Министерство образования и науки Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Южно-Уральский государственный университет
(национальный исследовательский университет)»

**Высшая школа электроники и компьютерных наук**

**Кафедра «Защита информации»**

ДОПУСТИТЬ К ЗАЩИТЕ
Заведующий кафедрой,
к.т.н., доцент
_____ А.Н. Соколов
_____ 2017 г.

# Модернизация системы защиты информации частного охранного предприятия "Витязь"

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА
К ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЕ

Автор проекта,
студент группы КЭ- 431
_____ Хмарина, Я. А.
_____ 2017 г.

Нормоконтролер,
к.т.н., доцент
_____ В.П. Мартынов
_____ 2017 г.

Челябинск 2017

ОГЛАВЛЕНИЕ

# СПИСОК СОКРАЩЕНИЙ

АРМ - Автоматизированное рабочее место;
ИСПДн - Информационная система персональных данных;
КЗ - Контролируемая зона;
КИС - Компьютерная информационная система;
МЭ - Межсетевой экран;
НДВ - Недекларированные возможности;
НСД - Несанкционированный доступ;
ООО - Общество с ограниченной ответственностью;
ПДн - Персональные данные;
ПО - Программное обеспечение;
СЗИ - Средства защиты информации;
СЗПДн – средства защиты персональных данных;
СКУД - Система контроля управления доступом;
СНГ - Содружество независимых государств;
ФСТЭК - Федеральная служба по техническому и экспортному контролю;
ЧОП - Частное охранное предприятие;
РФ - Российская Федерация;
АТЭС - Азиатско-Тихоокеанское экономическое сотрудничество;
ООН - Организация Объединенных Наций;
США - Соединенные Штаты Америки;
ЕС - Евросоюз;
ОЭСР - Организация по экономическому сотрудничеству и развитию;
ПЭМИН - Побочные электромагнитные излучения и наводки;
ЭВМ - Электронно-вычислительная машина;
ККС - Корпоративная компьютерная сеть;
ГУ МВД - Главное управление министерства внутренних дел;
ГБР - Группа быстрого реагирования.

# ВВЕДЕНИЕ

Информационная безопасность в настоящее время становится одним из важнейших аспектов в общей деятельности современной организации, характеризуя состояние защищенности ее бизнес-среды. Каждый день организации сталкиваются с проблемами, связанными с угрозами информационной безопасности, они являются неотъемлемой частью ведения бизнеса.

Существуют различные типы угроз информационной безопасности. Под угрозой понимается возможное событие, действие, процесс или явление, которые могут привести к нанесению ущерба чьим-либо интересам.

Источниками угроз могут выступать как субъекты, так и объективные проявления, например, конкуренты, преступники, коррупционеры. Источники угроз при этом преследуют такие цели: ознакомление с охраняемой информацией, ее модификация в корыстных целях и уничтожение для нанесения ущерба.

Частное охранное предприятие «Витязь» занимается оказанием различного рода услуг, связанных с личной охраной, сопровождением, охраной квартир, офисов, коттеджей, торговых и развлекательных комплексов. В связи с характером предоставляемых услуг, предприятие сталкивается с необходимостью обработки персональных данных клиентов. Клиентская база ООО ЧОП «Витязь» содержит порядка 10000 наименований и представляет собой крупную ИСПДн. В настоящее время персональные данные людей имеют большую ценность и являются объектом интереса для различных видов злоумышленников. Это обуславливает необходимость защиты персональных данных.

Со временем появляются новые и более опасные угрозы информационной безопасности, что делает необходимым постоянное совершенствование системы защиты информации.

Целью работы является модернизация системы защиты информации ООО ЧОП «Витязь».

Для выполнения цели работы необходимо определить ряд сопутствующих задач, а именно:

- проанализировать объект защиты, его род деятельности;
- определить защищаемую информацию;
- составить модель угроз, соответствующего типа;
- рассмотреть и проанализировать опыт разных стран в сфере информационной безопасности;
- сформировать рекомендации по защите информации от актуальных угроз;
- составить недостающие организационно-правовые документы.

Объектом исследования в данной работе является система защиты информации на предприятии ООО ЧОП «Витязь».

Предметом исследования является модернизация системы защиты информации ООО ЧОП «Витязь».

# 1 АНАЛИЗ ИНФОРМАЦИОННОЙ СИСТЕМЫ ОБЪЕКТА

## 1.1 Описание деятельности предприятия

Группа охранных предприятий «Витязь» является одной из крупных охранных структур по меркам общероссийского уровня. Компания успешно работает на рынке Челябинска с 1997 года и специализируется на охране коммерческих объектов, квартир и коттеджей. Признанием профессионализма предприятия стали многочисленные награждения от имени ГУМВД России по Челябинской области, а также многочисленные награды:

- 2006 г. - получено звание «Лучший охранный пульт России-2006»;
- 2007 г. - лучшее охранное предприятие по результатам опроса жителей г. Челябинска (проект «Телефонная книга отзывов»);
- 2007 г**.** - премия «Бизнес-прорыв: семь компаний, перевернувших рынки»;
- 2008 г. - внесены в реестр «Надежная репутация». Исследование проводилось Автономной некоммерческой организацией «Надежная репутация» и департаментом статистики и экспертизы ООО «Статэксперт»;
- 2009 г**.** - лауреат национального конкурса «Лучшие охранные предприятия России»;
- 2009 г. - получено звание «Лучший охранный пульт России-2009» (наш пульт был признан лучшим среди 60-ти аналогичных пультов охраны по всей стране);
- 2010 г. - лучшее охранное агентство Челябинска по версии 74.ru;
- 2010 г**.** - охранное предприятие «Витязь» прошло сертификацию на соответствие стандарту ИСО 9001-2008.

Группа охранных предприятий «Витязь» обладает большой материальной базой. Специалисты работают в современных офисных помещениях, в распоряжении группы компаний имеются гаражные комплексы, автотранспорт, помещения инженерно-технических служб, оружейные комнаты. Все это в комплексе обеспечивает возможность оказания охранных услуг на высоком уровне.

В качестве основных направлений работы компании можно выделить следующие:

- пультовая охрана коммерческих объектов, квартир и коттеджей;
- монтаж охранно-пожарной и тревожной сигнализации, систем контроля доступа и видеонаблюдения;
- физическая охрана офисов, торговых и промышленных предприятий;
- вооруженное сопровождение материальных ценностей и грузов по городу и в пределах РФ;
- услуги охраны мобильных объектов (автомобилей).

Качество оказываемых охранных услуг зависит прежде всего от подготовки и профессионализма сотрудников охранного предприятия, материально-технического оснащения персонала охранного предприятия, используемых систем охраны, качества монтажа системы охраны.

Специалисты ООО ЧОП «Витязь» самостоятельно выполняют монтаж систем охраны различного вида и уровня сложности. До проведения работ по установке систем охраны, сотрудники осведомляют клиента о порядке работы систем охраны, принципах функционирования отдельного оборудования и элементов системы.

Проведение монтажа силами охранного предприятия, которое в последствие будет оказывать услуги охраны, имеет ряд преимуществ:

- клиент всегда может оперативно внести изменения в имеющуюся систему без ущерба безопасности охраняемому объекту;
- в случае необходимости настройки, модификации или ремонта системы нет необходимости согласовывать действия охранного предприятия и организации выполнившей монтаж оборудования;
- охранное предприятие, имеющее в штате технических специалистов, всегда может оперативно исправить возникшие неполадки или изменить настройки систем по желанию клиента;
- будучи ответственным за эксплуатацию и обслуживание систем охраны, охранное предприятие применяет наиболее эффективные и надежные системы из существующих на рынке.

Системы охраны, используемые группой охранных предприятий «Витязь», имеют возможность передачи сообщений на пульт централизованного наблюдения по нескольким каналам связи: радиосигнал, каналы GSM, проводная телефонная связь или международная телекоммуникационная сеть, что повышает их уровень надежности – при выходе из строя одного из каналов связи остается возможность использования резервного.

Личный кабинет (облачный сервис) - это дополнительная услуга, позволяющая все делать самостоятельно и оперативно: удалённо снять и поставить объекты на охрану, посмотреть живое видео с камер и короткие видеоролики в случае срабатывания сигнализации, просмотреть историю постановок, снятий и тревог. Клиентам не нужно тратить деньги за формирование выписок по событиям и не требуется дозваниваться в «час пик» оператору ООО ЧОП «Витязь», чтобы узнать, поставлен ли объект на охрану. Личный кабинет доступен с любого компьютера, в любом браузере и из любой точки мира, где есть интернет или с телефона, поддерживающего MyAlarm Android, MyAlarm iOS

Вооруженные группы быстрого реагирования состоят из трех охранников, что само по себе повышает оперативность и эффективность группы. Каждая группа оснащена средствами индивидуальной защиты (бронежилетами, защитными шлемами), огнестрельным оружием (пистолеты, гладкоствольные карабины). Все автомобили ГБР, оснащены планшетными компьютерами со специальным приложением, позволяющим мгновенно получить информацию о событии на планшет, оптимизировать маршрут и сократить время прибытия на тревожный объект. Дополнительно связь между группами реагирования и пультом централизованного наблюдения обеспечивается радиостанциями, установленными стационарно в автомобилях, а также переносными радиостанциями, входящими в индивидуальную экипировку охранников. Пульт централизованного наблюдения име-

ет возможность отслеживать перемещения групп быстрого реагирования посредством системы спутникового наблюдения.

## 1.2 Паспорт предприятия

Численность предприятия на сегодняшний день составляет более 650 человек. Площадь офисных помещений около 1000 кв.м. Главный офис находится в г. Челябинске по адресу: г. Челябинск ул. Молодогвардейцев д. 37а. Организация занимает трехэтажное здание, пристроенное к девятиэтажному дому, который значится с таким же адресом. Здание ООО ЧОП «Витязь» обнесено забором.

Внешний вид и расположение здания показаны на рисунке 1.

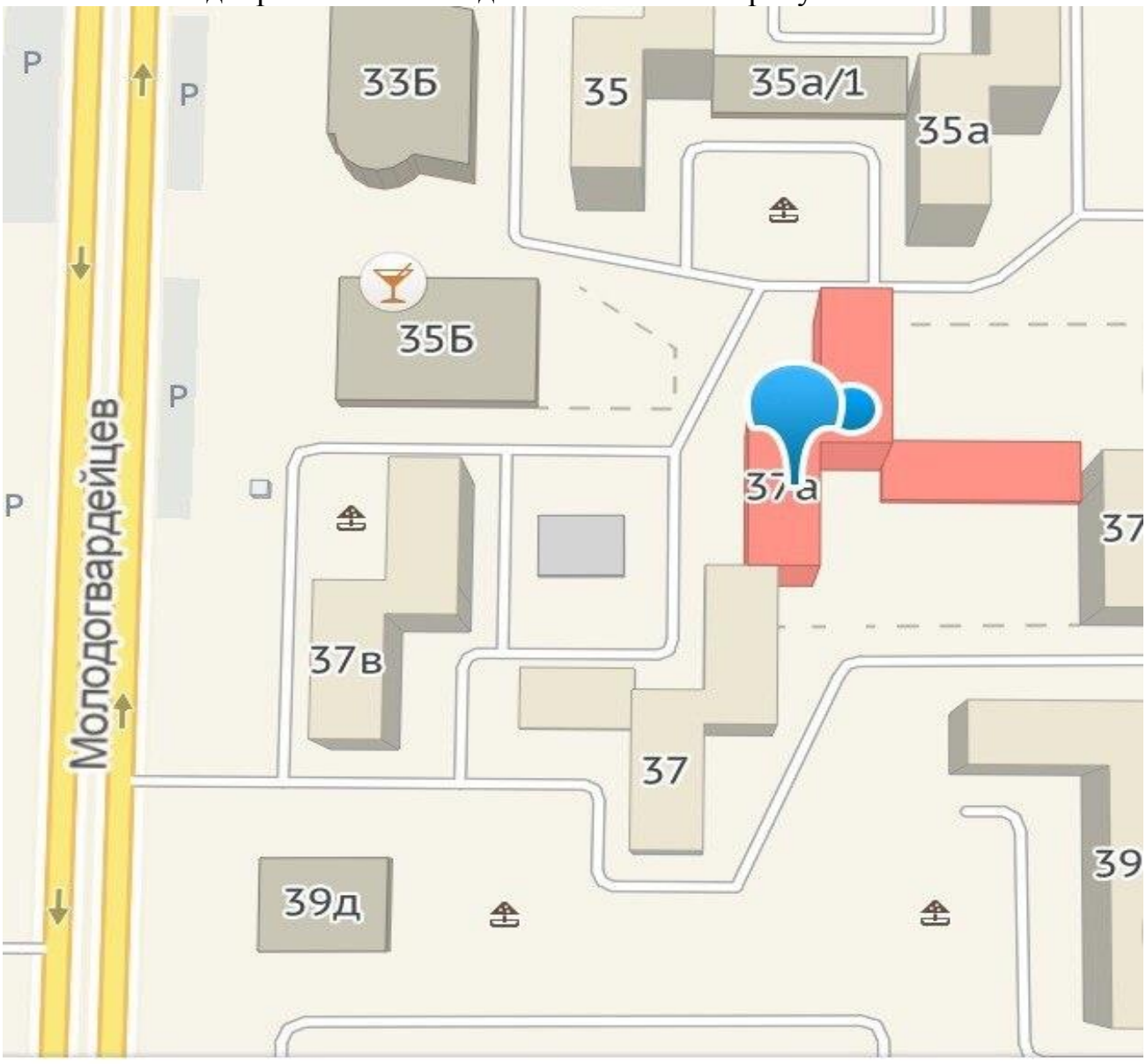


Рисунок 1. Внешний вид и расположение ЧОП Витязь.

По форме капитала, предприятие является обществом с ограниченной ответственностью. Организация функционирует в соответствии с действующим законодательством Российской Федерации и Уставом предприятия. Компания по-

строена по классическому, линейно-функциональному типу структуры управления, что стимулирует деловую и профессиональную специализацию, улучшает координацию и уменьшает дублирование усилий и потребление материальных ресурсов в функциональных областях. ООО ЧОП «Витязь» возглавляет генеральный директор, в высшее звено руководства так же входит заместитель генерального директора и начальники основных отделов.

Стоит отметить, что в компании ООО ЧОП «Витязь» функционирует отдел по защите информации, сотрудники которого осуществляют внедрение организационных и технических мероприятий по защите информации, выявляют возможные каналы утечки информации, в том числе по техническим каналам и разрабатывают меры по их предотвращению и устранению.

Организационно-штатная структура предприятия представлена на рисунке 2.

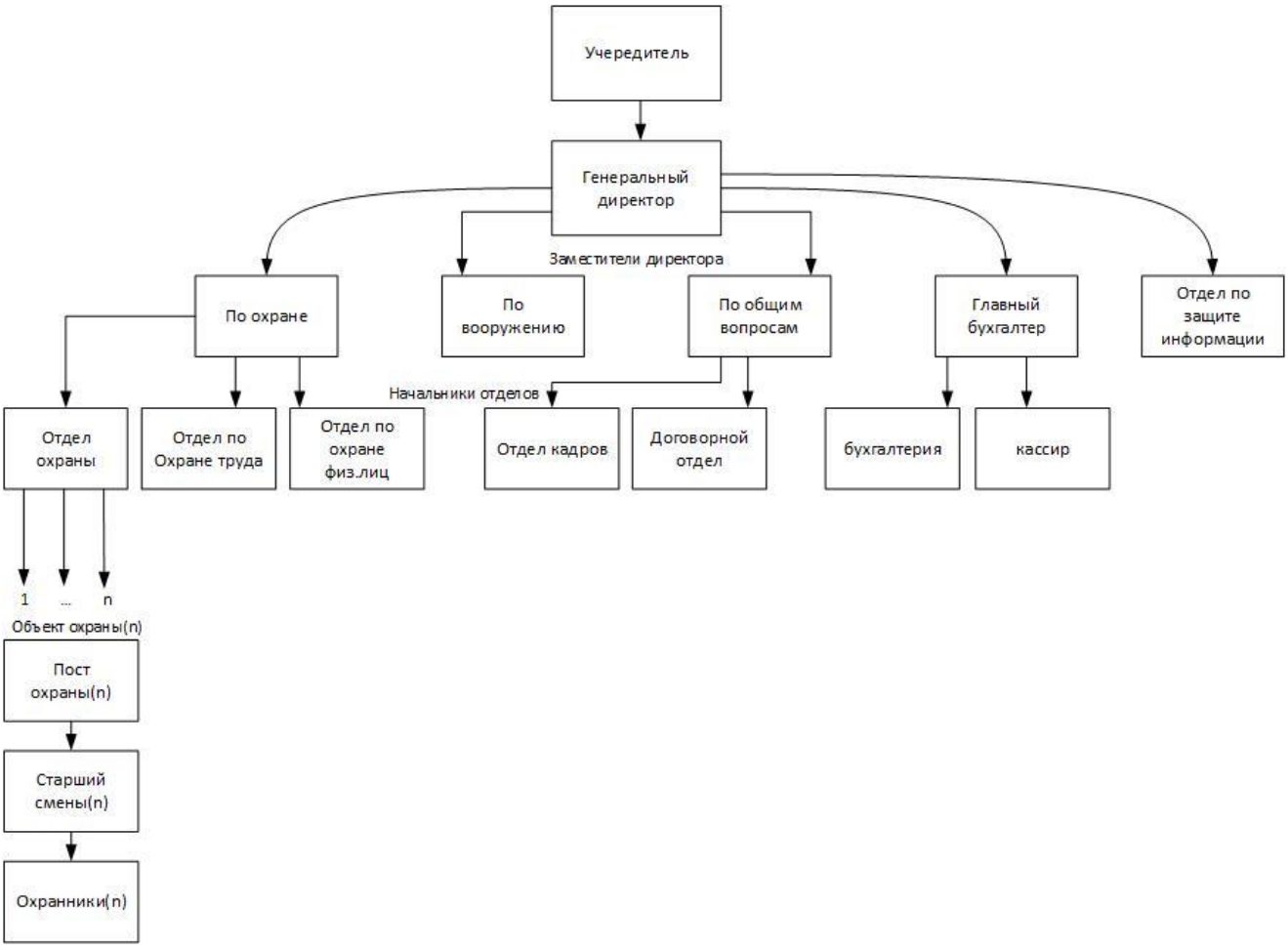


Рисунок 2. Организационно-штатная структура предприятия ЧОП Витязь.

### 1.3 Обследование информационной системы персональных данных

Модернизацию системы защиты персональных данных необходимо начать с описания предметной области и архитектуры ИСПДн. В данной работе речь пойдет о персональных данных клиентов. Базы данных о клиентах хранятся в электронном виде и представляют собой текстовую информацию и отсканированные документы. На данный момент количество охраняемых объектов составляет около 10000.

Обследование является одним из основных этапов работ по защите ПДн и позволяет оценить текущий уровень соответствия ИСПДн требованиям нормативных документов по защите ПДн.

Детальное изучение информационной системы подразумевает собой план действий, охватывающий все манипуляции, связанные со сбором, обработкой, хранением и передачей информации. Для этого был составлен план обследования:

- комплексный анализ процесса обработки ПДн;
- анализ структуры локальной вычислительной сети (далее - ЛВС), наличия подключения ЛВС к сетям общего доступа;
- составление технического паспорта на ИСПДн - перечень ПО, установленного на каждом АРМ;
- формирование планов помещений, в которых находятся аппаратные компоненты ИСПДн (АРМ, сетевое, серверное, коммутационное оборудование ЛВС);
- анализ действующей организационно-распорядительной документации, согласно которой осуществляется обработка ПДн, проверка соответствия данной документации с действующими требованиями законодательных и нормативно-правовых актов, действующих на территории Российской Федерации.

Перечень действий с ПДн: сбор, систематизация, накопление, хранение, уточнение (изменение, обновление), блокирование, уничтожение. Персональные данные по международной телекоммуникационной сети не передаются.

Организация охраны и контроля доступа.

ИСПДн ООО ЧОП «Витязь» расположена на втором этаже 3-этажного здания, находящегося в собственности ООО ЧОП «Витязь». Здание обнесено забором, осуществляется круглосуточная физическая охрана здания и прилегающей территории, так же ведется видеонаблюдение. Вход в здание в нерабочие часы закрыт, в рабочее время вход свободный, за исключением помещений, вход в которые осуществляется по пропускному режиму. Доступ в помещения, где обрабатываются ПДн, осуществляется по бесконтактным картам, имеющимся только у ограниченного списка лиц. Все помещения организации оборудованы охранно-пожарной сигнализацией.

## 1.4 Описание информационной среды предприятия

ИСПДн ООО ЧОП «Витязь» - защищенная локально-вычислительная сеть. Она состоит из 8 автоматизированных рабочих мест операторов, 4 сканеров поточного сканирования, одной рабочей станции администратора и одного сервера. Типология ИСПДн – «звезда», используемые протоколы - TCP/IP. Архитектура системы построена таким образом, что рабочие станции могут независимо обращаться к серверу. Подключение ЛВС к международным телекоммуникационным сетям - отсутствует.

В ООО ЧОП «Витязь» используются самое основное, лицензионное программное обеспечение. В этот список входят следующие программы: Microsoft Office, NOD32, SecretNet, CRM, 1С Предприятие, 1С Бухгалтерия, WinRAR и многие другие.

Microsoft Office - пакет офисных приложений, созданных корпорацией Microsoft для операционных систем Microsoft Windows, AppleMac OS X. В пакет входит ПО для работы с различными типами документов: электронными таблицами, текстами, базами данных и др.

ESET NOD32 – это антивирусный пакет, выпускаемый фирмой ESET. Этот антивирус является комплексным антивирусным решением для защиты в реальном времени. Подавляющая половина кода антивируса написана на ассемблере, поэтому для него характерно малое использование системных ресурсов и высокая скорость проверки с настройками по умолчанию.

CRM-система - это прикладное ПО для организаций, оно предназначено для автоматизации взаимодействия с заказчиками (клиентами), в частности, для повышения уровня продаж, оптимизации маркетинга и улучшения обслуживания клиентов.

1С:Предприятие – это программный продукт компании «1С», предназначенный для автоматизации деятельности на предприятии.

1С: Бухгалтерия - это одно из самых распространенных решений для автоматизации бухгалтерского учёта.

WinRAR - это архиватор файлов в форматы RAR и ZIP для 32- и 64-разрядных операционных систем Windows и ReactOS. Он считается одним из самых лучших архиваторов по соотношению скорости работы к степени сжатия.

## 1.5 Фактическая защита предприятия

### 1.5.1.Правовое обеспечение

Правовое обеспечение - это комплекс мероприятий по разработке нормативно-правовой базы конкретно под условия деятельности данного предприятия. Для разработки документации используются нормы действующего законодательства, упор делается на потребности и задачи организации.

Правовая защита информации строится на основе таких документов, как:

- Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ;
- Постановление Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных"
- Указ Президента РФ от 06.03.1997 N 188 (ред. от 13.07.2015) "Об утверждении Перечня сведений конфиденциального характера";
- Постановление Правительства РФ от 26 июня 1995 г. №608 "О сертификации средств защиты информации" (с изменениями от 21 апреля 2010 г.).

Она существует для того, чтобы обеспечить государственную законодательную базу и нормативное обоснование комплексной системы защиты информации на предприятии. Кроме законов и других государственных нормативных документов, правовое обеспечение системы защиты конфиденциальной информации так же включает в себя комплекс внутренней нормативно-организационной документации, в которую входят такие документы предприятия, как:

- устав;

- коллективный трудовой договор;
- трудовые договоры с сотрудниками предприятия;
- правила внутреннего распорядка служащих предприятия;
- должностные обязанности руководителей, специалистов и служащих предприятия.
- инструкции пользователей информационно-вычислительных сетей и баз данных;
- положение об обработке ПДн; (Приложение А)
- инструкции администраторов ИВС и БД;
- положение о подразделении по защите информации;
- концепция системы защиты информации на предприятии;
- положение об использовании носителей информации; (Приложение Б)
- инструкции сотрудников, допущенных к защищаемым сведениям;
- правила пользования ККС; (Приложение В)
- инструкции сотрудников, ответственных за защиту информации;
- памятка сотрудника о сохранении коммерческой или иной тайны;
- договорные обязательства.

### 1.5.2.Организационное обеспечение

Организационные средства - организационно-технические и организационно-правовые мероприятия по регламентации поведения персонала.

На территории предприятия организован пропускной режим, не позволяющий проникнуть в определенные помещения людям без доступа, а так же препятствующий несанкционированному вносу туда ЭВМ и сотовых телефонов. Работает контрольно-пропускной пункт. Доступ в закрытые от свободного доступа помещения предприятия, а так же во все кабинеты дирекции осуществляется по бесконтактным картам. Устанавливать, ограничивать и изменять доступ могут только специалисты отдела информационной безопасности. При каждом использовании карты вся информация регламентируется в электронном журнале. Это такие сведения, как: владелец карты, время использования, помещение в которое он зашел и т.д.

### 1.5.3.Программно-аппаратное обеспечение защиты информации

Программно-аппаратные СЗИ - это сервисы безопасности, встроенные в сетевые операционные системы. К сервисам безопасности относятся: идентификация и аутентификация, протоколирование и аудит, управление доступом, экранирование, криптография.

На ООО ЧОП «Витязь» используются такие средства защиты, как:

- SecretNet;
- NOD32.

Персональные данные, обрабатываемые в ИСПДн.

Перечень персональных данных, обрабатываемых в ИСПДн:

- фамилия, имя, отчество;
- дата, месяц, год рождения;
- адрес проживания и прописки;

- серия, номер, дата выдачи основного документа, удостоверяющего личность и информация о выдавшем его органе;
- адрес охраняемого объекта (для клиентов).

Категории субъектов ПДн:
- клиенты предприятия;

### 1.5.4.Кадровое обеспечение

Систему кадрового обеспечения предприятия можно разделить на 4 основных пункта:
- кадровое планирование и прогнозирование потребности в персонале;
- набор и отбор персонала;
- развитие и обучение персонала;
- контроль и оценка персонала.

Для осуществления данного процесса на ООО ЧОП «Витязь» сформирован отдел кадров, который контролирует все пункты, перечисленные выше. Так же стоит отметить, что все сотрудники перед приемом на работу проходят полиграф, этот этап является одним из основополагающих для вынесения решения о сотрудничестве.

### 1.5.5.Технологический процесс обработки ИСПДн

Технологический процесс обработки информации отражает фактический порядок обработки информации в ООО ЧОП «Витязь» и дополнен с точки зрения требований безопасности, определяемых в соответствии с законодательством РФ.

Технологическому процессу обработки информации в информационных системах персональных данных ООО ЧОП «Витязь» обязаны следовать все сотрудники, имеющие доступ к персональным данным, обрабатываемым с использованием средств автоматизации.

Допуск к персональным данным субъекта могут иметь только те сотрудники, которым персональные данные необходимы в связи с исполнением ими своих трудовых обязанностей.

Каждый сотрудник должен иметь доступ к минимально необходимому набору персональных данных субъектов, необходимых ему для выполнения служебных (трудовых) обязанностей. Описание технологического процесса обработки информации в информационных системах персональных данных находится в приложении.

### 1.5.6. Объекты защиты

К документам, подлежащим защите относятся:
- организационно-правовые документы предприятия (устав, учредительный договор, структура и штатная численность, штатное расписание, должностные инструкции, правила внутреннего трудового распорядка);
- распорядительные документы предприятия (приказы по основной деятельности, распоряжения, решения);

- документы по личному составу предприятия (приказы по л/с, трудовые контракты (договоры), личные дела, личные карточки, лицевые счета по зарплате, трудовые книжки);

- финансово-бухгалтерские документы предприятия (главная книга, годовые отчеты, бухгалтерские балансы, счета прибылей и убытков, акты ревизий, инвентаризаций, планы, отчеты, сметы, счета, кассовые книги);

- информационно-справочные документы предприятия (акты, письма, факсы справки, телефонограммы, докладные записки, протоколы);

- коммерческие контракты (договоры).

### 1.5.7. Помещение, подлежащее защите

Защищаемым помещением является кабинет договорного отдела ООО ЧОП «Витязь», который находится на первом этаже трёхэтажного здания. План этажа представлен на рисунке 3.

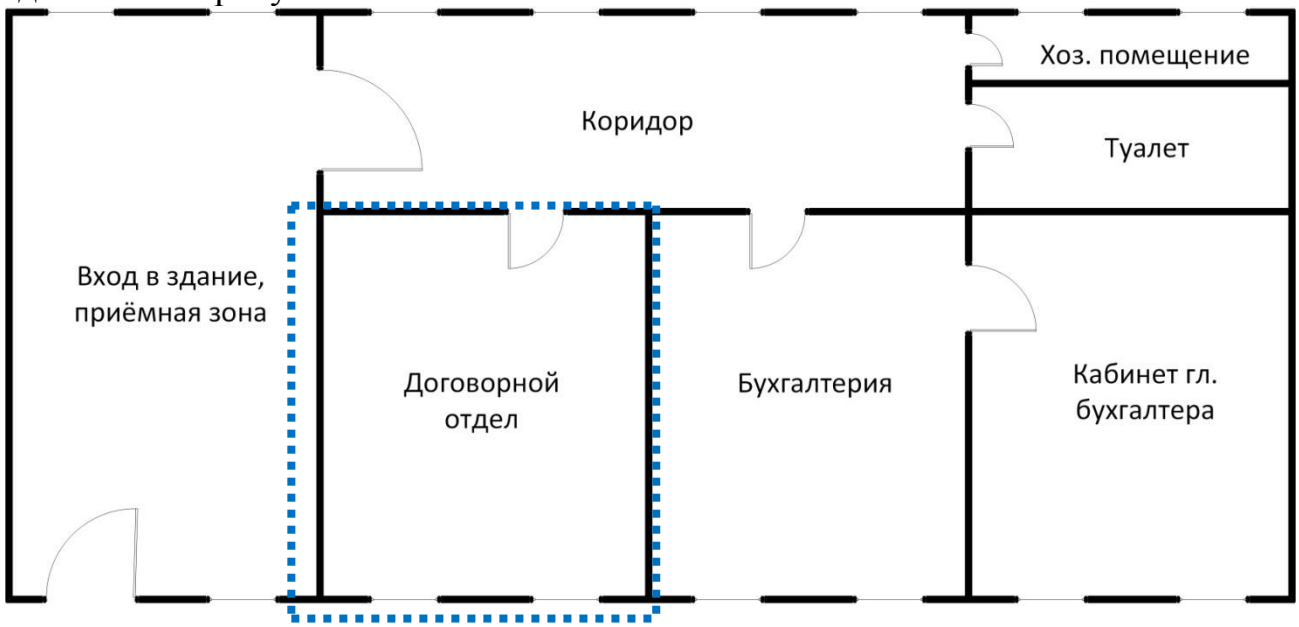


Рисунок 3. План этажа, где находится защищаемое помещение.

## 1.6. Модель угроз

### 1.6.1. Модель вероятного нарушителя

Составление модели угроз ООО ЧОП «Витязь» необходимо начать с модели вероятного нарушителя информационной безопасности. Модель вероятного нарушителя составляется на основе методического документа, утвержденного ФСТЭК России «Методика определения угроз безопасности информации в информационных системах».

Целью определения угроз безопасности информации ООО ЧОП «Витязь» является установление того, существует ли реальная возможность нарушения конфиденциальности, целостности или доступности информации, содержащейся в информационной системе, и приведет ли нарушение хотя бы одного из указанных свойств безопасности информации к наступлению неприемлемых негативных последствий для обладателя информации или оператора, а в случае обработки персональных данных и для субъектов персональных данных. Определение угроз

безопасности информации на предприятии ООО ЧОП «Витязь» должно носить систематический характер и осуществляться как на этапе создания информационной системы и формирования требований по ее защите, так и в ходе эксплуатации информационной системы. Систематический подход к определению угроз безопасности информации нужен для того, чтобы определить потребности в конкретных требованиях к защите информации и создать адекватную эффективную СЗИ в информационной системе. Меры защиты информации, принимаемые обладателем информации и оператором, должны обеспечивать эффективное и своевременное выявление и блокирование угроз безопасности информации, в результате реализации которых возможно наступление неприемлемых негативных последствий. Систематический подход к определению угроз безопасности информации ООО ЧОП «Витязь» предусматривает реализацию непрерывного процесса, в пределах которого устанавливается область применения процесса определения угроз, идентифицируются источники угроз и угрозы безопасности информации, оценивается возможность реализации угроз безопасности информации и степень возможного ущерба в случае такой реализации, осуществляется мониторинг и переоценка угроз безопасности информации.

Целью оценки возможных нарушителей по реализации угроз безопасности информации ООО ЧОП «Витязь» является формирование предположения о типах, видах нарушителей, которые могут реализовать угрозы безопасности информации в информационной системе с заданными структурно-функциональными характеристиками и особенностями функционирования, а также потенциале этих нарушителей и возможных методах реализации угроз безопасности информации. Результаты оценки возможностей нарушителей включаются в модель нарушителя, которая является составной частью модели угроз безопасности информации и содержит:

- типы, виды и потенциал нарушителей, которые могут обеспечить реализацию угроз безопасности информации;
- цели, которые могут преследовать нарушители каждого вида при реализации угроз безопасности информации;
- возможные способы реализации угроз безопасности информации.

С учетом наличия прав доступа и возможностей по доступу к информации и к компонентам информационной системы нарушители подразделяются на два типа:

- внешние нарушители (тип I) – лица, не имеющие права доступа к информационной системе, ее отдельным компонентам и реализующие угрозы безопасности информации из-за границ информационной системы;
- внутренние нарушители (тип II) – лица, имеющие право постоянного или разового доступа к информационной системе, ее отдельным компонентам.

Наибольшими возможностями по реализации угроз безопасности на предприятии ООО ЧОП «Витязь» обладают внутренние нарушители. На предприятии установлен пропускной порядок допуска физических лиц к информационной системе и ее компонентам, вход в помещения осуществляется по бесконтактным картам. Внешнего нарушителя нужно учитывать как актуального, так как ИСПДн обрабатывается в ЛВС .

Существует большое количество видов нарушителей с различным потенциалом. Исходя из описания деятельности и масштабности ООО ЧОП «Витязь», были выделены подходящие, они находятся в таблице1 и таблице2.

Таблица 1 - Виды нарушителей.

| № вида | Виды нарушителя | Типы нарушителя | Возможные цели (мотивация) реализации угроз безопасности информации |
|---|---|---|---|
| 1 | 2 | 3 | 4 |
| 1 | Преступные группы (криминальные структуры) | Внешний | Причинение имущественного ущерба путем мошенничества или иным преступным путем. Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды |
| 2 | Внешние субъекты (физические лица) | Внешний | Идеологические или политические мотивы. Причинение имущественного ущерба путем мошенничества или иным преступным путем. Любопытство или желание самореализации (подтверждение статуса). Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды |
| 3 | Конкурирующие организации | Внешний | Получение конкурентных преимуществ. Причинение имущественного ущерба путем обмана или злоупотребления доверием |
| 4 | Разработчики, производители, поставщики программных, технических и программно-технических средств | Внешний | Внедрение дополнительных функциональных возможностей в программное обеспечение или программно-технические средства на этапе разработки. Причинение имущественного ущерба путем обмана или злоупотребления доверием. Непреднамеренные, неосторожные или неквалифицированные действия |

Продолжение Таблицы 1

| 1 | 2 | 3 | 4 |
|---|---|---|---|
| 5 | Лица, привлекаемые для установки, наладки, монтажа, пусконаладочных и иных видов работ | Внутренний | Причинение имущественного ущерба путем обмана или злоупотребления доверием. Непреднамеренные, неосторожные или неквалифицированные действия |
| 6 | Лица, обеспечивающие функционирование информационных систем или обслуживающие инфраструктуру оператора(администрация, охрана, уборщики и т.д.) | Внутренний | Причинение имущественного ущерба путем обмана или злоупотребления доверием. Непреднамеренные, неосторожные или неквалифицированные действия |
| 7 | Пользователи информационной системы | Внутренний | Причинение имущественного ущерба путем мошенничества или иным преступным путем. Любопытство или желание самореализации (подтверждение статуса). Месть за ранее совершенные действия. Непреднамеренные, неосторожные или неквалифицированные действия |
| 8 | Администраторы информационной системы и администраторы безопасности | Внутренний | Причинение имущественного ущерба путем мошенничества или иным преступным путем. Любопытство или желание самореализации (подтверждение статуса). Месть за ранее совершенные действия. Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды. Непреднамеренные, неосторожные или неквалифицированные действия |
| 9 | Бывшие работники (пользователи) | Внешний | Причинение имущественного ущерба путем мошенничества или иным преступным путем. Месть за ранее совершенные действия |

Возможности каждого вида нарушителя по реализации угроз безопасности информации характеризуются его потенциалом. Потенциал нарушителя определяется компетентностью, ресурсами и мотивацией, требуемыми для реализации угроз безопасности информации в информационной системе с заданными структурно-функциональными характеристиками и особенностями функционирования. В зависимости от потенциала, требуемого для реализации угроз безопасности информации, нарушители подразделяются на: нарушителей, обладающих базовым потенциалом нападения при реализации угроз безопасности информации в информационной системе; нарушителей, обладающих базовым повышенным потенциалом нападения при реализации угроз безопасности информации в информационной системе; нарушителей, обладающих высоким потенциалом нападения при реализации угроз безопасности информации в информационной системе.

Таблица 2 - Потенциал нарушителей.

| № | Потенциал нарушителей | Виды нарушителей | Возможности по реализации угроз безопасности информации |
|---|---|---|---|
| 1 | 2 | 3 | 4 |
| 1 | Нарушители с базовым потенциалом | Внешние субъекты , лица, обеспечивающие функционирование информационных систем или обслуживающих инфраструктуру оператора, пользователи информационной системы, бывшие работники, лица, привлекаемые для установки, наладки, монтажа, пусконаладочных и иных работ | Имеют возможность получить информацию об уязвимостях отдельных компонент информационной системы, опубликованную в общедоступных источниках. Имеют возможность получить информацию о методах и средствах реализации угроз безопасности информации , опубликованных в общедоступных источниках, и самостоятельно осуществляет создание методов и средств реализации атак и реализацию атак на информационную систему |

Продолжение Таблицы 2

| 1 | 2 | 3 | 4 |
|---|---|---|---|
| 2 | Нарушители с базовым повышенным (средним) потенциалом | Террористические, экстремистские группировки, преступные группы, конкурирующие организации, разработчики, производители, поставщики программных, технических и программно - технических средств, администраторы информационной системы и администраторы безопасности | Обладают всеми возможностями нарушителей с базовым потенциалом. Имеют осведомленность о мерах защиты информации, применяемых в информационной системе данного типа. Имеют возможность получить информацию об уязвимостях отдельных компонент информационной системы путем проведения, с использованием имеющихся в свободном доступе программных средств, анализа кода прикладного программного обеспечения и отдельных программных компонент общесистемного программного обеспечения. Имеют доступ к сведениям о структурно-функциональных характеристиках и особенностях функционирования информационной системы |

1.6.2. Возможные способы реализации угроз информационной безопасности

Целью определения возможных способов реализации угроз безопасности информации ООО ЧОП «Витязь» является формирование предположений о возможных сценариях реализации угроз безопасности информации, описывающих последовательность действий отдельных видов нарушителей или групп нарушителей и применяемые ими методы и средства для реализации угроз безопасности информации.

При определении способа реализации угроз безопасности информации ООО ЧОП «Витязь» необходимо учитывать то, что угрозы безопасности информации могут быть реализованы непосредственно за счет доступа к компонентам информационной системы и информации или опосредовано за счет создания условий и средств, обеспечивающих такой доступ, и за счет доступа или воздействия на обслуживающую инфраструктуру, за которую оператор не отвечает.

Так же возможные способы реализации угроз безопасности информации зависят от структурно-функциональных характеристик и особенностей функционирования информационной системы. Угрозы безопасности информации на предприятии ООО ЧОП «Витязь» могут быть реализованы нарушителями за счет:

- несанкционированного доступа и воздействия на объекты на аппаратном уровне (программы (микропрограммы), «прошитые» в аппаратных компонентах (чипсетах));

- несанкционированного доступа и воздействия на объекты на общесистемном уровне (базовые системы ввода-вывода, гипервизоры, операционные системы);

- несанкционированного доступа и воздействия на объекты на прикладном уровне (системы управления базами данных, браузеры, web-приложения, иные прикладные программы общего и специального назначения);

- несанкционированного физического доступа и воздействия на линии, (каналы) связи, технические средства, машинные носители информации;

- воздействия на пользователей, администраторов безопасности, администраторов информационной системы или обслуживающий персонал (социальная инженерия).

### 1.6.3.Исходный уровень защищенности ИСПДн

Под общим уровнем защищенности понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПДн ($Y_1$).

В таблице представлены характеристики уровня исходной защищенности для ИСПДн ТБ.

Таблица 3 - Исходный уровень защищенности.

| Позиция | Технические и эксплуатационные характеристики | Уровень защищенности |
|---|---|---|
| 1 | 2 | 3 |
| 1 | По территориальному размещению: локальная ИСПДн, развернутая в пределах одного здания | Высокий |
| 2 | По наличию соединения с сетями общего пользования: ИСПДн, физически отделенная от сети общего пользования | Высокий |
| 3 | По встроенным (легальным) операциям с записями баз персональных данных: запись, удаление, сортировка; | Средний |
| 4 | По разграничению доступа к персональным данным: ИСПДн, к которой имеют доступ определенные перечнем сотрудники организации, являющейся владельцем ИСПДн, либо субъект ПДн; | Средний |
| 5 | По наличию соединений с другими базами ПДн иных ИСПДн: ИСПДн, в которой используется одна база ПДн, принадлежащая организации – владельцу данной ИСПДн | Высокий |

Продолжение Таблицы 3

| 1 | 2 | 3 |
|---|---|---|
| 6 | По уровню (обезличивания) ПДн: ИСПДн, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта ПДн) | Низкий |
| 7 | По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки: ИСПДн, предоставляющая часть ПДн; | Средний |

ИСПДн имеет средний уровень исходной защищенности, если не выполняются условия по пункту 1 и не менее 70% характеристик ИСПДн соответствуют уровню не ниже «средний»

При составлении перечня актуальных угроз безопасности ПДн каждой степени исходной защищенности ставится в соответствие числовой коэффициент Y1 , а именно: 5 – для средней степени исходной защищенности;

### 1.6.4.Вероятность реализации угроз

Под частотой реализации угрозы на ООО ЧОП «Витязь» понимается определяемый экспертным путем показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности ПДн для данной ИСПДн в складывающихся условиях обстановки. Вводятся четыре вербальных градации этого показателя:

- маловероятно – отсутствуют объективные предпосылки для осуществления угрозы (например, угроза хищения носителей информации лицами, не имеющими легального доступа в помещение, где последние хранятся);
- низкая вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (например, использованы соответствующие средства защиты информации);
- средняя вероятность - объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны;
- высокая вероятность - объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности ПДн не приняты.

При составлении перечня актуальных угроз безопасности ПДн каждой градации вероятности возникновения угрозы ставится в соответствие числовой коэффициент Y2 , а именно:

0 – для маловероятной угрозы;
2 – для низкой вероятности угрозы;
5 – для средней вероятности угрозы;
10 – для высокой вероятности угрозы.

При обработке персональных данных в ИСПДн можно выделить следующие угрозы.

### 1.6.5. Угрозы утечки информации по техническим каналам

#### 1.6.5.1. Угрозы утечки акустической информации

Возникновение угроз утечки акустической информации, содержащейся непосредственно в произносимой речи пользователя ИСПДн, при обработке ПДн в ИСПДн, возможно при наличии функций голосового ввода ПДн в ИСПДн или функций воспроизведения ПДн акустическими средствами ИСПДн.

В ИСПДн ООО ЧОП «Витязь» функции голосового ввода ПДн или функции воспроизведения ПДн акустическими средствами отсутствуют.

Вероятность реализации угрозы – маловероятна.

#### 1.6.5.2. Угрозы утечки видовой информации

Реализация угрозы утечки видовой информации на ООО ЧОП «Витязь» возможна за счет просмотра информации с помощью оптических средств с экранов дисплеев и других средств отображения средств вычислительной техники, информационно-вычислительных комплексов, технических средств обработки графической, видео и буквенно-цифровой информации, входящих в состав ИСПДн.

В здании ООО ЧОП «Витязь» введен контроль доступа в контролируемую зону, АРМ с ИСПДн расположены на втором этаже здания, окна выходят во двор контролируемой зоны так, что практически исключен визуальный просмотр посторонними лицами информации на мониторе.

Вероятность реализации угрозы – маловероятна.

#### 1.6.5.3. Угрозы утечки информации по каналам побочных электромагнитных излучений и наводок

Угрозы утечки информации по каналу ПЭМИН на ООО ЧОП «Витязь» возможны из-за наличия паразитных электромагнитных излучений у элементов ИСПДн.

Угрозы данного класса высоко вероятны, т.к. размер контролируемой зоны ООО ЧОП «Витязь» небольшой, а элементы ИСПДн, находятся на маленьком расстоянии от ее границы и не экранируются несущими стенами.

#### 1.6.5.4. Угрозы несанкционированного доступа к информации в информационной системе персональных данных

Реализация угроз НСД к информации на ООО ЧОП «Витязь» может приводить к следующим видам нарушения ее безопасности:

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

#### 1.6.5.5. Кража ПЭВМ

Угроза осуществляется путем НСД нарушителями в помещения, где расположены элементы ИСПДн.

В здании ООО ЧОП «Витязь» введен круглосуточный контроль доступа в защищаемое помещение, вход в которое осуществляется по картам доступа, что делает вынос компьютерный техники за пределы здания практически невозможным.

Вынос компьютерной техники из здания осуществляется только по специальным разрешениям.

Вероятность реализации угрозы – маловероятной.

1.6.5.6. Кража носителей информации

Угроза осуществляется путем НСД внешними и внутренними нарушителями к носителям информации.

В здании ООО ЧОП «Витязь» введен контроль доступа в защищаемое помещение, носители информации хранятся в этом же помещении, но стоит отметить, что учет носителей не ведется.

Вероятность реализации угрозы – средняя вероятность.

1.6.5.7. Кража ключей и атрибутов доступа

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где происходит работа пользователей.

В здании ООО ЧОП «Витязь» введен контроль доступа в защищаемое помещение, двери закрываются на замок, но пользователи имеют личные проксимити-карты, которые могут быть украдены злоумышленниками за пределами предприятия.

Вероятность реализации угрозы – средняя вероятность.

1.6.5.8. Кражи, модификации, уничтожения информации

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где расположены элементы ИСПДн и средства защиты, а так же происходит работа пользователей.

В здании ООО ЧОП «Витязь» введен контроль доступа в защищаемое помещение, двери закрываются на замок.

Вероятность реализации угрозы – маловероятна

1.6.5.9. Вывод из строя узлов ПЭВМ, каналов связи

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где расположены элементы ИСПДн и проходят каналы связи.

В здании ООО ЧОП «Витязь» введен контроль доступа в защищаемое помещение, двери закрываются на замок.

Вероятность реализации угрозы – маловероятна

1.6.5.10. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ

На предприятии ООО ЧОП «Витязь» техническое обслуживание ПЭВМ осуществляется своими сотрудниками.

Вероятность реализации угрозы – маловероятна

1.6.5.11. Несанкционированное отключение средств защиты

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где расположены средства защиты ИСПДн.

В здании ООО ЧОП «Витязь» введен контроль доступа в защищаемое помещение, двери закрываются на замок, пользователи ИСПДн проинструктированы о работе с ПДн.

Вероятность реализации угрозы – низкая вероятность

1.6.6.Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа с применением программно-аппаратных и программных средств

1.6.6.1.Недекларированные возможности системного ПО и ПО для обработки персональных данных

Недекларированные возможности – функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Разработку и сопровождение программного обеспечения ИСПДн ООО ЧОП «Витязь» осуществляет доверенная организация.

Вероятность реализации угрозы – маловероятна.

1.6.6.2. Установка ПО не связанного с исполнением служебных обязанностей

Угроза осуществляется путем несанкционированной установки ПО внутренними нарушителями, что может привести к нарушению конфиденциальности, целостности и доступности всей ИСПДн или ее элементов.

Все пользователи ИСПДн ООО ЧОП «Витязь» проинструктированы о политике установки ПО и осуществляется контроль.

Вероятность реализации угрозы – низкая вероятность.

1.6.7. Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера

1.6.7.1.Утрата ключей и атрибутов доступа

Угроза осуществляется за счет действия человеческого фактора пользователей ИСПДн, которые нарушают положения парольной политике в части их создания (создают легкие или пустые пароли, не меняют пароли по истечении срока их жизни или компрометации и т.п.) и хранения (записывают пароли на бумажные носители, передают ключи доступа третьим лицам и т.п.) или не осведомлены о них.

На предприятии ООО ЧОП «Витязь» введена парольная политика, предусматривающая требуемую сложность пароля, осуществляется контроль за ее выполнением, пользователи проинструктированы о парольной политике и о действиях в случаях утраты или компрометации паролей.

Вероятность реализации угрозы – средняя вероятность.

1.6.7.2. Непреднамеренная модификация (уничтожение) информации сотрудниками

Угроза осуществляется за счет действия человеческого фактора пользователей ИСПДн, которые нарушают положения принятых правил работы с ИСПДн или не осведомлены о них.

На предприятии ООО ЧОП «Витязь» осуществляется резервное копирование обрабатываемых ПДн.

Вероятность реализации угрозы – маловероятна.

1.6.7.3. Непреднамеренное отключение средств защиты

Угроза осуществляется за счет действия человеческого фактора пользователей ИСПДн, которые нарушают положения принятых правил работы с ИСПДн и средствами защиты или не осведомлены о них.

На предприятии ЧОП «Витязь» введен контроль доступа в защищаемое помещение, двери закрываются на замок, осуществляется разграничение доступа к настройкам режимов средств защиты, пользователи проинструктированы о работе с ИСПДн.

Вероятность реализации угрозы – маловероятна.

1.6.8. Выход из строя аппаратно-программных средств

Угроза осуществляется вследствие несовершенства аппаратно-программных средств, из-за которых может происходить нарушение целостности и доступности защищаемой информации.

На предприятии ООО ЧОП «Витязь» осуществляется резервирование ключевых элементов ИСПДн.

Вероятность реализации угрозы – средняя вероятность.

1.6.9. Сбой системы электроснабжения

Угроза осуществляется вследствие несовершенства системы электроснабжения, из-за чего может происходить нарушение целостности и доступности защищаемой информации.

На предприятии ООО ЧОП «Витязь» отсутствуют источники бесперебойного питания.

Вероятность реализации угрозы – высокая вероятность.

1.6.10. Стихийное бедствие

Угроза осуществляется вследствие несоблюдения мер пожарной безопасности.

На предприятии ООО ЧОП «Витязь» установлена пожарная сигнализация, пользователи проинструктированы о действиях в случае возникновения внештатных ситуаций.

Вероятность реализации угрозы – маловероятна.

1.6.11. Угрозы непреднамеренных действий внутренних нарушителей

Доступ к средствам ИСПДн ООО ЧОП «Витязь» имеет только ограниченный круг пользователей, а остальные сотрудники осведомлены о технике безопасности при работе с техническими средствами, что практически исключает риск данной угрозы.

Вероятность реализации угрозы – маловероятна

1.6.12. Угрозы несанкционированного доступа по каналам связи

В соответствии с «типовой моделью угроз безопасности персональных данных, обрабатываемых в распределенных ИСПДн, имеющих подключение к сетям общего пользования и (или) международного информационного обмена», можно рассматривать следующие угрозы, реализуемые с использованием протоколов межсетевого взаимодействия.

1.6.12.1. Угроза «Анализ сетевого трафика» с перехватом передаваемой по сети информации

Эта угроза реализуется с помощью специальной программы-анализатора пакетов, перехватывающей все пакеты, передаваемые по сегменту сети и выделяющей среди них те, в которых передаются идентификатор и пароль пользователя.

В ИСПДн ООО ЧОП «Витязь» возможен перехват трафика только в пределах КЗ, то есть внутренними нарушителями.

Вероятность осуществления угрозы – средняя вероятность.

1.6.12.2. Угроза выявления паролей по сети

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 «проход» для будущего доступа, который будет действовать, даже если на хосте изменить пароль доступа.

Вероятность осуществления угрозы – средняя вероятность.

1.6.12.3. Угроза удаленного запуска приложений

Угроза заключается в стремлении запустить на хосте ИСПДн ООО ЧОП «Витязь» различные предварительно внедренные вредоносные программы, основная цель которых – нарушение конфиденциальности, целостности и доступности информации.

Вероятность осуществления угрозы – средняя вероятность.

1.6.12.4. Угроза внедрения по сети вредоносных программ

Программно-математическое воздействие - это воздействие с помощью вредоносных программ. Программой с потенциально опасными последствиями или вредоносной программой (вирусом) называют некоторую самостоятельную про-

грамму (набор инструкций), которая способна выполнять любое непустое подмножество следующих функций:

- скрывать признаки своего присутствия в программной среде компьютера;
- обладать способностью к самодублированию, ассоциированию себя с другими программами и (или) переносу своих фрагментов в иные области оперативной или внешней памяти;
- разрушать (искажать произвольным образом) код программ в оперативной памяти;
- выполнять без инициирования со стороны пользователя (пользовательской программы в штатном режиме ее выполнения) деструктивные функции (копирования, уничтожения, блокирования и т.п.);
- сохранять фрагменты информации из оперативной памяти в некоторых областях внешней памяти прямого доступа (локальных или удаленных);
- искажать произвольным образом, блокировать и (или) подменять выводимый во внешнюю память или в канал связи массив информации, образовавшийся в результате работы прикладных программ, или уже находящиеся во внешней памяти массивы данных.

На предприятии ООО ЧОП «Витязь» на всех элементах ИСПДн установлена антивирусная защита, а на АРМ, где обрабатываются ПДн, нету доступа к сети интернет, что практически исключает возможность заражения вредоносными программами. Пользователи проинструктированы о мерах предотвращения вирусного заражения.

Вероятность реализации угрозы – маловероятна.

### 1.7. Расчет рисков для объектов защиты

По итогам оценки уровня защищенности ($Y_1$) и вероятности реализации угрозы ($Y_2$), рассчитывается коэффициент реализуемости угрозы (Y) и определяется возможность реализации угрозы. Коэффициент реализуемости угрозы Y будет определяться соотношением $Y = (Y_1 + Y_2)/20$

Оценка реализуемости УБПДн представлена в таблице 4.

Таблица 4 - Реализуемость УБПДн.

| Тип угроз безопасности ПДн | Коэффициент реализуемости угрозы (Y) | Возможность реализации |
|---|---|---|
| 1 | 2 | 3 |
| Угрозы утечки акустической информации | 0,25 | Низкая |
| Угрозы утечки видовой информации | 0,25 | Низкая |
| Угрозы утечки информации по ПЭМИн | 0,75 | Высокая |
| Кража ПЭВМ | 0,25 | Низкая |
| Кража носителей информации | 0,5 | Средняя |

Продолжение Таблицы 4

| 1 | 2 | 3 |
|---|---|---|
| Кража ключей и атрибутов доступа | 0,25 | Низкая |
| Кража, модификация и уничтожение информации | 0,25 | Низкая |
| Вывод из строя узлов ПЭВМ, каналов связи | 0,25 | Низкая |
| НСД к информации при техническом обслуживании узлов ПЭВМ | 0,25 | Низкая |
| Несанкционированное отключение средств защиты | 0,35 | Средняя |
| Недекларированные возможности системного ПО и ПО для обработки ПДн | 0,25 | Низкая |
| Установка ПО не связанного с исполнением служебных обязанностей | 0,35 | Средняя |
| Утрата ключей и атрибутов доступа | 0,5 | Средняя |
| Непреднамеренная модификация информации сотрудниками | 0,25 | Низкая |
| Непреднамеренное отключение средств защиты | 0,25 | Низкая |
| Выход из строя ПА средств | 0,5 | Средняя |
| Сбой системы электроснабжения | 0,75 | Высокая |
| Стихийное бедствие | 0,25 | Низкая |
| Угрозы непреднамеренных действий внутренних нарушителей | 0,25 | Низкая |
| Анализ сетевого трафика | 0,5 | Средняя |
| Угрозы выявления паролей по сети | 0,5 | Средняя |
| Угрозы удаленного запуска приложений | 0,5 | Средняя |

Продолжение Таблицы 4

| 1 | 2 | 3 |
|---|---|---|
| Угрозы внедрения по сети вредоносных программ | 0,25 | Низкая |

Оценка опасности УБПДн представлена таблице 5

Таблица 5 - Оценка опасности УБПДн.

| Тип угроз безопасности ПДн | Опасность угрозы |
|---|---|
| Угрозы утечки акустической информации | Низкая |
| Угрозы утечки видовой информации | Низкая |
| Угрозы утечки информации по ПЭМИн | Низкая |
| Кража ПЭВМ | Низкая |
| Кража носителей информации | Низкая |
| Кража ключей и атрибутов доступа | Высокая |
| Кража, модификация и уничтожение информации | Средняя |
| Вывод из строя узлов ПЭВМ, каналов связи | Низкая |
| НСД к информации при техническом обслуживании узлов ПЭВМ | Низкая |
| Несанкционированное отключение средств защиты | Низкая |
| Недекларированные возможности системного ПО и ПО для обработки ПДн | Низкая |
| Установка ПО не связанного с исполнением служебных обязанностей | Низкая |
| Утрата ключей и атрибутов доступа | Низкая |
| Непреднамеренная модификация информации сотрудниками | Низкая |
| Непреднамеренное отключение средств защиты | Низкая |
| Выход из строя ПА средств | Низкая |
| Сбой системы электроснабжения | Высокая |
| Стихийное бедствие | Низкая |
| Угрозы непреднамеренных действий внутренних нарушителей | Низкая |
| Анализ сетевого трафика | Высокая |
| Угрозы выявления паролей по сети | Высокая |
| Угрозы удаленного запуска приложений | Высокая |
| Угрозы внедрения по сети вредоносных программ | Высокая |

## 1.8. Перечень актуальных угроз ИСПДн

Отнесение угрозы к актуальной производится по правилам, приведенным в Методике определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной ФСТЭК России 14.02.2008, по таблице 6.

Таблица 6 - Определение актуальности угрозы.

| Возможность реализации угрозы | Показатель опасности угрозы | | |
|---|---|---|---|
| | Низкая | Средняя | Высокая |
| Низкая | неактуальная | неактуальная | актуальная |
| Средняя | неактуальная | актуальная | актуальная |
| Высокая | Актуальная | актуальная | актуальная |
| Очень высокая | Актуальная | актуальная | актуальная |

Таблица 7 - Актуальность угроз.

| Угроза безопасности ПДн | Актуальность угрозы |
|---|---|
| Угрозы утечки акустической информации | Неактуальная |
| Угрозы утечки видовой информации | Неактуальная |
| Угрозы утечки информации по ПЭМИн | Неактуальная |
| Кража ПЭВМ | Неактуальная |
| Кража носителей информации | Неактуальная |
| Кража ключей и атрибутов доступа | Актуальная |
| Кража, модификация и уничтожение информации | Неактуальная |
| Вывод из строя узлов ПЭВМ, каналов связи | Неактуальная |
| НСД к информации при техническом обслуживании узлов ПЭВМ | Неактуальная |
| Несанкционированное отключение средств защиты | Неактуальная |
| Недекларированные возможности системного ПО и ПО для обработки ПДн | Неактуальная |
| Установка ПО не связанного с исполнением служебных обязанностей | Неактуальная |
| Утрата ключей и атрибутов доступа | Неактуальная |
| Непреднамеренная модификация информации сотрудниками | Неактуальная |
| Непреднамеренное отключение средств защиты | Неактуальная |
| Выход из строя ПА средств | Неактуальная |
| Сбой системы электроснабжения | Актуальная |
| Стихийное бедствие | Неактуальная |
| Угрозы непреднамеренных действий внутренних нарушителей | Неактуальная |
| Анализ сетевого трафика | Актуальная |
| Угрозы выявления паролей по сети | Актуальная |
| Угрозы удаленного запуска приложений | Актуальная |
| Угрозы внедрения по сети вредоносных программ | Актуальная |

Таким образом, воспользовавшись «базовой моделью угроз безопасности персональных данных при их обработке в информационных системах персональных данных ФСТЭК России», была составлена модель угроз для ООО ЧОП «Витязь», на основе которой выявлены актуальны угрозы безопасности ПДн в ИСПДн ООО ЧОП «Витязь». Ими являются:

- кража ключей доступа;
- сбой системы электроснабжения;
- анализ сетевого трафика;
- угрозы выявления паролей по сети;
- угрозы удаленного запуска приложений;
- угрозы внедрения по сети вредоносных программ.

## 2. ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

### 2.1.Определение персональных данных

Персональные данные – это любая информация, которая относится к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных). В современном демократическом обществе права человека и особенно право на неприкосновенность личной жизни имеют важное значение. Изменения, связанные с регулированием ПДн (информации о частной жизни человека), происходят сейчас во многих государствах. Этому очень много причин, таких как: глобализация бизнеса, активное использование цифровых технологий, возрастание сетевого пиратства, активное расширение социальных сетей и других медиа, стремительно увеличивающееся желание государств контролировать массовые и сетевые коммуникации и заинтересованность бизнеса в интернет-рекламе и повышении ее эффективности.

### 2.2.Защита персональных данных. Мировая практика

Существует множество подходов, которых придерживаются государства, устанавливающие правоотношения в сфере ПДн: от максимальной защиты неприкосновенности таких данных, до почти полного отрицания права на анонимность в сетевых коммуникациях. Если подумать, иногда раскрытие ПДн в интересах правообладателей становится самым распространенным и очень надежным инструментом защиты интеллектуальных прав.

Такое раскрытие необходимо при сборе сведений о лицах, которые скачивают или распространяют контрафактные произведения, и при установлении глобальных систем контроля и фильтрации потребляемого трафика, и при введении запретов на доступ к определенным сайтам пользователям из определенных стран, и при внедрении прав доступа к контенту в отношении различных групп пользователей, и в ряде других случаев. Таким образом, любой стране выгоден высокий уровень использования ПДн, который позволит настраивать глобальные, технологически высокоэффективные, экономичные системы защиты прав на объекты интеллектуальной собственности. А именно они в подавляющем большинстве случаев граничат с нарушением основных прав человека. Поэтому изучение тенденций изменения правового регулирования ПДн является весьма важным и интересным. А так как подобные метаморфозы сейчас очень активно обсуждаются и внедряются во многих странах, не вызывает никаких сомнений.

Углубимся в суть. Сведения о гражданах собираются и аккумулируются различными государственными и частными структурами при рождении и получении документов, удостоверяющих личность, при обращении в медицинские учреждения, при поступлении на работу, при покупке недвижимости, при создании частных предприятий и во многих других случаях. Делая покупки в интернет-магазинах, покупатель вынужден сообщать свои ПДн. Но при этом владельцы подобных магазинов далеко не всегда обеспечивают охрану ПДн (в том числе банковских карт), а отсутствие соответствующего законодательства создает пробел в правовом регулировании. К самим ПДн относятся личные характеристики, биографические и опознавательные данные, сведения о семейном, социальном поло-

жении, образовании, профессии, состоянии здоровья, служебном и финансовом положении и другие.

Изначально на проблемы с защитой ПДн на международном уровне обратила внимание Организация по экономическому сотрудничеству и развитию (ОЭСР), успешно принявшая в 1980 г. Директиву о защите неприкосновенности частной жизни и международных обменов персональными данными. Вследствие все эти принципы были детально изложены в Конвенции Совета Европы «Об охране личности в отношении автоматизированной обработки персональных данных» (1981 г.), в Директиве Европейского сообщества о защите граждан в плане обработки информации личного характера от 27 июля 1990г., в Директиве Европейского Союза и Парламента 95/46/ЕС от 24 октября 1995 г. о защите прав частных лиц применительно к обработке персональных данных и свободном движении таких данных и Директиве 97/66/ЕС от 15.12.97 по обработке персональных данных защите, конфиденциальности в телекоммуникационном секторе.

В вышеперечисленных актах были определены главные принципы организации обработки ПДн и обеспечения прав граждан на защиту персональных данных. Такие как:

- данные персонального характера должны быть собраны только для определенных целей и в строгом соответствии с законом;
- данные должны соответствовать требованиям, быть точными, полными и вовремя обновленными;
- цели, для достижения которых собираются и обрабатываются персональные данные, должны быть определены и утверждены до начала деятельности и использоваться только в этих целях;
- в системах учета персональных данных должны быть внедрены механизмы, предотвращающие потери или неправильное (или злоумышленное) использование персональных данных;
- деятельность организаций (как государственных, так и частных), имеющих базы данных, содержащих персональные данные, должна быть открытой;
- держатели данных должны быть подконтрольными для обеспечения соблюдения настоящих принципов, для этих целей должно быть предусмотрено создание независимого контролируемого органа как важного элемента защиты личности при автоматизированной обработке информации личного характера.

Исходя из всего вышеперечисленного, можно говорить о важности практики иностранных государств по правовой защите информации и неприкосновенности частной жизни, и о вопросах защиты компьютерных БД и свободы информации. Такая практика в основном разработана в странах континентальной Европы, особенно в Германии, и в меньшей - в Канаде и США.

## 2.3. Особенности правового регулирования защиты персональных данных в России и за рубежом

### 2.3.1. Модели правового регулирования защиты ПДн.

Проанализируем регулирование правил защиты ПДн на федеральном и региональном уровнях в разных странах и наличие органов власти по контролю за со-

блюдением требований по защите ПДн. Существует два типа систем правого регулирования: централизованная и децентрализованная.

Признаки децентрализованной системы:

- отсутствие единого подхода к защите ПДн в рамках отраслевого законодательства;
- регламентация защиты ПДн осуществляется за счет профильных нормативных актов комплексных отраслей законодательства (здравоохранение, финансовый сектор) или на различных уровнях власти (например, в США Health Insurance Portability and Accountability Act (HIPAA 1996) и Gramm-Leach-Bliley Act (GLB 1999));
- акты рекомендательного характера играют значительную роль (методики, + индустриальные стандарты);
- отсутствие единого надзорного органа. Примеры: США, Канада и Австралия.

Признаки централизованной системы:

- прямое действие международных норм, гармонизирующих национальные законодательства государств (Конвенция о защите физических лиц при автоматизированной обработке ПДн, Директива 95/46/ЕС, Директива 2002/58/ЕС);
- наличие национальных отраслевых законов, содержащих общеобязательные нормы в отношении защиты ПДн (например, в Германии Bundesdatenschutzgesetz (BDSG));
- регулирование обработки ПДн посредством учреждения единого надзорного ведомства («мегарегулятора»).

Страны ЕС, Израиль, Гонконг, Мексика, Сингапур, Швейцария. Также можно выделить смешанную систему правового регулирования. Признаком смешанной системы является наличие одного или нескольких признаков, позволяющих отнести систему правого регулирования защиты ПДн государства к централизованной или децентрализованной системе. В Японии и на Тайване действуют единые законы о защите ПДн, отсутствуют единые надзорные ведомства, применяются акты рекомендательного характера. В Бразилии правовое регулирование осуществляется на основании общих норм, конституционных принципов и непрофильных законов, при этом присутствует единый надзорный орган.

В Гражданском кодексе предусмотрено также, что физическое лицо может просить помощи в связи с любой угрозой его личным правам и что личная жизнь физического лица является неприкосновенной. Широкую защиту предоставляет также Кодекс защиты прав потребителей. Он в основном предусматривает права потребителей на доступ к любым зарегистрированным ПДн и на внесение в них правок. Также можно добавить, что Бразилия вместе с Германией продвинула в ООН первую резолюцию, которая была посвящена защите ПДн в информационно-телекоммуникационных сетях международного обмена. В ней говорилось, о том, что право на неприкосновенность частной жизни должно обеспечиваться как в реальной жизни, так и в Сети. Для страны, где электронную переписку защищают по тем же правилам, что и обычную, это очевидный подход. Южная Америка также переживает настоящий бум интернет - законотворчества.

Проекты рассматривались месяцами, а то и годами. В авангарде находится Аргентина, признанная Еврокомиссией единственной страной, в полной мере выполняющей требования по защите ПДн в интернете.

В Южной Африке нет специальных законов о защите ПДн, но при этом в ее Конституции закреплено право на конфиденциальность. Положения, касающиеся личной информации, содержатся также в Законе о защите прав потребителей 2008 года и в Законе об электронных коммуникациях и сделках 2002 года. Соблюдение норм последнего закона несет в себе добровольный характер и должно быть отражено в соглашении с субъектом данных.

Что можно сказать о скандинавских странах, то у них принято законодательство по защите компьютерных БД. И в этом плане Швеция является примером для подражания - она первая из стран, принявшая закон о свободе информации («О свободе изданий», 1776 г., который в 1949г. был модифицирован в закон о свободе печати, а в настоящее время является составной частью Конституции Швеции и гарантирует всем гражданам страны свободу получения информации в государственных органах на безвозмездной основе) и первая ввела законодательство по защите информации частного характера (в редакции Закона о конфиденциальности 1998 г.), хранящейся в компьютерных БД. Законодательство по защите компьютерных баз данных Швеции и Дании (Закон о защите данных 1979 года в редакции Закона об обработке персональных данных 2000 г.) главным образом ориентировано на компьютерную информацию в частном секторе.

В Китае принято множество релевантных актов иной отраслевой принадлежности, а также развито подзаконное регулирование, высока роль документов рекомендательного характера.

В Саудовской Аравии нет специальных законов о защите ПДн, хотя право на конфиденциальность закреплено в ряде ее законов. В частности, в Основном низаме правления Саудовской Аравии закреплён основной принцип, согласно которому вся переписка и все виды связи между сторонами строго конфиденциальны и раскрывать их не следует. В отсутствие применимого законодательства суды руководствуются нормами шариата (исламского права). На основании норм шариата может быть предъявлен иск за ущерб, причинённый в связи с незаконным раскрытием ПДн физического лица, если раскрытие ПДн принесло убытки физическому лицу или нанесло ему вред.

В ОАЭ нет специальных законов о защите ПДн, однако право на конфиденциальность закреплено в Конституции и в различных законах. В Конституции ОАЭ указано, что физическому лицу «гарантируется свобода и конфиденциальность переписки, передачи телеграфных сообщений и других средств связи в соответствии с законом». Кроме того, в Уголовном кодексе закреплены некоторые права на конфиденциальность и на защиту ПДн.

В Индии отсутствует конституционное право на конфиденциальность, хотя Верховный суд постановил, что принцип конфиденциальности следует считать составляющей права на жизнь и личную свободу. Сбор и обработка ПДн регламентируются Законом об информационных технологиях 2000 года, в котором указано, что компании должны принимать адекватные меры безопасности при обработке персональных данных и что при получении таких данных в соответствии с

договором их нельзя раскрывать без согласия субъекта данных в нарушение договора.

Япония является членом Азиатско-Тихоокеанского экономического сотрудничества (АТЭС) и поддерживает его политику конфиденциальности. Сбор и использование ПДн в Японии регламентируются Законом о защите личной информации. Он относится ко всем видам обработки данных, но при этом применяется только тогда, когда речь об информации, принадлежащей 5000 и более физических лиц. Этот закон устанавливает общие требования к разрешениям, безопасности и предоставлению информации, а также дополнительные требования по контролю за работниками и третьими лицами, занимающимися обработкой ПДн.

В Австралии существует регулирование как на федеральном, так и на региональном уровнях. Федеральный документ:

- The Federal Privacy Act 1988;
- The Privacy Amendment Act 2012.

Региональные документы:

- Information Act 2002;
- Privacy and Personal Information Protection Act 1998;
- Information Privacy Act 2009;
- Personal Information and Protection Act 2004;
- Information Privacy Act 2000.

Орган по контролю за защитой ПДн -The Office of the Australian Information Commissioner. Страны, больше выделяющиеся на фоне других, стоит отметить отдельно: Канада - с практической точки зрения огромный интерес вызывает Канадский Закон об охране персональной информации, который предусматривает реальные механизмы защиты ПДн и реализации права на доступ к сведениям о себе. В соответствии с этим законом, под персональной понимается информация о конкретном индивиде, записанная в любой форме, также и данные о национальности, религии, расе, возрасте, цвете кожи, образовании, состоянии здоровья, финансах, личных взглядах и другая. Под действие акта не попадает информация об индивиде, который был или является сотрудником государственного учреждения, его служебном адресе и телефоне, должности, уровне зарплаты и служебных обязанностях. Персональная информация не может быть использована без согласия индивида и не для тех целей, ради которых она собиралась. В ряде случаев персональная информация может быть раскрыта, например, по решению суда, для члена парламента, который помогает этому индивиду, в целях передачи в архив, сбора статистических данных. Каждый гражданин или постоянно проживающий в Канаде человек может получить доступ к информации о себе, содержащейся в различных учреждениях, и корректировать ее, если считает неверной. При возникновении спорных вопросов граждане имеют право опротестовать действия властей в офисе Комиссара по защите персональной информации, который является специальным чиновником, назначаемым и ответственным перед парламентом. Он наблюдает за исполнением данного закона, т.е. за сбором, использованием и распространением государством персональной информации о клиентах и работниках, и в том числе рассматривает различные жалобы. Таким образом полу-

чается регулирование и на федеральном и на региональном уровнях. Основные документы:

- Personal Information Protection and Electronic Documents Act;
- Personal Information Protection Act;
- Personal Information Protection Act;
- An Act Respecting the Protection of Personal Information in Private Sector.

Во всех регионах имеется свой орган по контролю:

- Office of the Privacy Commissioner of Canada;
- Office of the Information and Privacy Commissioner of Alberta;
- Office of the Information and Privacy Commissioner for British Columbia;
- Commission d'accès à l'information du Québec.

В том числе организации обязаны сообщать о возникновении утечек ПДн исключительно в провинции Альберте. Для остальных областей планируется дальнейшее введение аналогичных требований.

### 2.3.2. Германия

В Европе лидером в сфере правового регулирования ПДн является Германия. Первый закон о защите ПДн был принят в Германии в районе Гессен в 1970 г. До этого времени похожих законов в мире еще принято не было. Следом произошло принятие в 1977 г. ФЗ о защите ПДн, который в 1990 г. был пересмотрен.

Все 16 земель Германии имеют собственные законы о защите ПДн, распространяющиеся на государственный сектор административного управления землями. Контроль за исполнением закона осуществляет Федеральная комиссия по защите персональных данных. Соответствующие комиссии, которые обеспечивают исполнение местных законов о защите ПДн, имеются в каждой земле Германии. В частном секторе надзор осуществляется органом, указанным в законе, действующим в каждой из земель (как правило назначается комиссар по защите персональных данных).

Так же стоит обратить внимание на то, что почти все германские законы, которые напрямую или посредством поправок касаются проблем обращения с ПДн физических лиц, содержат в себе ссылки на соответствующий закон о защите ПДн, либо определенные положения, касательно правил обращения с ПДн, отражающие право на неприкосновенность частной жизни. ПДн полагается получать только от субъекта данных, за исключением тех случаев, когда данные необходимы по закону в действительных коммерческих целях, либо когда для получения данных лично от субъекта требуются непосильно большие усилия, и нет указаний на то, что интересы субъекта будут этим ущемлены. Помимо этого, в ФЗ о защите данных выделяется особое внимание разработке систем защиты данных, направленных на минимизацию объемов обрабатываемых ПДн, например способом предоставления отдельному субъекту данных анонимного статуса или дозволение использования псевдонимов. Таким образом, Закон о защите данных: Федеральный акт о защите данных (Bundesdatenschutzgesetz – BDSG 2001). Надзорный орган: Уполномоченное лицо Федеральной комиссии по защите данных. Основные полномочия надзорного органа: обеспечить выполнение положений Акта:

- уполномоченное лицо обязано контролировать исполнение положений Акта, что дает ему право доступа к информации, а также возможность проверять все документы и право доступа на территорию любых официальных учреждений в любое время;

- уполномоченное лицо может подавать жалобы в высшие инстанции (например, в компетентный высший федеральный орган), в случае нарушений законодательства о защите данных (ст.25);

- федеративное правительство может подавать запрос к Уполномоченному лицу, с целью получения рекомендаций по вопросам, связанным с законодательством о защите данных (ст.26).

Право сообщать надзорному органу о нарушениях имеет любое лицо. Санкции, которые имеет право наложить надзорный орган, в случае нарушения законодательства о защите данных: штрафы и заключение. Существует необходимость получить разрешение на осуществление обработки ПДн. Альтернатива, при которой получение разрешения является невозможным или нецелесообразным: Достаточно использовать альтернативные методы даже в тех случаях, когда это возможно или целесообразно. Регулирование на федеральном уровне: Европейская директива 95/46/ЕС реализована в Federal Data Protection Act “BDSG”. Организации должны предпринимать необходимые шаги для защиты данных, от несанкционированного доступа и нарушений политик обработки.

### 2.3.3.Соединенные Штаты Америки

В отличие от подавляющего большинства ведущих стран ЕС, в США до сих пор отсутствует федеральное законодательство о ПДн. В случае же нарушения прав субъектов ПДн применяются положения Конституции и практика прецедентного права, преобладающего в США. Отказ от общего закона связан с особой экономической и политической культурой, где власть способствует саморегуляции бизнеса. Так, свободу слова в конституции США гарантирует первая поправка, а право на неприкосновенность частной жизни при этом конкретно в ней не прописана и только подразумевается. Но эти принципы не мешают инициативам на уровнях штатов.

Известно, что общее законодательство в США, в большинстве направлено на регулирование деятельности государственных органов, входящих в структуру исполнительной власти, с целью создания прозрачного механизма управления и подотчетности обществу. Это в полной мере относится к сфере обработки ПДн, где основными действующими документами являются Privacy Act of 1974 и Privacy Protaction Act of 1980, которые регулируют деятельность органов государственной власти при обработке ПДн граждан. При этом, упомянутые нормативные акты, далеко не всегда отвечают стремительно меняющимся условиям современного мира, характеризующегося международной интеграцией и колоссальным прогрессом в области информационных технологий.

Ещё одной отличительной чертой защиты персональных данных в США является, так называемый зонтичный подход, обеспечивающий адекватную защиту данных в отдельных отраслях, который основан на использовании общего законодательства, отраслевых подзаконных актов и рекомендаций по защите информа-

ции, выраженных в том числе в примерах договоров. Наглядным примером такого зонтичного соглашения служит US Department of Commerce's Safe Harbor Privacy Principles (Принципы защиты информации Министерства торговли США) и Transfer of Air Passenger Name Record (PNR) Data (передача данных таможне и пограничной службе США) где, по заключению Еврокомиссии, обеспечивается адекватная защита данных. В качестве рекомендаций по обеспечению защиты данных широко применяются документы «Дирекции управления и бюджета» (OMB — Office of Management and Budget) и «Национального института стандартов и технологий» (NIST - National Institute of Standards and Technology). Указанные нормативные акты регулируют деятельность по защите ПДн в государственных структурах, для коммерческих же организаций они носят рекомендательный характер. Для борьбы с утечками конфиденциальной информации был задействован такой механизм: каждый штат принимает закон, обязывающий компании сообщать о любых утечках информации. К 2008 году такие законы были приняты почти во всех штатах Соединенных Штатов, но при этом реально снизить количество нарушений такими мерами к сожалению не удалось, о чем свидетельствует статистика утечек конфиденциальной информации за 2008 год.

Очередным шагом к централизованному регулированию отношений, связанных с обработкой ПДн граждан, является документ NIST Special Publication 800-122 Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) (Draft), проект которого появился в январе 2009 года. Цель документа - помощь государственным организациям и федеральным агентствам в защите ПДн граждан. NIST Special Publication 800-122 содержит общие рекомендации по защите ПДн и ссылается на многочисленные нормативно-правовые акты внутреннего законодательства Соединенных Штатов, в которых отражаются различные организационные, юридические, технические аспекты защиты ПДн.

Дополнительными мерами защиты являются: уменьшение объемов обрабатываемых и хранимых ПДн, обезличивание ПДн в ИСПДн для усложнения идентификации; группирование характеристик ПДн; скрытие части данных и другие.. Обеспечение безопасности ПДн: управление доступом к ПДн; разделение прав доступа; уменьшение количества привилегированных пользователей; запрет или ограничение на удаленный доступ; запрет или ограничение на хранение и обработку ПДн на мобильных устройствах; контроль попыток несанкционированного доступа к ПДн; мониторинг, анализ, уведомление; авторизация пользователей для доступа к ПДн; ограничение возможности копирования ПДн на внешние носители; шифрование ПДн, передаваемых за пределы организации и др. Возможно, после вступления в силу документа NIST Special Publication 800-122 порядок защиты ПДн в США будет более понятен, тем не менее, остается много вопросов по практическому применению данного механизма. С 2014 года в штате Калифорния действует закон, обязывающий сайты сообщать пользователям, отслеживают ли их поведение. Начиная с 2015 года жителям штата младше 18 лет также предоставят право быть забытыми, аналогичное европейскому.

Таким образом нет централизованного законодательства по защите ПДн на федеральном уровне. Существуют различные законодательные акты в разных штатах и ведомствах. Организации должны предпринимать необходимые шаги

для защиты данных, от НСД и нарушений политик обработки. В некоторых штатах также на законодательном уровне закреплены минимальные требования по защите информации. Нет единого органа по защите ПДн. Но для многих случаев Federal Trade Commission является контролирующим органом. Таким образом, их положения практически аналогичны принципам, лежащим в основе европейской системы защиты ПДн. Не смотря на это, практика защиты ПДн в США не является безупречной, чем, возможно, и объясняется включение США в список стран, не обеспечивающих должный уровень защиты ПДн, соответствующий порядок предусмотрен п.4 ст.25 Директивы ЕС 95/46/ЕС.

### 2.3.4. Россия

Существуют несколько категорий ПДн. К ним можно отнести общедоступные ПДн, специальные категории ПДн, категории ПДн, обрабатываемые в ИСПДн, биометрические ПДн и некоторые другие.

Общедоступные ПДн – это такие ПДн, когда общедоступными являются данные, доступ к которым предоставлен неограниченному кругу лиц с согласия субъекта ПДн или на которые, в соответствии с федеральными законами, не распространяются требования соблюдения конфиденциальности (фамилию, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные ПДн). Источниками такой информации могут являться, например, адресные книги, справочники, и так далее. Сведения о субъекте ПДн могут быть в любое время изъяты из общедоступных источников по первому требованию субъекта или по решению суда и уполномоченных государственных органов.

Специальные категории ПДн – это ПДн, касающиеся расовой, национальной принадлежности, религиозных или философских убеждений, политических взглядов, интимной жизни, состояния здоровья. Их обработка допускается только в нескольких случаях: субъект ПДн дал свое согласие в письменной форме на обработку своих персональных данных; ПДн являются общедоступными; ПДн относятся к состоянию здоровья субъекта персональных данных и получение его согласия на данный момент невозможно, или обработка ПДн осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством Российской Федерации сохранять врачебную тайну; обработка ПДн осуществляется согласно законодательству Российской Федерации о безопасности, об оперативно-розыскной деятельности и в соответствии с уголовно-исполнительным законодательством Российской Федерации, либо необходима в связи с осуществлением правосудия.

Категории ПДн, обрабатываемых в ИСПДн: Постановление Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных" определяет:

- Информационная система является информационной системой, обрабатывающей специальные категории персональных данных, если в ней обрабатываются персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъектов персональных данных.

- Информационная система является информационной системой, обрабатывающей биометрические персональные данные, если в ней обрабатываются сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных, и не обрабатываются сведения, относящиеся к специальным категориям персональных данных.

- Информационная система является информационной системой, обрабатывающей общедоступные персональные данные, если в ней обрабатываются персональные данные субъектов персональных данных, полученные только из общедоступных источников персональных данных, созданных в соответствии со статьей 8 Федерального закона "О персональных данных".

- Информационная система является информационной системой, обрабатывающей иные категории персональных данных, если в ней не обрабатываются персональные данные, указанные в абзацах первом - третьем настоящего пункта.

Биометрические персональные данные – это сведения, которые характеризуют физиологические особенности человека, на основе которых можно идентифицировать его личность. Биометрические ПДн обрабатываются в соответствии со статьей 11 Федерального закона Российской Федерации от 27 июля 2006 г. N 152-ФЗ «О персональных данных». Они могут обрабатываться исключительно при наличии согласия в письменной форме субъекта ПДн.

Обработка биометрических ПДн без согласия субъекта персональных данных может осуществляться в связи с осуществлением правосудия и в случаях, предусмотренных законодательством Российской Федерации о безопасности, об оперативно-розыскной деятельности, о государственной службе, о порядке выезда из Российской Федерации и въезда в Российскую Федерацию, уголовно-исполнительным законодательством. Оператор персональных данных – согласно федеральному закону от 27.07.2006 N 152-ФЗ операторами персональных данных являются государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и осуществляющие обработку ПДн, а также определяющие цели и содержание обработки ПДн.

Под обработкой персональных данных понимаются операции с ПДн, включая сбор, систематизацию, накопление, хранение, уточнение, использование, распространение, обезличивание, блокирование, уничтожение ПДн. Обеспечение конфиденциальности в соответствии с российским законодательством не требуется лишь для обезличенных и общедоступных персональных данных. ПДн могут быть общедоступными только с письменного согласия субъекта персональных данных. Они могут включать фамилию, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, предоставленные субъектом ПДн.

Обеспечение безопасности ПДн при их обработке в ИСПДн достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование и распространение персональных данных. Обязанность по обеспечению безопасности персональных данных при их обработке в

ИСПДн полностью возлагается на оператора ПДн. Безопасность персональных данных при их обработке в ИСПДн обеспечивает оператор, который на основании договора производит обработку ПДн. При этом оператор обязан заключать договор с уполномоченным лицом, если таковое имеется. Важным условием такого договора является обязанность уполномоченного лица обеспечивать конфиденциальность и безопасность ПДн при их обработке в ИСПДн. Для разработки и осуществления мероприятий по обеспечению безопасности ПДн при их обработке в ИСПДн оператором можно назначить структурное подразделение или должностное лицо, несущее ответственность за обеспечение безопасности ПДн.

В соответствии со статьей 23 Федерального Закона «О персональных данных» для обеспечения контроля и надзора за соответствием обработки персональных данных требованиями ФЗ назначается Уполномоченный орган по защите прав субъектов ПДн. Такие функции возложены на три организации:

- Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) в части, касающейся соблюдения норм и требований по обработке персональных данных;
- Федеральную службу безопасности Российской Федерации в части, касающейся соблюдения требований по организации и обеспечению функционирования шифровальных средств в случае их использования для обеспечения безопасности персональных данных при их обработке в ИСПДн;
- Федеральную службу по техническому и экспортному контролю в части, касающейся контроля и выполнения требований по организации и техническому обеспечению безопасности ПДн при их обработке в ИСПДн.

Таким образом, Государство создает необходимые условия для выполнения требований по безопасности ПДн. Оно определяет понятия ПДн и оператора, который эти данные обрабатывает. Регулирование на федеральном уровне:

- Федеральный закон от 19 декабря 2005 г. N 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных»;
- Федеральный закон от 27.07.2006 N 152-ФЗ «О персональных данных» (27 июля 2006 г.);
- Федеральный закон от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Несколько подзаконных актов, включая Постановления Правительства РФ, Указы Президента, и нормативные акты отдельных ведомств.

Организации обязаны предпринимать необходимые шаги для защиты данных, от НСД и нарушений политик обработки. Также на законодательном уровне закреплены минимальные требования по защите информации. Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор). Защита персональных данных при трансграничной передаче. Модели трансграничной передачи ПДн. Нормативно-правовые акты: Конвенция о защите физических лиц при автоматизированной обработке персональных данных с изменениями от 15 июня 1999 г. Дополнительный протокол к Конвенции о защите частных лиц в отношении автоматизированной обработки данных личного характера, о наблюдательных органах и трансграничной передаче информации»

ETS N 181 (Страсбург, 08 ноября 2001 г.). Статья 2. Трансграничная передача персональных данных получателю, не являющемуся субъектом права Стороны Конвенции. Она гласит:

- Каждая Сторона предусматривает передачу персональных данных получателю – субъекту права Государства или организации, не являющейся Стороной Конвенции, только если это Государство или организация обеспечат адекватный уровень защиты данных, предназначенных для передачи.

- Каждая Сторона может разрешить передачу персональных данных:

a. если национальное право предусматривает это ввиду: определенно заинтересованности в отношении субъекта данных или законных интересов, наиболее важных государственных интересов;

b. если гарантии, которые могут быть, в частности, результатом условий договора, предусмотренные ответственным за передачу контролером, признаются адекватными.

В законодательстве Российской Федерации большое внимание уделяется безопасности персональных данных при их передаче за пределы РФ. До начала осуществления трансграничной передачи ПДн оператор персональных данных должен убедиться в том, что иностранным государством, на территорию которого осуществляется ввоз ПДн, обеспечивается должная защита прав субъектов персональных данных. Министерство связи и массовых коммуникаций Российской Федерации (Минкомсвязи) в своем письме РФ от 13.05.2009 N ДС-П11-2502 «Об осуществлении трансграничной передачи персональных данных» (13 мая 2009 г.) определило «адекватную защиту» как защиту, при которой «обеспечивается уровень защищенности прав субъектов ПДн не ниже, чем в Российской Федерации».

Одним из критериев оценки государства в этом аспекте может выступать факт ратификации им «Конвенции о защите прав физических лиц при автоматизированной обработке персональных данных» от 28 января 1981 г., ETS № 108. На сегодняшний день в число стран, подписавших и ратифицировавших указанную Конвенцию, входят: Австрия, Андорра, Бельгия, Болгария, Дания, Великобритания, Венгрия, Германия, Греция, Израиль, Ирландия, Исландия, Испания, Италия, Латвия, Литва, Лихтенштейн, Люксембург, Мальта, Нидерланды, Норвегия, Польша, Португалия, Румыния, Сербия, Словакия, Словения, Финляндия, Франция, Хорватия, Черногория, Чехия, Швейцария, Швеция, Эстония. В США отсутствуют нормативные положения, которые бы ограничивали трансграничную передачу данных. Норма Конституции США о регулировании торговли («commerce clause» - п. 3 разд. 8 ст. 1 Конституции США) тоже не допускает установление подобных ограничений на уровне штатов. Особенности: США не рассматривается в качестве страны, обеспечивающей надлежащий уровень защиты персональных данных, с точки зрения европейского законодательства. Последствия: В целях гармонизации был создан механизм утверждения международными корпорациями специальных, единых корпоративных правил обработки данных (Binding Corporate Rules – ст. 26 (2) Директивы 95/46/ЕС), а также выработаны специальные принципы (Safe Harbor – Решение Комиссии ЕС от 26 июля 2000 г. N 2000/520/Е). В ЕС Европейская комиссия утверждает список таких стран. Передача данных внутри интеграционного образования данному ограничению не подле-

жит. В некоторых случаях для третьих стран предусмотрены исключения (ст. 26 Директивы 95/46/ЕС). Особенности: Несмотря на то, что данные ограничения являются дополнительной нагрузкой на бизнес, в ЕС стараются не столько урегулировать рынок методом запретов, сколько «настроить» организационный механизм трансграничной передачи данных, например, через разработку модельных контрактов, консультаций с операторами и т.п. (Решения Комиссии ЕС от 15 июня 2001 года № 2001/497/ЕС, от 27 декабря 2014 № 2004/915/ЕС). В общем, устанавливается, что оператор – это единственный субъект, надлежащий к привлечению ответственности. Обработчик не несёт никаких обязанностей конкретно перед субъектом ПДн. Ответственность за его действия несёт исключительно оператор. Такой порядок на данный момент предусмотрен в Директиве 95/46/ЕС (ст. 16, 17 и 23). Обработчик несет ответственность перед оператором в рамках договорных отношений. Ответственность за нарушение законодательства о защите персональных данных. В Российской Федерации законом предусматривается гражданская, уголовная, административная, дисциплинарная и иная ответственность за нарушение требований. Таким образом, Кодекс об административных правонарушениях предусматривает максимальный штраф в 500000 рублей за невыполнение законного предписания Роскомнадзора (ст. 19.5 КоАП). Тот же Кодекс предусматривает приостановление деятельности организации на срок до 90 суток при осуществлении деятельности по защите ПДн без лицензии (ст. 19.20 КоАП). В уголовном кодексе говорится о штрафе в 300000 руб., обязательных работах на срок до 1-го года, аресте до 6-ти месяцев и лишении права занимать должность на срок до 5-ти лет в случае осуществления защиты ПДн без лицензии в случаях, если это деяние причинило крупный ущерб гражданам (ст. 171 УК При систематических и грубых нарушениях Роскомнадзор имеет право ходатайствовать об отзыве лицензий на основной вид его деятельности. Сумма штрафов в некоторых странах, Австралия - 1 500 000, Великобритания -800 000, Индия - 700 000, Германия - 400 000, Канада - 100 000.

Таким образом, после изучения российского законодательства и рассмотрения нормативно-правовой базы других зарубежных стран в сфере защиты ПДн, контролирующих так же сбор и обработку ПДн, можно сделать вывод, что наиболее перспективным и эффективным механизмом охраны и защиты персональных данных является законодательство Германии, а именно, ФЗ «О защите данных» от 2001 года. Несмотря на то, что Германия относится к континентальной правовой системе, государственно-территориальное устройство федеративного типа, как и в нашей стране, всё же служит отличным примером надежной и «адекватной» системы защиты персональных данных.

Проанализировав современную практику разных стран, а так же международное законодательство и опыт в сфере правового обеспечения защиты ПДн, мы можем констатировать факт наличия устойчивой и весьма заметной тенденции к развитию универсализма в этой области, что ярко выражается в формировании общих подходов к правовому регулированию общественных отношений, связанных с защитой ПДн и международных стандартов государственно-правовой защиты этих данных. Последние выступают правовым ориентиром в развитии рос-

сийского законодательства, устанавливающего правовые механизмы защиты ПДн, а так же для соответствующей правоприменительной практики. И всё же, в заключение можно сказать о том, что как бы не трудились «ученые умы» любой страны, данный вопрос всегда будет оставаться открытым.

Прогресс не стоит на месте, и в соответствии с ярко выраженной тенденцией роста значения информационных технологий и их «просачивания» в каждую сферу жизнедеятельности, законодательство просто не сможет успеть за ними, и всегда найдутся как плюсы, так и минусы в любом нормативно-правовом акте и любой правовой системы касательно данного вопроса.

# 3. ПРЕДЛОЖЕНИЯ ПО МОДЕРНИЗАЦИИ СИСТЕМЫ ЗАЩИТЫ

На предприятии ООО ЧОП «Витязь» осуществляется комплекс мер по защите ПДн. По результатам составленной модели угроз были выявлены актуальные угрозы, фактическая защищенность от которых на данный момент не обеспечена. По этому предложен ряд мер, для повышения уровня защищенности ПДн в ИС-ПДн на предприятии ООО ЧОП «Витязь».

## 3.1. Межсетевой экран

Межсетевой экран - это совокупность программных средств, позволяющих анализировать и фильтровать весь трафик, проходящий по сети, а при возникновении опасности - блокировать опасные пакеты или вирусы.

Установка межсетевого экрана на предприятии ООО ЧОП «Витязь» позволит обеспечить защиту от актуальных угроз, таких как:

- анализ сетевого трафика;
- угрозы выявления паролей по сети;
- угрозы удаленного запуска приложений;
- угрозы внедрения по сети вредоносных программ;

Для анализа и последующего выбора межсетевого экрана были выбраны три продукта разных категорий МЭ:

- межсетевой экран StoneGate Firewall;
- межсетевой экран «Киберсейф: Межсетевой экран»;
- VipNet Office Firewall.

Характеристики вышеперечисленных МЭ перечислены в таблице 8.

Таблица 8 - Технические характеристики межсетевых экранов.

| Программный продукт | StoneGate Firewall | «Киберсейф: Межсетевой экран» | VipNet Office Firewall |
|---|---|---|---|
| 1 | 2 | 3 | 4 |
| Фильтрация доступа | Да | Да | Да |
| Контроль доступа | Да | Да | Да |
| Регламентирование доступа | Да | Да | Да |
| Контроль трафика | Да | Да | Да |
| NAT | Да | Да | Да |
| Переадресация пакетов | Да | Да | Да |
| Маскировка портов | нет | Да | Нет |
| Регулирование нагрузки | Да | Да | Нет |
| Многопользовательский режим | Да | Да | Нет |
| Контроль целостности | Да | Да | Да |
| Восстановление работоспособности | Да | Да | Да |

Продолжение Таблицы 8

| 1 | 2 | 3 | 4 |
|---|---|---|---|
| Защита до входа в систему | Да | Да | Нет |
| Развертывание в Active Directory | нет | Да | Нет |
| Удаленное администрирование извне | Да | Да | Нет |

Таблица 9 - Оценка межсетевых экранов.

| Продукт | Цена | Класс защищенности | Наличие сертификата |
|---|---|---|---|
| StoneGate Firewall | 89000 | 2 | Есть |
| «Киберсейф: Межсетевой экран» | 9000 | 3 | Есть |
| VipNet Office Firewall | 36000 | 4 | Есть |

Все эти программные продукты, согласно реестру ФСТЭК, сертифицированы как межсетевые экраны (Приложение Г). Согласно приказу ФСТЭК России №21 от 18 февраля 2013 г. каждый из представленных в таблице межсетевых экранов может использоваться для обеспечения необходимого уровня защищенности.

По результатам анализа всех характеристик, перечисленных в таблицах был выбран межсетевой экран третьей категории «Киберсейф: Межсетевой экран».

### 3.2. Источник бесперебойного питания

ИБП защищает технику от скачков напряжения и вызванных ими отказов оборудования, обеспечивает надежность и стабильность работы электроники.

Для анализа характеристик было выбрано три устройства из различных ценовых категорий, они приведены в таблице 10:

Таблица 10 - Характеристики ИБП.

| Производитель | APC | Ippon | PowerCom |
|---|---|---|---|
| 1 | 2 | 3 | 4 |
| Модель | BACK-UPS CS 500VA 230V (BK500EI) | Back Power Pro 500 | Warrior WAR-500A |

Продолжение Таблицы 10

| 1 | 2 | 3 | 4 |
|---|---|---|---|
| Тип | Резервный (stand-by); частота и напряжение на выходе определяются частотой и напряжением на входе | Линейно-интерактивный (line-interactive); обеспечивает стабилизацию напряжения на выходе; при этом частоты на входе и выходе совпадают | Линейно-интерактивный (line-interactive); обеспечивает стабилизацию напряжения на выходе; при этом частоты на входе и выходе совпадают |
| Номинальное выходное напряжение | 230В | 230В | 230В |
| Время зарядки | 6 часов | 4 часа | 6 часов |
| Время работы при полной нагрузке | 5 мин | 5 мин | 8 мин |
| Максимальная выходная мощность | 500 ВА | 500 ВА | 500 ВА |
| Эффективная мощность батареи | 300 Ватт | 300 Ватт | 250 Ватт |
| Защита от перегрузки | Есть | Есть | Есть |
| Защита от высоковольтных импульсов | Есть | Есть | Есть |
| Индикация | Есть | Нет | Есть |
| Защита от короткого замыкания | Есть | Есть | Есть |
| Управление с ПК | Есть | Есть | Нет |
| Время реакции | 4-8мс | 3 мс | 4 мс |
| Входы/выходы | 1 разъём IEC 320 C13 (Защита от всплесков напряжения); 3 разъёма IEC 320 C13 (Батарейное резервное питание); 2 разъёма IEC Jumpers (Батарейное резервное питание) защита коммуникационных линий | 3 разъёма IEC 320 C13 (из них с питанием от батарей — 3) | 2 разъёма IEC 320 C13 (из них с питанием от батарей — 2) |

Продолжение Таблицы 10

| 1 | 2 | 3 | 4 |
|---|---|---|---|
| Макс. поглощаемая энергия импульса | 310 Дж | 320 Дж | 460 Дж |
| AVR (Автоматическая регулировка напряжения) | Нет | Есть | Есть |
| Входное напряжение | 180 — 260 В | 165 — 275 В | 165 — 253 В |
| Габариты | 91x165x284 мм | 100x140x330 мм | 91x125x254 мм |
| Вес | 6.32 кг | 6 кг | 4.45 кг |
| Цена | 3 094 руб. | 1 788 руб. | 1 529 руб. |

Проанализировав все характеристики устройств, был выбран источник бесперебойного питания Ippon Back Power Pro 500.

### 3.3. Биометрические средства защиты

Биометрическая аутентификация это процесс доказательства и проверки подлинности заявленного пользователем имени, через предъявление пользователем биометрического образа и путем преобразования этого образа в соответствии с заранее определенным протоколом аутентификации.

В настоящее время существует множество методов биометрической аутентификации. Для того, чтобы выбрать оптимальное средство защиты для ООО ЧОП «Витязь» необходимо сравнить различные методы и выявить их положительные и отрицательные стороны. Характеристики биометрических средств защиты представлены в таблице 11.

Таблица 11 - Характеристики биометрических средств защиты.

| Биометрические характеристики | Отпечаток пальца | Сетчатка глаза | Радужная оболочка глаза | Вены руки |
|---|---|---|---|---|
| Устойчивость к подделке | 6 | 10 | 10 | 10 |
| Устойчивость к окружающей среде | 10 | 10 | 9 | 7 |
| Стабильность признака во времени | 9 | 9 | 10 | 7 |
| Простота использования | 9 | 6 | 8 | 9 |
| Скорость | 10 | 6 | 10 | 8 |
| Стоимость | 10 | 3 | 7 | 7 |

Проанализировав данные можно сказать, что для ООО ЧОП «Витязь» оптимальным будет доступ по отпечатку пальца.

Дактилоскопия – распознавание отпечатков пальцев – наиболее распространенный и разработанный метод биометрической аутентификации в наше время. Он приобрел такую популярность за счет широкого применения в криминалистике в 20 веке.

Папиллярный узор отпечатка пальцев каждого человека уникален, за счет этого и становится возможна идентификация. На отпечатках присутствуют характерные точки, которые используются алгоритмами: окончания линий узора, разветвления линий, одиночные точки. Такие особенности папиллярного узора преобразовываются в уникальный код, сохраняющий информативность изображения узора. Коды отпечатков пальцев сохраняются в базу данных, используемую для поиска и сравнения. Обычно время преображения изображения отпечатка пальца в код и его последующая идентификация не занимает более 1 секунды.

Для того, чтобы выбрать подходящий сканер отпечатков пальцев для ООО ЧОП «Витязь», рассмотрим несколько альтернативных вариантов и сравним их характеристики, которые представлены в таблице 12.

Таблица 12 - Характеристики сканеров отпечатков пальцев.

| Продукт | ANVIZ P7 POE | BioSmart-WTC2 |
|---|---|---|
| Максимальное количество пользователей | 3000 | 5000 |
| Максимальное количество хранимых событий | 50000 | 100000 |
| Время идентификации | 0,5с | 1с |
| Вероятность ложного отказа | 0,001% | 0,0001% |
| Вероятность ложного допуска | 0,00001% | 0,00001% |
| Экран | OLED 128мм*64мм | TFT 3,5” разрешение 320x240 dpi |
| Встроенный считыватель карт | Да | Да |
| Датчик открытой двери | Да | Нет |
| Тревога, при вскрытии корпуса | Да | Да |
| Функция "Запрет двойного прохода" | Да | Нет |
| Размер | 54мм*170мм*41мм | 142ммх123ммх41мм |
| Материал | Износостойкий промышленный пластик | Накладной пластиковый корпус |
| Гарантия | 5 лет | 3 года |
| Стоимость | 16000 | 20000 |

Проанализировав данные, оптимальным для установки на ООО ЧОП «Витязь», было выбрано оборудование Anviz P7 POE. Оно удовлетворяет требованиям по количеству пользователей, имеет приемлемую стоимость и большой функционал. При принятии решения о внедрении биометрических средств защиты ин-

формации будет необходимо составить еще одну модель угроз, подходящую для такого типа данных.

### 3.4. Организационно-распорядительные документы

На предприятии ООО ЧОП «Витязь» уже существует ряд организационно-распорядительной документации, проанализировав который были выявлены недостающие положения и акты.

Так же стоит отметить, что внедрение новых аппаратных и программных средств защиты информации тоже влечет за собой составление новых организационно-распорядительных документов, описывающих политику работы с новыми средствами и продуктами.

Было принято решение составить и ввести в эксплуатацию ряд следующих документов:

- приказ об утверждении списка лиц, допущенных к ПДн (Приложение Д);
- порядок доступа работников в помещения, в которых ведется обработка ПДн (Приложение Е);
- инструкция по работе с МЭ;
- инструкция о порядке работы с ПДн;
- акт уничтожения ПДн на электронных носителях.

В ходе работы мной были разработаны и приложены к рекомендациям по модернизации системы защиты информации следующие документы:

- приказ об утверждении списка лиц, допущенных к ПДн;
- порядок доступа работников в помещения, в которых ведется обработка ПДн.

Таким образом, на основании составленной модели угроз и выявленных в последствии актуальных угрозах для предприятия ООО ЧОП «Витязь» был сформирован список рекомендаций для усовершенствования существующей системы защиты. Для защиты от актуальных угроз были предложены меры:

- установка межсетевого экрана третьей категории «Киберсейф: Межсетевой экран»;
- установка источников бесперебойного питания «Ippon Back Power Pro 500»;
- установка сканера отпечатков пальцев Anviz P7 POE.

Часть необходимых организационно-распорядительных документов была составлена и приложена к рекомендациям.

# БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1.Блинов А.М. «Информационная безопасность», 2010г. – 96с.
2.Политика информационной безопасности - опыт разработки и рекомендации - 2013г. [Электронный ресурс]. - Режим доступа:
https://habrahabr.ru/post/174489/
3.Оценка информационной безопасности в деятельности организаций – 2012г. [Электронный ресурс]. - Режим доступа:
https://habrahabr.ru/post/158143/
4.Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка). ФСТЭК России, 2008 г. [Электронный ресурс]. - Режим доступа:
http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/379-bazovaya-model-ugroz-bezopasnosti-personalnykh-dannykh-pri-ikh-obrabotke-v-informatsionnykh-sistemakh-personalnykh-dannykh-vypiska-fstek-rossii-2008-god
5.Методический документ методика определения угроз безопасности информации в информационных системах. Проект, 2015 г.[Электронный ресурс]. - Режим доступа:
http://fstec.ru/component/attachments/download/812
6.Постановление Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных", 2012г. [Электронный ресурс]. - Режим доступа:
http://www.consultant.ru/document/cons_doc_LAW_137356/
7.Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ, 2006г. [Электронный ресурс]. - Режим доступа:
http://www.consultant.ru/document/cons_doc_LAW_61798/
8.Указ Президента РФ от 06.03.1997 N 188 (ред. от 13.07.2015) "Об утверждении Перечня сведений конфиденциального характера", 2015г.[Электронный ресурс]. - Режим доступа:
http://www.consultant.ru/document/cons_doc_LAW_13532/
9.Постановление Правительства РФ от 26 июня 1995 г. №608 "О сертификации средств защиты информации" (с изменениями от 23 апреля 1996 г., 29 марта 1999 г., 17 декабря2004 г.), 2004г. [Электронный ресурс]. - Режим доступа:
http://base.garant.ru/102670/
10. Аверченков В.И, Рытов М.Ю. Гайнулин Т.Р «Защита персональных данных в организации» Москва Флинта, 2016г – 125с.

ПРИЛОЖЕНИЕ А

**ПОЛОЖЕНИЕ**

**ОБ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ**

**В ООО ЧОП «Витязь»**

ОБЩИЕ ПОЛОЖЕНИЯ

Положение об обработке персональных данных в ООО ЧОП "Витязь" (далее – Положение) разработано в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – ФЗ-152), Трудовым кодексом Российской Федерации (далее – ТК РФ), а также «Перечнем сведений конфиденциального характера», утвержденным Указом Президента Российской Федерации от 06.03.1997 № 188.

Настоящее Положение определяет порядок обработки персональных данных и устанавливает общие требования к обеспечению безопасности персональных данных, обрабатываемых в ООО ЧОП "Витязь" (далее – Оператор) как с использованием средств автоматизации, так и без использования таких средств.

В Положении используются следующие основные понятия:

**автоматизированная обработка персональных данных** – обработка персональных данных с помощью средств вычислительной техники;

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

**информационная система персональных данных** – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

**обезличивание персональных данных** – действия, в результате которых невозможно определить без использования дополнительной информации принадлежность персональных данных конкретному субъекту персональных данных;

**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, предоставле

ние, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

**оператор –** 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;

**персональные данные** – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

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

**распространение персональных данных** – действия, направленные на раскрытие персональных данных неопределенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом;

**трансграничная передача персональных данных** – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому или иностранному юридическому лицу;

**уничтожение персональных данных** – действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

Действие Положения распространяется на все структурные подразделения Оператора.

Настоящее Положение должно быть доведено до каждого работника Оператора, осуществляющего обработку персональных данных, под роспись.

## 2. СУБЪЕКТЫ И ЦЕЛИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Цели обработки персональных данных, основания для их обработки, возможные действия (операции), совершаемые с персональными данным, сроки обработки и состав обрабатываемых персональных категорий субъектов персональных данных, обрабатываемых у Оператора, указаны в указаны в Перечне обрабатываемых персональных данных.

## 3. ОРГАНИЗАЦИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

### 3.1. Назначение ответственных лиц

Для организации обработки персональных данных у Оператора назначается ответственное лицо.

Для определения уровня защищенности информационных систем персональных данных, проверки готовности средств защиты информации к использованию, а также уничтожения персональных данных приказом руководителя Оператора назначается Комиссия по приведению в соответствие с требованиями законодательства Российской Федерации в области персональных данных (далее – Комиссия).

В своей работе Комиссия руководствуется Положением о комиссии по приведению в соответствие с требованиями законодательства Российской Федерации в области персональных данных, утвержденным приказом руководителя Оператора.

3.2. Допуск работников к обработке персональных данных

Допуск работников Оператора к обработке персональных данным осуществляется на основании приказа о назначении на должность в соответствии с Перечнем должностей и третьих лиц, имеющих доступ к персональным данным.

Работники Оператора получают доступ к обработке персональных данных для выполнения ими служебных (трудовых) обязанностей, после выполнения следующих мероприятий:

- ознакомления под роспись с руководящими документами Оператора и нормативными актами Российской Федерации по обработке и обеспечению безопасности персональных данных;
- оформления письменного обязательства о неразглашении персональных данных, форма которого утверждена приказом руководителя Оператора.

Работники Оператора, имеющие допуск к персональным данным, имеют право получать только те персональные данные, которые необходимы им для выполнения служебных (трудовых) обязанностей.

3.3. Получение персональных данных

Персональные данные субъекта получаются от него самого или от него законного представителя. В случае, если персональные данные получены не от субъекта персональных данных, Оператор до начала обработки таких персональных данных обязан уведомить субъекта о получении его персональных данных.

3.4. Систематизация, накопление, уточнение и использование персональных данных

Систематизация, накопление, уточнение и использование персональных данных осуществляется путем оформления и ведения документов учета и баз данных субъектов персональных данных.

Работники Оператора, имеющие доступ к персональным данным, должны обеспечить их обработку, исключающую несанкционированный доступ к ним третьих лиц.

3.5. Передача персональных данных

Передача персональных данных субъектов третьим лицам может осуществляться только при наличии письменного согласия субъекта, если иное не предусмотрено федеральным законодательством.

При передаче персональных данных субъектов третьим лицам, с третьим лицом должно быть подписано Соглашение о соблюдении безопасности персональных данных, переданных на обработку, форма которого утверждена приказом руководителя Оператора.

Передача персональных данных субъектов между подразделениями Оператора должна осуществляться только между работниками, допущенными к обработке персональных данных.

3.6. Хранение персональных данных

Хранение персональных данных субъектов осуществляется на бумажных и машинных носителях информации в специально выделенных хранилищах подразделений Оператора, а также в информационных системах Оператора, обеспечивающих сохранность персональных данных и их защиту от несанкционированного доступа.

Уничтожение персональных данных в информационных системах, на машинных и бумажных носителях информации должно производиться в течение тридцати дней с даты достижения цели обработки (предельного срока хранения) персональных данных. При невозможности уничтожения персональных данных в течение тридцати дней с даты достижения цели обработки персональных данных, обеспечивается их блокирование и уничтожение в срок, не превышающий шести месяцев.

Порядок и правила учета, хранения и уничтожения персональных данных описаны в Регламенте по учету, хранению и уничтожению носителей персональных данных.

3.7. Уведомление об обработке персональных данных

Согласно ст. 22 ФЗ-152 Оператор уведомляет Уполномоченный орган по защите прав субъектов персональных данных об обработке персональных данных.

В случае изменения сведений, указанных в уведомлении, а также в случае прекращения обработки персональных данных Оператор также уведомляет об этом Уполномоченный орган.

## 4. ОСОБЕННОСТИ ОРГАНИЗАЦИИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОСУЩЕСТВЛЯЕМОЙ БЕЗ ИСПОЛЬЗОВАНИЯ СРЕДСТВ АВТОМАТИЗАЦИИ

Персональные данные при их обработке без использования средств автоматизации обособляются от иной информации путем фиксации их на отдельных материальных носителях персональных данных, в специальных разделах или на полях форм (бланков).

При фиксации персональных данных на материальных носителях не допускается запись на одном материальном носителе персональных данных, цели обработки которых заведомо несовместимы. При обработке различных категорий персональных данных без использования средств автоматизации для каждой категории персональных данных должен использоваться отдельный материальный носитель.

При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных, должны соблюдаться следующие условия:

- типовая форма должна содержать сведения о цели обработки персональных данных, наименование и адрес Оператора, фамилию, имя, отчество и

адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки персональных данных;

- типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных – при необходимости получения письменного согласия на обработку персональных данных;
- типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;
- типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных.

Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе.

Уточнение персональных данных при их обработке без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, – путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными.

Лица, осуществляющие обработку персональных данных без использования средств автоматизации, должны быть проинформированы:

- о факте обработки ими персональных данных, обработка которых осуществляется без использования средств автоматизации;
- о категориях обрабатываемых персональных данных;
- об особенностях и правилах осуществления такой обработки.

5. ОРГАНИЗАЦИЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Персональные данные обрабатываются у Оператора как с использованием средств автоматизации, так и без использования таких средств.

Порядок обработки и защиты персональных данных в информационных системах Оператора определяется Положением об обеспечении безопасности персональных данных

Защита персональных данных от неправомерного их использования или утраты обеспечивается Оператором за счет собственных средств.

Работники Оператора, которые в рамках исполнения должностных обязанностей имеют доступ к персональным данным, обязаны соблюдать режим конфиденциальности персональных данных на всех этапах их обработки.

В отсутствие работника на его рабочем месте не должно быть документов и машинных носителей информации, содержащих персональные данные.

Доступ работников Оператора и иных лиц в помещения, в которых осуществляется обработка и хранение персональных данных, ограничивается организационными мерами и применением системы контроля и управления доступом.

Учитывая массовость и единые места обработки и хранения, гриф «конфиденциально» на документах, содержащих персональные данные, не ставится.

Организацию обработки персональных данных субъектов, контроль соблюдения мер их защиты в структурных подразделениях Оператора, сотрудники которых имеют доступ к персональным данным, осуществляют их непосредственные руководители.

Мероприятия по защите персональных данных осуществляются в соответствии с Планом мероприятий по приведению в соответствие с требованиями законодательства Российской Федерации в области персональных данных, утверждаемых руководителем Оператора.

Разработка и осуществление мероприятий по обеспечению безопасности персональных данных, обрабатываемых в информационных системах, может осуществляться сторонними организациями на договорной основе, имеющими лицензии на право проведения соответствующих работ.

## 6. ПОРЯДОК ОБРАБОТКИ ОБРАЩЕНИЙ И ЗАПРОСОВ ПО ВОПРОСАМ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Порядок обработки запросов субъектов персональных данных описан в Регламенте по реагированию на запросы субъектов персональных данных.

Порядок обработки запросов уполномоченных органов в области персональных данных описан в Регламенте по взаимодействию с органами государственной власти в области персональных данных.

## 7. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

Иные права и обязанности работников, в функции которых входит обработка персональных данных, определяются Инструкцией пользователя информационных систем персональных данных.

Лица, виновные в нарушении норм, регулирующих обработку и защиту персональных данных, несут материальную, дисциплинарную, административную, гражданско-правовую или уголовную ответственность в порядке, установленном федеральными законами.

Разглашение персональных данных, их публичное раскрытие, утрата документов и иных носителей, содержащих персональные данные, а также иные нарушения обязанностей по их защите и обработке, установленных настоящим Положением, другими локальными нормативными актами (приказами, распоряжениями) Оператора, влечет наложение на сотрудника, имеющего доступ к персональным данным, дисциплинарного взыскания – замечания, выговора, увольнения.

Работник, имеющий доступ к персональным данным и совершивший указанный дисциплинарный проступок, несет полную материальную ответственность в случае причинения его действиями ущерба работодателю (п. 7 ст. 243 ТК РФ).

Работники Оператора, имеющие доступ к персональным данным, виновные в их незаконном разглашении или использовании без согласия субъектов персональных данных из корыстной или иной личной заинтересованности и причинившие крупный ущерб, несут уголовную ответственность в соответствии со ст. 183 Уголовного кодекса Российской Федерации.

Обновление и актуализация настоящего положения осуществляется в соответствии с Регламент по проведению контрольных мероприятий и реагированию на инциденты информационной безопасности.

ПРИЛОЖЕНИЕ Б

**Положение об использовании носителей информации в ООО ЧОП «Витязь»**

1. Общие положения

1.1. Настоящее Положение устанавливает порядок использования мобильных устройств и носителей информации, предоставляемых ООО ЧОП «Витязь» (далее Организация) для использования в ИС.

1.2. Действие настоящего Положения распространяется на работников Организации, подрядчиков и третью сторону.

2. Основные термины, сокращения и определения

- Администратор ИС – технический специалист, обеспечивает ввод в эксплуатацию, поддержку и последующий вывод из эксплуатации ПО и оборудования вычислительной техники.
- АРМ – автоматизированное рабочее место пользователя (ПК с прикладным ПО) для выполнения определенной производственной задачи.
- ИБ – информационная безопасность – комплекс организационно-технических мероприятий, обеспечивающих конфиденциальность, целостность и доступность информации.
- ИС – информационная система Организации – система, обеспечивающая хранение, обработку, преобразование и передачу информации Организации с использованием компьютерной и другой техники.
- Носитель информации – любой материальный объект, используемый для хранения и передачи электронной информации.
- Паспорт ПК – документ, содержащий полный перечень оборудования и программного обеспечения АРМ.
- ПК – персональный компьютер.
- ПО – Программное обеспечение вычислительной техники.
- ПО вредоносное – ПО или изменения в ПО, приводящие к нарушению конфиденциальности, целостности и доступности критичной информации.
- ПО коммерческое – ПО сторонних производителей (правообладателей). Предоставляется в пользование на возмездной (платной) основе.
- Пользователь – работник Организации, использующий мобильные устройства и носители информации для выполнения своих служебных обязанностей.
- Организация – ООО ЧОП «Витязь».

- Реестр – документ «Реестр разрешенного к использованию ПО». Содержит перечень коммерческого ПО, разрешенного к использованию в Организации.

## 3. Порядок использования носителей информации

3.1. Под использованием носителей информации в ИС Организации понимается их подключение к инфраструктуре ИС с целью обработки, приема/передачи информации между ИС, а также носителями информации.

3.2. В ИС допускается использование только учтенных носителей информации, которые являются собственностью Организации и подвергаются регулярной ревизии и контролю.

3.3. К предоставленным Организацией носителям информации предъявляются те же требования ИБ, что и для стационарных АРМ (целесообразность дополнительных мер обеспечения ИБ определяется администраторами ИС).

3.4. Носители информации предоставляются работникам Организации по инициативе Руководителей структурных подразделений в случаях:

- необходимости выполнения вновь принятым работником своих должностных обязанностей;
- возникновения у работника Организации производственной необходимости.

3.5. Процесс предоставления работнику Организации носителей информации состоит из следующих этапов:

3.5.1. Подготовка заявки в утвержденной форме, осуществляется Руководителем структурного подразделения на имя Руководителя Организации.

3.5.2. Согласование подготовленной заявки (для получения заключения о возможности предоставления работнику Организации заявленного носителя информации) с начальником отдела ИТ.

3.5.3. Передача оригинала заявки в отдел ИТ для учета предоставленного носителя информации и внесения изменений в «Список работников Организации, имеющих право работы с носителями информации вне территории ООО ЧОП «Витязь», а также выполнение технических настроек по использованию носителей информации на АРМах Организации (в случае согласования заявки Руководителем Организации).

3.6. Внос на территорию Организации предоставленных носителей информации работниками Организации, а также вынос их за его пределы производится только на основании «Списка работников Организации, имеющих право работы с носи-

телями информации вне территории ООО ЧОП «Витязь», который ведется отделом ИТ на основании утвержденных заявок и передается в службу безопасности.

3.7. При использовании предоставленных работникам Организации и носителей информации необходимо:

3.7.1. Соблюдать требования настоящего Положения.

3.7.2. Использовать носители информации исключительно для выполнения своих служебных обязанностей.

3.7.3. Ставить в известность администраторов ИС о любых фактах нарушения требований настоящего Положения.

3.7.4. Бережно относится к носителям информации.

3.7.5. Эксплуатировать и транспортировать носители информации в соответствии с требованиями производителей.

3.7.6. Обеспечивать физическую безопасность носителей информации всеми разумными способами.

3.7.7. Извещать администраторов ИС о фактах утраты (кражи) носителей информации.

3.8. При использовании предоставленных работникам Организации и носителей информации запрещено:

3.8.1. Использовать носители информации в личных целях.

3.8.2. Передавать носители информации другим лицам (за исключением администраторов ИС).

3.8.3. Оставлять носители информации без присмотра, если не предприняты действия по обеспечению их физической безопасности.

3.9. Любое взаимодействие (обработка, прием/передача информации) инициированное работником Организации между ИС и неучтенными (личными) носителями информации, рассматривается как несанкционированное (за исключением случаев оговоренных с администраторами ИС заранее). Организация оставляет за собой право блокировать или ограничивать использование таких устройств и носителей информации.

3.10. Информация об использовании работниками Организации носителей информации в ИС протоколируется и, при необходимости, может быть предоставлена Руководителям структурных подразделений

3.11. При подозрении работника Организации в несанкционированном и/или нецелевом использовании носителей информации инициализируется служебная проверка, проводимая комиссией, состав которой определяется Руководителем Организации.

3.12. По факту выясненных обстоятельств составляется акт расследования инцидента и передается Руководителю структурного подразделения для принятия мер согласно локальным нормативным актам Организации и действующему законодательству. Акт расследования инцидента и сведения о принятых мерах подлежат передаче в отдел ИТ.

3.13. Информация, хранящаяся на предоставляемых Организацией носителях информации, подлежит обязательной проверке на отсутствие вредоносного ПО.

3.14. В случае увольнения или перевода работника в другое структурное подразделение Организации, предоставленные ему носители информации изымаются.

## 4. Ответственность

4.1. Работники, нарушившие требования настоящего Положения, несут ответственность в соответствии с действующим законодательством и локальными нормативными актами Организации.

## 5. Внесение изменений и дополнений

5.1. Изменения и дополнения в настоящее Положение вносятся работниками отдела ИТ по указанию начальника отдела, и после согласования с Руководителями служб Организации утверждаются приказом Руководителя Организации.

5.2. Все изменения и дополнения настоящего Положения вступают в силу с момента их утверждения.

ПРИЛОЖЕНИЕ В

**Правила пользования корпоративной компьютерной сетью ООО ЧОП «Витязь»**

## I. Общие положения

Корпоративной компьютерной сетью ООО ЧОП «Витязь» (в дальнейшем ККС) называется совокупность компьютеров, кабельной системы, сетевых адаптеров, активного сетевого оборудования, работающих под управлением сетевых операционных систем и прикладного программного обеспечения.

Настоящие правила содержат необходимые требования по обеспечению совместной работы в ККС, сохранности информации пользователей сети и соблюдения прав на ее распространение, в том числе и защиты личной информации пользователей.

Настоящие правила предназначены для регулирования распределения ресурсов коллективного пользования и поддержания необходимого уровня защиты информации, ее сохранности и соблюдения прав доступа к информации, установленных ее собственником, в том числе и соблюдения конфиденциальности личной информации. Правила служат интересам всех пользователей, поэтому в случае появления у пользователя сведений или подозрений о фактах нарушения настоящих правил, а, в особенности, о фактах несанкционированного доступа к информации, размещенной на его компьютере или каком-либо другом, он должен немедленно сообщить администратору сети или лицу, ответственному в сети за компьютерную безопасность.

## II. Права и обязанности администрации ККС

Администрацией сети являются сотрудники отдела по защите информации, наделенные административными правами.

*Администрация сети в рамках настоящих правил несет ответственность за:*

1. Функционирование ККС в целом;
2. Функционирование базовых сервисов сети;
3. Нарушение функционирования ККС вследствие некорректного управления маршрутизацией;
4. Нарушение функционирования ККС вследствие некорректного управления базовыми сетевыми сервисами (DNS, DHCP, AD).

*Администрация ККС не несет ответственности за:*

1. Информацию, находящуюся на компьютерах в сети подразделений, входящих в ККС, установленные права доступа к компьютерам в локальных сетях подразделений и за деятельность, ведущуюся на этих компьютерах;
2. Работоспособность компьютеров и оборудования сети подразделений, работоспособность и физическое состояние линий связи и других средств коммуникаций внутри сети подразделений;
3. Содержание проходящих по сети данных.

**Администрация обязана:**

1. Ограничивать доступ сотрудников и посетителей в помещения, в которых установлены серверы и коммутационное оборудование ККС;
2. Обеспечивать контроль структуры сети и пресечение несанкционированного подключения к ККС;

*Технические мероприятия включают в себя:*

- регулярную смену сетевых паролей;
- отслеживание запуска и пресечение использования программного обеспечения затрудняющего или нарушающего нормальную работоспособность сети, компьютеров в ней и нарушающего безопасность сети;
- настройка доменных политик безопасности.

3. Принимать организационные и технические меры к пресечению попыток несанкционированного доступа на компьютеры из внешних сетей и с компьютеров ККС, а также к пресечению распространения информации, запрещенной действующим законодательством.

**Администрация имеет право:**

1. В случае злоупотребления сетью частично или полностью отстранять нарушителей от пользования ККС;
2. Удалять программное обеспечение, нарушающее работу ККС.

## III. Права и обязанности пользователей ККС

Пользователями ККС ООО ЧОП «Витязь» являются сотрудники предприятия, ознакомленные с настоящими правилами и соблюдающие их требования в процессе работы.

Пользователь несет полную ответственность за все действия, связанные с использованием компьютерных сетей, от его имени или с закрепленного за ним рабочего места. За действия связанные с настройкой сетевых параметров несет ответственность администратор рабочего места. Лица, допустившие нарушения требований настоящих правил, несут дисциплинарную ответственность. В особо серьезных случаях, нарушители подвергаются судебному преследованию в установленном законом порядке, (см. Приложение 1).

Пользователи должны уважать права других пользователей на конфиденциальность и право на пользование общими ресурсами.

**Пользователь имеет право:**

1. На доступ ко всем ресурсам ККС ООО ЧОП «Витязь» в пределах требований настоящих правил;
2. Обращаться за справочной информацией и консультацией к соответствующему техническому персоналу, обслуживающему ККС.

**Пользователь обязан:**

1. Использовать ресурсы ККС исключительно в рабочих целях;
2. Выполнять все требования администрации сети, не противоречащие настоящим правилам;
3. Соблюдать правила техники безопасности при работе с техническими средствами;
4. Обеспечивать неразглашение идентификационной информации, используемой для доступа к ресурсам ККС (паролей и прочих кодов авторизованного доступа);
5. Препятствовать несанкционированному и недобросовестному использованию ресурсов
ККС;

6. Содействовать сохранности и дальнейшему развитию ресурсов и технических средств
ККС;
7. Пользоваться антивирусными программами.
8. Сообщать о замеченных неисправностях сетевого оборудования и недостатках в работе программного обеспечения.

**9.** Ознакомиться с настоящими правилами и правилами работы в ККС до начала работы на компьютере подключенному к сети.

## IV. Общие рекомендации и правила пользования ККС

**Использование учетной записи:**

Для надежной и безопасной работы в ККС администрация настоятельно рекомендует пользователям придерживаться следующих правил при работе с учетными записями:

1. Контролировать доступ к своей учетной записи, следить за содержимым своей общедоступной папки (если таковая имеется), за появлением файлов неизвестного происхождения (особенно скрытых).
2. Обеспечивать безопасность учетной записи, устанавливать пароль в соответствии с требованиями к нему:

- пароль должен содержать не менее 8 символов;
- пароль обязательно должен содержать цифры, строчные и заглавные символы;
- пароль не должен содержать имя для входа в систему, имя, фамилию, отчество, сочетание инициалов, дату рождения, телефон, другую личную информацию и английское слово;
- пользователь должен известить системного администратора об удалении ненужной учетной записи из системы;
- запрещается передавать свои пароли от сервисов другим пользователям;
- пароль должен меняться хотя бы раз в 6 месяцев, для смены пароля пользователю необходимо обратиться к администратору, назвав при этом старый пароль и придумав новый.

**Рекомендации к пользованию компьютерной корпоративной сетью:**

1. Отключать компьютерную технику и сетевой кабель во время грозы;
2. Хранить и помнить свои пароли доступа в сеть;
3. Знать и соблюдать настоящие правила;
4. Пользоваться антивирусными программами;
5. Сообщать свои замечания и предложения о работе сети системному администратору.

**Правила работы с персональным компьютером в ККС:**

1. Пользователь компьютера, включенного в ККС университета, должен быть ознакомлен с настоящими правилами.
2. Разрешение на подключение компьютера к сети дается администратором сети. Самовольное подключение является серьезнейшим нарушением правил пользования сетью. При подключении к сети пользователю выдается IP-адрес его компьютера. Так как передача данных в сеть с использованием других IP-адресов в качестве адреса отправителя является распространением ложной информации и созда

ет угрозу организации защиты информации других компьютеров, то передача таких данных категорически запрещена. В целях контроля за использованием ресурсов сети и обеспечения необходимых мер компьютерной безопасности на передачу данных в ККС с использованием протоколов, отличных от общепринятых, требуется разрешения администратора сети.
3. Пользователь несет личную ответственность за весь информационный обмен между его компьютером и другими компьютерами в ККС. В случае, если с данного компьютера производился несанкционированный доступ к информации на других компьютерах и в случаях других серьезных нарушений правил пользования сетью, по решению администратора сети компьютер отключается от сети, а к пользователю данного компьютера применяются меры, предусмотренные административным или уголовным законодательством.

## V. Пользователям ККС категорически запрещается

1. Использовать вычислительную технику для несанкционированного доступа к другим компьютерам сети и нарушения системы безопасности в целом;
2. Подключать компьютеры к сети без специального разрешения системного администратора;
3. Категорически запрещается самовольно изменять IP-адреса компьютеров в сети, принадлежность компьютера к домену, сетевое имя компьютера, настройки шлюзов и основных серверов;
4. Распространять и использовать программное обеспечение и любые материалы, полностью или частично защищенные авторскими правами, без разрешения владельца.
5. Преднамеренно/непреднамеренно распространять компьютерные вирусы и зараженные ими файлы;
6. Перехватывать чужую информацию, передаваемую по сети;
7. Использовать программное обеспечение, ориентированное на нарушение системы безопасности сети ("троянские кони", бэкдоры и другое шпионское программное обеспечение).
8. Обмениваться информацией, запрещенной действующим законодательством РФ: пропаганда насилия, разжигание расовых, национальных и религиозных распрей, порнография, любая информация, несущая оскорбления и клевету, а также распространяемая с целью хищения чужих денежных средств или имущества путем обмана или злоупотребления доверием;
9. Несанкционированный доступ (или его попытки) к закрытым ресурсам в сети. Участвовать в проведении "сетевых атак" и "сетевого взлома";

*Эти действия определяются как:*

- использование против компьютеров или оборудования компьютерных сетей специальных средств, позволяющих получить нелегальный доступ к содержащейся информации;
- передача компьютерам или оборудованию компьютерных сетей бессмысленной или бесполезной информации, создающей паразитическую нагрузку на аппаратуру;
- уничтожение/модификация программного обеспечения или данных, не принадлежащих пользователю, без согласования с владельцами или администраторами этого программного обеспечения или данных;
- фальсификация своего сетевого адреса при передаче данных в сеть;
- фальсификация контактной информации, предъявленной владельцам или администраторам ресурсов или сетей;

- использование псевдонимов и анонимность, кроме случаев, когда право пользования соответствующими ресурсами или сетей разрешают анонимность при их использовании.

10. Сканировать порты на удаленных хостах. Это может быть расценено как попытка взлома, со всеми вытекающими последствиями;

***Сканированием*** *считается выдача запросов, в том числе и единичных, на предмет наличия того или иного сервиса или опрос наличия работающих машин на группу адресов, либо опрос диапазона портов с целью определения работающих сервисов на одной машине или группе машин, а также выдача запросов, обработка которых не санкционирована принимающей стороной, не предусматривается сетевым сервисом или не разрешена администрацией ресурса.*

11. Использовать сеть во вред другим пользователям, путем самостоятельного или с помощью третьих лиц вмешательства в действие аппаратуры и оборудования, а также иным способом;
12. Использовать доступ к компьютерным сетям для создания "сетевого шума" или "спама";
13. Распространять информацию, оскорбляющую честь и достоинство других пользователей и персонала компьютерных сетей;
14. Физически повреждать оборудование сети;
15. Устанавливать серверные операционные системы без специального разрешения системного администратора;
16. Пользователям, работающим с конфиденциальными документами категорически запрещается пользоваться на рабочем месте различного рода мессенджерами (ICQ, MSN, Miranda, QIP, Mail.Ru агентами, Google messenger и т.д.);
17. Просмотр видео и прослушивание аудио через сеть, за исключением случаев, связанных со служебной необходимостью;
18. Хранение на локальных и публичных сетевых дисках файлов, не относящихся к выполнению служебных обязанностей сотрудника (игры, видео, музыку, фотографии, виртуальные CD и т.п.);
19. Просмотр в рабочее время сайтов развлекательной направленности и сайтов, содержание которых не относится напрямую к служебным обязанностям работника;
20. Играть в рабочее время в онлайн игры;
21. Устанавливать нелицензионное программное обеспечение, а также свободно распространяемое (FreeWare) программное обеспечение, способное нарушить работу ККС;
22. Разрабатывать или распространять любые виды компьютерных вирусов, «троянских коней» или «логических бомб»;
23. Открывать файлы и запускать программы на локальном компьютере из непроверенных источников или принесённых с собой на переносных носителях без предварительной проверки антивирусной программой.
24. Самовольная организация доступа к ЛВС ООО ЧОП «Витязь» через машины конечных пользователей или другие устройства.

Использовать ККС в деятельности, противоречащих законодательству Российской Федерации (см. Приложение 1).

**Приложение 1.**

**Статья 272 УК РФ. Неправомерный доступ к компьютерной информации.**

Продолжение Приложения В

1. Неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтоже-

2. ние, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети, - наказывается штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо лишением свободы на срок до двух лет.

3. То же деяние, совершенное группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети, - наказывается штрафом в размере от пятисот до восьмисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от пяти до восьми месяцев, либо исправительными работами на срок от одного года до двух лет, либо арестом на срок от трех до шести месяцев, либо лишением свободы на срок до пяти лет.

ПРИЛОЖЕНИЕ Г

# СИСТЕМА СЕРТИФИКАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Система сертификации № РОСС RU.0001.01БИ00

**ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ**
**№ РОСС RU.0001.01БИ00**

## СЕРТИФИКАТ СООТВЕТСТВИЯ
## № 3417

Выдан 4 июня 2015 г.
Действителен до 4 июня 2018 г.

Настоящий сертификат удостоверяет, что **Межсетевой экран «Киберсейф: Межсетевой Экран»**, разработанный и производимый ООО «ДОРФ» в соответствии с техническими условиями RU.49462663.00001-02 98 01, функционирующий в среде операционных систем, указанных в формуляре RU.49462663.00001-02 30 01, является программным средством защиты информации, обрабатываемой в локальных вычислительных сетях с TCP/IP протоколом, от несанкционированного доступа из внешних вычислительных сетей, соответствует требованиям руководящих документов «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1997) – по **3** классу защищенности и «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (Гостехкомиссия России, 1999) – по **4** уровню контроля при выполнении указаний по эксплуатации, приведенных в формуляре.

Сертификат выдан на основании результатов сертификационных испытаний, проведенных испытательной лабораторией ООО «ЛИССИ-Софт» (аттестат аккредитации от 16.10.2012 № СЗИ RU. 1858.Б017.077) – техническое заключение от 18.05.2015, и экспертного заключения от 26.05.2015 органа по сертификации ООО «Центр безопасности информации» (аттестат аккредитации от 09.02.2007 № СЗИ RU.117.A10.004).

| | |
|---|---|
| Заявитель: | ООО «ДОРФ» |
| Адрес: | 350049, г. Краснодар, ул. Красных Партизан, д. 218 |
| Телефон: | (861) 204-0161 |

Контроль маркирования знаками соответствия сертифицированной продукции и инспекционный контроль её соответствия требованиям руководящих документов, указанных в настоящем сертификате, осуществляется испытательной лабораторией ООО «ЛИССИ-Софт».

**ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ**

**А.Куц**

**Настоящий сертификат внесен в Государственный реестр сертифицированных средств защиты информации 4 июня 2015 г.**

ПРИЛОЖЕНИЕ Д

ООО ЧОП «Витязь»

от _____ № _____

**ПРИКАЗ**

**О допуске сотрудников ООО ЧОП «Витязь» к обработке персональных данных**

В целях исполнения Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»

ПРИКАЗЫВАЮ:

1. Утвердить список сотрудников ООО ЧОП «Витязь», доступ которых к персональным данным, обрабатываемым в информационных системах персональных данных, необходим для выполнения служебных обязанностей (прилагается).
2. Допустить указанных сотрудников к обработке персональных данных.

Генеральный директор

_____

Продолжение Приложения Д
Приложение к приказу
ООО ЧОП «Витязь»

от
_____№_____

Список сотрудников ООО ЧОП «Витязь», доступ которых к персональным данным, обрабатываемым в информационных системах персональных данных, необходим для выполнения служебных (трудовых) обязанностей

| № | Фамилия Имя Отчество | Должность | Информационная система персональных данных |
|---|---|---|---|
| 1. | | | |
| 2. | | | |
| 3. | | | |
| 4. | | | |
| 5. | | | |
| 6. | | | |
| 7. | | | |
| 8. | | | |
| 9. | | | |
| 10. | | | |

ПРИЛОЖЕНИЕ Е

ООО ЧОП «Витязь»

от _____ № _____

**ПРИКАЗ**

**Порядок доступа работников ООО ЧОП «Витязь» в помещения, в которых ведется обработка персональных данных**

1. Настоящий Порядок доступа работников ООО ЧОП «Витязь» в помещения, в которых ведется обработка персональных данных (далее – Порядок) разработан в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных».

2. Персональные данные относятся к конфиденциальной информации. Должностные лица, уполномоченные на обработку персональных данных, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

3. Размещение информационных систем, в которых обрабатываются персональные данные, осуществляется в охраняемых помещениях, исключая возможность неконтролируемого проникновения и пребывания в этих помещениях посторонних лиц.

4. При хранении носителей персональных данных должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный доступ к ним. (Положение об использовании носителей информации)

5. В помещения, где размещены технические средства, позволяющие осуществлять обработку персональных данных, а также хранятся носители информации, допускаются только должностные лица, уполномоченные на обработку персональных данных приказом ООО ЧОП «Витязь».

6. Ответственными за организацию доступа в помещения, в которых ведется обработка персональных данных, являются руководители структурных подразделений ООО ЧОП «Витязь».

7. Нахождение лиц, в помещениях ООО ЧОП «Витязь», предназначенных для обработки персональных данных, не являющихся уполномоченными на обработку персональных данных, возможно только в сопровождении сотрудника,

уполномоченного на обработку персональных данных на время, обусловленное производственной необходимостью.

Генеральный директор

_____