Муниципальное бюджетное учреждение дополнительного образования
«Детско-юношеский центр»

Приказ

17.04.2024 **№ 69 о.д.**

Об утверждении Положения об обеспечении
безопасности персональных данных

Во исполнение требований Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», приказа ФСТЭК России от 18 февраля 2013г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» и прочих нормативных документов по защите информации МБУ ДО ДЮЦ **приказываю:**

1.Утвердить и ввести в действие Положение об обеспечении безопасности персональных данных, обрабатываемых в информационных системах персональных данных МБУ ДО ДЮЦ (далее – Положение) (положение 1).

2.Ответственному за обеспечение безопасности персональных данных в информационных системах обеспечить выполнение требований Положения.

3.Требования Положения довести до работников, непосредственно осуществляющих защиту персональных данных в информационных системах персональных данных.

4.Контроль за исполнением настоящего Приказа оставляю за собой.

Директор Н.П.Шпенькова

Приложение 1
к приказу МБУ ДО ДЮЦ
от 17.04.2024 № 69 о.д

ПОЛОЖЕНИЕ
об обеспечении безопасности персональных данных,
обрабатываемых в информационных системах персональных данных
Муниципального бюджетного учреждения дополнительного образования
«Детско-юношеский центр»

1.Термины и определения

*Автоматизированная обработка персональных данны*х – 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

2.1.Настоящее Положение об обеспечении безопасности персональных данных, обрабатываемых в информационных системах персональных данных МБУ ДО ДЮЦ (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 ДЮЦ (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.

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;

–оценка эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию СЗПДн;

–обнаружение фактов несанкционированного доступа кПДн 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 Учреждения

–Ответственный за обеспечение безопасности ПДн в ИСПДн – работник, отвечающий за правильность использования и нормальное функционирование установленной СЗПДн.

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 определения 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 ДЮЦ (приложение 1).

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 ДЮЦ» (приложение 2).

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 ДЮЦ» (приложение 3).

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 СЗИв 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 ДЮЦ» (приложение 4).

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 ДЮЦ» (приложение 5)

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 ДЮЦ (приложение 6).

5.10. Организация обновления программного обеспечения и СЗИ

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

5.12.1.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.

5.13. Обнаружение фактов несанкционированного доступа к ПДн и принятие мер

5.13.1.Ответственному за обеспечение безопасности ПДн в 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.

5.13.2. Разбор инцидентов информационной безопасности проводится в соответствии с «Регламентом реагирования на инциденты информационной безопасности в информационных системах персональных данных МБУ ДО ДЮЦ (приложение 7).

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.

Приложение 1
к Положению об обеспечении безопасности
персональных данных, обрабатываемых в
информационных системах персональных
данных МБУ ДО ДЮЦ

ПОЛОЖЕНИЕ
о разрешительной системе доступа
в информационных системах персональных данных Муниципального бюджетного учреждения дополнительного образования «Детско-юношеский центр»

1.Общие положения

1.1. Настоящее Положение разработано в соответствии с Конституцией Российской Федерации, Федеральным законом «О персональных данных» от 27.07.2006 № 152-ФЗ, постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и другими нормативными документами.

1.2. Разрешительная система допуска к информационным системам персональных данных (далее –ИСПДн) муниципального бюджетного учреждения дополнительного образования «Детско-юошеский центр» (далее – Учреждение) представляет собой совокупность процедур оформления права субъектов на доступ к информационным ресурсам (объекты доступа) организации, содержащим персональные данные, и ответственных лиц, осуществляющих реализацию этих процедур.

1.3. Объектами доступа являются:

– документированная информация на бумажных носителях в виде отдельных документов или дел;

– информационные ресурсы в информационной системе в виде баз данных, библиотек, архивов и их копий на машинных носителях.

1.4. Субъектами доступа являются:

– работники Учреждения;

– юридические и физические лица.

1.5. Субъекты доступа несут персональную ответственность за соблюдение ими установленного в Учреждении порядка обеспечения защиты информационных ресурсов.

1.6. Ответственными лицами Учреждения, осуществляющими реализацию процедур оформления прав субъектов на доступ к информационным ресурсам, являются:

– руководитель;

– заместители руководителя;

– ответственный за обеспечение безопасности персональных данных (администратор безопасности).

2.Перечень используемых определений, обозначений и сокращений

АРМ – автоматизированное рабочее место.

ИБ – информационная безопасности.

ИС – информационная система.

ИСПДн – информационная система персональных данных.

3.Порядок формирования информационных ресурсов организации

3.1. Формирование информационных ресурсов на бумажных носителях осуществляется в учреждении и регламентируется внутренними документами Учреждения.

3.2. Информационные ресурсы, формируемые в ИС подразделяются на:

– сетевые ресурсы с доступом одной группы пользователей (ресурсы отдела);

– сетевые ресурсы с доступом нескольких групп пользователей (базы данных и т.п.);

– ресурсы общего пользования (справочно-информационные системы, библиотеки, каталоги и т.п.);

– сетевой ресурс почтового обмена;

– сетевые принтеры;

– ресурсы пользователя (сетевые или локальные).

4.Допуск к информационным ресурсам работников Учреждения

4.1. Допуск работников к информации, содержащей персональные данные, осуществляется в соответствии с занимаемой должностью и в объеме, необходимом для выполнения ими должностных обязанностей.

4.2. Допуск к персональным данным разрешается руководителем, только уполномоченным лицам с соблюдением требований Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных.

4.3. Допуск работника к информационным ресурсам ИСПДн, оформляется заявкой ответственному, которая предоставляется начальником соответствующего отдела после согласования с руководителем. В заявке указывается, к каким ресурсам и с какими правами (полномочиями) допустить конкретного работника.

4.4. Процедура предоставления (или изменения) прав доступа пользователя к ресурсам Учреждения инициируется заявкой курирующего работу сотрудника членом административно-управленческого персонала.

4.5. При наступлении момента прекращения срока действия полномочий пользователя (окончание договорных отношений, увольнение сотрудника) учетная запись должна немедленно блокироваться. Предпочтительно использовать механизмы автоматического блокирования учетных записей уволенных сотрудников, используя
соответствующие ИС.

При невозможности автоматического блокирования учетных записей, сотрудникам сопоставляются временные учетные записи (с фиксированным сроком действия), о чем делается отметка в заявке при ее исполнении и в обязательном порядке доводится до инициатора заявки. Допускается регистрация постоянных учетных записей при отсутствии механизмов автоматической блокировки. По окончании внесения изменений в заявке делается отметка о выполнении задания за подписями исполнителей.

В случае необходимости сохранения персональных документов (профайла пользователя) на АРМ сотрудника, после прекращения срока действия его полномочий, сотрудник (или его непосредственный руководитель) должен своевременно (не позднее, чем за 3 суток до момента прекращения срока действия своих полномочий) подать заявку на блокирование учетной записи пользователя с указанием срока хранения указанной информации. Заявка должна подаваться даже в случае применения механизмов

автоматической блокировки учетных записей уволенных сотрудников.
4.6. Исполненные заявки передаются АИБу, и хранятся в архиве в течение 5 лет с момента окончания предоставления доступа. В случае невозможности исполнения инициатору заявки направляется
мотивированный отказ с приложением Заявки.
4.7. Администратором безопасности (или ответственным лицом) проверяется соответствие требуемых прав доступа с реально необходимыми для выполнения должностных (функциональных) обязанностей данного работника.
4.8. Согласованная заявка является разрешением на допуск и основанием для регистрации пользователя в сети администратором ИСПДн.

5.Допуск к информационным ресурсам сторонних организаций, деятельность которых не связана с исполнением функций организации

5.1. К организациям, деятельность которых не связана с исполнением функций организации, могут относиться:
– правоохранительные органы;
– судебные органы;
– органы статистики;
– органы исполнительной и законодательной власти субъектов Российской Федерации;
– средства массовой информации и пр.
5.2. Допуск к информационным ресурсам сторонних организаций, деятельность которых не связана с исполнением функций организации, регламентируется законодательством Российской Федерации, договорами и соглашениями об информационном обмене и другими нормативными актами.

6 . Допуск к информационным ресурсам организации сторонних организаций, выполняющих работы в организации на договорной основе

6.1. К организациям, выполняющим работы на договорной основе, могут относиться:
– организации, выполняющие строительные работы и осуществляющие ремонт зданий, систем инженерно-технического обеспечения (отопления, освещения, водоснабжения, канализации, электропитания, кондиционирования и т.п.);
– организации, осуществляющие монтаж и настройку технических средств ИСПДн, сопровождение программно-прикладного обеспечения;
– организации, оказывающие услуги в области защиты информации (проведение специальных проверок и исследований, монтаж и настройка средств защиты информации, контроль эффективности системы защиты информации, аттестация объектов информатизации и т.п.);
– организации, осуществляющие поставку товаров для обеспечения повседневной деятельности (мебели, канцтоваров, оргтехники, расходных материалов и т.п.);
– организации и частные лица, оказывающие юридические услуги, услуги по информационно-техническому обеспечению, осуществляющие преподавательскую деятельность и т.п.
6.2. Порядок допуска определяется в договоре на выполнение работ (оказание услуг), в соответствии с Положением об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных.
6.3. Решением о допуске является подписанный в установленном порядке договор на выполнение работ или оказание услуг.

6.4. В договор на оказание услуг включается условие о неразглашении сведений, составляющих персональные данные, а также служебной информации, ставшей известной в ходе выполнения работ, если для их выполнения предусмотрено использование таких сведений. Со всех работников сторонней организации, участвующих в выполнении работ, в этом случае берется подписка о неразглашении таких сведений.

7.Доступ к информационным ресурсам организации

7.1. Правила и процедуры доступа к информационным ресурсам Учреждения определяются Положением об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных и Положением о разрешительной системе допуска.

7.2. Администрирование прав доступа к информации в ИСПДн, производится Ответственным.

7.3. После регистрации пользователя в ИСПДн, Ответственный вносит изменения в Матрицу разграничения доступа для последующего контроля прав и полномочий пользователя.

8.Контроль функционирования разрешительной системы допуска к информационным ресурсам Учреждения

8.1. Контроль функционирования разрешительной системы допуска к информационным ресурсам организуется в соответствии с:

– планом основных мероприятий по защите информации на текущий год;

– функциональными обязанностями должностных лиц;

– приказами руководителя.

8.2. Контроль функционирования разрешительной системы допуска к информационным ресурсам осуществляется ответственными лицами.

Организация контроля возлагается на администратора безопасности.

Приложение 2
к Положению об обеспечении безопасности
персональных данных, обрабатываемых в
информационных системах персональных
данных МБУ ДО ДЮЦ

Порядок доступа работников в помещения, в которых ведется обработка персональных данных в Муниципальном бюджетном учреждении дополнительного образования «Детско-юношеский центр»

1.Настоящий Порядок доступа работников Учреждения в помещения, в которых ведется обработка персональных данных (далее – Порядок) разработан в соответствии с требованиями: Федерального закона от 27.07.2006 № 152 ФЗ «О персональных данных», от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами» и другими нормативными правовыми актами.

2.Целью настоящего Порядка является исключение несанкционированного доступа к персональным данным субъектов персональных данных в помещения МБУ ДО ДЮЦ (далее - Учреждение).

3.Персональные данные относятся к конфиденциальной информации. Работники и должностные лица, получившие доступ к персональным данным обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

4.Обеспечение безопасности персональных данных от уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных достигается, в том числе, установлением правил доступа в помещения, где обрабатываются персональные данные в информационной системе персональных данных и без использования средств автоматизации.

5.Для помещений, в которых обрабатываются персональные данные, организуется режим обеспечения безопасности, при котором обеспечивается сохранность носителей персональных данных и средств защиты информации, а также исключается возможность неконтролируемого проникновения и пребывания в этих помещениях посторонних лиц.
При хранении материальных носителей персональных данных должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный доступ к ним.

6.В помещения, где размещены технические средства, позволяющие осуществлять обработку персональных данных, а также хранятся носители информации, допускаются только работники и должностные получившие доступ к персональным данным.

7.Работники и должностные лица, получившие доступ к персональным данным не должны покидать помещение, в котором ведется обработка персональных данных, оставляя в нем без присмотра посторонних лиц, включая работников, не уполномоченных на обработку

персональных данных. После окончания рабочего дня дверь каждого помещения закрывается на ключ.

8.Ответственными за организацию доступа в помещения, в которых ведется обработка персональных данных, являются должностные лица.

9.Внутренний контроль за соблюдением порядка доступа в помещения, в которых ведется обработка персональных данных, проводится руководителем.

Приложение 3
к Положению об обеспечении безопасности
персональных данных, обрабатываемых в
информационных системах персональных
данных МБУ ДО ДЮЦ

ПОРЯДОК
обращения со съемными машинными носителями персональных данных
в Муниципальном бюджетном учреждении дополнительного образования
«Детско-юношеский центр»

1.Общие положения

1.1.Настоящий Порядок обращения со съемными машинными носителями персональных данных в МБУ ДО ДЮЦ (далее - Порядок), разработан в соответствии с законодательством Российской Федерации о персональных данных и нормативно-методическими документами федеральных органов исполнительной власти по вопросам безопасности ПДн при их обработке в информационных системах персональных данных.
1.2.Настоящий Порядок определяет:
-правила обращения со съемными машинными носителями информации, в том числе и ПДн (далее - СМНИ);
-порядок организации учета СМНИ;
-порядок уничтожения СМНИ.
1.3.Под СМНИ в настоящем Порядке понимаются следующие носители информации:
-оптические диски (CD, DVD) однократной и многократной записи;
-электронные накопители информации (флэш-память, съемные жесткие диски);
- иные носители информации.
1.4.Требования настоящего Порядка являются обязательными для исполнения всеми работниками Учреждения, использующими в своей работе СМНИ.
1.5. Все работники Учреждения, использующие СМНИ, должны быть ознакомлены с требованиями настоящим Порядком под подпись.
1.6. Настоящий Порядок является дополнением к действующим локальным нормативным актам (внутренним документам) по вопросам обеспечения безопасности сведений конфиденциального характера, в том числе и ПДн, и не исключает обязательного выполнения их требований.

2.Правила обращения со съемными машинными носителями персональных данных

2.1. Обращение со СМНИ должно осуществляется таким образом, чтобы исключались их утрата, порча и несанкционированный доступ к ним посторонних лиц.
2.2. При обращении со СМНИ, выполняются следующие основные правила:
- СМНИ учитываются и выдаются под подпись;
- СМНИ, срок эксплуатации которых истек, уничтожаются в установленном порядке;
- для выноса СМНИ за пределы контролируемой зоны, запрашивается специальное разрешение у ответственного за обеспечение безопасности ПДн в ИСПДн (далее - Ответственный), а факт выноса фиксируется; право на перемещение СМНИ за пределы контролируемой зоны, имеют только те лица, которым оно необходимо для выполнения своих должностных обязанностей (функции);

- все СМНИ должны хранится в сейфах (металлических шкафах), оборудованных внутренними замками с двумя или более дубликатами ключей и приспособленными для опечатывания замочных скважин или кодовыми замками;
- допускается хранение СМНИ вне сейфов (металлических шкафов) при условиях уничтожения (стирания) ПДн и остаточной информации (информации, которую можно восстановить после удаления с помощью нештатных средств и методов) с использованием средств стирания данных и остаточной информации, либо если на съемном машинном носителе ПДн
2.3. СМНИ должен использоваться, не более срока эксплуатации, установленного изготовителем материального носителя.

3.Порядок хранения и учета съемных машинных носителей персональных данных

3.1. СМНИ, должны иметь специальную маркировку.
3.2. Все находящиеся на хранении и в обращении СМНИ учитываются ответственным в «Журнале учета съемных машинных носителей персональных данных в
3.3.В нерабочее время и время отсутствия необходимости использования ПДн СМНИ должны храниться в хранилищах СМНИ.
3.4.Пользователи для выполнения работ получают СМНИ у ответственного. При получении делаются соответствующие записи в «Журнале учета съемных машинных носителей персональных данных в МБУ ДО ДЮЦ.

4.Порядок уничтожения съемных машинных носителей персональных данных

4.1.Уничтожение ПДн производится только в следующих случаях:
- обрабатываемые ПДн подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом;
- ПДн являются незаконно полученными или не являются необходимыми для заявленной цели обработки;
- в случае выявления неправомерной обработки ПДн, если обеспечить правомерность обработки ПДн невозможно;
- в случае достижения цели обработки ПДн;
- в случае отзыва субъектом ПДн согласия на обработку его ПДн и в случае, если сохранение ПДн более не требуется для целей обработки ПДн.
4.2. СМНИ, пришедшие в негодность или отслужившие установленный срок, подлежат уничтожению.
4.3.Уничтожение СМНИ осуществляется комиссией по уничтожению, назначенной приказом директора Учреждения.
4.4.При уничтожении СМНИ необходимо:
-убедиться в необходимости уничтожения СМНИ;
-убедиться в том, что уничтожаются только та информация, которая предназначена для уничтожения;
-уничтожить СМНИ подходящим способом, в соответствии с настоящим Порядком или способом, указанным в соответствующем требовании или распорядительном документе.
4.5.При уничтожении СМНИ применяются следующие способы:
- измельчение в бумагорезательной (бумагоуничтожительной) машине - для документов, исполненных на бумаге;

- тщательное вымарывание (с проверкой тщательности вымарывания) информации, подлежащей уничтожению - для сохранения возможности обработки иных данных, зафиксированных в документе;
- измельчение в специальной мультирезательной (мультиуничтожительной) машине или физическое уничтожение (разрушение) носителей информации - для СМНИ на оптических дисках;
- физическое уничтожение частей СМНИ — разрушение или сильная деформация
- для носителей информации на жестком магнитном диске (уничтожению подлежат внутренние диски и микросхемы); SSD-дисках, USB- и Flash- носителях (уничтожению подлежат модули и микросхемы долговременной памяти);
- стирание с помощью сертифицированных средств уничтожения информации - для записей в базах данных и отдельных документов на машинном носителе.

4.6.По результатам уничтожения СМНИ комиссией составляется «Акт уничтожения съемных машинных носителей персональных данных».

5.Ответственность

5.1.Ответственным за хранение, учет и выдачу СМНИ, является ответственный.

5.2.Все работники Учреждения, использующие СМНИ и ответственный, несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящим Порядком, в пределах, определенных действующим законодательством Российской Федерации. За несоблюдение требований законодательства Российской Федерации предусмотрена гражданская, уголовная, административная, дисциплинарная ответственность.

6.Срок действия и порядок внесения изменений

6.1.Настоящий Порядок вступает в силу с момента его утверждения и действует бессрочно.

6.2.Изменения и дополнения в настоящий Порядок вносятся приказом директора Учреждения.

Приложение 4
к Положению об обеспечении безопасности
персональных данных, обрабатываемых в
информационных системах персональных
данных МБУ ДО ДЮЦ

ИНСТРУКЦИЯ
по организации резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в информационных системах персональных данных Муниципального бюджетного учреждения дополнительного образования «Детско-юношеский центр»

1.Общие положения

1.1. Настоящая Инструкция по организации резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в информационных системах персональных данных МБУ ДО ДЮЦ (далее - Инструкция) устанавливает основные требования к организации резервного копирования (восстановления) программ и данных, хранящихся в базах данных информационных систем персональных данных (далее - ИСПДн) МБУ ДО ДЮЦ (далее - Учреждение), а также к резервированию аппаратных средств.
1.2.Настоящая Инструкция разработана с целью:
-определения категории информации, подлежащей обязательному резервному копированию; определения процедуры резервирования данных для последующего восстановления работоспособности ИСПДн при полной или частичной потере информации, вызванной сбоями или отказами аппаратного или программного обеспечения, ошибками пользователей, чрезвычайными обстоятельствами (пожаром, стихийными бедствиями и т.д.);
-определения порядка восстановления информации в случае возникновения такой необходимости;
-упорядочения работы и определения ответственности должностных лиц, связанной с резервным копированием и восстановлением информации.
1.3.Действие настоящей Инструкции распространяется на всех пользователей ИСПДн Учреждения, а также на основные системы обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций, в том числе:
-системы жизнеобеспечения технических средств;
-системы обеспечения отказоустойчивости;
-системы резервного копирования и хранения данных;
1.4.Под резервным копированием информации понимается создание избыточных копий защищаемой информации в электронном виде для быстрого восстановления работоспособности ИСПДн в случае возникновения аварийной ситуации, повлекшей за собой повреждение или утрату данных.
1.5.Резервному копированию подлежит информация следующих основных категорий:
- информация, обрабатываемая пользователями в ИСПДн, а также информация, необходимая для восстановления работоспособности ИСПДн, в т.ч. систем управления

базами данных (далее - СУБД) общего пользования и справочно информационных систем общего использования;
-рабочие копии установочных компонентов программного обеспечения общего назначения и специализированного программного обеспечения серверов и рабочих станций;
-информация, необходимая для восстановления серверов и систем управления базами данных ИСПДн, локальной вычислительной сети, системы электронного документооборота;
- регистрационная информация систем защиты информации;
-другая информация ИСПДн, по мнению пользователей, администраторов ИСПДн и ответственного за обеспечение безопасности персональных данных (далее - ПДн) в ИСПДн, являющаяся критичной для работоспособности ИСПДн.
1.6. Настоящая Инструкция является дополнением к действующим локальным нормативным актам (внутренним документам) по вопросам обеспечения безопасности сведений конфиденциального характера, в том числе и ПДн, и не исключает обязательного выполнения их требований.

2.Общие требования к резервному копированию

2.1.В Инструкции резервного копирования описываются действия при выполнении следующих мероприятий:
-резервное копирование с указанием конкретных резервируемых данных и аппаратных средств (в случае необходимости);
-контроль резервного копирования;
-хранение резервных копий;
-полное или частичное восстановление данных.
2.2.Архивное копирование резервируемой информации производится при помощи специализированных программно-аппаратных систем резервного копирования. Система резервного копирования должна обеспечить производительность, достаточную для сохранения информации, указанной в п. 2.5, в установленные сроки и с заданной периодичностью.
2.3.Требования к техническому обеспечению систем резервного копирования:
-комплекс взаимосвязанных технических средств на единой технологической платформе, обеспечивающих процессы сбора, передачи, обработки и хранения информации;
-имеет возможность расширения (замены) состава технических средств, входящих в комплекс, для улучшения их эксплуатационно-технических характеристик по мере возрастания объемов обрабатываемой информации;
- обеспечивает выполнение функций, перечисленных в п. 3.1.
2.4. Требования к программному обеспечению систем резервного копирования:
-лицензионное системное программное обеспечение и программное обеспечение резервного копирования;
- программное обеспечение резервного копирования обеспечивает простоту процесса инсталляции, конфигурирования и сопровождения.
2.5. Хранение отдельных магнитных носителей архивных копий организуется в отдельном хранилище. Физический доступ к архивным копиям строго ограничен.
2.6. Доступ к носителям архивных копий имеют только уполномоченные работники, которые несут персональную ответственность за сохранность архивных копий и невозможность ознакомления с ними лиц, не имеющих на то полномочий.

2.7. Уничтожение отделяемых магнитных носителей архивных копий производится установленным порядком в случае прихода их в негодность или замены типа носителя с обязательным составлением акта об уничтожении.

3.Ответственность за состояние резервного копирования

3.1.Ответственность за контроль над своевременным осуществлением резервного копирования и соблюдением соответствующей Инструкции, а также за выполнением требований по хранению архивных копий и предотвращению несанкционированного доступа к ним возлагается на ответственного за обеспечение безопасности ПДн в ИСПДн и администраторов ИСПДн.

3.2. В случае обнаружения попыток несанкционированного доступа к носителям архивной информации, а также иных нарушениях информационной безопасности, произошедших в процессе резервного копирования, сообщается ответственному за обеспечение безопасности ПДн в ИСПДн в течение рабочего дня после обнаружения указанного события.

4.Периодичность резервного копирования

4.1.Резервное копирование специализированного программного обеспечения производится при его получении (если это предусмотрено инструкцией по его применению и не противоречит условиям его распространения), а также при его обновлении и получении исправленных и обновленных версий.

4.2.Резервное копирование открытой информации делается не позднее чем через сутки после ее изменения, но не реже одного раза в месяц.

4.3. Информация, содержащаяся в постоянно изменяемых базах данных, сохраняется в соответствии со следующим графиком:

- ежедневно проводится копирование измененной и дополненной информации (носители с ежедневной информацией должны храниться в течение недели);
- еженедельно проводится резервное копирование всей базы данных (носители с еженедельными копиями хранятся в течение месяца);
- ежемесячно производится резервное копирование на специально выделенный носитель длительного хранения, информация на котором хранится постоянно.

4.4.Не реже одного раза в год на носители длительного хранения записывается информация, не относящаяся к постоянно изменяемым базам данных (приказы, распоряжения, открытые издания и т.д.).

5.Восстановление информации из резервных копий

5.1.В случае необходимости, восстановление данных из резервных копий производится ответственными работниками.

5.2. Восстановление данных из резервных копий происходит в случае ее исчезновения или нарушения вследствие несанкционированного доступа в систему, воздействия вирусов, программных ошибок, ошибок работников и аппаратных сбоев.

5.3. Восстановление системного программного обеспечения и программного обеспечения общего назначения производится с их носителей в соответствии с инструкциями производителя.

5.4.Восстановление специализированного программного обеспечения производится с дистрибутивных носителей или их резервных копий в соответствии с инструкциями по установке или восстановлению данного программного обеспечения.

5.5.Восстановление информации, не относящейся к постоянно изменяемым базам данных, производится с резервных носителей. При этом используется последняя копия

информации.

5.6. При частичном нарушении или исчезновении записей баз данных восстановление производится с последней ненарушенной ежедневной копии. Полностью информация восстанавливается с последней еженедельной копии, которая затем дополняется ежедневными частичными резервными копиями.

6.Срок действия и порядок внесения изменений

6.1.Настоящая Инструкция вступает в силу с момента ее утверждения и действует бессрочно.

6.2.Изменения и дополнения в настоящую Инструкцию вносятся приказом директора Учреждения.

Приложение 5
к Положению об обеспечении безопасности
персональных данных, обрабатываемых в
информационных системах персональных
данных МБУ ДО ДЮЦ

ИНСТРУКЦИЯ
по парольной защите информации в Муниципальном бюджетном учреждении дополнительного образования «Детско-юношеский центр»

1.Общие положения

Настоящая инструкция устанавливает основные правила введения парольной защиты информационной системы персональных данных Муниципального бюджетного учреждения дополнительного образования «Детско-юношеский центр» (далее– Учреждение). Инструкция регламентирует организационно-техническое обеспечение генерации, смены и прекращения действия паролей в информационные системы персональных данных, а также контроль за действиями пользователей системы при работе с паролями. Настоящая инструкция оперирует следующими основными понятиями:

− *Идентификация* - присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

− *ИСПДн* – информационная система персональных данных.

− *Компрометация*- факт доступа постороннего лица к защищаемой информации, а также подозрение на него.

− *Объект доступа* - единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа.

− *Пароль* – уникальный признак субъекта доступа, который является его (субъекта) секретом.

− *Правила доступа* - совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

− *Субъект доступа* - лицо или процесс, действия которого регламентируются правилами разграничения доступа.

− *Несанкционированный доступ* - доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или АС.

2.Правила генерации паролей

Персональные пароли должны генерироваться специальными программными средствами административной службы.

2.1 Длина пароля должна быть не менее 8 символов.

2.2 В составе пароля должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы.

2.3 Пароль не должен включать в себя:

− легко вычисляемые сочетания символов;

− клавиатурные последовательности символов и знаков;
− общепринятые сокращения;
− аббревиатуры;
− номера телефонов, автомобилей;
− прочие сочетания букв и знаков, ассоциируемые с пользователем;
− при смене пароля новое сочетание символов должно отличаться от предыдущего не менее чем на 2 символа.
2.4 Допускается использование единого пароля для доступа субъекта доступа к различным информационным ресурсам одной ИСПДн объекта образования.

3.Порядок смены паролей

3.1 Полная плановая смена паролей пользователей должна проводиться регулярно.
3.2 Полная внеплановая смена паролей всех пользователей должна производиться случае прекращения полномочий администраторов средств защиты или других сотрудников, которым по роду службы были предоставлены полномочия по управлению парольной зашитой.
3.3 Полная внеплановая смена паролей должна производиться в случае компрометации личного пароля одного из администраторов ИСПДн.
3.4 В случае компрометации личного пароля пользователя надлежит немедленно ограничить доступ к информации с данной учетной записи, до момента вступления в силу новой учетной записи пользователя или пароля.

4.Обязанности пользователей при работе с парольной защитой

4.1 При работе с парольной защитой пользователям запрещается:
− разглашать кому-либо персональный пароль и прочие идентифицирующие сведения;
− предоставлять доступ от своей учетной записи к информации, хранящейся в ИСПДн посторонним лицам;
− записывать пароли на бумаге, файле, электронных и прочих носителях информации, в том числе и на предметах.
4.2 Хранение пользователем своего пароля на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе.
4.3 При вводе пароля пользователь обязан исключить возможность его перехвата сторонними лицами и техническими средствами.

5.Случаи компрометации паролей

5.1 Под компрометацией следует понимать:
− физическая утеря носителя с информацией;
− передача идентификационной информации по открытым каналам связи;
− проникновение постороннего лица в помещение физического хранения носителя парольной информации или алгоритма или подозрение на него (срабатывание сигнализации, повреждение устройств контроля НСД (слепков печатей), повреждение замков и т. п.);
− визуальный осмотр носителя идентификационной информации посторонним лицом;
− перехват пароля при распределении идентификаторов;
− сознательная передача информации постороннему лицу.
5.2 Действия при компрометации пароля:
− скомпрометированный пароль сразу же выводится из действия, взамен его вводятся

запасной или новый пароль;
− о компрометации немедленно оповещаются все участники обмена информацией.
Пароль вносится в специальные списки, содержащие скомпрометированные пароли и учетные записи.

6 Ответственность пользователей при работе с парольной защитой

6.1 Повседневный контроль за действиями сотрудников Учреждения при работе с паролями, соблюдением порядка их смены, хранения и использования, возлагается на ответственного за систему защиты информации в информационной системе персональных данных.
6.2 Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.
6.3 Ответственность за организацию парольной защиты возлагается ответственного за систему защиты информации в информационной системе персональных данных.
6.4 Ответственность в случае несвоевременного уведомлении ответственного за систему защиты информации в информационной системе персональных данных о случаях утери, кражи, взлома или компрометации паролей возлагается на владельца взломанной учетной записи.

Приложение 6
к Положению об обеспечении безопасности
персональных данных, обрабатываемых в
информационных системах персональных
данных МБУ ДО ДЮЦ

Инструкция
по организации антивирусной защиты в
Муниципальном бюджетном учреждении дополнительного образования
«Детско-юношеский центр»

1.Общие положения

1.1. Настоящая инструкция предназначена для организации порядка проведения антивирусного контроля в муниципальном бюджетном учреждении дополнительного образования «Детско-юношеский центр»(далее-Учреждение) и предотвращения возникновения фактов заражения программного обеспечения компьютерными вирусами, а также фильтрации доступа пользователей Учреждения к непродуктивным Интернет-ресурсам и контроля их электронной переписки.
1.2. В Учреждении может использоваться только лицензионное антивирусное программное обеспечение либо свободно-распространяемое программное обеспечение.
1.4. Установка, настройка и регулярное обновление антивирусных средств осуществляется только ответственным лицом.
1.5. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы, почтовые сообщения), получаемая и передаваемая по телекоммуникационным каналам связи, а также информация, находящаяся на съемных носителях (магнитных дисках, лентах, CD-ROM, DVD, flash-накопителях и т.п.).
1.6. Контроль информации на съёмных носителях производится непосредственно перед её использованием.
1.7. Файлы, помещаемые в электронный архив или на сервер, должны в обязательном порядке проходить антивирусный контроль.
1.8. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов.
1.9. Факт выполнения антивирусной проверки должен регистрироваться в специальном журнале за подписью ответственного лица.

2.Мероприятия, направленные на решение задач по антивирусной защите

2.1. Установка только лицензированного программного обеспечения либо бесплатного антивирусного программного обеспечения.
2.2. Регулярное обновление и профилактические проверки.
2.3. Непрерывный контроль над всеми возможными путями проникновения вредоносных программ, мониторинг антивирусной безопасности и обнаружение деструктивной активности вредоносных программ на всех объектах информационно-коммуникационной системы.

2.4. Проведение профилактических мероприятий по предотвращению и ограничению вирусных эпидемий, включающих загрузку и развертывание специальных правил нейтрализации (отражению, изоляции и ликвидации) вредоносных программ на основе рекомендаций по
контролю атак, подготавливаемых разработчиком средств защиты от вредоносных программ и другими специализированными экспертными антивирусными службами до того, как будут выпущены файлы исправлений, признаков и антивирусных сигнатур.
2.5. Внешние носители информации неизвестного происхождения следует проверять на наличие
вирусов до их использования.
2.6. Необходимо строго придерживаться установленных процедур по уведомлению о случаях
поражения автоматизированной информационной среды компьютерными вирусами и принятию мер по ликвидации последствий от их проникновения.
2.7. Обеспечение бесперебойной работы Учреждения для случаев вирусного заражения, в том числе резервного копирования всех необходимых данных и программ и их восстановления.

3 Требования к проведению мероприятий по антивирусной защите

3.1. Ежедневно в начале работы при загрузке компьютера (для серверов ЛВС – при перезагрузке) в автоматическом режиме должно выполняться обновление антивирусных баз и серверов и проводиться антивирусный контроль всех дисков и файлов персонального компьютера и съёмных носителей.
3.2. Периодические проверки компьютеров должны проводиться не реже одного раза в неделю.
3.3. Внеочередной антивирусный контроль всех дисков и файлов персонального компьютера должен выполняться:
3.3.1. непосредственно после установки (изменения) программного обеспечения компьютера.
3.3.2.при возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.);
3.3.3. при отправке и получении электронной почты оператор электронной почты обязан проверить электронные письма и их вложения на наличие вирусов.

4 Действия сотрудников при обнаружении компьютерного вируса

4.1. В случае обнаружения зараженных компьютерными вирусами файлов или электронных писем пользователи обязаны:
4.1.1.приостановить работу;
4.1.2.немедленно поставить в известность о факте обнаружения зараженных вирусом файлов ответственного лица.
4.1.3.совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;
4.1.4.провести лечение или уничтожение зараженных файлов.
4.2. При возникновении подозрения на наличие компьютерного вируса ответственный должен провести внеочередной антивирусный контроль.

5.Ответственность

5.1. Ответственность за организацию антивирусной защиты и выполнение положений данной инструкции возлагается на ответственное лицо.

Приложение 7
к Положению об обеспечении безопасности
персональных данных, обрабатываемых в
информационных системах персональных
данных МБУ ДО ДЮЦ

РЕГЛАМЕНТ
реагирования на инциденты информационной безопасности
в информационных системах персональных данных Муниципального бюджетного учреждения дополнительного образования «Детско-юношеский центр»

1.Общие положения

1.1. Настоящий Регламент реагирования на инциденты информационной безопасности в информационных системах персональных данных Муниципального бюджетного учреждения дополнительного образования «Детско-юношеский центр» (далее – Регламент), разработан в соответствии с законодательством Российской Федерации о персональных данных (далее –ПДн) и нормативно-методическими документами федеральных органов исполнительной власти по вопросам безопасности ПДн при их обработке в информационных системах персональных данных (далее – ИСПДн).

1.2.Настоящий Регламент определяет:

– порядок регистрации событий безопасности;

–порядок выявления инцидентов информационной безопасности и реагированию на них;

– порядок проведения анализа инцидентов информационной безопасности, в том числе определение источников и причин возникновения инцидентов.

1.3. Регламент обязателен для исполнения всеми работниками Муниципального бюджетного учреждения дополнительного образования «Детско-юношеский центр» (далее –Учреждение), непосредственно осуществляющими защиту ПДн в ИСПДн.

2.Инциденты информационной безопасности

2.1.К инцидентам ИБ относятся:

–несоблюдение требований по защите ПДн:

– использование ЭВМ в целях, не связанных с выполнением трудовых (служебных, должностных, функциональных) обязанностей;

– утрата носителя ПДн;

– утрата ключевых документов, ключей от помещений и хранилищ, личных
печатей, удостоверений, пропусков.

– попытки НСД к ПДн:

– подбор чужого идентификатора и пароля, последующий доступ с использованием чужого пароля;

– изменение настроек, состава, паролей технических средств ИСПДн;

– изменение (увеличение) полномочий доступа;

– нарушение целостности установленных защитных пломб;

– копирование ПДн на неучтенные съемные носители ПДн;

– заражение рабочего места и/или сервера ИСПДн вредоносной программой;

– хищение носителей ПДн;

– хищение технических средств ИСПДн;
– умышленное нарушение работоспособности технических средств ИСПДн;
– хищение криптосредств, ключевых документов, ключей от помещений и хранилищ, личных печатей, удостоверений, пропусков;
– несанкционированное проникновение в помещения ИСПДн;
– очистка электронных журналов мониторинга.
– сбои в работе технических средств ИСПДн Общества.
2.2.К инцидентам ИБ не относятся:
–неудачные попытки вторжений, которые были обнаружены и нейтрализованы с использованием СЗИ;
– неудачные попытки заражения рабочих мест и/или серверов ИСПДн вредоносной программой, которые были обнаружены и нейтрализованы с использованием СЗИ

3.Порядок регистрации событий безопасности

3.1.Регистрация событий безопасности в ИСПДн осуществляется в следующей последовательности:
1) Определение событий безопасности, подлежащих регистрации, и сроков их хранения.
2) Определение состава и содержания информации о событиях безопасности, подлежащих регистрации.
3) Сбор, запись и хранение информации о событиях безопасности.
4) Реагирование на сбои при регистрации событий безопасности.
5) Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них.
6) Генерирование временных меток и (или) синхронизация системного времени в ИСПДн.
7) Защита информации о событиях безопасности.
3.2. События безопасности, подлежащие регистрации в ИСПДн, должны определяться с учетом способов реализации угроз безопасности ПДндля ИСПДн. К событиям безопасности, подлежащим регистрации в ИСПДн, должны быть отнесены любые проявления состояния ИСПДн и ее системы защиты, указывающие на возможность нарушения конфиденциальности, целостности или доступности ПДн, доступности компонентов ИСПДн, нарушения процедур, установленных организационно-распорядительными документами по защите ПДн, а также на нарушение штатного функционирования средств защиты информации (далее – СЗИ).
3.3. События безопасности, подлежащие регистрации в ИСПДн, и сроки хранения соответствующих записей регистрационных журналов должны обеспечивать возможность обнаружения, идентификации и анализа инцидентов информационной безопасности, возникших в ИСПДн.
3.4. В ИСПДн подлежат регистрации следующие события:
– вход (выход), а также попытки входа субъектов доступа в ИСПДн и загрузки (остановка) операционной системы;
– подключение съемных машинных носителей ПДн и вывод ПДн на носители;
–запуск (завершение) программ и процессов (заданий, задач), связанных с обработкой ПДн;
–обновление или ошибки при обновлении программных средств ИСПДн и СЗИ;
–попытки доступа программных средств к определяемым защищаемым объектам доступа (техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, файлам, записям, полям записей) и иным объектам доступа;

–попытки удаленного доступа.
3.5.Состав и содержание информации о событиях безопасности, включаемой в записи регистрации о событиях безопасности, должны, как минимум, обеспечить возможность идентификации типа события безопасности, даты и времени события безопасности, идентификационной информации источника события безопасности, результат события безопасности (успешно или неуспешно), субъекта доступа (пользователя и (или) процесса), связанного с данным событием безопасности.
3.6.При регистрации входа (выхода) субъектов доступа в ИСПДн и загрузки (остановка) операционной системы состав и содержание информации должны, как минимум, включать дату и время входа (выхода) в систему (из системы) или загрузки (остановки) операционной системы, результат попытки входа (успешная или неуспешная), результат попытки загрузки (остановка) операционной системы (успешная или неуспешная), идентификатор, предъявленный при попытке доступа.
3.7.При регистрации подключения съемных машинных носителей ПДн и вывода ПДн на съемные носители состав и содержание регистрационных записей должны, как минимум, включать дату и время подключения съемных машинных носителей ПДн и вывода ПДн на съемные носители, логическое имя (номер) подключаемого съемного машинного носителя ПДн, идентификатор субъекта доступа, осуществляющего вывод ПДн на съемный носитель ПДн.
3.8.При регистрации запуска (завершения) программ и процессов (заданий, задач), связанных с обработкой ПДнсостав и содержание регистрационных записей должны, как минимум, включать дату и время запуска, имя (идентификатор) программы (процесса, задания), идентификатор субъекта доступа (устройства), запросившего программу (процесс, задание), результат запуска (успешный, неуспешный).
3.9.При регистрации попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам состав и содержание регистрационных записей должны, как минимум, включать дату и время попытки доступа к защищаемому файлу с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), спецификацию защищаемого файла (логическое имя, тип).
3.10. При регистрации попыток доступа программных средств к защищаемым объектам доступа (техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, записям, полям записей)состав и содержание информации должны, как минимум, включать дату и время попытки доступа к защищаемому объекту с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), спецификацию защищаемого объекта доступа (логическое имя (номер).
3.11. При регистрации попыток удаленного доступа к ИСПДн состав и содержание информации должны, как минимум, включать дату и время попытки удаленного доступа с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), используемый протокол доступа, используемый интерфейс доступа и (или) иную информацию о попытках удаленного доступа к ИСПДн.
3.12. Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения должен предусматривать:
–возможность выбора Ответственным за обеспечение безопасности ПДн в ИСПДни (или) Администратором ИСПДн событий безопасности, подлежащих регистрации в текущий момент времени из перечня событий безопасности, определенных в пункте 4.4 настоящего Регламента;

–генерацию (сбор, запись)записей регистрации (аудита) для событий безопасности, подлежащих регистрации (аудиту) в соответствии с составом и содержанием информации, определенными в соответствии с пунктами 4.6–4.11 настоящего Регламента;

–хранение информации о событиях безопасности в течение времени, установленного в пункте 4.3 настоящего Регламента.

3.13. Объем памяти для хранения информации о событиях безопасности должен быть рассчитан и выделен с учетом типов событий безопасности, подлежащих регистрации в соответствии с составом и содержанием информации о событиях безопасности, подлежащих регистрации, в соответствии с пунктами 4.7 – 4.11настоящего Регламента, прогнозируемой частоты возникновения подлежащих регистрации событий безопасности, срока хранения информации о зарегистрированных событиях безопасности.

3.14. В ИСПДн должно осуществляться реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти.

3.15. Реагирование на сбои при регистрации событий безопасности должно предусматривать:

– предупреждение (сигнализация, индикация) о сбоях (аппаратных и программных ошибках, сбоях в механизмах сбора информации или переполнения объема (емкости) памяти) при регистрации событий безопасности;

–реагирование на сбои при регистрации событий безопасности путем изменения Ответственным за обеспечение безопасности ПДн в ИСПДн о событиях безопасности, в том числе отключение записи информации о событиях безопасности от части компонентов ИСПДн, запись поверх устаревших хранимых записей событий безопасности.

3.16. В случае выявление признаков инцидентов информационной безопасности в ИСПДн осуществляется планирование и проведение мероприятий по реагированию на выявленные инциденты безопасности в соответствии с порядком проведения разбирательств по фактам возникновения инцидентов в ИСПДн.

3.17. Получение меток времени, включающих дату и время, используемых при генерации записей регистрации (аудита) событий безопасности в ИСПДн, достигается посредством применения внутренних системных часов ИСПДн.

3.18. Защита информации о событиях безопасности (записях регистрации (аудита)) обеспечивается применением мер защиты информации от неправомерного доступа, уничтожения или модифицирования и в том числе включает защиту средств ведения регистрации (аудита) и настроек механизмов регистрации событий.

3.19. Доступ к записям аудита и функциям управления механизмами регистрации (аудита) должен предоставляться только уполномоченным должностным лицам:

–ответственному за обеспечение безопасности ПДн в ИСПДн;

4.Порядок выявления инцидентов информационной безопасности и реагирования на них

4.1.За выявление инцидентов информационной безопасности и реагирование на них отвечают:

–ответственный за обеспечение безопасности ПДн в ИСПДн;

4.2.Работники Учреждения, должны сообщать ответственным за выявление инцидентов информационной безопасности о любых инцидентах, в которые входят:

–факты попыток и успешной реализации несанкционированного доступа в ИСПДн, в помещения, в которых осуществляется обработка ПДн, и к хранилищам ПДн;

– факты сбоя или некорректной работы систем обработки информации;
– факты сбоя или некорректной работы СЗИ;
–факты разглашения ПДн;
–факты разглашения информации о методах и способах защиты и обработкиПДн.
4.3.Все нештатные ситуации, факты вскрытия и опечатывания технических средств, выполнения профилактических работ, установки и модификации аппаратных и программных средств обработки ПДн в ИСПДн должны быть занесены ответственными за выявление инцидентов информационной безопасности в «Журнал учета нештатных ситуаций, фактов вскрытия и опечатывания технических средств, выполнения профилактических работ, установки и модификации аппаратных и программных средств обработки персональных данных в Учреждении.
4.4.Анализ инцидентов информационной безопасности, в том числе определение источников и причин возникновения инцидентов, осуществляется согласно порядку проведения разбирательств по фактам возникновения инцидентов информационной безопасности в ИСПДн.

5.Основные этапы процесса реагирования на инциденты

5.1. Ответственный должен обеспечить защиту ИСПДн и проинформировать пользователей, о важности мер по обеспечению информационной безопасности.
5.2.Ответственный должен определить, является ли обнаруженное ими с помощью различных систем обеспечения информационной безопасности событие инцидентом или нет. Для этого могут использоваться публичные отчеты, потоки данных об угрозах, средства статического и динамического анализа образцов программного обеспечения и другие источники информации.
Статический анализ выполняется без непосредственного запуска исследуемого образца и позволяет выявить различные индикаторы, например, строки, содержащие URL-адреса или адреса электронной почты.
Динамический анализ подразумевает выполнение исследуемой программы в защищенной среде (Песочнице) или на изолированной машине с целью выявления поведения образца и сбора артефактов его работы.
5.3.Ответсвенный должен идентифицировать скомпрометированные компьютеры и настроить правила безопасности таким образом, чтобы заражение не распространилось дальше по сети. Кроме того, на этом этапе необходимо перенастроить сеть таким образом, чтобы ИСПДн могли продолжать работать без зараженных машин.
5.4.Далее лица, занимающиеся реагированием на инциденты, удаляют вредоносное программное обеспечение, а также все артефакты, которые оно могло оставить на зараженных компьютерах в ИСПДн.
5.5.Ранее скомпрометированные компьютеры вводятся обратно в сеть. При этом лица, занимающиеся реагированием на инциденты, некоторое время продолжают наблюдать за состоянием этих машин и ИСПДн в целом, чтобы убедиться в полном устранении угрозы.
5.6.Лица, занимающиеся реагированием на инциденты, анализируют произошедший инцидент, вносят необходимые изменения в конфигурацию программного обеспечения и оборудования, обеспечивающего информационной безопасности, и формируют рекомендации для того, чтобы в будущем предотвратить подобные инциденты. При невозможности полного предотвращения будущей атаки составленные рекомендации позволят ускорить реагирование на подобные инциденты.

6.Порядок проведения разбирательств по фактам возникновения инцидентов

информационной безопасности

6.1.Для проведения разбирательств по фактам возникновения инцидентов информационной безопасности создаётся комиссия, состоящая не менее чем из трех человек с обязательным включением в её состав:

– ответственного за обеспечение безопасности ПДн в ИСПДн;

6.2. Председатель комиссии организует работу комиссии, решает вопросы взаимодействия комиссии с руководителями и работниками структурных подразделений организации, готовит и ведёт заседания комиссии, подписывает протоколы заседаний. По окончании работы комиссии готовится заключение по результатам проведённого разбирательства, которое передается на рассмотрение Директору Учреждения.

6.3.При проведении разбирательства устанавливаются:

–наличие самого факта совершения инцидента информационной безопасности, служащего основанием для вынесения соответствующего решения;

–время, место и обстоятельства возникновения инцидента, а также оценка его последствий;

–конкретный работник, совершивший инцидент информационной безопасности или повлекший своими действиями возникновения инцидента;

–наличие и степень вины работника, совершившего инцидент информационной безопасности или повлекшего своими действиями возникновение инцидента;

–цели и мотивы, способствовавшие совершению инцидента информационной безопасности.

6.4. В целях проведения разбирательства все работникиобязаны по первому требованию членов комиссии предъявить для проверки все числящиеся за ними материалы и документы, дать устные или письменные объяснения об известных им фактах по существу заданных им вопросов.

6.5. Работник, совершивший инцидент информационной безопасности или повлекший своими действиями возникновения инцидента, обязан по требованию комиссии представить объяснения в письменной форме не позднее трех рабочих дней с момента получения соответствующего требования. Комиссия вправе поставить перед работником перечень вопросов, на которые работник обязан ответить. В случае отказа работника от письменных объяснений, комиссией составляется акт.

6.6.Работник имеет право, по согласованию с председателем комиссии, знакомиться с материалами разбирательства, касающимися лично его, и давать по поводу них свои комментарии, предоставлять дополнительную информацию и документы. По окончании разбирательства работнику для ознакомления предоставляется итоговый акт с выводами комиссии.

6.7. В случае давления на работника со стороны других лиц (не из состава комиссии) в виде просьб, угроз, шантажа и др., по вопросам, связанным с проведением разбирательства, работник обязан сообщить об этом председателю комиссии.

6.8.До окончания работы комиссии и вынесения решения членам комиссии запрещается разглашать сведения о ходе проведения разбирательства и ставшие известные им обстоятельства.

6.9. В процессе проведения разбирательства комиссией выясняются:

–перечень разглашенных сведений;

–причины разглашения сведений;

–лица, виновные в разглашении сведений;

–размер (экспертную оценку) причиненного ущерба;

–недостатки и нарушения, допущенные работниками при работе с ПДн;
–иные обстоятельства, необходимые для определения причин разглашения ПДн, степени виновности отдельных лиц, возможности применения к ним мер воздействия.
6.10. По завершении разбирательства комиссией составляется заключение. В заключении указываются:
–основание для проведения в разбирательства;
–состав комиссии и время проведения разбирательства;
–сведения о времени, месте и обстоятельствах возникновения инцидента информационной безопасности;
–сведения о работнике, совершившем инцидент информационной безопасности или повлекшем своими действиями возникновения инцидента (должность, фамилия, имя, отчество, год рождения, время работы в Учреждении, а также в занимаемая должность);
–цели и мотивы работника, способствовавшие совершению инцидента информационной безопасности;
–причины и условия возникновения инцидента информационной безопасности;
–данные о характере и размерах причиненного в результате инцидента ущерба;
–предложения о мере ответственности работника, совершившего инцидент информационной безопасности или повлекшего своими действиями возникновения инцидента.
6.11. На основании заключения выносится решение о применении мер ответственности к работнику, совершившему инцидент или повлекшему своими действиями возникновению инцидента, также о возмещении ущерба виновным работником (или его законным представителем), которое доводится до указанного работника в письменной форме под расписку.
6.12. Все материалы разбирательства относятся к информации ограниченного доступа и хранятся в течение 5 лет. Копии заключения и распоряжения по результатам разбирательства приобщаются к личному делу работника, в отношении которого оно проводилось.

7.Ответственность

7.1.Все работники, осуществляющие защиту ПДн, обязаны ознакомиться с данным Регламентом под подпись.
7.2.Работники несут персональную ответственность за выполнение требований настоящего Регламента.

8.Срок действия и порядок внесения изменений

8.1.Настоящий Регламент вступает в силу с момента его утверждения и действует бессрочно.
8.2.Изменения и дополнения в настоящий Регламент вносятся приказом Директора Учреждения.

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП

Сертификат 460837604057956529703830632163952415623550190485

Владелец Шпенькова Наталья Павловна

Действителен С 17.10.2023 по 16.10.2024