Общество с ограниченной ответственностью
«Единый расчетно-информационный центр»
(ООО «ЕРИЦ»)

УТВЕРЖДЕНО
Приказом Генерального директора
ООО «ЕРИЦ» В.М.Решетникова
№ 07-04/8/5 от 13.05.2013

Положение о защите персональных данных
Положение -ПДн-3 (Редакция 1)

СОДЕРЖАНИЕ

1. Общие положения.

1.1. Настоящее положение по защите персональных данных (далее – Положение) в информационных системах персональных данных ООО «ЕРИЦ» (далее Организация), разработано в соответствии с требованиями Трудового кодекса Российской Федерации, Федеральных законов Российской Федерации "Об информации, информационных технологиях и о защите информации" № 149-ФЗ от 27 июля 2006 года, "О персональных данных" № 152-ФЗ от 27 июля 2006 года, постановления Правительства Российской Федерации от 01.11.2012 № 1119, нормативно-методическими документами ФСТЭК, ФСБ и Мининформсвязи России по защите персональных данных.

1.2. Положение определяет порядок организации работ по защите персональных данных (ПДн), обрабатываемых в информационных системах персональных данных (ИСПДн), применяемые организационные и технические меры по их защите, распределение обязанностей и ответственность должностных лиц Организации по защите персональных данных, порядок планирования работ и контроль правильности применения мер защиты и их эффективности.

1.3. В Организации подлежат защите персональные данные работников, как действующих, так и кандидатов на вакантные должности и уволенных, а также персональные данные потребителей.

1.4. Персональные данные сотрудников, обрабатываемые в Организации, предоставляются субъектами персональных данных.

1.5. Персональные данные потребителей предоставляются как субъектами персональных данных, так и третьей стороной – управляющими компаниями.

1.6. В договорах с потребителями – субъектами персональных данных должны быть указаны цели обработки ПДн, перечень подлежащих сбору и обработке персональных данных, способы обработки ПДн и совершаемые с ними действия, срок обработки ПДн, порядок отзыва согласия на обработку ПДн, а также юридические последствия для субъекта в случае отказа от предоставления и обработки его персональных данных. Если обработка будет поручена третьему лицу, то в договоре указывается наименование и адрес организации или лица, осуществляющего обработку ПДн по поручению оператора.

1.7. Для передачи персональных данных потребителей и обработки их в ООО «ЕРИЦ» управляющие компании должны получить согласие у субъектов персональных данных на передачу их ПДн третьим лицам, в том числе ООО «ЕРИЦ».

1.8. В Организации запрещено осуществлять сбор и обработку персональных данных о политических, религиозных и иных убеждениях субъектов персональных данных, а так же сведений об их состоянии здоровья.

1.9. Обработка персональных данных работников осуществляется исключительно в целях выполнения нормативных правовых актов и соблюдения законодательства РФ (трудового, налогового, пенсионного, страхового, архивного, по бухгалтерскому учёту и др.), ведения кадровой работы, содействия работникам в трудоустройстве, обучении и продвижении по службе, а также обеспечения контроля количества и качества выполняемой работы.

1.10. ООО «ЕРИЦ» не имеет права собирать и обрабатывать персональные данные работников об их членстве в общественных объединениях или профсоюзной деятельности, за исключением случаев, предусмотренных федеральным законодательством.

1.11. ООО «ЕРИЦ» не имеет права сообщать персональные данные работника третьей стороне без его письменного согласия, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в случаях, установленных федеральными законами.

1.12. Работники Организации должны быть ознакомлены в необходимом объеме под роспись с настоящим Положением, с другими организационно-распорядительными документами, устанавливающими порядок обработки персональных данных в ООО «ЕРИЦ», а также с правами и обязанностями работников в этой области.

1.13. Работы по информационной безопасности направлены на предотвращение (нейтрализацию) угроз безопасности ПДн в ИСПДн, на восстановление нормального функционирования ИСПДн после нейтрализации угрозы, минимизации как непосредственного, так и опосредованного ущерба от возможной реализации таких угроз.

1.14. Цели обеспечения информационной безопасности ПДн субъектов персональных данных достигаются посредством постоянного поддержания на необходимом уровне таких свойств информации как:

1.1.1. конфиденциальность и защищенность от уничтожения для ИСПДн, обрабатывающей персональные данные потребителей;

1.1.2. конфиденциальность для ИСПДн, обрабатывающей персональные данные сотрудников.

1.15. Работы по информационной безопасности (ИБ) являются неотъемлемой частью работ по созданию и эксплуатации информационных систем персональных данных и должны реализовываться в виде системы защиты персональных данных (СЗПДн).

1.16. Система защиты персональных данных включает:

1.1.3. мероприятия по управлению информационной безопасностью ПДн;

1.1.4. мероприятия по организации обеспечения информационной безопасности ПДн;

1.1.5. мероприятия по техническому обеспечению безопасности ПДн при их обработке в ИСПДн, в том числе:

1.1.5.1. мероприятия по размещению, специальному оборудованию, охране и организации режима допуска в помещения, где ведется обработка ПДн;

1.1.5.2. мероприятия по защите ПДн от несанкционированного доступа, от вредоносных программ (программно-математических воздействий);

1.1.5.3. мероприятия по закрытию технических каналов утечки ПДн при их обработке в ИСПДн;

1.1.5.4. мероприятия по защите ПДн в каналах связи с использованием шифровальных (криптографических) средств.

1.1.6. Мероприятия по защите персональных данных проводятся в отношении следующих ресурсов ИСПДн:

1.1.6.1. технических и программных средств, участвующих в технологическом процессе обработки защищаемой информации;

1.1.6.2. используемых в ИСПДн информационных технологий;

1.1.6.3. собственно персональных данных;

1.1.6.4. помещений, в которых установлены технические и программные средства обработки ПДн.

1.17. При создании и эксплуатации системы защиты персональных данных ООО «ЕРИЦ» следует придерживаться следующих принципов обеспечения информационной безопасности:

1.1.7. законности, соблюдения баланса интересов и законных прав субъектов персональных данных и Организации;

1.1.8. систематичности проведения работ, т.е. планирование, реализация и совершенствование согласованных по целям, месту и времени мер информационной безопасности;

1.1.9. комплексного подхода к решению вопросов ИБ по всем направлениям и во всех подразделениях Организации;

1.1.10. своевременности обнаружения угроз ИБ, потенциально способных повлиять на защищенность ПДн;

1.1.11. адекватности защитных мер, моделям угроз, а также сопоставимости затрат на их осуществление и объема возможных потерь от реализации угроз;

1.1.12. эффективности реализации принятых защитных мер;

1.1.13. персонификации и адекватному разделению ролей и ответственности должностных лиц за принимаемые решения;

1.1.14. баланса с одной стороны мер по контролю соблюдения персоналом установленного порядка обработки ПДн и требований по ИБ, а с другой стороны мер доверия и наделения полномочиями, необходимыми для выполнения работниками своих функциональных обязанностей;

1.1.15. наблюдаемости и оцениваемости процессов и процедур информационной безопасности, т.е. чтобы результат применения любых защитных мер был явно наблюдаем (прозрачен) и мог быть оценен администратором информационной безопасности.

2. Организационные меры по защите персональных данных. Распределение обязанностей должностных лиц.

2.1.1. Ответственность за организацию работ по защите персональных данных в Организации, в соответствии с действующим законодательством, возложена на директора ООО «ЕРИЦ», который распределяет функции и роли персонала при обработке персональных данных, организует порядок доступа к ПДн и ресурсам ИСПДн. При необходимости генеральный директор ООО «ЕРИЦ» может делегировать часть своих обязанностей другим работникам, обладающим необходимыми должностными полномочиями (например, заместителю директора, начальникам структурных подразделений, администратору информационной безопасности).

2.1.2. Организация работ по планированию мероприятий по обеспечению безопасности персональных данных, координация взаимодействия структурных подразделений по защите персональных данных, санкционирование доступа к ПДн и ресурсам ИСПДн работников структурных подразделений, согласование информации, передаваемой гражданам и сторонним организациям по их запросам, и определение порядка ее предоставления, определение порядка действий работников в нештатной ситуации, контроль своевременности и качества выполнения работниками своих обязанностей по защите персональных, назначение разбирательств по фактам нарушений требований информационной безопасности возлагается на рабочую группу по вопросам защиты информации (далее – Рабочая группа или РГ), созданную приказом генерального директора.

2.1.3. Осуществление мероприятий по обеспечению безопасности персональных данных, администрирование и техническое обслуживание ИСПДн и средств защиты ПДн, обучение персонала правилам эксплуатации программных и технических средств ИСПДн и средств защиты информации, проведение соответствующих инструктажей работников, учет СЗИ и носителей ПДн, разработка проектов внутренних организационно-распорядительных документов по вопросам информационной безопасности, осуществление контроля правильности и полноты выполнения предусмотренных мер

по защите информации, проведение по указанию руководства Организации разбирательств по фактам нарушения (инцидентам) информационной безопасности, разработка планов реализации мероприятий по обеспечению безопасности ПДн и контроля их эффективности, разработка предложений и мероприятий по совершенствованию СЗПДн возлагается на администратора информационной безопасности. Работники, осуществляющие роли системного администратора (администратора информационной безопасности) назначаются приказом генерального директора.

2.1.4. На руководителей подразделений возлагается ответственность за выполнение подчиненными работниками требований руководящих и организационно-распорядительных документов по информационной безопасности, оформление заявок на доступ подчиненных работников к ресурсам ИСПДн, организация обучения подчиненных работников правилам обработки ПДн с использованием прикладного программного обеспечения.

2.1.5. Пользователи, допущенные к обработке персональных данных, несут персональную ответственность за соблюдение предписанных мер по защите информации.

2.1.6. Срочность и важность выполняемых сотрудниками Организации работ не должны являться основанием для нарушения требований по защите информации.

2.1.7. Пользователь не вправе изменять программную и аппаратную конфигурацию автоматизированного рабочего места (далее – АРМ), а также совершать действия, направленные на обход или противодействие применяемым, в том числе в отношении него, средствам обеспечения информационной безопасности.

2.1.8. Если пользователь допустил нарушения, которые привели к нарушению конфиденциальности и целостности защищаемой информации или иных требований по информационной безопасности, а также перебоям в работе ИСПДн, то по факту нарушения директор ООО «ЕРИЦ» может назначать служебное разбирательство.

2.1.9. За нарушение требований по защите информации виновные лица могут привлекаться к дисциплинарной, административной, гражданской и уголовной ответственности в соответствии с законодательством Российской Федерации.

3. Порядок обращения с носителями персональных данных и их учет.

3.1. Все носители ПДн (съемные и несъемные накопители на жестких и гибких МД, магнитооптические диски, флэш-накопители и т.п.) подлежат учету в специально предназначенном для этого журнале. Кроме того, учету подлежат средства идентификации и аутентификации, ключевые носители и др. средства (далее – идентификаторы), используемые для доступа к ресурсам ИСПДн и СЗИ, а также в защищаемые помещения.

3.2. Ответственным за учет носителей ПДн и идентификаторов (далее – носителей ПДн) и их выдачу пользователям ИСПДн является администратор информационной безопасности.

3.3. На учтенных носителях конфиденциальной информации проставляются следующие реквизиты:

3.3.1.учетный номер;

3.3.2.назначение носителя (может соответствовать названию структурного подразделения, задаче обработки персональных данных или др. классификации);

3.3.3. сокращенное название организации – ООО «ЕРИЦ»;

3.3.4. дата постановки на учет;

3.3.5. роспись работника, поставившего носитель на учет.

3.3. На флеш-накопители и другие носители маленького размера разрешается наносить только учетный номер.

3.4. Выдача носителей ПДн пользователям осуществляется под роспись в соответствующем журнале.

3.5. Носители ПДн могут быть сняты с учета в случае служебной необходимости или порчи носителя. В этом случае производится уничтожение конфиденциальных сведений, хранящихся на носителе, а в случае невозможности уничтожения информации с носителя в связи с его порчей производится уничтожение самих носителей.

3.6. Для уничтожения ПДн с носителей в Организации создается комиссия, в состав которой включается администратор информационной безопасности. По результатам уничтожения информации составляется соответствующий акт, который утверждается директором ООО «ЕРИЦ». После уничтожения информации носитель может быть снят с учета, о чем делается соответствующая отметка в Журнале учета.

3.7. Хранение носителей ПДн разрешается у работников, которым они выданы для выполнения своих должностных обязанностей, или у администратора информационной безопасности. Хранение носителей ПДн в нерабочее время осуществляется в сейфах, запираемых шкафах или ящиках. Хранение ключевых носителей систем криптографической защиты осуществляется в приспособленных для опечатывания сейфах, запираемых шкафах или ящиках.

3.8. В ООО «ЕРИЦ» проводится ежегодная проверка наличия носителей ПДн. Для этого приказом по Организации создается комиссия, в состав которой в обязательном порядке включается администратор информационной безопасности. Результаты проверки наличия носителей ПДн, порядка их использования и хранения оформляются актом и доводятся до руководства ООО «ЕРИЦ».

3.9. В случае неисправности носителя персональных данных или если надобность в его использовании отпала, то данный носитель подлежит сдаче администратору информационной безопасности.
3.10. В случае утери носителя ПДн или не сдачи его при увольнении работник, которому данный носитель был выдан для эксплуатации, несет дисциплинарную ответственность. По факту утери назначается служебное разбирательство, которое проводит администратор информационной безопасности или созданная распоряжением по Организации комиссия.

4. Планирование и контроль выполнения требований по защите персональных данных.

4.1. С целью поддержания СЗПДн в эффективном состоянии в ООО «ЕРИЦ» осуществляется планирование деятельности по защите ПДн и контроль выполнения требований по защите информации.
4.2. План работ по защите ПДн разрабатывается ежегодно администратором информационной безопасности, согласовывается с руководителями структурных подразделений, привлекаемых к работам по защите ПДн, и утверждается генеральным директором Организации. Отдельным разделом в плане предусматривается проведение контрольных мероприятий. План работ по защите ПДн в части финансирования расходов на поддержание эксплуатации средств защиты информации, модернизацию системы защиты, обучение персонала и другим вопросам обеспечения должен быть согласован с финансовым планом (бюджетом) Организации.
4.3. В соответствии с требованиями руководящих документов по ИБ администратором информационной безопасности, осуществляет постоянный мониторинг состояния ИСПДн и АРМ пользователей, настроек средств защиты от НСД, журналов аудита событий в ИСПДн, а также контроль выполнения пользователями ИСПДн требований по защите ПДн и использования ими защищаемых ресурсов.
4.4. Плановый контроль соблюдения требований по защите ПДн в ИСПДн, правил применения средств защиты информации, а также выявление угроз безопасности ПДн проводится ежемесячно согласно утвержденному графику. Внеплановый контроль проводится при выявлении фактов нарушения требований по защите информации.
4.5. Проверка наличия и правильности учета носителей ПДн проводится не реже 1 раза в год.
4.6. Кроме того, надзорными органами (Роскомсвязьнадзор, ФСТЭК РФ, ФСБ РФ, лицензиаты ФСТЭК) может проводиться внешний аудит (контроль) выполнения требований по информационной безопасности.
4.7. При выявлении фактов нарушения требований по информационной безопасности директор Организации назначает служебное разбирательство, которое проводит администратор информационной безопасности с привлечением необходимых специалистов или специально созданная комиссия.
4.8. На основе анализа результатов контроля определяются практические мероприятия по устранению выявленных угроз. Результаты контроля и предложения по совершенствованию системы управления ИБ и механизмов защиты ПДн по мере необходимости докладываются директору.
4.9. С целью реализации порядка допуска пользователей к ресурсам ИСПДн, поддержания их ответственности за выполнение требований по ИБ на необходимом уровне, информировании работников об изменениях в порядке организации работ по защите ПДн в ООО «ЕРИЦ» осуществляется инструктаж пользователей по вопросам информационной безопасности с проставлением росписи инструктируемого работника в соответствующем журнале учета инструктажей. Инструктаж может быть:
4.9.1. вводным – проводится при первоначальном предоставлении пользователю доступа к ресурсам ИСПДн;
4.9.2.периодическим – проводится не реже 1 раза в год, а также при необходимости доведения до пользователей новых требований по информационной безопасности, вводе в действие организационно-распорядительных документов по защите ПДн;
4.9.3. внеплановый – проводится по указанию генерального директора ООО «ЕРИЦ» с нарушителями порядка обработки ПДн и требований по информационной безопасности

5. Обеспечение защиты программных и технических средств ИСПДн на стадиях жизненного цикла.

5.1. Информационная безопасность ИСПДн должна обеспечиваться на всех стадиях жизненного цикла (ЖЦ) информационной системы с учетом всех сторон, вовлеченных в процессы ЖЦ (разработчиков, заказчиков, поставщиков продуктов и услуг, эксплуатирующих и надзорных служб).
5.2. Технические задания (требования), проекты, постановки задач, планы работ, договоры, техническая документация и т.д., в части требований по обеспечению ИБ, на этапах проектирования (доработки) ИСПДн и ее отдельных элементов, испытаний (тестирования) и ввода в эксплуатацию должны согласовываться с администратором информационной безопасности.

5.3. Ввод в действие, эксплуатация, снятие с эксплуатации программного обеспечения и технических средств ИСПДн, в части вопросов обеспечения ИБ, должны осуществляться при участии администратора информационной безопасности с привлечением специализированных организаций.
5.4. Привлекаемые для разработки и/или проведения работ в области информатизации и защиты информации в ИСПДн на договорной основе специализированные организации должны иметь соответствующие документы, подтверждающие их квалификацию в соответствии с законодательством РФ (лицензии на соответствующий вид деятельности, сертификаты, свидетельства и пр.).
5.5. При приобретении готовых элементов ИСПДн (ПО, телекоммуникационного оборудования, средств вычислительной техники, средств защиты информации и пр.) разработчиком (поставщиком) должна быть предоставлена документация, содержащая, в том числе, описание защитных мер, предпринятых разработчиком в отношении угроз, характерных для стадий жизненного цикла, а также относительно безопасности разработки, безопасности поставки и эксплуатации, поддержки жизненного цикла. Данная документация может быть представлена в виде декларации о соответствии или быть результатом оценки соответствия изделия, проведенной в рамках соответствующей системы оценки (например, сертификации по требованиям безопасности информации).
5.6. При поставке элементов ИСПДн должны быть решены вопросы по сопровождению и обслуживанию поставляемых изделий на весь срок их службы. С этой целью может проводиться обучение (подготовка, переподготовка) персонала, приобретение полного комплекта рабочей конструкторской документации на изделие, приобретение лицензий, заключение договоров со специализированными организациями на техническое обслуживание и другие экономически обоснованные и/или законодательно установленные меры.
5.7. Перед сдачей в эксплуатацию элементы ИСПДн должны пройти процедуру тестирования. В проведении тестирования должен обязательно участвовать администратор информационной безопасности.
5.8. При проведении тестирования, а также в ходе проведения обслуживания или ремонтных работ, должна быть исключена возможность доступа специалистов сторонних организаций (разработчиков, программистов, обслуживающего персонала и пр.) к информации ограниченного доступа, защищаемым персональным данным. Если же в силу объективных причин этого нельзя добиться, то специалисты сторонних организаций должны подписывать письменные обязательства о неразглашении защищаемых сведений.
5.9. После успешного тестирования:
5.9.1. ПО заносится в перечень программного обеспечения Организации (Перечень-ПДн-3), носители с дистрибутивами передаются на хранение администратору информационной безопасности. С целью обеспечения восстановления ИСПДн после сбоев создаются резервные копии дистрибутивов ПО, которые хранятся отдельно от оригиналов;
5.9.2. носители информации, которые будут участвовать в обработке ПДн, маркируются и ставятся на учет в соответствии с настоящим Положением;
5.9.3.корпуса технических средств и оборудования, которые будут участвовать в обработке персональных данных, опечатываются.
5.10. С момента ввода в эксплуатацию на вышеуказанных ресурсах ИСПДн ответственному за информационную безопасность сотруднику должны предоставляться соответствующие права доступа в ИСПДн для исполнения им своих функциональных обязанностей.
5.11. На стадии снятия элементов ИСПДн с эксплуатации или направлении вычислительной техники в ремонт должно быть обеспечено гарантированное удаление (уничтожение) из постоянной памяти СВТ и/или со съемных и несъемных носителей персональных данных и информации, несанкционированное использование которой может нанести какой-либо ущерб субъекту персональных данных или Организации. Порядок удаления информации с носителей определен в разделе 3.3 настоящего Положения.
5.12. Требования по обеспечению ИБ должны включаться во все договора (контракты, соглашения и т.д.) на проведение работ и/или оказание услуг на всех стадиях ЖЦ ИСПДн Организации.

6. Организация работ по использованию ресурсов сетей общего пользования.

6.1. Предоставление работнику Организации доступа к ресурсам сети Интернет, электронной почте или другим ресурсам общего пользования (далее – Интернет) осуществляется только в служебных целях. Использование сети Интернет в других целях категорически **запрещено**.
6.2. Порядок доступа работников к ресурсам Интернета аналогичен установленному для доступа к защищаемым ресурсам в «Положении о разрешительной системе доступа» (Положение-ПДн-4). Все работники, имеющие доступ к Интернету, должны пройти инструктаж по правилам обеспечения информационной безопасности, который впоследствии на плановой основе проводится ежегодно администратором информационной безопасности.

6.3. Системному администратору, а также администратору информационной безопасности **категорически запрещается** использовать свои действующие в ИСПДн администраторские логины и пароли для работы в Интернет (включая отдельные АРМ, мобильные компьютеры и пр.).
6.4. При наличии технических возможностей рекомендуется организовывать подключение к сетям общего пользования с отдельной ПЭВМ, не входящей в состав ИСПДн и не подключенной к ЛВС Организации.
6.5. Все данные, полученные из сети Интернет, должны проверятся пользователями на отсутствие вирусов с использованием антивирусных программ. В случае обнаружения «вируса» или другого вредоносного кода, а также при необычном поведении компьютера или программы работник должен немедленно информировать об этом специалистов ответственных за обеспечение безопасности персональных данных.
6.6.При работе в сети Интернет (использовании электронной почты) **запрещается**:
6.6.1. публиковать, загружать и распространять программы для осуществления несанкционированного доступа к защищаемым ресурсам, а также серийные номера к коммерческим программным продуктам и программы для их генерации, логины, пароли и прочие средства для получения несанкционированного доступа к защищаемым ресурсам и платным ресурсам в Интернете, а также размещать ссылки на вышеуказанную информацию;
6.6.2. принимать участие в онлайн общении, конференциях, форумах, если это не предусмотрено служебными обязанностями;
6.6.3. запрашивать и получать из Интернета программное обеспечение, кроме случаев, связанных со служебной необходимостью и согласованных с администратором информационной безопасности. Внедрение и эксплуатация полученного таким образом ПО разрешается только после выполнения всех необходимых процедур, предусмотренных разделом 3.5 настоящего Положения.
6.7. Работники несут дисциплинарную ответственность за нецелевое использование служебного времени и телекоммуникационных ресурсов при работе в Интернете.
6.8. Работник, заметивший какие-либо нарушения обеспечения безопасности, должен сразу сообщить об этом нарушении администратору информационной безопасности или руководителю структурного подразделения.
6.9. Проведение анализа электронной почты пользователей или других ресурсов общего пользования на предмет отсутствия в них защищаемой информации может быть осуществлено администратором информационной безопасности в плановом порядке или по решению генерального директора Организации.

7. Прочие организационные меры по защите персональных данных

7.1. Кроме приведенных выше в ООО «ЕРИЦ» осуществляются следующие организационные меры:
7.1.1. оформляется перечень персональных данных, подлежащих защите в Организации (Перечень-ПДн-1);
7.1.2. классифицируются информационных систем персональных данных в целях реализации дифференциального подхода к обеспечению безопасности ПДн и оптимизации расходов на создание и эксплуатацию системы защиты ПДн;
7.1.3. разрабатывается система защиты ПДн, обеспечивающая нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационных систем;
7.1.4. система защиты ПДн описывается во внутренних организационно-распорядительных документах;
7.1.5. осуществляется учет применяемых средств защиты информации, эксплуатационной и технической документации к ним;
7.1.6. хранение документации и носителей осуществляется в специально предназначенных для этого местах (сейфах, шкафах и пр.);
7.1.7. проводится обучение лиц, эксплуатирующих применяемые в ИСПДн средства защиты информации, правилам работы с ними;
7.1.8. используется лицензионное ПО.

8. Технические меры по обеспечению безопасности ПДн при их обработке в ИСПДн

8.1. Основные технические меры по защите персональных данных:
8.1.1.управление доступом пользователей к ресурсам ИСПДн с использованием сертифицированных по требованиям безопасности информации средств защиты от несанкционированного доступа;
8.1.2. выделение рабочих станций, обрабатывающих ПДн, в обособленный сегмент локальной вычислительной сети с использованием межсетевого экрана;
8.1.3. использование для защиты персональных данных, передаваемых по открытым каналам связи, сертифицированных по требованиям безопасности информации, средств криптографической защиты информации;

8.1.4. использование систем обнаружения вторжений для выявления внешних сетевых угроз безопасности ПДн;
8.1.5. применение средств анализа защищенности для выявления уязвимостей ИСПДн;
8.1.6. контроль целостности программного обеспечения и состава аппаратных средств защиты ИСПДн;
8.1.7. использование антивирусного программного обеспечения с целью предотвращения внедрения программ-вирусов и программных закладок;
8.1.8. архивирование баз данных и других информационных ресурсов, содержащих защищаемые ПДн, с целью восстановления информации после сбоев в функционировании технических и программных средств или инцидентов информационной безопасности;
8.1.9. резервирование критически важных технических элементов информационной инфраструктуры (серверов, телекоммуникационного оборудования, ключевых носителей СКЗИ и т.п.) с целью обеспечения непрерывности деятельности Организации;
8.1.10. периодическое тестирование ПО ИСПДн и носителей информации с целью предотвращения сбоев при работе с ними, при необходимости дублирование дистрибутивов ПО: общесистемного, прикладного и СЗИ;
8.1.11. затруднение просмотра данных, выводимых на экран монитора, со стороны окна и мест размещения посетителей;
8.1.12. использование технических средств охраны и сигнализации в помещениях;
8.1.13. сдача в нерабочее время помещений, в которых находятся технические средства ИСПДн, под охрану.
8.2. Для защиты ПДн должны применяться только сертифицированные по требованиям безопасности информации средства защиты. Порядок их применения, установка и ввод в эксплуатацию осуществляется в соответствии с эксплуатационной и технической документацией и требованиями к конкретной ИСПДн, установленными нормативно-методическими документами ФСТЭК и ФСБ России.
8.3.Все программно-аппаратные СЗИ должны иметь независимые журналы регистрации событий, и, по возможности, средства удаленного администрирования.
8.4.Программные и программно-аппаратные комплексы защиты от НСД обеспечивают:
8.4.1. предоставление доступа к ПЭВМ путем идентификации пользователей и их аутентификации по индивидуальному паролю;
8.4.2.блокировку загрузки с отчуждаемых носителей (FDD, CD ROM, ZIP Drive и др.) и прерывания контрольных процедур с клавиатуры;
8.4.3. защиту от несанкционированных модификаций программ и данных;
8.4.4. создание и поддержку изолированной программной среды, возможность реализации функционально замкнутых информационных систем на базе ПЭВМ;
8.4.5. контроль целостности системных областей жестких дисков, программ и данных, а также конфигурации технических средств ПЭВМ;
8.4.6. разграничение доступа пользователей к ресурсам ИСПДн в соответствии с уровнем их полномочий;
8.4.7. управление потоками информации на основе принципов дискреционного доступа;
8.4.8. регистрацию в электронном журнале контролируемых событий, в том числе несанкционированных действий пользователей. Доступ к журналу обеспечивается только Администратором безопасности ИТ.
8.5.Межсетевые экраны должны обеспечивать разделение и контроль информационных потоков как между обособленным сегментом локальной вычислительной сети – ИСПДн, в которой обрабатываются персональные данные, и общедоступными ресурсами ЛВС, так и внутри защищаемого сегмента между ИСПДн (АРМ) различного класса защищенности. При этом должны выполняться следующие требования:
8.5.1.пользователям ИСПДн может быть предоставлен доступ к общедоступным ресурсам ЛВС в соответствии со служебной необходимостью;
8.5.2. пользователи ЛВС, не допущенные установленным порядком к автоматизированной обработке ПДн, не должны иметь доступа к ресурсам ИСПДн;
8.5.3. легальным пользователям ИСПДн должно быть запрещено в любом виде распространение (копирование) защищаемых ПДн из защищаемого сегмента ЛВС в общедоступный;
8.5.4. межсетевые экраны должны соответствовать требованиям не ниже 3 класса защищенности, установленным «Руководящим документом. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации», утвержденном Гостехкомиссией России 25.07.97 г.
8.6. На всех АРМ, включенных в ИСПДн, для защиты компьютеров и информации от поражения компьютерными вирусами в обязательном порядке устанавливается антивирусная программа, которая запускается автоматически при включении компьютера и проверяет все запускаемые программы и открываемые файлы на предмет наличия вируса. Сканирование локальных дисков АРМ и обновление антивирусных баз программы осуществляется автоматически.

8.7. В случае обнаружения вируса пользователь должен незамедлительно сообщить об этом администратору безопасности ИТ и действовать согласно его указаниям.
8.8. Для обеспечения защиты персональных данных, передаваемых по открытым каналам связи, используются средства криптографической защиты информации (СКЗИ).
8.9. Хранение документации, дистрибутивов программного обеспечения и резервных ключевых носителей СКЗИ организуется у администратора информационной безопасности в специально выделенном для этих целей сейфе (ящике, хранилище) в условиях, исключающих бесконтрольный доступ к ним посторонних лиц, а также их непреднамеренное уничтожение. При этом должно быть обеспечено раздельное хранение действующих и резервных ключевых документов и носителей. Аппаратные средства, на которых осуществляется штатное функционирование криптографических средств, а также помещения, в которых они установлены, должны быть оборудованы средствами контроля их вскрытия (опечатаны, опломбированы). Место опечатывания (опломбирования) криптографических и аппаратных средств должно быть доступно для визуального контроля.
8.10. С целью выполнения требований ФСБ России по эксплуатации СКЗИ на рабочих местах распоряжением по Организации назначаются ответственные пользователи СКЗИ. Ответственные пользователи несут персональную ответственность за использование СКЗИ по назначению; за соблюдение правил хранения носителей ключевой информации, исключающих их компрометацию, копирование или утрату; за архивирование обрабатываемых документов в электронной форме.
8.11. Под компрометацией ключа понимается утрата доверия к тому, что используемые ключи обеспечивают безопасность информации. К событиям, связанным с компрометацией ключей относятся, включая, но, не ограничиваясь, следующие:.
8.11.1.Потеря ключевых носителей
8.11.2. Потеря ключевых носителей с их последующим обнаружением.
8.11.3. Увольнение работников, имевших доступ к ключевой информации.
8.11.4. Нарушение правил хранения и уничтожения (после окончания срока действия) закрытого ключа.
8.11.5. Возникновение подозрений на утечку информации или ее искажение в системе конфиденциальной связи.
8.11.6. Нарушение печати на сейфе с ключевыми носителями.
8.11.7. Случаи, когда нельзя достоверно установить, что произошло с ключевыми носителями (в том числе случаи, когда ключевой носитель вышел из строя и доказательно не опровергнута возможность того, что, данный факт произошел в результате несанкционированных действий злоумышленника).
8.12. Различают два вида компрометации закрытого ключа: явную и неявную. Первые четыре события должны трактоваться как явная компрометация ключей. Три следующих события требуют специального рассмотрения в каждом конкретном случае
8.13. Система обнаружения вторжений предназначена для анализа всего сетевого трафика, автоматического выявления воздействий на защищаемую ИСПДн, которые на основании сигнатурного анализа могут быть классифицированы как сетевые компьютерные атаки.
8.14. Настройка ИСПДн, обрабатывающих персональные данные потребителей и сотрудников, программно-аппаратных средств защиты должна осуществляться таким образом, чтобы обеспечить выполнение требований, предъявляемых к ИСПДн в соответствии с установленным в акте классификации классом. Данные требования изложены в нормативно-методическом документе ФСТЭК России «Положение о методах и способах защиты информации в информационных системах персональных данных».
8.15. Для исключения визуального просмотра выводимой на экран мониторов защищаемой информации окна помещений, в которых установлены технические средства ИСПДн, оборудуются жалюзи (шторами), мониторы на рабочих местах размещаются таким образом, чтобы исключить непосредственное наблюдение выводимой на них информации лицами, не допущенными к обработке ПДн.
8.16. Для пользователей, эксплуатирующих средства защиты информации на своих АРМ, разрабатываются инструкции, определяющие правила их использования, действия пользователя при возникновении нештатных ситуаций
8.17. Обработка ПДн с использованием технических средств разрешается только после выполнения всего комплекса мероприятий по защите информации согласно настоящему Положению.