Министерство образования Саратовской области

Государственное автономное профессиональное образовательное учреждение Саратовской области «Базарнокарабулакский техникум агробизнеса»

ПРИНЯТО
Общим собранием (конференцией)
работников и обучающихся
ГАПОУ СО «БТА»
Протокол № 3 от 27.08. 2015 г

УТВЕРЖДАЮ
Директор ГАПОУ СО
«Базарнокарабулакский
техникум агробизнеса»
_____Н.А. Крупнова
Приказ № 373/3 от 27.08.2015г.

ПОЛОЖЕНИЕ
по обеспечению безопасности и защиты персональных данных при их обработке в информационных системах персональных данных

Базарный Карабулак

Должностная инструкция
ответственного за организацию обработки персональных данных в ГАПОУ СО «Базарнокарабулакский техникум агробизнеса»

1. Общие положения

1.1. Настоящая Должностная инструкция определяет основные обязанности, права и ответственность ответственного за организацию обработки персональных данных в ГАПОУ «Базарнокарабулакский техникум агробизнеса» (далее – техникум).

1.2. Ответственный за организацию обработки персональных данных назначается приказом директором техникума.

1.3. Ответственный за организацию обработки персональных данных в своей работе руководствуется Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», настоящей инструкцией, Политикой в отношении обработки персональных данных и Положением об обработке персональных данных.

1.4. Ответственный за организацию обработки персональных данных получает указания непосредственно от директора техникума и подотчетно ему.

1.5. Ответственный за организацию обработки персональных данных несет персональную ответственность за свои действия.

2. Обязанности ответственного за организацию обработки персональных данных

2.1 Ответственный за организацию обработки персональных данных обязан:

2.1.1 Знать и выполнять требования действующих нормативных правовых актов и руководящих документов, а также внутренних инструкций и распоряжений, регламентирующих организацию обработки персональных данных (далее – ПДн).

2.1.2 Знать перечень и условия обработки ПДн.

2.1.3 Участвовать в определении полномочий пользователей информационных систем персональных данных (далее – ИСПДн), минимально необходимых им для выполнения служебных (трудовых) обязанностей.

2.1.4 Осуществлять учёт документов, содержащих ПДн, их уничтожение, либо контроль процедуры их уничтожения.

2.1.5 Блокировать доступ к ПДн при обнаружении нарушений порядка их обработки.

2.1.6 Проводить мероприятия по предотвращению попыток несанкционированного доступа к ПДн.

2.1.7 Контролировать осуществление мероприятий по установке и настройке средств защиты информации.

2.1.8 Вносить свои предложения по совершенствованию мер защиты персональных данных в ИСПДн.

2.1.9 Осуществлять внутренний контроль за соблюдением законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных.

2.1.10 Доводить до сведения работников положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных.

2.1.11 Организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов.

2.1.12 Выполнять иные мероприятия в соответствии с действующими нормативными правовыми актами и руководящими документами.

3. Права ответственного за организацию обработки персональных данных

3. Ответственный за организацию обработки персональных данных имеет право:

3.1 Требовать от сотрудников выполнения локальных нормативно-правовых актов в части работы с ПДн.

3.2 Блокировать доступ к ПДн любых пользователей, если это необходимо для предотвращения нарушения режима защиты ПДн.

3.3 Проводить служебные расследования и опрашивать пользователей по фактам несоблюдения условий хранения носителей ПДн, нарушения правил работы с техническими и программными средствами ИСПДн, в том числе со средствами защиты информации, или по другим нарушениям, которые могут привести к снижению уровня защищённости ПДн.

4. Ответственность ответственного за организацию обработки персональных данных

4.1 Ответственный за организацию обработки персональных данных несет ответственность:

4.1.1 За ненадлежащее исполнение или неисполнение своих должностных обязанностей, предусмотренных настоящей инструкцией, другими организационно-распорядительными документами, в соответствии с трудовым законодательством Российской Федерации.

4.1.2 За нарушения действующего законодательства Российской Федерации.

4.1.3 За разглашение сведений конфиденциального характера и другой защищаемой информации в пределах, определенных законодательством Российской Федерации.

Государственное автономное профессиональное образовательное учреждение Саратовской области «Базарнокарабулакский техникум агробизнеса»

«Согласовано»	«Утверждено»
Председатель профкома ГАПОУ СО «БТА»	Директор ГАПОУ СО «БТА»
_____ Сукманова А.В.	_____ Н.А. Крупнова
Протокол № от г.	Приказ № 373/3 от 27.08.2015 г.

Должностная инструкция администратора безопасности информационных систем персональных данных ГАПОУ СО «Базарнокарабулакский техникум агробизнеса»

1. Общие положения

1.1. Настоящий документ определяет основные обязанности, права и ответственность администратора безопасности информационных систем персональных данных (далее – ИСПДн) ГАПОУ «Базарнокарабулакский техникум агробизнеса» (далее – техникум).

1.2. Администратор безопасности ИСПДн (далее – администратор безопасности) назначается директором техникума.

1.3. Администратор безопасности в своей работе руководствуется Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», настоящей инструкцией, Политикой в отношении обработки персональных данных и Положением об обработке персональных данных.

1.4. Администратор безопасности является ответственным должностным лицом, уполномоченным на проведение работ по поддержанию достигнутого уровня защиты ИСПДн и ее ресурсов на этапах промышленной эксплуатации и модернизации.

1.5. Администратор безопасности осуществляет методическое руководство операторов, системных администраторов и других лиц, допущенных к работе в ИСПДн, в вопросах обеспечения защиты персональных данных (далее – ПДн).

1.6. Требования администратора безопасности, связанные с выполнением им своих должностных обязанностей, обязательны для исполнения всеми пользователями ИСПДн.

1.7. Администратор безопасности несет персональную ответственность за качество проводимых им работ по контролю действий пользователей при работе в ИСПДн, состояние и поддержание установленного уровня защиты ИСПДн.

2. Должностные обязанности администратора безопасности

2.1. Администратор безопасности обязан:

2.2.1. Знать перечень и состав ИСПДн, перечень задач, решаемых их использованием.

2.2.2. Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций и распоряжений, регламентирующих порядок действий по обеспечению защиты ПДн.

2.2.3. Осуществлять установку, настройку и сопровождение систем защиты информации (далее – СЗИ).

2.2.4. Осуществлять учет применяемых систем защиты информации (далее – СЗИ), эксплуатационной и технической документации к ним.

2.2.5. Участвовать в контрольных и тестовых испытаниях и проверках элементов ИСПДн.

2.2.6. Участвовать в приемке новых программных средств.

2.2.7. Обеспечить доступ к защищаемой информации пользователям ИСПДн согласно Разрешительной системе доступа к информационным ресурсам, программным и техническим средствам ИСПДн.

2.2.8. Уточнять в установленном порядке обязанности пользователей ИСПДн.

2.2.9. Проводить резервирование ПДн.

2.2.10. Вести учет носителей ПДн.

2.2.11. Выдавать пользователям личные пароли доступа к средствам ИСПДн.

2.2.12. Анализировать состояние защиты ИСПДн и ее отдельных подсистем.

2.2.13. Контролировать неизменность состояния СЗИ их параметров и режимов защиты.

2.2.14. Контролировать физическую сохранность средств и оборудования ИСПДн.

2.2.15. Контролировать исполнение пользователями ИСПДн введенного режима безопасности, а так же правильность работы с элементами ИСПДн и СЗИ.

2.2.16. Контролировать исполнение пользователями парольной защиты.

2.2.17. Контролировать работу пользователей в сетях общего пользования и международного обмена.

2.2.18. Своевременно анализировать журналы учета событий, с целью выявления возможных нарушений.

2.2.19. Не допускать установку, использование, хранение и размножение в ИСПДн программных средств, не связанных с выполнением функциональных задач.

2.2.20. Осуществлять периодические контрольные проверки рабочих станций и тестирование правильности функционирования СЗИ ИСПДн.

2.2.21. Оказывать помощь пользователям ИСПДн в части применения СЗИ и консультировать по вопросам введенного режима защиты.

2.2.22. Периодически представлять руководству отчет о состоянии защиты ИСПДн, о нештатных ситуациях на объектах ИСПДн и допущенных пользователями нарушениях установленных требований по защите информации.

2.2.23. В случае отказа работоспособности СЗИ ИСПДн принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.

2.2.24. Принимать меры по реагированию, в случае возникновения нештатных и аварийных ситуаций, с целью ликвидации их последствий, участвовать в расследовании причин их возникновения.

3. Организация парольной защиты

3.1. Личные пароли доступа к средствам ИСПДн выдаются пользователям администратором безопасности или другим уполномоченным лицом.

3.2. Полная плановая смена паролей в ИСПДн проводится не реже одного раза в 3 месяца.

3.3. Правила формирования пароля:

пароль не может содержать имя учетной записи пользователя или какую-либо его часть;

пароль должен состоять не менее чем из 8 символов;

в пароле должны присутствовать символы трех категорий из числа следующих четырех:

б) прописные буквы английского алфавита от A до Z;

в) строчные буквы английского алфавита от a до z;

г) десятичные цифры (от 0 до 9);

д) символы, не принадлежащие алфавитно-цифровому набору (например, !, $, #, %);

запрещается использовать в качестве пароля имя входа в систему, простые пароли типа «123», «111», «qwerty» и им подобные, а так же имена и даты рождения своей личности

и своих родственников, номера автомобилей, телефонов и другие пароли, которые можно угадать, основываясь на информации о пользователе;

запрещается выбирать пароли, которые уже использовались ранее.

4. Права администратора безопасности

4.1. Администратор безопасности имеет право:

4.1.1. Отключать любые элементы СЗПДн при изменении конфигурации, регламентном техническом обслуживании или устранении неисправностей в установленном порядке.

4.1.2. В установленном порядке изменять конфигурацию элементов ИСПДн и СЗПДн.

4.1.3. Требовать от сотрудников соблюдения правил работы в ИСПДн, приведенных в должностных инструкциях.

4.1.4. Требовать от пользователей безусловного соблюдения установленной технологии обработки ПДн и выполнения требований локальных документов, регламентирующих вопросы обеспечения защиты ПДн.

4.1.5. Требовать прекращения обработки информации в случае нарушения установленной технологии обработки ПДн или нарушения функционирования СЗИ.

4.1.6. Вносить свои предложения по совершенствованию СЗПДн.

4.1.7. Инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения защиты ПДн в ИСПДн.

5. Ответственность администратора безопасности

5.1. Администратор безопасности несет ответственность:

5.1.1. За ненадлежащее исполнение или неисполнение своих должностных обязанностей, предусмотренных настоящей инструкцией, другими организационно-распорядительными документами, в соответствии с трудовым законодательством Российской Федерации.

5.1.2. За нарушения действующего законодательства Российской Федерации.

5.1.3. За разглашение сведений конфиденциального характера и другой защищаемой информации в пределах, определенных законодательством Российской Федерации.

4.2. На администратора безопасности возлагается персональная ответственность за работоспособность и надлежащее функционирование СЗИ ИСПДН.

Министерство образования Саратовской области

Государственное автономное профессиональное образовательное учреждение Саратовской области «Базарнокарабулакский техникум агробизнеса»

ПРИНЯТО
Общим собранием (конференцией)
работников и обучающихся
ГАПОУ СО «БТА»
Протокол № 3 от 27.08. 2015 г

УТВЕРЖДАЮ
Директор ГАПОУ СО
«Базарнокарабулакский
техникум агробизнеса»
_____Н.А. Крупнова
Приказ № 373/3 от 27.08.2015г.

ПОЛОЖЕНИЕ
по обеспечению безопасности и защиты персональных данных при их обработке в информационных системах персональных данных

Базарный Карабулак

Назначение Положения

Настоящее Положение определяет порядок организации и проведения работ по обеспечению безопасности и защиты персональных данных (далее – ПДн) при их обработке в информационных системах персональных данных (далее – ИСПДн) в государственном автономном профессиональном образовательном учреждении Саратовской области «Базарнокарабулакский техникум агробизнеса» (далее – оператор).

Данный документ направлен на достижение следующих целей:

- выполнение требований законодательства в области персональных данных;
- защита прав и свобод граждан РФ при обработке их ПДн в ИСПДн оператора;
- защита ПДн, обрабатываемых оператором, от несанкционированного доступа и других несанкционированных действий.

1. Область действия

Требования настоящего Положения распространяются на все подразделения оператора, 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 оператора, а также другие лица, допущенные к работе в ИСПДн.

2. Общие положения

Настоящее Положение разработано в соответствии со следующими нормативными актами:

- Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- Федеральным законом от 27 июля 2006 г. №1 49-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Постановлением Правительства Российской Федерации от 15 сентября 2008 г. №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Постановления Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Приказа 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»
- методическими документами ФСБ России, ФСТЭК России, Роскомнадзора.

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 угроз безопасности персональных данных;
- 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 в ИСПДн.

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 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 с использованием сертифицированных систем защиты информации (далее – СЗИ).

Настоящее Положение определяет:

– роли, полномочия, ответственность за обеспечение безопасности и защиту ПДн, подразделений оператора;

– порядок организации и проведения работ по обеспечению безопасности и защите ПДн при их обработке в ИСПДн;

– мероприятия по защите ПДн;

– требования по управлению процессом обеспечения безопасности ПДн;

– требования к составу и содержанию документов оператора, регламентирующих защиту и работу с ПДн.

Целью создания системы защиты персональных данных (далее – 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:
- конфиденциальность ПДн;
- целостность ПДн;
- доступность ПДн.

Конкретный состав целей защиты ПДн зависит от конкретной ИСПДн и определяется по результатам разработки модели угроз и нарушителя 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 ПДн;

– разработка и актуализация Перечня сведений конфиденциального характера;

– уничтожение ПДн;

– управление взаимодействиями с внешними контрагентами по вопросам обработки ПДн;

– взаимодействие с субъектами ПДн по вопросам обработки их ПДн;

– определение уровня защищенности 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,

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 ПДн;

– аттестация (декларирование соответствия) по требованиям безопасности информации;

– получение лицензий ФСТЭК России и ФСБ России в области защиты ПДн.

Оператор должен проводить 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 в ИСПДн оператора;

– проведения контрольных и проверочных мероприятий на предмет оценки соответствия процессов обработки ПДн заявленным принципам.

Отнесение сведений оператором к ПДн, безопасность которых должна обеспечиваться СЗПДн представляет собой процесс обоснованного установления (документального оформления и утверждения) критериев их выделения из всей совокупности сведений, находящихся в обращении.

В качестве такого критерия у оператора разрабатывается и утверждается Перечень персональных данных, подлежащих защите в (указывается наименование оператора).

3. Организационная структура системы защиты персональных данных

СЗПДн является частью общей системы обеспечения информационной безопасности оператора.

Основу организационной структуры СЗПДн как правило составляют следующие организационные структуры:

– руководство;

– ответственные за обеспечение безопасности ПДн;

– администраторы безопасности ИСПДн;

– ответственные за техническое сопровождение ИСПДн;

– структурные подразделения, участвующие в процессах обработки ПДн;

– сотрудники оператора.

Руководство осуществляет следующие основные функции в области обеспечения безопасности ПДн:

– обеспечивает общую организацию работ по защите ПДн;

– издает приказы по вопросам организации СЗПДн;

– утверждает Перечень сведений конфиденциального характера;

– назначает ответственных за обеспечение безопасности ПДн;

– утверждает список лиц, допущенных к обработке ПДн;

– рассматривает и утверждает нормативные документы оператора, регламентирующие обработку и защиту ПДн;

– заслушивает при необходимости ответственных за обеспечение безопасности ПДн и других должностных лиц о состоянии работ по защите ПДн.

Ответственные за обеспечение безопасности ПДн осуществляют следующие основные функции:

– разрабатывают Перечень сведений конфиденциального характера;

– участвуют в проведении определении уровня защищенности ИСПДн;

– распределяют ответственность по вопросам обработки и защиты ПДн;

– определяют допустимые сроки хранения ПДн по каждой категории ПДн;

– организуют подачу уведомлений в уполномоченный орган по защите прав субъектов ПДн;

– заслушивают руководителей структурных подразделений о принимаемых мерах по состоянию и совершенствованию СЗПДн;

– организуют работы по разработке, изменению и уточнению политик, регламентов, стандартов в части защиты ПДн;

– осуществляют организацию плановых и внеплановых проверочных мероприятий;

– организуют выполнение требований по защите ПДн у оператора;

– проводят разработку и актуализацию локальных нормативных документов, регламентирующих защиту ПДн у оператора;

– проводит ознакомление сотрудников с нормативными документами в области защиты ПДн;

– проводят оценку эффективности принятых мер и применяемых средств защиты ПДн;

– проводят занятия с сотрудниками по изучению организационно-распорядительных документов по всему комплексу вопросов защиты ПДн;

– разрабатывают и актуализируют частные модели угроз безопасности ПДн и технические задания на СЗПДн;

– определяют необходимость обучения сотрудников по вопросам обеспечения безопасности ПДн, а также определяют формы и программы обучения сотрудников оператора в области защиты ПДн;

– контролируют выполнение сотрудниками требований по защите ПДн;

– организуют работы по сбору сведений об изменениях в составе и структуре ИСПДн;

– осуществляют контроль соответствия изменений в составе и архитектуре ИСПДн требованиям нормативных документов по защите ПДн, а также внутренних организационно-распорядительных документов оператора;

– контролируют исполнение требований по уничтожению ПДн;

– разрабатывают рекомендации по оптимизации существующих и новых информационных процессов обработки ПДн по критериям соответствия требованиям по защите ПДн и минимизации затрат на создание и эксплуатацию системы защиты ПДн;

– контролируют исполнение требований нормативных документов оператора в области обеспечения безопасности ПДн, структурными подразделениями и сотрудниками;

– организуют и осуществляют взаимодействие с регуляторами по вопросам защиты ПДн;

– участвуют в аттестации (декларировании соответствия) ИСПДн оператора по требованиям безопасности информации;

– управляют проектами по внедрению систем и средств защиты ПДн;

– контролируют ввод в действие, эксплуатацию СЗПДн;

– проводят расследования инцидентов, связанных с нарушением безопасности ПДн, правил обработки ПДн, принимают меры по недопущению повторения нештатных ситуаций;

– осуществляют плановый контроль эффективности процесса обеспечения безопасности ПДн.

Администраторы безопасности ИСПДн осуществляют следующие основные функции:

– осуществляют сопровождение средств и систем защиты ПДн;

– проводят оперативный контроль функционирования средств и систем защиты ПДн;

– проводят резервирование ПДн;

– ведут учет носителей ПДн;

– осуществляют выявление и регистрацию попыток НСД к компонентам ИСПДн, информационным ресурсам;

– контролируют соответствие технических, программных и программно-аппаратных средств ИСПДн требованиям, предъявляемым к ним средствами и СЗПДн;

– осуществляют учет применяемых СЗИ, эксплуатационной и технической

документации к ним;

– контролируют выполнение сотрудниками подразделения требований по защите ПДн;

– участвуют в расследованиях причин возникновения нештатных ситуаций;

– готовят предложения по совершенствованию СЗПДн;

– выполняют комплекс мероприятий по защите информации при проведении ремонтных и регламентных работ;

– обеспечивают защиту ПДн при выводе из эксплуатации компонентов ИСПДн;

– осуществляют текущий контроль эффективности процесса обеспечения безопасности ПДн.

Ответственные за техническое сопровождение ИСПДн осуществляют следующие основные функции:

– осуществляют техническое сопровождение средств и систем ИСПДн.

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

– осуществляют взаимодействие с субъектами ПДн по вопросам обработки их ПДн;

– осуществляют уведомление субъектов ПДн в случаях определенных нормативными актами;

– эксплуатируют СЗПДн в соответствии с документацией на нее.

Сотрудники оператора выполняют следующие основные функции:

– соблюдают требования нормативных документов по защите ПДн;

– осуществляют обработку ПДн в соответствии с заданием и предоставленными полномочиями.

Конкретное распределение функций администраторов безопасности, ответственных за техническое сопровождение ИСПДн, сотрудников определяется в должностных инструкциях.

Распределение ролей, полномочий осуществляется в соответствии с Разрешительной системой доступа к информационным ресурсам, программным и техническим средствам информационных систем персональных данных.

4. Порядок организации и проведения работ по обеспечению безопасности и защите персональных данных

Работы по обеспечению безопасности и защите 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.

5. Допуск персонала к обработке персональных данных

При допуске к ПДн оператор руководствуется утвержденным списком лиц, допущенных к обработке ПДн.

6. Контроль изменений в составе и структуре информационных систем персональных данных

Все изменения в составе и структуре ИСПДн должны контролироваться и регламентироваться ответственными за обеспечение безопасности ПДн.

Контролю подлежат следующие изменения:

– внесение новых устройств в состав ИСПДн (автоматизированных рабочих мест (далее – АРМ), серверов, сетевого и телекоммуникационного оборудования и т.п.);

– изменение мест включения существующих компонент ИСПДн;

– удаление устройств из состава ИСПДн;

– изменение мест установки устройства из состава ИСПДн;

– прокладка новых кабельных линий связи и внешних линий связи или удаление старых кабельных линий связи;

– существенное изменение состава и конфигурации системного и прикладного программного обеспечения, участвующего в обработке 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 ИСПДн. При необходимости должна производиться модернизация СЗПДн.

7. Защита от несанкционируемого доступа к элементам информационных систем персональных

Мероприятия по физическому контролю доступа включают:

– мероприятия по контролю доступа на территорию;

– 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 обеспечивают контролируемое нахождение посетителей на территории оператора.

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

Двери помещений, в которых размещаются АРМ пользователей ИСПДн, должны быть оборудованы замками, либо 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), должно производиться только в присутствии сотрудников, участвующих в соответствующих технологических процессах.

Расположение мониторов рабочих станций должно препятствовать их несанкционированному просмотру со стороны других лиц, не допущенными к обработке ПДн.

При выносе устройств, хранящих ПДн, за пределы КЗ для ремонта, замены и т.п. должно быть обеспечено гарантированное уничтожение информации хранимой на этих устройствах.

8. Резервирование персональных данных

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

Резервированию должна подвергаться информация на серверах ИСПДн.

Резервирование должно осуществляться на различные 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.

Доступ к резервным копиям должен быть строго регламентирован.

9. Контроль эффективности процесса обеспечения безопасности персональных данных

Для обеспечения контроля эффективности процесса обеспечения безопасности ПДн проводится:

- контроль за соблюдением требований по обработке и защите ПДн;
- контроль за соблюдением условий использования средств защиты ПДн, предусмотренных эксплуатационной и технической документацией;
- контроль эффективности средств защиты ПДн.

Контрольные мероприятия могут быть:

- текущими;
- внезапными;
- плановыми внешними;
- плановыми внутренними.

Ответственность за текущий контроль эффективности процесса обеспечения безопасности ПДн возлагается на администраторов безопасности ИСПДн.

Ответственность за плановый контроль эффективности процесса обеспечения безопасности ПДн возлагается на ответственных за обеспечение безопасности ПДн. Данные проверки должны включаться в план аудитов информационной безопасности на год.

Для планового контроля эффективности СЗПДн должны использоваться средства выявления уязвимостей информационной безопасности.

Внезапные проверки эффективности при необходимости могут проводиться специальными группами по решению ответственных за обеспечение безопасности ПДн.

При проведении контроля эффективности в общем случае должно проверяться:

- наличие установленных СЗИ;
- корректность настроек СЗИ;
- выполнение пользователями и администраторами требований инструктивных материалов по защите ПДн;
- исполнение требований к процедурам обработки ПДн (уничтожению ПДн, сбору согласий, допуску персонала к ПДн и т.п.);
- правильность организации работы с носителями ПДн;
- правильность обращения ключевой информации;
- соответствие СЗПДн реальному положению дел у оператора.

10. Реагирование на нештатные ситуации

Оператор должен проводить 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.