

УТВЕРЖДЕНО

Приказом № 148§1- од от 05.10.2021 г.

Директор ГБОУ СОШ

с. Кротково

Т.В.Клюшина



ПОЛОЖЕНИЕ

**об обеспечении безопасности персональных данных,
обрабатываемых в информационных системах персональных данных
государственного бюджетного общеобразовательного учреждения
Самарской области средней общеобразовательной школе
с. Кротково муниципального района Похвистневский
Самарской области**

1. Основные термины и определения

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

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

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых 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;

Основные технические средства и системы – технические средства и системы, а также их коммуникации, используемые для обработки, хранения и передачи персональных данных;

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

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

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

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

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.

2. Общие положения

Настоящее Положение об обеспечении безопасности персональных данных, обрабатываемых в информационных системах персональных данных ГБОУ СОШ с.Кротково (далее – Положение), разработано в соответствии с законодательством Российской Федерации о персональных данных (далее – ПДн) и нормативными правовыми актами (методическими документами) федеральных органов исполнительной власти по вопросам безопасности ПДн при их обработке в информационных системах персональных данных (далее – ИСПДн).

Настоящее Положение определяет состав и содержание организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн.

Положение обязательно для исполнения всеми работниками ГБОУ СОШ с.Кротково (далее – Учреждения), непосредственно осуществляющими защиту ПДн, обрабатываемых в ИСПДн.

3. Цели и задачи обеспечения безопасности персональных данных

Основной целью обеспечения безопасности ПДн, при их обработке в ИСПДн, является защита ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн.

Задачей, которую необходимо решить для достижения поставленной цели, является обеспечение безопасности ПДн при их обработке в ИСПДн с помощью системы

защиты персональных данных (далее – СЗПДн), нейтрализующей актуальные угрозы, определенные в соответствии с частью 5 статьи 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

СЗПДн в себя организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности ПДн и информационных технологий, используемых в ИСПДн.

4. Основные принципы построения системы защиты информации

СЗПДн основывается на следующих принципах:

- системности;
- комплексности;
- непрерывности защиты;
- разумной достаточности;
- гибкости;
- простоты применения средств защиты информации (далее – СЗИ).

Принцип системности – предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения безопасности ПДн.

Принцип комплексности – предполагает, что СЗПДн должна включать совокупность объектов защиты, сил и средств, принимаемых мер, проводимых мероприятий и действий по обеспечению безопасности ПДн от возможных угроз всеми доступными законными средствами, методами и мероприятиями.

Принцип непрерывности защиты – это процесс обеспечения безопасности ПДн, осуществляемый руководством, ответственным за обеспечение безопасности ПДн в ИСПДн и работниками всех уровней. Это не только и не столько процедура или политика, которая осуществляется в определенный отрезок времени или совокупность СЗИ, сколько процесс, который должен постоянно идти на всех уровнях внутри Учреждения, и каждый работник должен принимать участие в этом процессе.

Принцип разумной достаточности – предполагает соответствие уровня затрат на обеспечение безопасности ПДн ценности информационных ресурсов и величине возможного ущерба от их разглашения, утраты, утечки, уничтожения и искажения.

Принцип гибкости – СЗПДн должна быть способна реагировать на изменения внешней среды и условий осуществления своей деятельности.

Принцип простоты применения СЗИ – механизмы защиты должны быть интуитивно понятны и просты в применении. Применение СЗИ не должно быть связано со знанием каких-либо языков или требовать дополнительных затрат на её применение, а также не должно требовать выполнения рутинных малопонятных операций.

5. Основные мероприятия по обеспечению безопасности персональных данных

Для обеспечения защиты ПДн, обрабатываемых в ИСПДн, проводятся следующие мероприятия:

- определение ответственных лиц за обеспечение защиты ПДн;
- определение актуальных угроз безопасности ПДн;
- определение уровня защищенности ПДн;
- реализация правил разграничения доступа и введение ограничений на действия пользователей ИСПДн;
- ограничение доступа в помещения, где размещены основные технические средства и системы, позволяющие осуществлять обработку ПДн;
- учет и хранение съемных машинных носителей ПДн;
- организация резервирования и восстановления работоспособности программного обеспечения, баз данных ПДн и СЗИ;

- организация парольной защиты;
- организация антивирусной защиты;
- организация обновления программного обеспечения и СЗИ;
- использование СЗИ;
- использование средств шифровальной (криптографической) защиты информации (далее – СКЗИ);
- оценка эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию СЗПДн;
- обнаружение фактов несанкционированного доступа к ПДн и принятие мер;
- контроль за принимаемыми мерами по обеспечению безопасности ПДн.

Определение ответственных лиц за обеспечение безопасности ПДн

За вопросы обеспечения безопасности ПДн, обрабатываемых в ИСПДн, отвечают:

- Директор Учреждения.
- Ответственный за организацию обработки ПДн – работник, отвечающий за организацию и состояние процесса обработки ПДн.
- Ответственный за обеспечение безопасности ПДн в ИСПДн – работник, отвечающий за правильность использования и нормальное функционирование установленной СЗПДн.
- Администратор ИСПДн – работник, отвечающий за правильность использования и бесперебойное, стабильное функционирование установленных систем обработки ПДн.

Определение актуальных угроз безопасности ПДн

Актуальные угрозы безопасности ПДн, обрабатываемых в ИСПДн, определяются по результатам оценки возможностей (потенциала, оснащенности и мотивации) внешних и внутренних нарушителей, анализа возможных уязвимостей ИСПДн, возможных способов реализации угроз безопасности ПДн и последствий от нарушения свойств безопасности информации (конфиденциальности, целостности, доступности).

Для определения угроз безопасности ПДн и разработки «Модели угроз безопасности персональных данных» применяются методические документы, разработанные и утвержденные ФСТЭК России в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085.

Определение уровня защищенности ПДн

5.4.1. Уровень защищенности ПДн, обрабатываемых в ИСПДн, определяется, в соответствии с постановлением Правительства Российской Федерации от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и оформляется в виде «Акта об определения уровня защищенности персональных данных», форма которого приведена в Приложении 1 к настоящему Положению.

Определение класса защищенности ИСПДн

5.5.1. Класс защищенности ИСПДн определяется в соответствии с требованиями приказа ФСТЭК России № 21 от 18 февраля 2013г. «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

Реализация правил разграничения доступа и введение ограничений на действия пользователей ИСПДн

Реализация правил разграничения доступа, к ПДн, обрабатываемым в ИСПЛн, осуществляется в соответствии с «Положением о разрешительной системе доступа в информационных системах персональных данных ГБОУ СОШ с.Кротково», утвержденным приказом Директора Учреждения.

Основные технические средства и системы ИСПДн располагаются в помещениях, находящихся в пределах границы контролируемой зоны, определенной приказом Директора Учреждения, с максимальным удалением от её границ.

Доступ в помещения, в которых ведется обработка ПДн, осуществляется в соответствии с «Правилами доступа работников в помещения, в которых ведется обработка персональных данных в ГБОУ СОШ с.Кротково», утвержденными приказом Директора Учреждения.

Учет и хранение съемных машинных носителей ПДн

5.7.1. Работа со съемными машинными носителями ПДн в ИСПДн осуществляется в соответствии с «Инструкцией по обращению со съемными машинными носителями персональных данных в ГБОУ СОШ с.Кротково», утвержденным приказом Директора Учреждения.

Организация резервирования и восстановления работоспособности программного обеспечения, баз данных ПДн и СЗИ

5.8.1. Организация резервирования и восстановления работоспособности программного обеспечения, баз данных ПДн и СЗИ в ИСПДн осуществляется в соответствии с «Инструкцией по организации резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в информационных системах персональных данных ГБОУ СОШ с.Кротково», утвержденной приказом Директора Учреждения.

Организация парольной защиты

5.9.1. Организация парольной защиты в ИСПДн осуществляется в соответствии с «Инструкцией по парольной защите информации в ГБОУ СОШ с.Кротково», утвержденной приказом Директора Учреждения.

Организация антивирусной защиты

5.10.1. Организация антивирусной защиты в ИСПДн осуществляется в соответствии с «Инструкцией по организации антивирусной защиты информации в ГБОУ СОШ с.Кротково», утвержденной приказом Директора.

Организация обновления программного обеспечения и СЗИ

5.11.1. Организация обновления программного обеспечения и СЗИ в ИСПДн осуществляется в соответствии с «Инструкцией ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных ГБОУ СОШ с.Кротково» и «Инструкцией администратора информационных систем персональных данных ГБОУ СОШ с.Кротково», утвержденные приказом Директора Учреждения.

Применение СЗИ

Для обеспечения защиты ПДн, обрабатываемых в ИСПДн, применяются СЗИ, прошедшие оценку соответствия в форме обязательной сертификации на соответствие требованиям по безопасности информации, в соответствии со статьей 5 Федерального закона от 27 декабря 2002 №184-ФЗ «О техническом регулировании».

Все СЗИ, эксплуатационная и техническая документация к ним, учитываются и заносятся ответственным за обеспечение безопасности ПДн в ИСПДн в «Журнал учета средств защиты информации, эксплуатационной и технической документации к ним в ГБОУ СОШ с.Кротково», форма которого утверждена Приложением 2 к настоящему Положению.

Установка и настройка СЗИ в ИСПДн проводится в соответствии с эксплуатационной документацией на СЗПДн и документацией на СЗИ.

Использование СКЗИ

5.13.1. Для обеспечения защиты ПДн, обрабатываемых в ИСНДн, при их передаче по открытым каналам связи, применяются СКЗИ. Обращение с СКЗИ, эксплуатируемыми в ИСПДн, осуществляется в соответствии с «Инструкцией по обращению с шифровальными

(криптографическими) средствами защиты информации в ГБОУ СОШ с.Кротково», утвержденной приказом Директора Учреждения.

Оценка эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию СЗПДн

На этапах внедрения СЗПДн проводится оценка эффективности принимаемых мер по обеспечению безопасности ПДн, которая включает в себя:

- предварительные испытания СЗПДн;
- опытную эксплуатацию СЗПДн;
- анализ уязвимостей ИСПДн и принятие мер по их устранению;
- приемочные испытания СЗПДн.

Обнаружение фактов несанкционированного доступа к ПДн и принятие мер

Ответственному за обеспечение безопасности ПДн в ИСПДн или администратору ИСПДн должны сообщаться любые инциденты информационной безопасности, в которые входят:

- факты попыток и успешной реализации несанкционированного доступа в ИСПДн;
- факты попыток и успешной реализации несанкционированного доступа в помещения, в которых ведется обработка ПДн;
- факты сбоя или некорректной работы систем обработки ПДн;
- факты сбоя или некорректной работы СЗИ;
- факты разглашения ПДн, обрабатываемых в ИСПДн;
- факты разглашения информации о методах и способах защиты и обработки ПДн в ИСПДн.

Разбор инцидентов информационной безопасности проводится в соответствии с «Регламентом реагирования на инциденты информационной безопасности в информационных системах персональных данных ГБОУ СОШ с.Кротково», утвержденным приказом Директора Учреждения.

Контроль за принимаемыми мерами по обеспечению безопасности ПДн

5.16.1. Контроль за принимаемыми мерами по обеспечению безопасности ПДн осуществляется в соответствии с «Регламентом проведения внутреннего контроля соответствия обработки персональных данных в ГБОУ СОШ с.Кротково», утвержденным приказом Директора Учреждения.

6. Ответственность

Все работники, допущенные в установленном порядке к работе с ПДн, несут административную, материальную, уголовную ответственность в соответствии с действующим законодательством Российской Федерации за необеспечение сохранности и несоблюдение правил работы с ПДн.

Ответственность за доведение требований настоящего Положения до работников Учреждения и обеспечение мероприятий по их реализации несет ответственный за обеспечение безопасности ПДн в ИСПДн.

Приложение 1
к Положению об обеспечении
безопасности персональных данных,
обрабатываемых в информационных
системах персональных данных ГБОУ
СОШ с.Кротково

ФОРМА

АКТ

«___» 20___ г.

№ _____

Определения уровня защищенности
персональных данных
в информационной системе
персональных данных
«_____»
(наименование информационной системы)

Комиссия в составе:

Председатель:

Члены комиссии:

1. _____

2. _____

3. _____

на основании исходных данных об информационной системе персональных данных
«_____»
(наименование информационной системы)

(далее – ИСПДн) определила:

1. В ИСПДн обрабатываются _____ категории
(биометрические, специальные, иные, общедоступные)
персональных данных _____ субъектов персональных данных
(менее 100 000, более 100 000)
ГБОУ СОШ с.Кротково;
(не) являющимися работниками

2. ИСПДн располагается в пределах Российской Федерации;

3. Для ИСПДн актуальны угрозы 3 типа, не связанные с наличием
недокументированных (недекларированных) возможностей в системном и прикладном
программном обеспечении, используемом в ИСПДн.

в соответствии с постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении
требований к защите персональных данных при их обработке в информационных системах
персональных данных», установила необходимость обеспечения
уровня защищенности персональных данных.

(первого, второго, третьего, четвертого)

Председатель:

Члены комиссии: