Администрация МО «Ахтубинский район»

Утверждено

Приказом от __.__.____ № ____

ПОЛОЖЕНИЕ

О ПОРЯДКЕ ОРГАНИЗАЦИИ И ПРОВЕДЕНИЯ РАБОТ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В АДМИНИСТРАЦИИ МО «АХТУБИНСКИЙ РАЙОН»

г. Ахтубинск 2013г

СОДЕРЖАНИЕ

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

В настоящем документе используются следующие термины и их определения:

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

Доступ к информации — возможность получения информации и ее использования.

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.

Информационные технологии — процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способ осуществления таких процессов и методов.

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

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

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

Оператор — государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

Технические средства информационной системы персональных данных — средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (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).

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.

Правила разграничения доступа — совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Программное (программно-математическое) воздействие — несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

Средства вычислительной техники — совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

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

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.

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.

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

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).

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

Таблица 1. Условные обозначения и сокращения

Сокращение	Значение
АС	Автоматизированная система
ИСПДн	Информационная система персональных данных
ЛВС	Локальные вычислительные сети
ОРД	Организационно-распорядительная документация
ПДн	Персональные данные
ПДТК	Постоянно действующая техническая комиссия
Роскомнадзор	Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций
СВТ	Средство вычислительной техники
СЗПДн	Система защиты персональных данных
СТР-К	Нормативно-методический документ. «Специальные требования и рекомендации по технической защите конфиденциальной информации» (утвержден приказом Гостехкомиссии России от 30 августа 2002 г. № 282)
ФСБ России	Федеральная служба безопасности Российской Федерации
ФСТЭК России	Федеральная служба по техническому и экспортному контролю

1 ОБЩИЕ ПОЛОЖЕНИЯ

Настоящее Положение о порядке организации и проведения работ по защите персональных данных в Администрации МО «Ахтубинский район» (далее — Положение) определяет содержание и порядок осуществления мероприятий по защите персональных данных, обрабатываемых с использованием средств автоматизации, в Администрации МО «Ахтубинский район».

Настоящее Положение о порядке организации и проведения работ по защите персональных данных в Администрации МО «Ахтубинский район», составлено в соответствии с Положением об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденным постановлением Правительства РФ от 01 ноября 2012 г. № 1119.

1.1 Цель Положения

Целью данного Положения является проведение работ по защите персональных данных (ПДн) и приведение существующих информационных систем в надлежащий вид в соответствии с требованиями информационной безопасности.

Мероприятия по защите ПДн с грифом «Конфиденциально» являются неотъемлемой составной частью деятельности в Администрации МО «Ахтубинский район».

Уровень технической защиты конфиденциальной информации, а также перечень необходимых мер защиты определяются дифференцированно по результатам обследования объекта информатизации, с учетом соотношения затрат на организацию технической защиты информации и величины ущерба, который может быть нанесен Администрации МО «Ахтубинский район».

1.2 Объекты защиты

В Администрации МО «Ахтубинский район» подлежат защите автоматизированные системы (АС), средства и системы связи и передачи информации, другие технические средства, используемые для обработки персональных данных.

Защита ПДн в Администрации МО «Ахтубинский район» обеспечивается выполнением комплекса организационных мероприятий и применением средств защиты информации от утечки по техническим каналам, несанкционированного доступа, программно-технических воздействий с целью нарушения целостности (модификации, уничтожения) и доступности информации в процессе ее обработки, передачи и хранения, а также обеспечения работоспособности технических средств.

1.3 Ответственные за защиту

Организация защиты информации на объекте информатизации возлагается на Сотрудника отвечающего за безопасность персональных данных Администрации МО «Ахтубинский район».

Должностные лица, в обязанность которых входит обработка ПДн, обязаны обеспечить каждому субъекту ПДн возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом.

Настоящее Положение является обязательным для исполнения всеми работниками, ответственными за защиту ПДн.

2 НОРМАТИВНО-МЕТОДИЧЕСКАЯ ДОКУМЕНТАЦИЯ

При организации и проведении работ по обеспечению безопасности ПДн необходимо руководствоваться следующими нормативными и методическими документами:

– Конституция Российской Федерации;

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

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

– Указ Президента от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера»;

– Положение об утверждении требований к защите персональных данных при обработке в информационных системах персональных данных (утв. постановлением Правительства Российской Федерации от 01 ноября 2012 г. № 1119);

– совместный приказ ФСТЭК/ФСБ/Мининформсвязи России от 13 февраля 2008 г. № 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных»;

– Базовая модель угроз безопасности персональных данных при их обработке в информационных системах (утв. заместителем директора ФСТЭК России 15 февраля 2008 г.);

– Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утв. заместителем директора ФСТЭК России 14 февраля 2008 г.);

– 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 (утв. руководством 8 Центра ФСБ России 21 февраля 2008 г. № 149/6/6-622);

– Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации (утв. руководством 8 Центра ФСБ России 21 февраля 2008 г. № 149/5-144);

– Приказ от 15 февраля 2010 г. № 58 «Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных»;

– Специальные требования и рекомендации по технической защите конфиденциальной информации (утв. приказом Гостехкомиссии России от 30 февраля 2002 г № 282).

3 ПОРЯДОК ОРГАНИЗАЦИИ И ПРОВЕДЕНИЯ РАБОТ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПДН ПРИ ИХ ОБРАБОТКЕ В ИСПДН

3.1 Организационные мероприятия

Организационные меры по защите ПДн в Администрации МО «Ахтубинский район» включают в себя следующие мероприятия:

– определение лиц, ответственных за защиту информации на предприятии;

– определение перечня ПДн, обрабатываемых на предприятии;

– определение цели обработки ПДн;

– определение сроков обработки и хранения ПДн;

– определение круга лиц, допущенных к обработке ПДн;

– организация доступа в помещения, где осуществляется обработка ПДн;

– обучение работников, допущенных к обработке ПДн, основам информационной безопасности;

– учет применяемых технических средств защиты ПДн;

– учет носителей ПДн;

– разработка организационно-распорядительных документов (далее — ОРД).

3.2 Определение лиц и подразделений, ответственных за защиту персональных данных в Администрации МО «Ахтубинский район»

Для определения лиц, ответственных за защиту ПДн, необходимо:

1) разработать и утвердить Положение о Сотруднике, отвечающем за защиту ПДн.

2) разработать и утвердить должностные инструкции (либо внести изменения в существующие должностные инструкции) Сотрудников, отвечающих за защиту ПДн.

3) определить состав и утвердить постоянно действующую техническую комиссию (далее — ПДТК) по защите информации в Администрации МО «Ахтубинский район».

3.3 Определение перечня персональных данных, обрабатываемых в Администрации МО «Ахтубинский район»

В рамках настоящего Положения к защищаемой информации относится документированная конфиденциальная информация, обрабатываемая в Администрации МО «Ахтубинский район», созданная в Администрации МО «Ахтубинский район» или полученная от юридических или физических лиц на законных основаниях.

В первую очередь, необходимо установить перечень ПДн, которые обрабатываются в Администрации МО «Ахтубинский район».

Конфиденциальность массивов документов, создаваемых на АРМ Администрации МО «Ахтубинский район» массивов документов, создаваемых в Администрации МО «Ахтубинский район» (библиотеках, архивах, банках данных), определяется ПДТК Администрации МО «Ахтубинский район». Состав ПДТК Администрации МО «Ахтубинский район» определяется приказом Главы администрации МО «Ахтубинский район».

Конфиденциальность массивов документов, массивов документов в информационных системах (библиотеках, архивах, фондах, банках данных), создаваемых вне Администрации

МО «Ахтубинский район», определяется органами государственной власти, в ведении которых они находятся, либо непосредственно их обладателем.

3.4 Определение цели обработки персональных данных

3.4.1 Цели обработки ПДн:

– выполнение обязательств работодателя по трудовому договору.

3.4.2 Определение сроков обработки и хранения ПДн

Сроки хранения и обработки информации, содержащей ПДн субъектов, определяются в соответствии с Перечнем типовых управленческих документов, образующихся в деятельности организаций, с указанием сроков хранения (утв. решением Росархива от 06 октября 2000 года); в соответствии с Федеральным законом от 7 августа 2001 года № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» (п. 4, ст. 7); и указываются в утвержденном Главой администрации МО «Ахтубинский район» Перечне персональных данных, обрабатываемых в Администрации МО «Ахтубинский район».

По достижении срока хранения и обработки информации, содержащей ПДн субъектов, данная информация должна быть уничтожена.

Сбор, хранение, использование и распространение информации о частной жизни лица без письменного его согласия не допускаются.

3.4.3 Определение круга лиц, допущенных к обработке ПДн

Круг лиц, допущенных к обработке ПДн, определяется каждым руководителем подразделения, в котором обрабатываются ПДн, и утверждается Главой администрации МО «Ахтубинский район».

Все лица, допущенные к обработке ПДн, должны быть ознакомлены с организационно-распорядительной документацией по защите ПДн в Администрации МО «Ахтубинский район».

В должностные инструкции работников, принимающих участие в обработке ПДн, должны быть внесены изменения в части защиты информации.

3.4.4 Организация доступа в помещения, где осуществляется обработка ПДн

Распоряжением Главы администрации МО «Ахтубинский район» утверждается перечень лиц, допущенных в помещение, где располагаются АРМы и телекоммуникационное оборудование.

В целях обеспечения ограниченного доступа в помещения с АРМ входная дверь должна быть изготовлена из металла, снабжена замком и опечатывалась. В случае если установка данной системы невозможна, необходимо регистрировать вход/выход работников в соответствии с перечнем лиц допущенных в помещение.

Доступ в помещения, где обрабатываются ПДн, лицам, не допущенным к обработке ПДн, должен быть по возможности запрещен. В случае невозможности запретить доступ в помещения, необходимо исключить возможность несанкционированного доступа к техническим средствам обработки ПДн, хищение и нарушение работоспособности, хищение носителей информации.

3.4.5 Обучение работников

Не реже одного раза в год сотруднику, ответственному за защиту ПДн, необходимо проводить обучение лиц, использующих средства защиты информации, применяемые в ИСПДн, правилам работы с ними. Также проводится обучение работников Администрации

МО «Ахтубинский район», допущенных к обработке ПДн, правилам обработки ПДн, в соответствии с утвержденными требованиями.

Сотруднику, проводившему обучение, необходимо заносить все мероприятия по обучению в Журнал инструктажа пользователей информационной системы персональных данных и обслуживающего персонала Администрации МО «Ахтубинский район» по правилам обработки персональных данных и в Журнал учета мероприятий по защите информации в Администрации МО «Ахтубинский район».

3.4.6 Учет применяемых технических средств защиты персональных данных

Учет технических средств защиты информации ведется в Техническом паспорте ИСПДн в соответствии с требованиями СТР-К.

3.4.7 Технические мероприятия

Технические меры защиты ПДн предполагают использование программно-аппаратных средств защиты информации. При обработке ПДн с использованием средств автоматизации применение технических мер защиты является обязательным условием, а их количество и степень защиты определяется в процессе предпроектного обследования информационных ресурсов Администрации МО «Ахтубинский район».

3.4.8 Требования к техническим и программным средствам.

Технические и программные средства, используемые для обработки ПДн в ИСПДн, должны удовлетворять установленным в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

Средства защиты информации, применяемые в ИСПДн, в установленном порядке проходят процедуру оценки соответствия, включая сертификацию на соответствие требованиям по безопасности информации.

3.4.9 Необходимость создания системы защиты персональных данных

Создание системы защиты персональных данных (далее — СЗПДн) является необходимым условием обеспечения безопасности ПДн в том случае, если существующие организационные и технические меры обеспечения безопасности не соответствуют требованиями к обеспечению безопасности ПДн для ИСПДн соответствующего класса и/или не покрывают всех угроз безопасности ПДн для данной ИСПДн.

3.4.10 Модернизация СЗПДн

Для функционирующих ИСПДн доработка (модернизация) СЗПДн должна проводиться в случае, если:

– изменился состав, или структура самой ИСПДн, или технические особенности ее построения (изменился состав или структура программного обеспечения, технических средств обработки ПДн, топологии ИСПДн);

– изменился состав угроз безопасности ПДн в ИСПДн;

– изменился класс ИСПДн.

Для определения необходимости доработки (модернизации) СЗПДн не реже одного раза в год должна проводиться проверка состава и структуры ИСПДн, состава угроз безопасности ПДн в ИСПДн и класса ИСПДн. Проверка проводится Сотрудником отвечающим за безопасность персональных данных Администрации МО «Ахтубинский район». Результаты проверки оформляются актом и утверждаются Главой администрации МО «Ахтубинский район».

Классификация ИСПДн проводится в соответствии с Порядком проведения классификации информационных систем персональных данных, утвержденным приказом ФСТЭК России, ФСБ России и Мининформсвязи России от 13 февраля 2008 г. № 55/86/20.

С целью своевременного выявления и предотвращения утечки информации по техническим каналам, исключения или существенного затруднения несанкционированного доступа и предотвращения специальных программно-технических воздействий, вызывающих нарушение конфиденциальности, целостности и доступности информации, в организации осуществляется периодический контроль за состоянием защиты информации.

Контроль осуществляется на основании Положения «О государственной системе защиты информации» и заключается в оценке:

– соблюдения нормативных и методических документов в области технической защиты информации;

– работоспособности применяемых средств защиты информации в соответствии с их эксплуатационной документацией;

– знаний и выполнения персоналом своих функциональных обязанностей в части защиты информации.

4 ДОСТУП К ПЕРСОНАЛЬНЫМ ДАННЫМ

4.1 Внутренний доступ

Доступ к персональным данным определяется в Перечне подразделений и сотрудников, допущенных к работе с ПДн, обрабатываемыми в ИСПДн Администрации МО «Ахтубинский район».

Разграничение прав доступа к ИСПДн возлагается на Сотрудника отвечающего за безопасность персональных данных Администрации МО «Ахтубинский район».

Уполномоченные лица имеют право получать только те ПДн, которые необходимы для выполнения конкретных функций в соответствии с должностной инструкцией указанных лиц.

4.2 Внешний доступ (другие организации и граждане)

Сообщение сведений о ПДн другим организациям и гражданам разрешается при наличии письменного согласия субъекта и заявления, подписанного руководителем организации либо гражданином, запросившим такие сведения.

Предоставление сведений о ПДн без соответствующего их согласия возможно в следующих случаях:

– в целях предупреждения угрозы жизни и здоровья субъекта;

– при поступлении официальных запросов в соответствии с положениями Федерального закона «Об оперативно-розыскных мероприятиях»;

– при поступлении официальных запросов из Федеральной налоговой службы РФ, Пенсионного фонда России, Фонда социального страхования РФ, судебных органов;

– в соответствии с федеральным законодательством Российской Федерации.

Субъект, о котором запрашиваются сведения, должен быть уведомлён о передаче его ПДн третьим лицам, за исключением случаев, когда такое уведомление невозможно в силу форс-мажорных обстоятельств, а именно: стихийных бедствий, аварий, катастроф.

Запрещается передача ПДн субъекта в коммерческих целях без его согласия.

5 КОНТРОЛЬ ЗА СОБЛЮДЕНИЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В АДМИНИСТРАЦИИ МО «АХТУБИНСКИЙ РАЙОН»

5.1 Общие правила

Контроль за состоянием защиты информации (далее — контроль) осуществляется с целью своевременного выявления и предотвращения утечки информации по техническим каналам, несанкционированного доступа к ней, преднамеренных программно-технических воздействий на информацию, а также хищения ПДн.

Контроль заключается в проверке выполнения актов законодательства Российской Федерации по вопросам защиты информации, решений Федеральной службы по техническому и экспортному контролю (ФСТЭК России), а также в оценке обоснованности и эффективности, принятых мер защиты для обеспечения выполнения утвержденных требований и норм по защите информации.

Постоянный контроль за состоянием защиты информации в Администрации МО «Ахтубинский район» осуществляет Сотрудник отвечающий за безопасность персональных данных.

Периодический контроль за деятельностью по защите информации в Администрации МО «Ахтубинский район» осуществляется комиссиями инспекции ФСТЭК России и Роскомнадзора.

Контроль за эффективностью применяемых в Администрации МО «Ахтубинский район» мер и средств защиты информации должен проводиться в соответствии с требованиями эксплуатационной документации на сертифицированные средства защиты, других нормативных документов, но не реже одного раза в год.

Обязательным является контроль за средствами защиты при вводе их в эксплуатацию, после проведения ремонта средств защиты, при изменении условий их расположения или эксплуатации.

5.2 Определение нарушений

Защита информации считается эффективной, если принимаемые меры соответствуют установленным требованиям или нормам.

Несоответствие мер установленным требованиям или нормам по защите информации является нарушением.

Нарушения по степени важности делятся на три категории:

– первая — невыполнение требований или норм по защите информации, в результате чего имелась или имеется реальная возможность ее утечки по техническим каналам;

– вторая — невыполнение требований по защите информации, в результате чего создаются предпосылки к ее утечке по техническим каналам;

– третья — невыполнение других требований по защите информации.

Нарушения для каждой ИСПДн Администрации МО «Ахтубинский район» описываются в Модели угроз.

5.3 Порядок действий при нарушениях безопасности ПДн

5.3.1 При обнаружении нарушений первой категории

При обнаружении нарушений первой категории руководители подразделений обязаны:

– немедленно прекратить работы на участке (рабочем месте), где обнаружены нарушения, и принять меры по их устранению;

– организовать в установленном порядке расследование причин и условий появления нарушений с целью недопущения их в дальнейшем и привлечения к ответственности виновных лиц;

– сообщить в ФСТЭК России о вскрытых нарушениях и принятых мерах.

Возобновление работ разрешается после устранения нарушений, проверки достаточности и эффективности принятых мер. Контроль за устранением этих нарушений осуществляется Сотрудником отвечающим за безопасность персональных данных.

5.3.2 При обнаружении нарушений второй и третьей категорий

При обнаружении нарушений второй и третьей категорий руководители отделов обязаны принять необходимые меры по их устранению в соответствии с организационно-распорядительной документацией.

Контроль за устранением этих нарушений осуществляется Сотрудником отвечающим за безопасность персональных данных.

5.3.3 Разбирательство

Разбирательство и составление заключений в обязательном порядке должно проводиться в случае выявления следующих фактов:

– несоблюдение условий хранения носителей ПДн;

– использование средств защиты информации, применение которых может привести к нарушению заданного уровня безопасности (конфиденциальность/целостность/доступность) ПДн или к снижению уровня защищенности ПДн;

– нарушение заданного уровня безопасности ПДн (конфиденциальность/ целостность/доступность).

В ходе разбирательства необходимо провести разработку и принятие мер по предотвращению возможных негативных последствий подобных нарушений.

По окончании разбирательства необходимо провести разработку (доработку) и принятие мер по предотвращению повторения подобных нарушений.

Для проведения разбирательства инцидентов утечки ПДн необходимо разработать Регламент проведения расследования утечки персональных данных.