МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ДОПОЛНИТЕЛЬНОГО ОБРАЗОВАНИЯ СТАРОДУБСКИЙ ЦЕНТР ДЕТСКОГО ТВОРЧЕСТВА

Подписан: МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ДОПОЛНИТЕЛЬНОГО ОБРАЗОВАНИЯ СТАРОДУБСКИЙ ЦЕНТР ДЕТСКОГО ТВОРЧЕСТВА
DN: C=RU, S=Брянская область, STREET="ул. Краснооктябрьская, д. 30", L=Стародуб, T=Директор, O=МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ДОПОЛНИТЕЛЬНОГО ОБРАЗОВАНИЯ СТАРОДУБСКИЙ ЦЕНТР ДЕТСКОГО ТВОРЧЕСТВА, ОГРН=1023200978371, СНИЛС=02948425983, ИНН ЮЛ=3227004245, ИНН=322702067811, E=mbouscdt.1012@yandex.ru, G=Татьяна Анатольевна, SN=Татьянок, CN=МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ДОПОЛНИТЕЛЬНОГО ОБРАЗОВАНИЯ СТАРОДУБСКИЙ ЦЕНТР ДЕТСКОГО ТВОРЧЕСТВА
Основание: я подтверждаю этот документ своей удостоверяющей подписью
Местоположение: место подписания
Дата: 2025.02.17 13:42:27+03'00'
Foxit Reader Версия: 10.1.1

Утверждаю
Приказ № 13 от 04.05.2017 года

Директор МБОУДО СЦДТ
_________________ Татьянок Т.А.

ПОЛОЖЕНИЕ
об организации и техническом обеспечении безопасности, обрабатываемых в информационных системах персональных данных работников МБОУДО СЦДТ

1. Общие положения

1.1. Настоящим Положением определяются мероприятия по организации и техническому обеспечению безопасности персональных данных (не криптографическими методами) при их обработке в информационных системах персональных данных работников МБОУДО СЦДТ.

1.2. Настоящее Положение разработано на основе Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» и в соответствии с Положением об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденным постановлением Правительства Российской Федерации от 17 ноября 2007 года № 781, иными нормативными актами, действующими на территории Российской Федерации, Брянской области.

1.3. Цель разработки Положения:

определение порядка проведения мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;

своевременного обнаружения фактов несанкционированного доступа к персональным данным;

недопущения воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;

возможности незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

постоянного контроля за обеспечением уровня защищенности.

Обеспечение безопасности персональных данных с использованием криптографических методов в настоящем Положении не рассматривается, Порядок организации и обеспечения указанных работ определяется в соответствии с нормативными документами Федеральной службы безопасности Российской Федерации.

1.4. Техническое обеспечение безопасности персональных данных (не криптографическими методами) при их обработке в информационных системах персональных данных работников СЦДТ возлагается на сотрудников СЦДТ

1.5. Настоящее Положение действует до замены его новым Положением.

1.6. Все изменения в Положение вносятся приказом.

2. Классификация информационных систем персональных данных СЦДТ

2.1. Классификация информационных систем персональных данных (далее – ИСПДн) осуществляется с учетом категорий и объема накапливаемых, обрабатываемых и распределяемых с их использованием персональных данных (далее – ПДн) с целью установления методов и способов защиты, необходимых для обеспечения безопасности ПДн. Состав и функциональное содержание методов и средств зависит от вида и степени ущерба, возникающего вследствие реализации угроз безопасности ПДн. При этом ущерб возникает за счет неправомерного или случайного уничтожения, изменения, блокирования, копирования, распространения ПДн или от иных неправомерных действий с ними. В зависимости от объекта, причинение ущерба которому, в конечном счете, вызывается неправомерными действиями с ПДн, рассматриваются два вида ущерба: непосредственный и опосредованный.

Непосредственный ущерб связан с причинением физического, материального, финансового или морального вреда непосредственно субъекту ПДн. Он возникает за счет незаконного использования (в том числе распространения) ПДн или за счет несанкционированной модификации этих данных и может проявляться в виде:

незапланированных и (или) непроизвольных финансовых или материальных затратах субъекта;

потери субъектом свободы действий вследствие шантажа и угроз, осуществляемых с использованием ПДн;

нарушение конституционных прав субъекта вследствие вмешательства в его личную жизнь путем осуществления контактов с ним по различным поводам без его на то желания (например – рассылка персонифицированных рекламных предложений и т.п.).

Опосредованный ущерб, связанный с причинением вреда обществу и (или) государству вследствие нарушения нормальной деятельности экономических, политических, военных, медицинских, правоохранительных, социальных, кредитно-финансовых и иных государственных органов, органов местного самоуправления, организаций различных форм собственности за счет неправомерных действий с ПДн.

2.2. Классификация ИСПДн проводится муниципальным учреждением Стародубский центр детского творчества, организующим и (или) осуществляющим обработку ПДн, а также определяющим цели и содержание обработки ПДн (операторами ИСПДн) в соответствии с Порядком проведения классификации информационных систем персональных данных, утвержденным приказом ФСТЭК России, ФСБ России и Мининформсвязи России от 13 февраля 2008 года № 55/86/20.

Результаты классификации информационных систем оформляются соответствующим актом оператора.

Класс информационной системы может быть пересмотрен:

по решению оператора на основе проведенных им анализа и оценки угроз безопасности персональных данных с учетом особенностей и (или) изменений конкретной информационной системы;

по результатам мероприятий по контролю за выполнением требований к обеспечению безопасности персональных данных при их обработке в информационной системе.

В целом обеспечение безопасности ПДн при их обработке в ИСПДн достигается реализацией совокупности организационных и технических мер, в интересах обеспечения безопасности ПДНн в обязательном порядке подлежат защите технические и программные средства, используемые при обработке ПДн, и носители информации.

3. Мероприятия по техническому обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных

3.1. В состав мероприятий по защите ПДн работников МБОУДО СЦДТ при их обработке в ИСПДн от несанкционированный действий (НСД) и неправомерных действий входят следующие мероприятия:

защита от НСД при однопользовательском режиме обработки ПДн;

защита от НСД при многопользовательском режиме обработки ПДн и равных правах доступа к ним субъектов доступа;

защита от НСД при многопользовательском режиме обработки ПДн и разных правах доступа;

защита информации при межсетевом взаимодействии ИСПДн;

антивирусная защита;

обнаружение вторжений.

3.2. Для ИСПДн СЦДТ при однопользовательском режиме обработки ПДн должны проводиться следующие мероприятия:

- защита входа в операционную систему паролем условно-постоянного действия, длиной не менее шести буквенно-цифровых символов;

- учет всех защищаемых носителей информации с помощью их любой маркировки и с занесением учетных данных в журнал (учетную карточку);

- обеспечение целостности программных средств защиты, а также неизменность программной среды;

- осуществление физической охраны ИСПДн (устройств и носителей информации), предусматривающей контроль доступа в помещения ИСПДн посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения ИСПДн и хранилище носителей информации;

- обеспечение операторов обработки ПДн, в обязательном порядке, съемными носителями (флеш – картами), обеспечивающими сохранность ПДн в копии, а также копий программных средств защиты информации, их периодическое обновление и контроль работоспособности;

- организация антивирусной защиты ИСПДн, с автоматическим режимом проверки при импорте или экспорте данных, периодическое обновление и контроль работоспособности;

- осуществление предотвращения попыток несанкционированного доступа к ИСПДн и регистрация их.