Приложение № 3
к Приказу № _____
от «____»_____20___г.

Положение

по обеспечению безопасности персональных данных в ГУП Республики Крым «Крымэкоресурсы»

СОДЕРЖАНИЕ

1. ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ 4
2. СПИСОК ТЕРМИНОВ 5
3. НАЗНАЧЕНИЕ ДОКУМЕНТА..... 11
4. ОБЛАСТЬ ДЕЙСТВИЯ 12
5. ОБЩИЕ ПОЛОЖЕНИЯ 13
6. ОРГАНИЗАЦИОННАЯ СТРУКТУРА СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ..... 19
7. ПОРЯДОК ОРГАНИЗАЦИИ И ПРОВЕДЕНИЯ РАБОТ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ..... 25
8. КАТЕГОРИРОВАНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ И ОПРЕДЕЛЕНИЕ УРОВНЯ ЗАЩИЩЕННОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННОЙ СИСТЕМЕ ПЕРСОНАЛЬНЫХ ДАННЫХ……..… ….29
9. ОЦЕНКА ВОЗМОЖНОСТИ ОПТИМИЗАЦИИ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ……32
10. МОДЕЛЬ УГРОЗ И НАРУШИТЕЛЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ…… ……...34
11. ОБУЧЕНИЕ ПЕРСОНАЛА, УЧАСТВУЮЩЕГО В ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ…… ….36
12. ОРГАНИЗАЦИЯ РАБОТЫ С МАШИННЫМИ НОСИТЕЛЯМИ ПЕРСОНАЛЬНЫХ ДАННЫХ…… ……38
13. КОНТРОЛЬ ИЗМЕНЕНИЙ В СОСТАВЕ И СТРУКТУРЕ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ…….. 39
14. ЗАЩИТА ОТ НЕСАНКЦИОНИРОВАННОГО ФИЗИЧЕСКОГО ДОСТУПА К ЭЛЕМЕНТАМ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ…….. 40
15. РЕЗЕРВИРОВАНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ..... ……42

16. КОНТРОЛЬ ЗА ОБЕСПЕЧЕНИЕМ НЕОБХОДИМОГО УРОВНЯ ЗАЩИЩЕННОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ……...…….. 43
17. РЕАГИРОВАНИЕ НА НЕШТАТНЫЕ СИТУАЦИИ…… .45
18. ПЕРЕЧЕНЬ НОРМАТИВНЫХ ПРАВОВЫХ АКТОВ, РУКОВОДЯЩИХ И МЕТОДИЧЕСКИХ ДОКУМЕНТОВ, ИСПОЛЬЗУЕМЫХ ПРИ ПРОВЕДЕНИИ МЕРОПРИЯТИЙ ПО ОРГАНИЗАЦИИ ОБРАБОТКИ И ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ...…..... ……..46
ПРИЛОЖЕНИЕ 1. ЛИСТ ОЗНАКОМЛЕНИЯ С ПОЛОЖЕНИЕМ…… …….49
ПРИЛОЖЕНИЕ 2. ФОРМА АКТА ОПРЕДЕЛЕНИЯ УРОВНЯ ЗАЩИЩЕННОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННОЙ СИСТЕМЕ ПЕРСОНАЛЬНЫХ ДАННЫХ……... ……50

1. ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

АС – автоматизированная система

ВТСС – вспомогательные технические средства и системы

ИБ – информационная безопасность

ИС – информационная система

ИСПДн – информационная система персональных данных

КЗ – контролируемая зона

ЛВС – локальная вычислительная сеть

МЭ – межсетевой экран

НСД – несанкционированный доступ

ОС – операционная система

ПДн – персональные данные

ПЭМИН – побочные электромагнитные излучения и наводки

СЗИ – средства защиты информации

СЗПДн – система (подсистема) защиты персональных данных

СКЗИ – средство криптографической защиты информации

ТКУИ – технические каналы утечки информации

УБПДн – угрозы безопасности персональных данных

2. СПИСОК ТЕРМИНОВ

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

Блокирование персональных данных – временное прекращение сбора, систематизации, накопления, использования, распространения, персональных данных, в том числе их передачи.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

Вспомогательные технические средства и системы – технические средства и системы, не предназначенные для передачи, обработки и хранения персональных данных, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки персональных данных или в помещениях, в которых установлены информационные системы персональных данных.

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Идентификация ИСПДн – выделение в информационно-телекоммуникационной инфраструктуре учреждения областей (отдельных рабочих станций, узлов и сегментов сети), в которых осуществляется обработка персональных данных, определение границ контролируемых зон для

выделенных областей, присвоение наименований отдельным информационным системам персональных данных в составе информационно-телекоммуникационной инфраструктуры учреждения.

Информационная система персональных данных – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

Использование персональных данных – действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

Контролируемая зона – пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

Межсетевой экран – локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

Модель угроз – физическое, математическое, описательное представление свойств или характеристик угроз безопасности информации.

Нарушитель безопасности персональных данных – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах 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.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

Носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Обезличивание персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

Обработка персональных данных – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Общедоступные персональные данные – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

Оператор (персональных данных) – государственный орган, муниципальный орган, юридическое или физическое лицо, организующее и (или)

осуществляющее обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

Персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Побочные электромагнитные излучения и наводки – электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

Пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

Раскрытие персональных данных – умышленное или случайное нарушение конфиденциальности персональных данных.

Распространение персональных данных – действия, направленные на передачу персональных данных определенному 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.

Специальные категории персональных данных – персональные данные, касающиеся расовой и национальной принадлежности, политических

взглядов, религиозных или философских убеждений, состояния здоровья и интимной жизни субъекта персональных данных.

Специальные информационные системы – информационные системы, в которых вне зависимости от необходимости обеспечения конфиденциальности персональных данных требуется обеспечить хотя бы одну из характеристик безопасности персональных данных, отличную от конфиденциальности (защищенность от уничтожения, изменения, блокирования, а также иных несанкционированных действий).

Субъект доступа (субъект) – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Субъект персональных данных – физическое лицо, к которому относятся определенные персональные данные либо которое может быть определено на основании определенных персональных данных.

Технические средства информационной системы персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

Технический канал утечки информации – совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

Типовые информационные системы – информационные системы, в которых требуется обеспечение только конфиденциальности персональных данных.

Угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

Утечка (защищаемой) информации по техническим каналам – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

Уничтожение персональных данных - действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

Уполномоченное оператором лицо - лицо, которому на основании договора оператор поручает обработку персональных данных.

Целостность информации - способность средства вычислительной техники или информационной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

3. НАЗНАЧЕНИЕ ДОКУМЕНТА

Настоящий документ определяет порядок организации и проведения работ по обеспечению безопасности ПДн в ГУП Республики Крым «Крымэкоресурсы» (далее – Предприятие) и содержит общие принципы защиты ПДн.

Данный документ направлен на достижение следующих целей:

– выполнение требований нормативных документов Российской Федерации в области обработки и обеспечения безопасности ПДн;

– защита прав и свобод граждан Российской Федерации при обработке их ПДн на Предприятии;

– защита ПДн, обрабатываемых в ИСПДн Предприятия, от НСД и от других несанкционированных действий.

4. ОБЛАСТЬ ДЕЙСТВИЯ

Требования настоящего Положения распространяются на все подразделения Предприятия, которые участвуют в обработке ПДн, либо в организации обработки ПДн, а также на подразделения, осуществляющие сопровождение, обслуживание и обеспечение функционирования ИСПДн.

Настоящий документ обязаны знать и использовать в работе все сотрудники Предприятия, допущенные к обработке ПДн.

Ознакомление сотрудников с требованиями настоящего Положения проводит ответственный за организацию обработки ПДн под роспись в листе ознакомления (приложение № 1).

5. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящее Положение устанавливает требования по защите ПДн, принципы обработки ПДн, направленные на защиту интересов Предприятия в области ее непосредственной деятельности.

Настоящее Положение разработано в соответствии со следующими нормативными актами:

- Федеральным законом Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
- Федеральным законом Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
- Постановлением Правительства Российской Федерации от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
- Приказом Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
- Приказом ФСБ России от 10 июля 2014 г. № 378 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

- Иными действующими нормативными правовыми актами в сфере организации обработки и обеспечения безопасности персональных данных.

Настоящее Положение является методологической основой для:

- формирования и проведения единой политики в области обеспечения безопасности ПДн;
- принятия управленческих решений и разработки практических мер по воплощению политики безопасности ПДн и выработки комплекса согласованных мер нормативно-правового, технического и организационно-технического характера, направленных на выявление, отражение и уменьшение УБПДн;
- координации деятельности при проведении работ по созданию, развитию и эксплуатации ИСПДн с соблюдением требований по обеспечению безопасности ПДн;
- разработки предложений по совершенствованию правового, нормативного, методического, технического и организационного обеспечения безопасности ПДн.

Принципы и требования по обеспечению безопасности ПДн распространяются:

- на все возможные формы существования информации, такие как:
  - физические поля (электрические, акустические, электромагнитные, оптические и т.п.);
  - носители на бумажной, магнитной, оптической, электронной и иной основе.
- на все возможные форматы представления ПДн, такие как:
  - документы;
  - голос;
  - изображения;
  - файлы;

- почтовые сообщения;
- базы данных;
- записи базы данных;
- другие информационные массивы.

Предотвращение несанкционированного и нелегитимного доступа к ИСПДн, технологиям и информационным ресурсам результатом которого может стать уничтожение, модификация, искажение, копирование, распространение, блокирование ПДн требует применения комплекса правовых, организационных, организационно-технических мер защиты информации с использованием сертифицированных СЗИ.

Настоящее Положение определяет:

- роли, полномочия, ответственность за обеспечение безопасности ПДн подразделений Предприятия;
- порядок организации и проведения работ по обеспечению безопасности ПДн;
- мероприятия по обеспечению безопасности ПДн;
- требования по управлению процессом обеспечения безопасности ПДн;
- требования к составу и содержанию документов Предприятия, регламентирующих защиту и работу с ПДн.

Целью создания СЗПДн является исключение неправомерного или случайного доступа к ПДн, уничтожения, изменения, блокирования, копирования, распространения ПДн, а также иных неправомерных действий.

В общем случае можно выделить следующие основные цели защиты ПДн, это обеспечение:

- конфиденциальности ПДн;
- целостности ПДн;
- доступности ПДн;
- неотказуемости;

- аутентичности.

Конкретный состав целей защиты ПДн зависит от конкретной ИСПДн и определяется по результатам разработки модели угроз и нарушителя (при необходимости) безопасности ПДн.

К основным задачам в области обеспечения безопасности ПДн относится:

- определение новых ИСПДн;
- инвентаризация и управление изменениями в составе и структуре ИСПДн;
- сбор согласий на обработку ПДн с субъектов персональных данных (при необходимости);
- формирование и актуализация перечней, обрабатываемых ПДн;
- контроль правомерности и целей обработки ПДн, состава обрабатываемых ПДн заявленным целям обработки;
- контроль сроков обработки ПДн;
- уничтожение ПДн;
- оптимизация информационных процессов обработки ПДн;
- управление взаимодействиями с внешними контрагентами по вопросам обработки ПДн;
- взаимодействие с субъектами персональных данных по вопросам обработки их ПДн;
- определение уровня защищенности ПДн при их обработке в ИСПДн;
- разработка (актуализация) документации на СЗПДн;
- выбор и внедрение необходимых и достаточных мер и средств защиты ПДн;
- эксплуатация СЗПДн в соответствии с документацией на нее;
- контроль уровня защищенности ПДн;
- обучение персонала по вопросам защиты ПДн;

- учет применяемых СЗИ, эксплуатационной и технической документации к ним;
- учет машинных носителей ПДн;
- учет лиц, допущенных к обработке ПДн;
- взаимодействие с регуляторными органами по вопросам защиты ПДн;
- актуализация и подача уведомлений в уполномоченный орган по защите прав субъектов персональных данных;
- реагирование на нештатные ситуации, расследование нештатных ситуаций, возникающих при обработке ПДн;
- аттестация ИСПДн на соответствие требованиям безопасности информации.

Обработка ПДн должна осуществляться в соответствии со следующими принципами:

- законности целей и способов обработки ПДн и добросовестности;
- соответствия целей обработки ПДн целям, заранее определенным и заявленным при сборе ПДн, а также полномочиям Предприятия;
- соответствия объема и характера обрабатываемых ПДн, способов обработки ПДн целям обработки ПДн;
- достоверности ПДн, их достаточности для целей обработки, недопустимости обработки ПДн, избыточных по отношению к целям, заявленным при сборе ПДн;
- недопустимости объединения созданных для несовместимых между собой целей баз данных ИСПДн.

В Обществе должен проводиться регулярный анализ соответствия процессов обработки ПДн указанным принципам. Данный анализ проводится в случае:

- создания новых ИСПДн;

- внесения изменений в технологические процессы, существующие в ИСПДн;
- изменения нормативной базы, затрагивающей принципы и (или) процессы обработки ПДн;
- проведения контрольных и проверочных мероприятий на предмет оценки соответствия процессов обработки ПДн заявленным принципам.

6. ОРГАНИЗАЦИОННАЯ СТРУКТУРА СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

СЗПДн является частью общей системы обеспечения информационной безопасности Общества.

Основу организационной структуры СЗПДн Общества составляют:

- руководство;
- ответственный за организацию обработки ПДн;
- ответственный за обеспечение безопасности ПДн;
- администратор безопасности информации;
- служба ЭВМ;
- структурные подразделения, участвующие в процессах обработки ПДн;
- сотрудники.

Руководство осуществляет следующие основные функции в области обеспечения безопасности ПДн:

- организует выполнение требований по организации обработки и защите ПДн на Предприятии;
- издает приказы по вопросам организации СЗПДн;
- утверждает Перечни обрабатываемых персональных данных;
- назначает ответственных за организацию обработки ПДн, за обеспечение безопасности ПДн, администраторов безопасности информации;
- утверждает Перечень сотрудников, допущенных к обработке ПДн;
- рассматривает и утверждает правовые и распорядительные документы, регламентирующие обработку и защиту ПДн на Предприятии;
- распределяет ответственность по вопросам обработки и защиты ПДн;

- определяет необходимость обучения сотрудников по вопросам обеспечения безопасности ПДн, а также определяют формы и программы обучения сотрудников;
- заслушивает ответственных за организацию обработки ПДн, за обеспечение безопасности ПДн и других должностных лиц о состоянии работ по организации обработки и защите ПДн;
- осуществляет реагирование на нештатные ситуации, расследование нештатных ситуаций, возникающих при обработке ПДн;
- организует расследование инцидентов, связанных с нарушением безопасности ПДн, правил обработки ПДн, принимает меры по недопущению повторения нештатных ситуаций.

Ответственный за организацию обработки ПДн осуществляет следующие основные функции:

- организует работы по разработке, изменению и уточнению документов Предприятия в части организации обработки и защиты ПДн;
- формирует и актуализирует Перечень сотрудников, допущенных к обработке ПДн;
- доводит до сведения сотрудников Предприятия положения законодательства Российской Федерации в области персональных данных, документов Предприятия по вопросам обработки и обеспечения безопасности персональных данных, требований к защите персональных данных;
- контролируют выполнение сотрудниками требований по защите ПДн;
- проводит анализ соответствия процессов обработки ПДн заявленным принципам обработки ПДн;
- организует сбор согласий на обработку ПДн с субъектов персональных данных (при необходимости);

- формирует и актуализирует Перечни персональных данных, подлежащих защите;
- определяет законность целей и способов обработки ПДн;
- определяет соответствие целей обработки ПДн целям, заранее определенным и заявленным при сборе ПДн, а также полномочиям Предприятия;
- определяет соответствие объема и характера обрабатываемых ПДн, способов обработки ПДн целям обработки ПДн;
- контролирует отсутствие ПДн, избыточных по отношению к целям, заявленным при сборе ПДн;
- определяет допустимые сроки хранения ПДн по каждой категории ПДн;
- контролирует выполнение требований по уничтожению ПДн;
- участвует в определении новых ИСПДн;
- организует определение уровня защищенности ПДн при их обработке в ИСПДн;
- контролирует уровень защищенности ПДн;
- осуществляет взаимодействие с субъектами персональных данных по вопросам обработки их ПДн;
- осуществляет взаимодействиями с внешними контрагентами по вопросам обработки ПДн;
- осуществляет взаимодействие с регуляторными органами по вопросам защиты ПДн;
- осуществляет подготовку и актуализацию уведомлений в уполномоченный орган по защите прав субъектов персональных данных;
- участвует в аттестации ИСПДн на соответствие требованиям безопасности информации;

- осуществляет внутренний контроль соответствия обработки ПДн требованиям к защите ПДн;
- готовит отчеты о состоянии работ по организации обработки и обеспечению безопасности персональных данных в Предприятии;
- участвует в проведении расследования инцидентов, связанных с нарушением безопасности ПДн и правил обработки ПДн.

Ответственный за обеспечение безопасности ПДн осуществляет следующие основные функции:

- участвует в определении новых ИСПДн;
- осуществляет инвентаризацию и управление изменениями в составе и структуре ИСПДн;
- участвует в определении уровня защищенности ПДн при их обработке в ИСПДн;
- участвует в разработке, изменении и уточнении документов Предприятия в части организации обработки и защиты ПДн;
- контролирует изменения в составе и структуре ИСПДн;
- осуществляет учет машинных носителей ПДн;
- осуществляет выбор и организует внедрение необходимых и достаточных мер и средств защиты ПДн;
- участвует в аттестации ИСПДн на соответствие требованиям безопасности информации;
- осуществляет эксплуатацию СЗПДн в соответствии с документацией на нее;
- осуществляет контроль соблюдения условий использования СЗИ, предусмотренных эксплуатационной и технической документацией к ним;
- контролирует соответствие изменений в составе и архитектуре ИСПДн требованиям нормативных правовых актов по защите ПДн;

- участвует во внутреннем контроле соответствия обработки ПДн требованиям к защите ПДн;
- готовит предложения по совершенствованию СЗПДн;
- участвует в проведении расследования инцидентов, связанных с нарушением безопасности ПДн и правил обработки ПДн.

Администратор безопасности информации выполняет следующие основные функции:

- обеспечивает функционирование и поддержание работоспособности средств и систем защиты информации;
- проводит оперативный контроль функционирования средств и систем защиты информации;
- обеспечивает антивирусный контроль в ИСПДн;
- проводит резервирование ПДн;
- осуществляет выявление и регистрацию попыток НСД к компонентам ИСПДн, информационным ресурсам;
- контролирует соответствие технических, программных и информационных ресурсов ИСПДн документации на нее;
- осуществляет учет применяемых СКЗИ, эксплуатационной и технической документации к ним;
- контролирует физическую сохранность средств и оборудования ИСПДн;
- контролирует правильность работы пользователей с элементами ИСПДн и СЗИ;
- осуществляет текущий контроль обеспечения безопасности ПДн при их обработке в ИСПДн;
- проводит инструктажи пользователей по правилам работы в ИСПДн и консультирует по вопросам обеспечения безопасности информации;

- участвуют в расследованиях причин возникновения нештатных ситуаций.

Служба ЭВМ:

- осуществляют сопровождение технических средств и систем ИСПДн;
- соблюдают требования нормативных и распорядительных документов по защите ПДн.

Структурные подразделения, участвующие в процессах обработки ПДн выполняют следующие основные функции:

- осуществляют взаимодействие с субъектами персональных данных по вопросам обработки их ПДн;
- осуществляют сбор согласий на обработку ПДн с субъектов персональных данных (при необходимости);
- осуществляют уведомление субъектов персональных данных в случаях определенных нормативными правовыми актами;
- осуществляют уничтожение ПДн;
- эксплуатируют СЗПДн в соответствии с документацией на нее.

Сотрудники Предприятия выполняют следующие основные функции:

- соблюдают требования нормативных правовых актов и распорядительных документов по защите ПДн;
- осуществляют обработку ПДн в соответствии с должностными обязанностями и предоставленными полномочиями.

Конкретное распределение функций ответственных за организацию обработки ПДн, обеспечение безопасности ПДн, администратора безопасности информации должно быть приведено в должностных инструкциях.

Распределение ролей, полномочий доступа в ИСПДн осуществляется в соответствии с разрешительной системой доступа к информационным ресурсам, программным и техническим средствам ИСПДн.

7. ПОРЯДОК ОРГАНИЗАЦИИ И ПРОВЕДЕНИЯ РАБОТ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Работы по обеспечению безопасности ПДн при их обработке в ИСПДн являются неотъемлемой частью работ, выполняемых в рамках жизненного цикла ИСПДн, на следующих этапах:

- инициация проекта ИСПДн;
- планирование проекта ИСПДн;
- реализация проекта ИСПДн, в составе:
    - выбор технического решения – концепция реализации;
    - проектирование ИСПДн;
    - производство ИСПДн;
    - приемка ИСПДн;
    - внедрение ИСПДн;
    - передача системы в эксплуатацию;
    - документирование проекта.
- эксплуатация ИСПДн;
- модернизация ИСПДн;
- вывод из эксплуатации.

Работы по защите ПДн с привязкой к этапам жизненного цикла ИСПДн приведены в таблице 1.

Таблица 1. Распределение работ по защите ПДн на стадии существования ИСПДн

№ п/п	**Стадия существования ИСПДн, работы по защите ПДн**	**Детализация проводимых работ по защите ПДн**
1.	Инициация проекта ИСПДн	
1.1.	Определение ИСПДн	При создании ИС или существенном изменении существующей ИС определяется необходимость обработки ПДн. Если такая необходимость имеется, то система объявляется - ИСПДн
1.2.	Определение существенной информации об ИСПДн	На данном этапе проводится: ▪ определение перечня ПДн, которые будут обрабатываться в ИСПДн; ▪ определение целей обработки ПДн, действий выполняемых с ПДн, допустимых сроков хранения ПДн; ▪ определение перечня типов технических средств, предполагаемые к использованию в ИСПДн, перечня системных и прикладных программных средств;

№ п/п	Стадия существования ИСПДн, работы по защите ПДн	Детализация проводимых работ по защите ПДн
		▪ определение степени участия персонала в обработке ПДн, характера взаимодействия персонала между собой и с системой
1.3.	Определение предварительной категории ПДн	Детализация проводимых работ приведена в разделе 8
1.4.	Определение предварительного уровня защищенности ПДн при их обработке в ИСПДн	Детализация проводимых работ приведена в разделе 8
1.5.	Оценивается возможность оптимизации ИСПДн	Детализация проводимых работ приведена в разделе 9
1.6.	Юридическая оценка возможности создания ИСПДн	На данном этапе производится юридическая оценка: ▪ целей обработки ПДн; ▪ операций, которые будут выполняться с ПДн; ▪ наличия (возможности сбора) согласий на обработку ПДн, необходимости сбора согласий на обработку ПДн; ▪ степени участия контрагентов в обработке ПДн и необходимые юридические основания для такой обработки; ▪ соответствия предполагаемых процессов обработки ПДн принципам их обработки (см. раздел 5)
1.7.	Проведение оценки возможных затрат на создание СЗПДн по срокам и стоимости	Оцениваются возможные затраты на создание СЗПДн, которые должны учитываться при защите проекта и планировании проекта
2.	Реализация проекта ИСПДн – концепция реализации ИСПДн/СЗПДн	
2.1.	Определяется необходимость корректировки Перечней обрабатываемых ПДн, при необходимости проводится их корректировка	
2.2.	Определение перечня актуальных угроз безопасности ПДн в конкретных условиях функционирования (разработка модели угроз и нарушителя безопасности ПДн)	Детализация проводимых работ приведена в разделе 10
2.3.	Определение категорий ПДн и уровня защищенности ПДн при их обработке в ИСПДн	Детализация проводимых работ приведена в разделе 8
2.4.	Определение необходимости создания СЗПДн	На данном этапе на основе класса ИСПДн определяется необходимость создания СЗПДн
2.5.	Разработка технического задания на разработку СЗПДн	На данном этапе определяются требования к техническим, программным, программно-аппаратным и организационным средствам и мерам обеспечения безопасности ПДн
3.	Реализация проекта ИСПДн – проектирование ИСПДн	
3.1.	Разработка эскизного проекта на СЗПДн	На данном этапе разрабатывается: ▪ пояснительная записка; ▪ схема структурная комплекса технических средств
3.2.	Проработка форм документов предполагающих включение в них ПДн	На данном этапе производится: ▪ определение форм документов, в которых будут содержаться ПДн; ▪ оценка соответствия форм требованиям, предъявляемым к ним нормативными документами Российской Федерации в области защиты ПДн; ▪ производится корректировка форм
3.3.	Разработка эксплуатационной документации на ИСПДн	Производится разработка положений, регламентов, инструкций, определяющих частный порядок защиты ПДн в конкретной ИСПДн
4.	Реализация проекта ИСПДн – производство ИСПДн	
4.1.	Внедрение комплекса средств и мер защиты ПДн	Производятся монтажные, пуско-наладочные работы СЗИ. Производится реализация комплекса организационно-технических мероприятий по защите ПДн

№ п/п	Стадия существования ИСПДн, работы по защите ПДн	Детализация проводимых работ по защите ПДн
4.2.	Реализация требований по физической защите компонентов ИСПДн и носителей ПДн	Производятся монтажные работы средств физической защиты (замков, шкафов, сейфов и т.п.)
4.3.	Заключаются договора с контрагентами, которые будут осуществлять обработку ПДн , с учетом требований по защите ПДн (при необходимости)	На данном этапе определяются договора, в которые должны быть внесены изменения. В данные договора вносятся требования по обеспечению конфиденциальности ПДн контрагентами, которые будут иметь к ним доступ
4.4.	Определение подразделений и назначение лиц, ответственных за эксплуатацию СЗИ	
5.	Реализация проекта ИСПДн – передача системы в опытно-промышленную эксплуатацию	
5.1.	Проводится обучение сотрудников по направлению обеспечения безопасности ПДн	Детализация проводимых работ приведена в разделе 11
5.2.	Проводится ознакомление сотрудников с нормативными правовыми актами в области защиты ПДн	
6.	Реализация проекта ИСПДн – опытная эксплуатация ИСПДн	
6.1.	Начинается сбор согласий на обработку ПДн с субъектов персональных данных (в случае необходимости их сбора определенной в п. 1.6)	
6.2.	Оценивается необходимость изменения уведомления об обработке ПДн	На данном этапе производится: ▪ определение необходимости изменения уведомления об обработке ПДн; ▪ подготовка, согласование и отправка нового уведомления об обработке ПДн в уполномоченный орган по защите прав субъектов персональных данных. Форма, состав уведомления определяется в соответствии с нормативными правовыми актами уполномоченного органа по защите прав субъектов персональных данных
6.3.	Производится опытная эксплуатация СЗИ в комплексе с другими техническими и программными средствами в целях проверки их работоспособности в составе ИСПДн	
6.4.	Разрабатывается программа и методика приемочных испытаний	
6.5.	Проводятся приемочные испытания СЗПДн	Приемочные испытания СЗПДн проводятся в соответствии с программой и методикой приемочных испытаний
7.	Реализация проекта ИСПДн – передача в промышленную эксплуатацию	
7.1.	Проводится оценка соответствия ИСПДн требованиям по безопасности информации	Аттестация на соответствие требованиям безопасности информации
8.	Эксплуатация ИСПДн	
8.1.	Допуск персонала к обработке ПДн	Формируется и утверждается правовым актом перечень сотрудников допущенных к обработке ПДн в ИСПДн
8.2.	Производится уничтожение ПДн	В случае достижения цели обработки ПДн уничтожаются
8.3.	Производится работа с машинными носителями ПДн	Детализация проводимых работ приведена в разделе 12
8.4.	Производится учет СКЗИ, эксплуатационной и технической документации к ним	Учет СКЗИ, эксплуатационной и технической документации производится администратором безопасности информации, в соответствии с установленными на Предприятии требованиями

№ п/п	Стадия существования ИСПДн, работы по защите ПДн	Детализация проводимых работ по защите ПДн
8.5.	Осуществляется контроль изменений в составе и структуре ИСПДн	Детализация проводимых работ приведена в разделе 13
8.6.	Обеспечивается защита от несанкционированного физического доступа к элементам ИСПДн	Детализация проводимых работ приведена в разделе 14
8.7.	Осуществляется резервирование ПДн	Детализация проводимых работ приведена в разделе 15
8.8.	Осуществляется эксплуатация СЗПДн в соответствии с документацией на нее	Эксплуатация системы защиты осуществляется в соответствии с проектом, регламентами и стандартами. Состав СЗПДн и мероприятий по защите ПДн определяется дифференцированно для различных ИСПДн, в зависимости от результатов разработки модели угроз и нарушителя безопасности ПДн и технического задания на СЗПДн
8.9.	Осуществляется контроль за обеспечением необходимого уровня защищенности ПДн	Детализация проводимых работ приведена в разделе 16
8.10.	Производится реагирование на нештатные ситуации	Детализация проводимых работ приведена в разделе 17
8.11.	Проводится обучение персонала правилам обеспечения безопасности ПДн	Детализация проводимых работ приведена в разделе 11
8.12.	Осуществляется взаимодействие с субъектами персональных данных по вопросам обработки их ПДн	Взаимодействие с субъектами персональных данных производится в порядке, определенном законодательством Российской Федерации
8.13.	Отслеживается необходимость получения лицензий ФСТЭК России и (или) ФСБ России	При необходимости производится инициация работ по получению лицензий ФСТЭК России и ФСБ России касающихся защиты ПДн
8.14.	Осуществляется взаимодействие с регуляторными органами по вопросам защиты ПДн	
9.	Модернизация ИСПДн	
9.1.	Осуществляется управление изменениями в ИСПДн	Детализация проводимых работ приведена в разделе 18
9.2.	Производится оценка существенности предполагаемой модернизации ИСПДн	Проводится анализ: ▪ возможности изменения уровня защищенности ПДн при их обработке в ИСПДн, актуальных угроз безопасности ПДн, требований к СЗПДн; ▪ необходимости корректировки документации на СЗПДн; ▪ необходимости проведения дополнительных мероприятий по защите ПДн
9.3.	На основе оценки существенности модернизации, проводится необходимый объем мероприятий указанный в пунктах **Ошибка! Источник ссылки не найден.**-7 данной таблицы	
10.	Вывод из эксплуатации ИСПДн	
10.1.	Производится уничтожение ПДн	В случае вывода из эксплуатации уничтожаются машинные носителей ПДн
10.2.	Производится уведомление субъектов персональных данных (а при необходимости и уполномоченного органа по защите прав субъектов	Взаимодействие с субъектами персональных данных производится в порядке, определенном законодательством Российской Федерации

№ п/п	Стадия существования ИСПДн, работы по защите ПДн	Детализация проводимых работ по защите ПДн
	персональных данных) об уничтожении ПДн	

8. КАТЕГОРИРОВАНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ И ОПРЕДЕЛЕНИЕ УРОВНЯ ЗАЩИЩЕННОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННОЙ СИСТЕМЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Категорирование ПДн и определение уровня защищенности ПДн при их обработке в ИСПДн должны проводиться для каждой ИСПДн на основании «Требований к защите персональных данных при их обработке в информационных системах персональных данных», утвержденных постановлением Правительства Российской Федерации от 01 ноября 2012 г. № 1119.

Процесс категорирования ПДн и определения уровня защищенности ПДн при их обработке в ИСПДн является основой для определения требований к уровню защиты ПДн. В соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» оператор персональных данных «обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных».

В соответствии с «Требованиями к защите персональных данных при их обработке в информационных системах персональных данных»:

- 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 выше.

Категорирование ПДн и определение уровня защищенности ПДн при их обработке в ИСПДн проводятся путем:

- сбора исходных характеристик, влияющих на категорию ПДн и уровень защищенности ПДн;
- указания предположений, влияющих на категорию ПДн и уровень защищенности ПДн;
- логического обоснования предполагаемых категории ПДн и уровня защищенности ПДн.

Исходные характеристики, а также выводы об уровне защищенности ПДн при их обработке в ИСПДн приводятся в акте. Форма акта определения уровня защищенности ПДн при их обработке в ИСПДн приведена в приложении № 2.

Оценка необходимости пересмотра уровня защищенности ПДн при их обработке в ИСПДн должна осуществляться каждый раз, после изменения характеристик, учитываемых при определении уровня защищенности ПДн.

9. ОЦЕНКА ВОЗМОЖНОСТИ ОПТИМИЗАЦИИ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Оценка возможности оптимизации ИСПДн имеет своей целью такую реструктуризацию ИСПДн, выполнение требований по защите ПДн в которой может быть обеспечено с минимальным уровнем затрат на создание и эксплуатацию СЗПДн.

При проведении оптимизации ИСПДн должна оцениваться возможность:

- снижения категории обрабатываемых ПДн;
- обезличивания ПДн;
- придания ПДн статуса общедоступных;
- изменения структуры и состава технических и программных средств ИСПДн, технологических процессов обработки ПДн.

Снижение категории ПДн, в общем случае, позволяет снизить уровень защищенности ПДн при их обработке в ИСПДн и, соответственно, уровень требований к ИСПДн.

Обезличивание ПДн и отнесение ПДн к общедоступным – это эффективный способ снижения уровня требований по обеспечению их безопасности, так как для обезличенных и общедоступных ПДн не требуется обеспечение их конфиденциальности.

Среди мероприятий по обезличиванию ПДн, можно выделить следующие:

- разделение ПДн – ПДн, позволяющих идентифицировать субъекта персональных данных и остальной информации по разным ИСПДн, базам или массивам данных;
- удаление ПДн, позволяющих идентифицировать субъекта персональных данных, в технологических процессах, в которых не требуется однозначного определения физического лица.

Придание ПДн статуса общедоступных возможно в следующих случаях:

- при наличии федерального закона, определяющего, что этот состав ПДн является общедоступным;
- при наличии возможности сбора согласий на общедоступность их ПДн с субъектов персональных данных.

Изменение структуры и состава технических и программных средств ИСПДн, технологических процессов обработки ПДн может проводиться, в том числе, с целью:

- уменьшения количества компонентов ИСПДн, на которые потребуется установка СЗИ;
- изменения возможности, степени опасности угроз для ИСПДн и, соответственно, уменьшения перечня актуальных угроз;
- изменения требований к характеристикам СЗИ, в результате которого возможно использование более оптимальных по стоимости СЗИ и т.п.

10. МОДЕЛЬ УГРОЗ И НАРУШИТЕЛЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

СЗПДн внедряется для нейтрализации актуальных УБПДн.

Оценка актуальности угроз производится посредством разработки модели угроз и нарушителя (при использовании СКЗИ) безопасности ПДн.

Методической базой для разработки модели угроз и нарушителя безопасности ПДн является:

- Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, ФСТЭК России 15 февраля 2008 г.
- Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, ФСТЭК России 14 февраля 2008 г.
- Приказ ФСБ России от 10 июля 2014 г. № 378 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».
- Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации, 8 Центра ФСБ России 21 февраля 2008 г., № 149/54-144.

Результатом разработки модели угроз и нарушителя безопасности ПДн должен являться:

- модель угроз (перечень актуальных угроз);

- модель нарушителя (вывод о типе нарушителя, существующем в ИСПДн и требуемом классе СКЗИ).

Модель угроз и нарушителя безопасности ПДн должна содержать:

- описание структуры и состава ИСПДн (категорию обрабатываемых ПДн, категорию субъектов ПДн, объем обрабатываемых ПДн, состав технических средств и программного обеспечения, существующие процессы обработки ПДн, схему организации связи и т.п.);
- обоснование типа угроз безопасности персональных данных, актуальных для ИСПДн, с учетом оценки возможного вреда, который может быть причинен субъектам ПДн;
- модель угроз (перечень угроз, оценку вероятностей угроз, показатели опасности угроз для ИСПДн, оценки возможностей реализации угроз, выводы об актуальности угроз);
- модель нарушителя (совокупность предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак, и определение на этой основе и с учетом типа актуальных угроз требуемого класса СКЗИ);

Модель угроз и нарушителя безопасности ПДн должна пересматриваться каждый раз, когда изменяются характеристики, влияющие на актуальность угроз безопасности ПДи и возможности, которые могут использоваться при создании способов, подготовке и проведении атак.

11. ОБУЧЕНИЕ ПЕРСОНАЛА, УЧАСТВУЮЩЕГО В ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Должно проводиться регулярное обучение сотрудников Предприятия по вопросам, связанным с обеспечением безопасности ПДн.

В общем случае, для различных категорий сотрудников форматы обучения должны отличаться.

Определены следующие форматы обучения:

- полные курсы;
- кратковременные курсы;
- внешние и внутренние семинары;
- конференции;
- инструктажи.

Полные и кратковременные курсы, конференции, внешние семинары проводятся в специализированных организациях для следующих категорий сотрудников:

- ответственного за организацию обработки ПДн;
- ответственного за обеспечение безопасности ПДн;
- администратора безопасности информации.

Для руководителей структурных подразделений, участвующих в процессах обработки ПДн, могут проводиться кратковременные курсы в специализированных организациях.

Для обучения остальных категорий персонала, участвующих в процессах обработки ПДн, должны проводиться:

- внутренние семинары;
- инструктажи.

Внутренние семинары проводятся ответственным за организацию обработки ПДн, ответственным за обеспечение безопасности ПДн, администратором безопасности информации, а также приглашенными специалистами.

При необходимости должны разрабатываться инструкции, описывающие особенности обработки ПДн в каждой ИСПДн, для отдельных категорий (групп) персонала.

Руководители структурных подразделений обязаны оказывать организационную, техническую и методическую помощь в проведении семинаров и инструктажей.

12. ОРГАНИЗАЦИЯ РАБОТЫ С МАШИННЫМИ НОСИТЕЛЯМИ ПЕРСОНАЛЬНЫХ ДАННЫХ

На Предприятии должна обеспечиваться безопасность ПДн при их обработке с использованием машинных носителей.

Для этого должны быть упорядочены и регламентированы следующие процедуры:

- учет машинных носителей, содержащих ПДн;
- оформление машинных носителей, содержащих ПДн;
- обращение с машинными носителями, содержащими ПДн;
- хранение машинных носителей, содержащих ПДн;
- уничтожение машинных носителей, содержащих ПДн;
- внутренний контроль наличия машинных носителей, содержащих ПДн.

Содержание перечисленных процедур на Предприятии устанавливается регламентом учета, хранения и уничтожения машинных носителей персональных данных.

13. КОНТРОЛЬ ИЗМЕНЕНИЙ В СОСТАВЕ И СТРУКТУРЕ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Все изменения в составе и структуре ИСПДн должны контролироваться и регламентироваться.

Контролю подлежат следующие изменения:

- внесение новых технических средств в состав ИСПДн (ПЭВМ, серверов, сетевого и телекоммуникационного оборудования и т.п.);
- изменение мест включения существующих компонентов ИСПДн;
- удаление технического средства из состава ИСПДн;
- изменение мест установки технического средства из состава ИСПДн;
- прокладка новых или изменение, удаление существующих кабельных линий связи;
- существенное изменение состава и конфигурации системного и прикладного программного обеспечения, используемого для обработки ПДн;
- создание новых и изменение существующих технологических процессов связанных с обработкой ПДн.

Каждое изменение состава ИСПДн, типов технических средств, топологии ИСПДн должно отслеживаться и анализироваться на предмет соответствия требованиям по защите ПДн. При необходимости должна пересматриваться модель угроз и нарушителя безопасности ПДн и производиться модернизация СЗПДн.

14. ЗАЩИТА ОТ НЕСАНКЦИОНИРОВАННОГО ФИЗИЧЕСКОГО ДОСТУПА К ЭЛЕМЕНТАМ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Мероприятия по физическому контролю доступа включают:

- мероприятия по контролю доступа на территорию Предприятия;
- мероприятия по контролю доступа в помещения с оборудованием ИСПДн;
- мероприятия по контролю доступа к техническим средствам ИСПДн;
- мероприятия по контролю перемещений физических компонентов ИСПДн.

Мероприятия по контролю доступа на территорию должны обеспечить контролируемое нахождение посетителей на территории Предприятия.

Перечень сотрудников Предприятия, имеющих право самостоятельного доступа в помещения, с оборудованием ИСПДн утверждается приказом Предприятия.

Помещения с серверным оборудованием ИСПДн должны иметь прочные входные двери с надежными замками и (или) приспособлениями для опечатывания. Двери должны быть постоянно закрыты на замок и открываться только для санкционированного прохода сотрудников.

Двери помещений, в которых размещаются ПЭВМ пользователей ИСПДн, должны быть оборудованы замками и в этих помещениях должны обеспечиваться мероприятия по контролю действий находящихся в них посторонних лиц.

Нахождение в помещении лиц, не участвующих в технологических процессах обработки ПДн (обслуживающий персонал, другие сотрудники, посетители), должно производиться только в присутствии сотрудников, участвующих в соответствующих технологических процессах.

Расположение мониторов ПЭВМ и принтеров должно препятствовать несанкционированному просмотру информации с них со стороны лиц, не допущенных к обработке ПДн.

При выносе технических средств содержащих ПДн, за пределы КЗ для ремонта, замены и т.п. должно быть обеспечено гарантированное уничтожение ПДн на этих технических средствах.

15. РЕЗЕРВИРОВАНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Резервирование ПДн должно обеспечить возможность восстановления информации при нарушении целостности основных хранилищ данных.

Резервированию должны подвергаться базы данных ИСПДн.

Резервирование должно осуществляться на различные машинные носители информации с соответствующим уровнем надежности и долговечности.

Хранение резервных копий должно осуществляться в надежных сейфах (металлических шкафах). Хранение (по возможности) должно осуществляться в месте, территориально удаленном от основного хранилища информации.

Порядок резервирования персональных данных на Предприятии устанавливается инструкцией по резервному копированию информационных ресурсов ИСПДн.

16. КОНТРОЛЬ ЗА ОБЕСПЕЧЕНИЕМ НЕОБХОДИМОГО УРОВНЯ ЗАЩИЩЕННОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Для обеспечения эффективности процесса обеспечения безопасности ПДн проводится:

- контроль соответствия обработки ПДн требованиям к защите ПДн;
- контроль за соблюдением условий использования СЗИ, предусмотренных эксплуатационной и технической документацией к ним;
- контроль эффективности СЗИ.

Контрольные мероприятия могут быть:

- текущими;
- плановыми;
- внезапными.

Ответственность за контроль соответствия обработки ПДн требованиям к защите ПДн возлагается на ответственного за организацию обработки ПДн на Предприятии.

Ответственность за контроль соблюдения условий использования СЗИ, предусмотренных эксплуатационной и технической документацией к ним возлагается на ответственного за обеспечение безопасности ПДн на Предприятии.

Контроль эффективности СЗИ производится организацией – лицензиатом в рамках аттестационных испытаний ИСПДн на соответствие требованиям безопасности информации.

План проведения контроля формируется ответственным за организацию обработки ПДн и утверждается руководством Предприятия ежегодно.

Текущий контроль обеспечения безопасности ПДн при их обработке в ИСПДн проводится администратором безопасности информации в рамках его должностных обязанностей.

Внезапные проверки эффективности при необходимости могут проводиться по решению руководства Предприятия.

При проведении контроля эффективности в общем случае должно проверяться:

- соблюдение требований к процедурам обработки ПДн (уничтожению ПДн, допуску сотрудников к ПДн, соблюдение целей, состава и сроков обработки ПДн)
- соблюдение порядка доступа в помещения, в которых ведется обработка ПДн;
- соблюдение сотрудниками правил парольной политики;
- соблюдение сотрудниками правил антивирусной защиты;
- соблюдение сотрудниками правил работы с машинными носителями персональных данных;
- соблюдение порядка работы с СЗИ.
- наличие установленных СЗИ;
- корректность настроек СЗИ;
- выполнение пользователями, администратором безопасности информации требований организационно-распорядительных документов по защите ПДн на Предприятии;
- соответствие СЗПДн реальному положению дел на Предприятии.

17. РЕАГИРОВАНИЕ НА НЕШТАТНЫЕ СИТУАЦИИ

На Предприятии должны проводиться расследования инцидентов, связанных с НСД и другими несанкционированными действиями затрагивающими безопасность ПДн.

В рамках данного процесса должны решаться следующие задачи:

- расследование инцидентов, связанных с безопасностью ПДн;
- ликвидация последствий инцидентов связанных с безопасностью ПДн;
- принятие мер по недопущению возникновения подобных инцидентов в дальнейшем.

18. ПЕРЕЧЕНЬ НОРМАТИВНЫХ ПРАВОВЫХ АКТОВ, РУКОВОДЯЩИХ И МЕТОДИЧЕСКИХ ДОКУМЕНТОВ, ИСПОЛЬЗУЕМЫХ ПРИ ПРОВЕДЕНИИ МЕРОПРИЯТИЙ ПО ОРГАНИЗАЦИИ ОБРАБОТКИ И ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Конституция Российской Федерации, 12 декабря 1993 г.

2. Конвенция Совета Европы «О защите физических лиц при автоматизированной обработке персональных данных». Страсбург, 28 января 1981 г.

3. Федеральный закон Российской Федерации от 19 декабря 2005 г. № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных».

4. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

5. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

6. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении Перечня сведений конфиденциального характера».

7. Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».

8. Постановление Правительства Российской Федерации от 6 июля 2008 г. № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных».

9. Постановление Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

10. Постановление Правительства Российской Федерации от 01 ноября 2012 г № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

11. Приказ ФСБ России от 9 февраля 2005 г., «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)».

12. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

13. Приказ ФСБ России от 10 июля 2014 г. № 378 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

14. Методический документ «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», ФСТЭК России, 14 февраля 2008 г.

15. Методический документ «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных», ФСТЭК России, 14 февраля 2008 г.

16. Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в

информационных системах персональных данных. ФСБ России, 21 февраля 2008 г., № 149/6/6-622.

17. Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации. ФСБ России, 21 февраля 2008 г, № 149/5-144.

Приложение № 1
к Положению по обеспечению
безопасности персональных данных в
ГУП Республики Крым
«Крымэкоресурсы»

Лист ознакомления
с Положением по обеспечению безопасности персональных данных в ГУП Республики Крым «Крымэкоресурсы»

№ п/п	**Фамилия, инициалы сотрудника**	**Дата ознакомления**	**Роспись сотрудника в ознакомлении**

Приложение № 2
к Положению по обеспечению
безопасности персональных данных в ГУП
Республики Крым «Крымэкоресурсы»

УТВЕРЖДАЮ

Директор
ГУП Республики Крым
«Крымэкоресурсы»
_____ Попко Д.А.
"____" _____ 2020 года

АКТ

определения уровня защищенности персональных данных при их обработке в информационной системе персональных данных
_____ в ГУП Республики Крым «Крымэкоресурсы»

Комиссия в составе: председателя комиссии – _____

членов комиссии: _____

_____

_____

_____

_____

рассмотрела исходные данные на информационную систему персональных данных _____ в в ГУП Республики Крым «Крымэкоресурсы»:

Актуальность угроз безопасности персональных данных, связанных с наличием недокументированных (недекларированных) возможностей в программном обеспечении	Системное программное обеспечение	Прикладное программное обеспечение	Отсутствуют
Категория обрабатываемых персональных данных			
Субъекты персональных данных			
Объем обрабатываемых персональных данных			

и в соответствии с «Требованиями к защите персональных данных при их обработке в информационных системах персональных данных», утвержденными постановлением Правительства Российской Федерации от 01 ноября 2012 г. № 1119

РЕШИЛА:

установить ____ уровень защищенности персональных данных при их обработке в информационной системе персональных данных _____.

Председатель комиссии - _____ Альберенко О.Е.

члены комиссии:
_____ Седов А.А.
_____ Шестопалов С.Н.
_____ Шабурова О.Н.
_____ Иванов Е.В
_____ Чеплянская Л.Н.
_____ Аверьянов Э.Р.