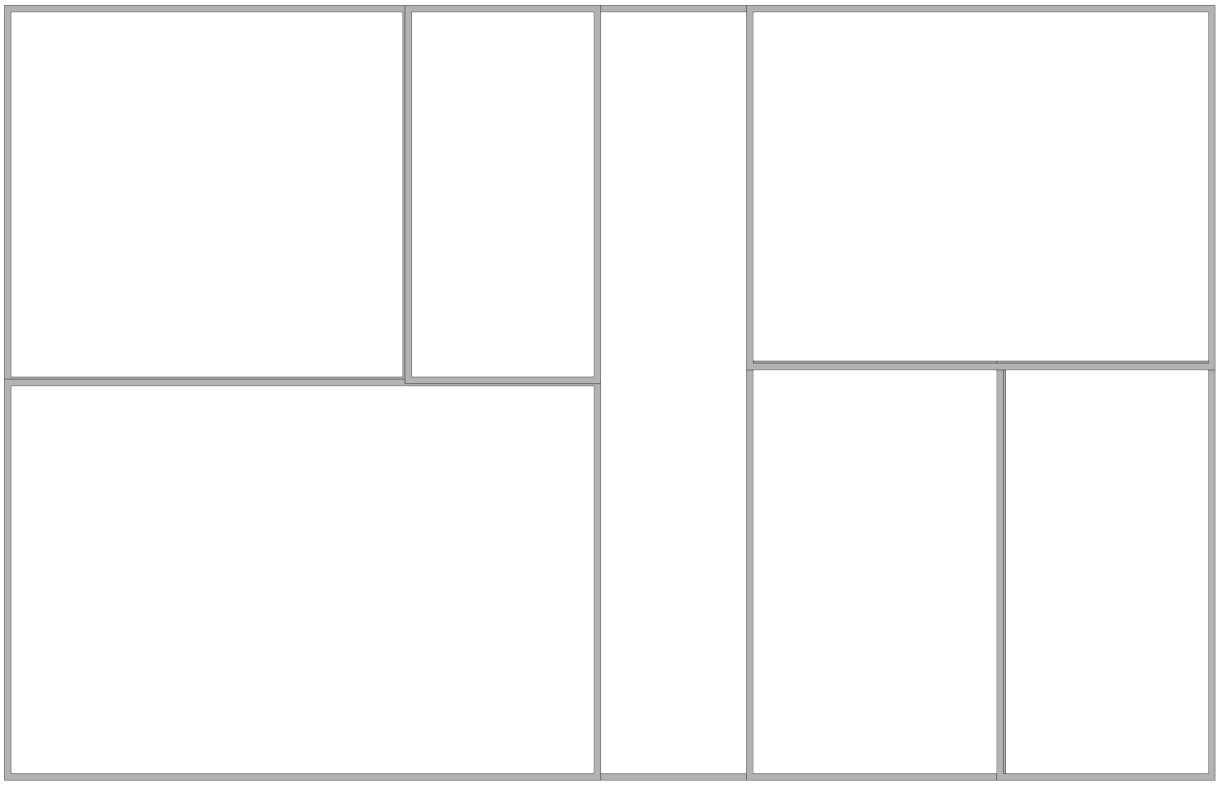
6. Приказ ФСТЭК России от 18.02.2013 N 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (Зарегистрировано в Минюсте России 14.05.2013 N 28375) // «Российская газета», N 107, 22.05.2013.
7. Аверченков В.И., Рытов М.Ю., Гайнулин Т.Р. Защита персональных данных в организациях. М.: Флинта, 2011.
8. Агапов А. Б. Основы государственного управления в сфере информатизации в Российской Федерации. М.: Юристъ, 2012.
9. Костин А. А., Костина А. А., Латышев Д. М., Молдовян А. А. Программные комплексы серии „АУРА“ для защиты информационных систем персональных данных // Изв. вузов. приборостроение. 2012. Т. 55, № 11.
10. Молдовян А. А. Криптография для защиты компьютерной информации (часть 1) // Интеграл. 2014. № 4 (18).
11. Бабаш, А.В. Информационная безопасность. Лабораторный практикум: Учебное пособие / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. - М.: КноРус, 2013. - 136 с.
Бирюков, А.А. Информационная безопасность: защита и нападение / А.А. Бирюков. - М.: ДМК Пресс, 2013. - 474 с.
12. Баранова Е. К. Информационная безопасность и защита информации: Учебное пособие/Баранова Е. К., Бабаш А. В., 3-е изд. - М.: ИЦ РИОР, НИЦ ИНФРА-М, 2016. - 322 с. URL: http://znanium.com/bookread2.php?book=495249
13. Глинская Е. В. Информационная безопасность конструкций ЭВМ и систем: Учебное пособие/ГлинскаяЕ.В., ЧичваринН.В. - М.: НИЦ

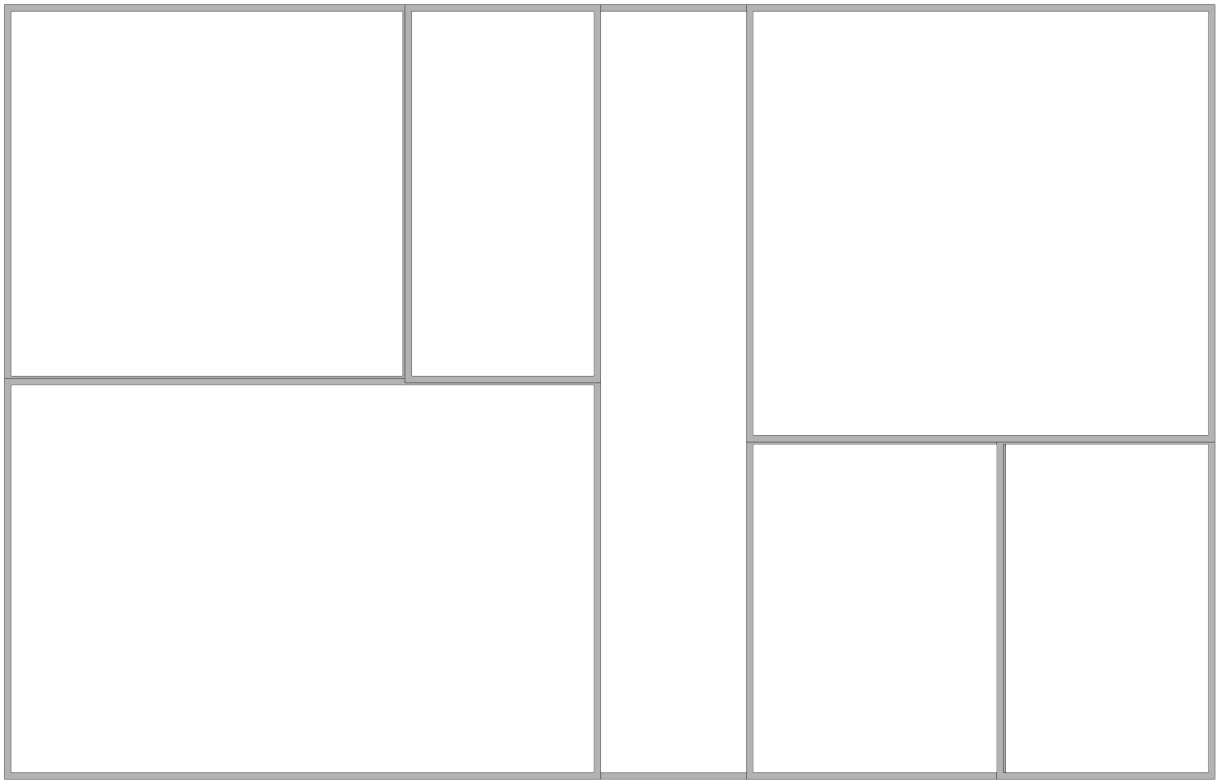
ИНФРА-М, 2016. - 118 с. URL: http://znanium.com/bookread2.php?book=507334

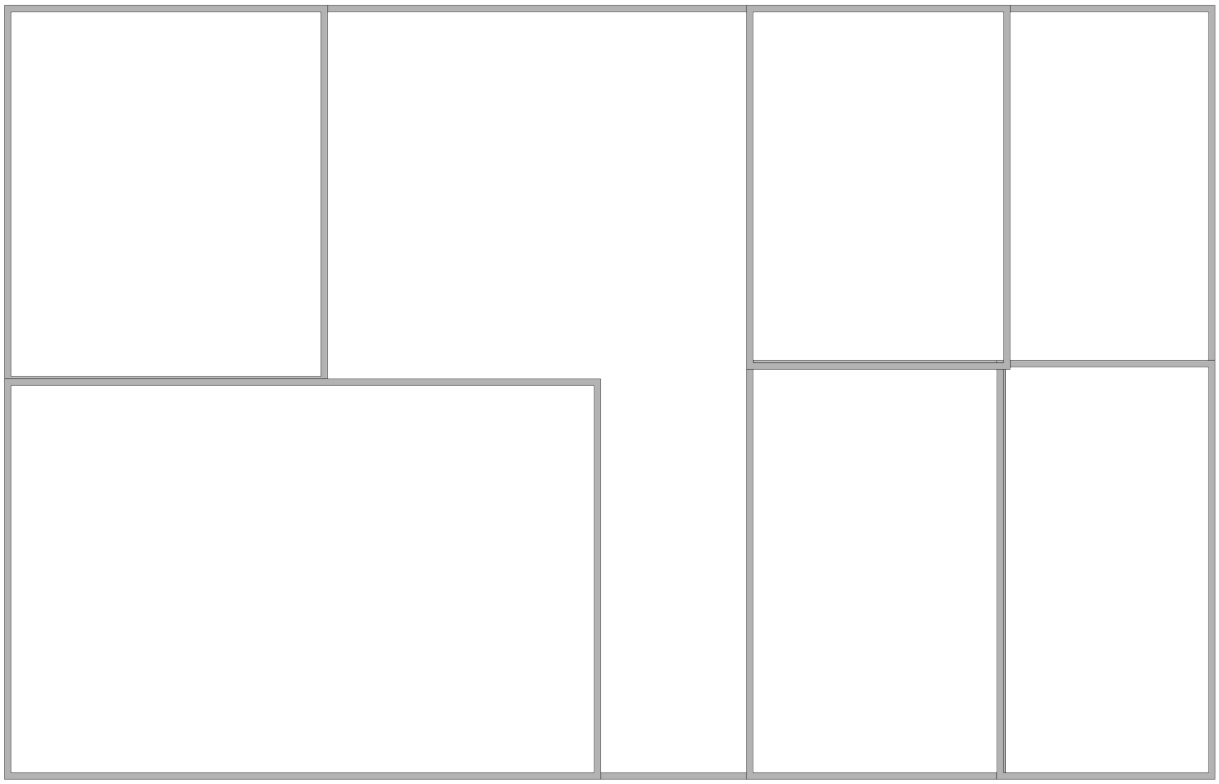
14. Жук А. П. Защита информации: Учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 2-е изд. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015. - 392 с. URL: http://znanium.com/bookread2.php?book=474838
15. Петров, С.В. Информационная безопасность: Учебное пособие / С.В. Петров, И.П. Слинькова, В.В. Гафнер. — М.: АРТА, 2012. — 296 с.

## Приложение 1. Горизонтальная СКС

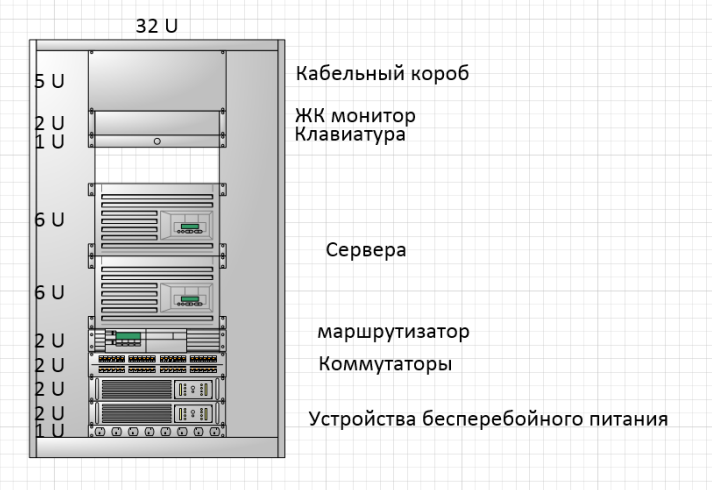








# Приложение 2. Телекоммуникационный шкаф



## Приложение 3. Схема устройств в сети

