МБОУ «Ардинская средняя общеобразовательная школа»

УТВЕРЖДАЮ
Директор
МБОУ «Ардинская средняя
общеобразовательная школа»
_____ В.П. Романова
«06» 09 2012 г.

ПОЛОЖЕНИЕ
по организации и проведению работ по обеспечению безопасности персональных данных при их обработке МБОУ «Ардинская средняя общеобразовательная школа»

с. Арда
2012

Содержание

1. Назначение документа 3
2. Основные понятия, термины и определения 4
3. Общие положения 6
4. Организация работ по обеспечению безопасности персональных данных 6
5. Выполнение работ по обеспечению безопасности персональных данных 8
6. Контроль выполнения работ по обеспечению безопасности персональных данных ... 12
7. Совершенствование системы защиты персональных данных 13

1. Назначение документа

Положение по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в МБОУ «Ардинская средняя общеобразовательная школа» (далее – Положение) разработано в целях выполнения требований законодательства Российской Федерации в области обеспечения безопасности персональных данных.

Настоящее Положение определяет содержание и порядок осуществления мероприятий по обеспечению безопасности персональных данных в МБОУ «Ардинская средняя общеобразовательная школа» (далее по тексту – Учреждение).

Настоящий документ учитывает положения основных нормативных правовых актов в области защиты персональных данных, а именно:

- Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных»;
- Постановления Правительства Российской Федерации от 17 ноября 2007 года № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Постановления Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Приказа ФСТЭК России, ФСБ России, Мининформсвязи России от 13 февраля 2008 года № 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных»;
- Приказа ФСТЭК России от 5 февраля 2010 года № 58 «Об утверждении положения о методах и способах защиты информации в информационных системах персональных данных»;
- Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной заместителем директора ФСТЭК России 15 февраля 2008 года;
- Методики определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной заместителем директора ФСТЭК России 14 февраля 2008 года;
- Методических рекомендаций по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации, утвержденных 8 Центром ФСБ России от 21 февраля 2008 года № 149/54-144;
- Типовых требований 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, утвержденных руководством 8 Центра ФСБ России 21 февраля 2008 года № 149/6/6-622;
- Положения об обработке персональных данных в МБОУ «Ардинская средняя общеобразовательная школа» и иных нормативных правовых актов Российской Федерации.

Плановая актуализация настоящего Положения проводится не реже одного раза в год. Внеплановая актуализация проводится при возникновении одного из следующих условий:

- изменение целей и (или) состава обрабатываемых персональных данных;
- возникновение условий, существенно влияющих на процессы обработки персональных данных и не регламентированных настоящим документом;
- по результатам контрольных мероприятий и проверок органом исполнительной власти Российской Федерации, выявивших несоответствия требованиям по обеспечению безопасности персональных данных;
- при появлении новых требований к обеспечению безопасности персональных данных со стороны законодательства Российской Федерации и органов исполнительной власти Российской Федерации.

Ответственным за пересмотр настоящего Положения и составление рекомендаций по его изменению является Администратор информационной безопасности Учреждения.

Все работники Учреждения, допущенные к работе с персональными данными, в обязательном порядке должны быть ознакомлены с настоящим Положением под роспись.

Настоящее Положение вступает в силу с момента его утверждения. Все изменения в Положение вносятся приказом директора Учреждения.

2. Основные понятия, термины и определения

В настоящем Положении используются следующие понятия, термины и определения:

информация – сведения (сообщения, данные) независимо от формы их представления;

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

Учреждение – юридическое лицо (МБОУ «Ардинская средняя общеобразовательная школа»), самостоятельно или совместно с другими лицами организующее и (или) осуществляющее обработку персональных данных, а также определяющее цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

субъекты персональных данных – работники Учреждения, воспитанники Учреждения, обучающиеся Учреждения и другие лица, персональные данные которых обрабатывает Учреждение;

работник – физическое лицо (субъект персональных данных), состоящее или состоявшее в трудовых отношениях с Учреждением, в том числе уволенные работники;

воспитанник – физическое лицо дошкольного возраста (субъект персональных данных), воспитывающееся и обучающееся в Учреждении, в том числе лица, готовящиеся к поступлению в Учреждение и лица воспитывавшиеся и обучавшиеся в Учреждении.

обучающийся – физическое лицо (субъект персональных данных), получающее, получившее или собирающееся получить общее образование в МБОУ «Ардинская средняя общеобразовательная школа»;

другие лица – физические лица (субъекты персональных данных), законные представители физических лиц, не относящиеся к категории работников, воспитанников и обучающихся, персональные данные которых обрабатывает Учреждение (кандидаты на замещение вакантных должностей, граждане, обращающиеся с заявлением, жалобами, предложениями; близкие родственники (законные представители) работников, близкие

родственники (законные представители) воспитанников; близкие родственники (законные представители) обучающихся; студенты учебных заведений, проходящие практику);

обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых Учреждением с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

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

распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

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

доступ к информации – возможность получения информации, содержащей персональные данные и ее использования;

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

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

уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;

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

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

конфиденциальность персональных данных – обязательное для соблюдения работниками Учреждения, иным получившим доступ к персональным данным лицами требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания;

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

информационно-телекоммуникационная сеть – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники;

информационные технологии – процессы, методы поиска, сбора, хранения,

обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

3. Общие положения

В соответствии с положениями Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» Учреждение является оператором персональных данных.

Учреждением осуществляется обработка персональных данных следующих категорий субъектов персональных данных: работников, воспитанников, обучающихся и других лиц, данные которых получены Учреждением в процессе осуществления своей деятельности.

Обработка персональных данных в Учреждении проводится с целью и в сроки, указанные в Перечне основных категорий персональных данных, обрабатываемых в Учреждении.

Обработка персональных данных осуществляется Учреждением с использованием средств автоматизации и без использования таких средств.

Действие Положения распространяется на информационные ресурсы Учреждения, содержащие персональные данные субъектов персональных данных. Информационными ресурсами Учреждения, содержащими персональные данные субъектов персональных данных являются:

- бумажные носители;
- электронные носители;
- информационные системы персональных данных;
- информационно-телекоммуникационные сети и иные информационные системы.

4. Организация работ по обеспечению безопасности персональных данных

Под организацией работ по обеспечению безопасности персональных данных в Учреждении понимается формирование и всестороннее обеспечение реализации совокупности согласованных по целям, задачам, месту и времени организационных и технических мероприятий, направленных на минимизацию как непосредственного, так и опосредованного ущерба от реализации угроз безопасности персональных данных и осуществляемых в целях:

- предотвращения возможных (потенциальных) угроз безопасности персональных данных;
- нейтрализации и или парирования реализуемых угроз безопасности персональных данных;
- ликвидации последствий реализации угроз безопасности персональных данных.

Организация работ по обеспечению безопасности персональных данных Учреждением должна осуществляться в соответствии с действующими нормативными правовыми актами и разработанными для этих целей организационно-распорядительными документами по защите персональных данных в Учреждении.

В целях исполнения требований настоящего Положения по организации работ по обеспечению безопасности персональных данных, директор утверждает План

мероприятий по обеспечению безопасности персональных данных, обрабатываемых Учреждением (далее – План мероприятий).

Задачи по приведению Учреждения в соответствие с требованиями законодательства Российской Федерации в области защиты персональных данных, указанные в Плане мероприятий, возлагаются на специально создаваемую для этих целей комиссию.

В случаях, когда Учреждение на основании договора поручает обработку персональных данных другому лицу (сторонней организации), необходимо выполнить одно из следующих условий:

- в тексте договора в требованиях к контрагенту прописать обязанность обеспечения контрагентом безопасности и конфиденциальности персональных данных;
- в случае невозможности или нецелесообразности изменения текста договора оформить дополнительное соглашение к договору или соглашение о конфиденциальности, в которых прописать обязанность обеспечения контрагентом конфиденциальности персональных данных и безопасности персональных данных при их обработке.

Работы по приведению Учреждения в соответствие с требованиями законодательства Российской Федерации ведутся по двум направлениям: обеспечение безопасности персональных данных, обрабатываемых без использования средств автоматизации (неавтоматизированная обработка), и обеспечение безопасности персональных данных с использованием средств автоматизации (автоматизированная обработка).

Работы по обеспечению безопасности персональных данных, обрабатываемых без использования средств автоматизации, ведутся по следующим направлениям:

- определение перечня лиц, осуществляющих неавтоматизированную обработку персональных данных в Учреждении;
- информирование работников Учреждения об установленных в Учреждении правилах обработки персональных данных и требований по их защите, повышение осведомленности в вопросах обеспечения безопасности персональных данных;
- учет и защита носителей персональных данных;
- разграничение доступа к носителям персональных данных;
- уничтожение персональных данных.

Организация и выполнение мероприятий по обеспечению безопасности персональных данных, обрабатываемых с использованием средств автоматизации, осуществляются в рамках системы защиты персональных данных в информационной системе персональных данных (далее – СЗПДн), развертываемой в ИСПДн в процессе ее создания или модернизации.

СЗПДн представляет собой совокупность организационных мер и технических средств защиты информации, а также используемых в ИСПДн информационных технологий, функционирующих в соответствие с определенными целями и задачами обеспечения безопасности персональных данных.

Система защиты персональных данных должна являться неотъемлемой составной частью каждой вновь создаваемой ИСПДн Учреждения.

Для существующих ИСПДн, в которых в процессе их создания не были предусмотрены меры по обеспечению безопасности персональных данных, должен быть проведен комплекс организационных и технических мероприятий по разработке и внедрению СЗПДн.

Структура, состав и основные функции СЗПДн определяются в соответствии с классом ИСПДн и моделью угроз безопасности персональных данных при их обработке в ИСПДн.

Проводимые в Учреждении мероприятия по обеспечению безопасности персональных данных учитываются в Журнале по учету мероприятий по контролю обеспечения защиты персональных данных в Учреждении.

5. Выполнение работ по обеспечению безопасности персональных данных

В ходе выполнения работ по обеспечению безопасности персональных данных в Учреждении, приказом директора Учреждения назначаются:

– уполномоченное лицо, ответственное за организацию обработки персональных данных;

– уполномоченное(ые) лицо(а), ответственное(ые) за обработку персональных данных;

– уполномоченное лицо, ответственное за проведение мероприятий по обеспечению безопасности персональных данных и поддержание необходимого уровня информационной безопасности (администратор информационной безопасности);

– уполномоченное(ые) лицо(а), ответственное(ые) за установку, настройку и обслуживание средств защиты информации, применяемых в Учреждении для обеспечения безопасности персональных данных, а также за организацию и проведение инструктажа работников по основам информационной безопасности при работе с персональными данными.

Указанные лица исполняют свои обязанности по обеспечению безопасности обрабатываемых персональных данных в соответствии с требованиями своих должностных инструкций и иных нормативных правовых актов Российской Федерации и Учреждения.

В целях оценки уровня защищенности обрабатываемых в Учреждении персональных данных и своевременного устранения несоответствий требованиям законодательства Российской Федерации в области защиты персональных данных в Учреждении не реже одного раза в год должен проводиться контроль за соблюдением требований по обеспечению безопасности персональных данных (реализуется путем внутренних проверок и аудитов). При проведении контроля осуществляется анализ изменений процессов защиты персональных данных.

Анализ изменений проводится по следующим основным направлениям:

– перечень лиц (подразделений), участвующих в обработке персональных данных, степень их участия в обработке персональных данных и характер взаимодействия между собой;

– перечень и объем обрабатываемых персональных данных;

– цели обработки персональных данных;

– процедуры сбора, записи, систематизации, накопления, хранения, уточнения (обновления, изменения), извлечения, использования, передачи (распространения, предоставления, доступа), обезличивания, блокирования, удаления и уничтожения персональных данных;

– способы обработки персональных данных (автоматизированная, неавтоматизированная);

– перечень сторонних организаций, в том числе государственных регулирующих органов, в рамках отношений с которыми осуществляется передача

персональных данных;

– перечень программно-технических средств, используемых для обработки персональных данных;

– конфигурация и топология ИСПДн в целом и ее отдельных компонентов, физические, функциональные и технологические связи как внутри этих систем, так и с другими системами различного уровня и назначения;

– способы физического подключения и логического взаимодействия компонентов ИСПДн, способы подключения к сетям связи общего пользования и международного информационного обмена с определением пропускной способности линий связи;

– режимы обработки персональных данных в ИСПДн в целом и в отдельных компонентах;

– состав используемого комплекса средств защиты персональных данных и механизмов идентификации, аутентификации и разграничения прав доступа пользователей ИСПДн на уровне операционных систем, баз данных и прикладного программного обеспечения;

– перечень организационно-распорядительной документации, определяющей порядок обработки и защиты персональных данных в Учреждении:

– физические меры защиты персональных данных, организация пропускного режима.

Результаты анализа изменений используются для оценки корректности требований по обеспечению безопасности персональных данных, обрабатываемых с использованием средств автоматизации и без использования таких средств и при необходимости их уточнения.

В Учреждении должен вестись учет действий, совершаемых с персональными данными в ИСПДн работниками Учреждения.

Доступ к персональным данным регламентируется Положением о разграничении прав доступа к обрабатываемым персональным данным в МБОУ «Ардинская средняя общеобразовательная школа».

Работники Учреждения, участвующие в обработке персональных данных, должны быть проинформированы:

– о факте обработки ими персональных данных – реализуется путем ознакомления лиц, обрабатывающих персональных данных с Разрешительной системой допуска сотрудников Учреждения, допущенных к обработке персональных данных;

– о категориях обрабатываемых персональных данных – реализуется путем ознакомления с утвержденным Перечнем персональных данных, обрабатываемых Учреждением;

– о правилах осуществления обработки персональных данных – реализуется путем ознакомления под роспись с организационно-распорядительными документами Учреждения, регламентирующими процессы обработки персональных данных;

– о правилах обеспечения безопасности персональных данных, обрабатываемых Учреждением.

Неавтоматизированная обработка персональных данных должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения материальных носителей и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.

В Учреждении должен вестись учет носителей персональных данных.

Фиксация персональных данных должна осуществляться на отдельных материальных носителях (отдельных документах). Персональные данные должны

отделяться от иной информации.

Фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо несовместимы, не допускается. В случае, если на одном материальном носителе все же зафиксированы персональные данные, цели обработки которых несовместимы, должны быть приняты меры по обеспечению раздельной обработки персональных данных, в частности:

– при необходимости использования или предоставления определенных персональных данных осуществляется копирование персональных данных, подлежащих предоставлению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных – например, копирование части страницы, содержащей персональных данных, которые необходимо использовать, предварительно закрыв остальную часть страницы чистым листом бумаги, либо копирование только необходимых страниц сшитого документа;

– при необходимости уничтожения или блокирования части персональных данных, уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию – например, копирование (в резерв) только необходимой части страницы, закрыв оставшуюся часть чистым листом бумаги.

В Учреждении должен осуществляться мониторинг фактов несанкционированного доступа к персональным данным и применяться соответствующие меры при их обнаружении. Мониторинг осуществляется Администратором информационной безопасности.

Администратором информационной безопасности Учреждения должен осуществляться контроль за принимаемыми мерами по обеспечению безопасности персональных данных.

При обработке персональных данных Учреждение должно иметь возможность и средство для восстановления персональных данных, при их модификации или уничтожении вследствие несанкционированного доступа к ним.

В Учреждении должен быть определен перечень помещений, используемых для обработки персональных данных. При этом организация режима безопасности, охрана этих помещений должны обеспечивать сохранность носителей персональных данных, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц, в том числе работников Учреждения, не допущенных к обработке персональных данных в Учреждении.

Приказом директора Учреждения устанавливается контролируемая зона Учреждения.

Технические средства, позволяющие осуществлять обработку персональных данных, размещаются в пределах контролируемой зоны.

Пользователи ИСПДн должны обеспечивать сохранность съемных носителей, содержащих персональные данные. В случае утраты носителя, пользователи должны немедленно сообщить об этом Администратору информационной безопасности.

Если при работе с персональными данными работнику Учреждения необходимо покинуть рабочее место, материальные носители персональных данных должны быть защищены от неконтролируемого доступа к ним. Для этого материальные носители запираются в отведенных для этого шкафах или сейфах.

В случае достижения цели обработки персональных данных Учреждение прекращает обработку персональных данных или обеспечивает ее прекращение (если

обработки персональных данных осуществляется другим лицом, действующим по поручению Учреждения) и уничтожает персональные данные или обеспечивает их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Учреждения) в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных.

Проведение работ по созданию (модернизации) СЗПДн Учреждения включает следующие стадии:

- предпроектная стадия;
- стадия проектирования;
- стадия реализации СЗПДн;
- стадия ввода в действие СЗПДн.

На предпроектной стадии проводится классификация ИСПДн, формируется модель угроз безопасности персональных данных при их обработке в ИСПДн, разрабатывается техническое задание на СЗПДн.

Классификация ИСПДн осуществляется в соответствии с требованиями Приказа ФСТЭК России, ФСБ России, Мининформсвязи России от 13 февраля 2008 года № 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных».

В связи с тем, что в ИСПДн Учреждения помимо обеспечения конфиденциальности обрабатываемых персональных данных требуется обеспечить целостность и доступность персональных данных, ИСПДн Учреждения является специальными информационными системами. ИСПДн Учреждения указаны в Перечне информационных систем персональных данных Учреждения.

Класс ИСПДн оформляется соответствующим актом.

Модель угроз безопасности персональных данных при их обработке в ИСПДн формируется на основании руководящих документов ФСТЭК России и ФСБ России.

Перечень актуальных угроз формируется для каждой ИСПДн Учреждения с учетом условий функционирования ИСПДн и особенностей обработки персональных данных.

По итогам классификации ИСПДн и результатам определения актуальных угроз безопасности персональных данных формируются требования по обеспечению безопасности персональных данных, обрабатываемых в ИСПДн. Данные требования оформляются в виде технического задания на СЗПДн.

Стадия проектирования СЗПДн включает разработку СЗПДн в составе ИСПДн, в именно разработку разделов задания и проекта проведения по созданию (модернизации) СЗПДн в соответствии с требованиями технического задания.

Стадия реализации СЗПДн включает:

- закупку совокупности используемых в СЗПДн сертифицированных технических, программных и программно-технических средств защиты информации и их установку;
- определение подразделений и назначение лиц, ответственных за эксплуатацию средств защиты информации с их обучением;
- приемо-сдаточные испытания средств защиты информации по результатам опытной эксплуатации.

На стадии ввода в действие СЗПДн осуществляются:

- предварительные испытания средств защиты информации в комплексе с другими техническими и программными средствами;
- устранение несоответствий по итогам предварительных испытаний;
- опытная эксплуатация средств защиты информации в комплексе с другими техническими и программными средствами в целях проверки их работоспособности в

составе ИСПДн.

В процессе функционирования ИСПДн может осуществляться модернизация СЗПДн. В обязательном порядке модернизация проводится в случае, если:

– произошло изменение номенклатуры обрабатываемых персональных данных, влекущее за собой изменение класса ИСПДн;

– произошло изменение номенклатуры и (или) актуальности угроз безопасности персональных данных;

– произошло изменение номенклатуры обрабатываемых персональных данных, влекущее за собой изменение класса ИСПДн;

– произошло изменение номенклатуры и или актуальности угроз безопасности персональных данных;

– изменилась структура ИСПДн или технические особенности ее построения (изменился состав или структура программного обеспечения, технических средств обработки персональных данных, топологии ИСПДн и т.п.).

При автоматизированной обработке персональных данных в Учреждении должны соблюдаться следующие меры:

– разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) и защиты информации;

– регистрация действий пользователей и обслуживающего персонала, контроль доступа и действий пользователей, обслуживающего персонала и посторонних лиц;

– резервирование технических средств, дублирование массивов и носителей информации;

– использование защищенных каналов связи;

– предотвращение внедрения в информационные системы вредоносных программ (программ-вирусов) и программных закладок.

Ремонтно-восстановительные работы технических средств обработки информации проводятся под контролем и в присутствии Администратора информационной безопасности с привлечением Администратора ИСПДн . В случае необходимости ремонт технических средств может быть проведен с привлечением сторонних специалистов на договорной основе с составлением актов выполненных работ.

Руководители подразделений, в которых происходит обработка персональных данных, являются лицами, ответственными за соблюдение требований Положения об обработке персональных данных в Учреждении и других установленных Учреждением требований.

6. Контроль выполнения работ по обеспечению безопасности персональных данных

Контроль выполнения работ по обеспечению безопасности персональных данных в Учреждении (далее – Контроль) осуществляется путем проведения периодических контрольных проверок и аудитов по фактам произошедших инцидентов информационной безопасности.

В рамках проведения контрольных мероприятий выполняется:

– проверка наличия и актуальности планов, регистрационных журналов, актов, договоров, отчетов, протоколов и других свидетельств выполнения мероприятий по обеспечению безопасности персональных данных за истекший период;

– проверка осведомленности и соблюдения персоналом требований к обеспечению безопасности персональных данных;

– проверка соответствия перечня лиц, которым предоставлен доступ к персональным данным, фактическому состоянию;

– проверка наличия и исправности функционирования технических средств защиты информации, используемых для обеспечения безопасности персональных данных, в соответствии с требованиями эксплуатационной и технической документации;

– инструментальная проверка соответствия настроек технических средств защиты информации требованиям к обеспечению безопасности персональных данных (при необходимости);

– проверка соответствия изделий угроз для информационных систем персональных данных условиям функционирования данных систем;

– проверка соответствия организационно-распорядительной документации по обеспечению безопасности персональных данных действующим требованиям законодательства Российской Федерации, руководящих документов ФСБ России, ФСТЭК России.

Все собранные в ходе проведения контрольных мероприятий свидетельства и сделанные по их результатам заключения должны быть зафиксированы документально.

Контрольные мероприятия проводятся как периодически в соответствии с планом, так и внепланово по решению директором Учреждения и в случае возникновения инцидентов информационной безопасности.

Внутренние проверки в Учреждении в обязательном порядке проводятся в случае выявления следующих фактов:

– нарушение конфиденциальности, целостности, доступности персональных данных;

– халатность и несоблюдение требований к обеспечению безопасности персональных данных;

– несоблюдение условий хранения носителей персональных данных;

– использование средств защиты информации, которые могут привести к нарушению заданного уровня безопасности (конфиденциальность/целостность/доступность) персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных.

Задачами внутренней проверки являются:

– установление обстоятельств нарушения, в том числе времени, места и способа его совершения;

– установление лиц, непосредственно виновных в данном нарушении;

– выявление причин и условий, способствовавших нарушению.

7. Совершенствование системы защиты персональных данных

Ежегодно приказом директора Учреждения формируется комиссия, которая составляет отчет о проделанных мероприятиях по выполнению плана работ по обеспечению безопасности персональных данных, обрабатываемых Учреждением вместе с перечнем предложений по совершенствованию системы защиты персональных данных.

Необходимость реализации мероприятий по совершенствованию системы защиты персональных данных может быть обусловлена:

– результатами проведенных аудитов и контрольных мероприятий;

– изменениями федерального законодательства в области персональных данных;

– изменениями структуры процессов обработки персональных данных Учреждением;

– результатами анализа инцидентов информационной безопасности;

– результатами мероприятий по контролю и надзору за обработкой персональных данных, проводимых уполномоченными органами;

– жалоб и запросов субъектов персональных данных.

На основании решения, принятого директором Учреждения по результатам рассмотрения ежегодного отчета и предложений по совершенствованию системы защиты персональных данных, комиссия составляет план работ по обеспечению безопасности персональных данных, обрабатываемых Учреждением на следующий год.