

ПОЛОЖЕНИЕ
об обеспечении безопасности персональных данных,
обрабатываемых в информационных системах персональных данных
МБУ ДО «ЦДОД»

1. Термины и определения

- 1.1. Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.
- 1.2. Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).
- 1.3. 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.
- 1.4. Основные технические средства и системы – технические средства и системы, а также их коммуникации, используемые для обработки, хранения и передачи персональных данных.
- 1.5. 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.
- 1.6. Персональные данные – любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных);
- 1.7. Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.
- 1.8. Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.
- 1.9. 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

- 2.1. Настоящее Положение об обеспечении безопасности персональных данных, обрабатываемых в информационных системах персональных данных МБУ ДО «ЦДОД» (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).

- 2.2. Настоящее Положение определяет состав и содержание организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн.
- 2.3. Положение обязательно для исполнения всеми работниками МБУ ДО «ЦДОД» (далее – Учреждение), непосредственно осуществляющими защиту ПДн, обрабатываемых в ИСПДн.

3. Цели и задачи обеспечения безопасности персональных данных

- 3.1. 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.
- 3.2. 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 июля 2006г. №152-ФЗ «О персональных данных».
- 3.3. СЗПДн включает 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

- 4.1. СЗПДн основывается на следующих принципах:
 - системности;
 - комплексности;
 - непрерывности защиты;
 - разумной достаточности;
 - гибкости;
 - простоты применения средств защиты информации (далее – СЗИ).
- 4.2. Принцип системности – предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения безопасности ПДн.
- 4.3. 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.
- 4.4. 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.

- 4.5. 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.
- 4.6. Принцип гибкости – СЗПДн должна быть способна реагировать на изменения внешней среды и условий осуществления своей деятельности.
- 4.7. 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

- 5.1. 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;
 - планирование мероприятий по защите ПДн в ИСПДн;
 - управление (администрирование) СЗПДн;
 - управление конфигурацией ИСПДн и СЗПДн;
 - реагирование на инциденты;
 - информирование и обучение персонала ИСПДн.
- 5.2. Определение ответственных лиц за обеспечение безопасности ПДн
 - 5.2.1. За вопросы обеспечения безопасности ПДн, обрабатываемых в ИСПДн, отвечают:
 - Директор.
 - 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.
- 5.3. Определение актуальных угроз безопасности ПДн в ИСПДн
- 5.3.1. 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).
- 5.3.2. 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.
- 5.4. Определение уровня защищенности ПДн
- 5.4.1. Уровень защищенности ПДн, обрабатываемых в ИСПДн, определяется в соответствии с постановлением Правительства Российской Федерации от 1 ноября 2012 г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и оформляется в виде «Акта об определении уровня защищенности персональных данных».
- 5.5. Реализация правил разграничения доступа и введение ограничений на действия пользователей ИСПДн
- 5.5.1. Реализация правил разграничения доступа, к ПДн, обрабатываемым в ИСПДн, осуществляется в соответствии с «Положением о разрешительной системе доступа в информационных системах персональных данных МБУ ДО «ЦДОД», утвержденным приказом Директора Учреждения.
- 5.5.2. 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.
- 5.5.3. Доступ в помещения, в которых ведется обработка ПДн, осуществляется в соответствии с «Правилами доступа работников в помещения, в которых ведется обработка персональных данных в МБУ ДО «ЦДОД», утвержденными приказом Директора Учреждения.
- 5.6. Учет и хранение съемных машинных носителей ПДн
- 5.6.1. Работа со съемными машинными носителями ПДн в ИСПДн осуществляется в соответствии с «Порядком обращения со съемными машинными носителями персональных данных в МБУ ДО «ЦДОД», утвержденным приказом генерального Директора Учреждения.
- 5.7. Организация резервирования и восстановления работоспособности программного обеспечения, баз данных ПДн и СЗИ.

- 5.7.1. 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 МБУ ДО «ЦДОД», утвержденной приказом Директора Учреждения.
- 5.8. Организация парольной защиты
- 5.8.1. Организация парольной защиты в ИСПДн осуществляется в соответствии с «Инструкцией по парольной защите информации в МБУ ДО «ЦДОД», утвержденной приказом Директора Учреждения.
- 5.9. Организация антивирусной защиты
- 5.9.1. Организация антивирусной защиты в ИСПДн осуществляется в соответствии с «Инструкцией по организации антивирусной защиты в МБУ ДО «ЦДОД», утвержденной приказом Директора Учреждения.
- 5.10. Организация обновления программного обеспечения и СЗИ
- 5.10.1. Организация обновления программного обеспечения и СЗИ в ИСПДн осуществляется в соответствии с «Инструкцией ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных МБУ ДО «ЦДОД» и «Инструкцией администратора информационных систем персональных данных МБУ ДО «ЦДОД», утвержденные приказом Директора Учреждения.
- 5.11. Применение СЗИ
- 5.11.1. 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 г. №184-ФЗ «О техническом регулировании».
- 5.11.2. Установка и настройка СЗИ в ИСПДн проводится в соответствии с эксплуатационной документацией на СЗПДн и документацией на СЗИ.
- 5.12. Использование СКЗИ
- 5.12.1. Для обеспечения защиты ПДн, обрабатываемых в ИСПДн, при их передаче по открытым каналам связи, применяются СКЗИ. Обращение с СКЗИ, эксплуатируемыми в ИСПДн, осуществляется в соответствии с «Инструкцией по обращению со средствами криптографической защиты информации в МБУ ДО «ЦДОД», утвержденной приказом Директора Учреждения.
- 5.13. Оценка эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию СЗПДн
- 5.13.1. 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.
- 5.14. Обнаружение фактов несанкционированного доступа к ПДн и принятие мер

5.14.1. 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.

5.14.2. Разбор инцидентов информационной безопасности проводится в соответствии с «Регламентом реагирования на инциденты информационной безопасности в информационных системах персональных данных МБУ ДО «ЦДОД», утвержденным приказом Директора Учреждения.

5.15. Контроль за принимаемыми мерами по обеспечению безопасности ПДн

5.15.1. Контроль за принимаемыми мерами по обеспечению безопасности ПДн осуществляется в соответствии с «Регламентом проведения внутреннего контроля соответствия обработки персональных данных в МБУ ДО «ЦДОД», утвержденным приказом Директора Учреждения.

6. Ответственность

- 6.1. 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.
- 6.2. Ответственность за доведение требований настоящего Положения до работников Учреждения и обеспечение мероприятий по их реализации несет ответственный за обеспечение безопасности ПДн в ИСПДн.

