Утверждаю
Директор МКУ «Центр обеспечения
деятельности образовательных организаций»
_____ О.Н.Маркова
«10» февраля 2017

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
информационной системы персональных данных «РИС обеспечения проведения ГИА обучающихся, освоивших основные образовательные программы основного общего и среднего общего образования на территории Увельского муниципального района»

п.Увельский
2017

Содержание

1 Основные термины и определения

В настоящем документе используются следующие термины и их определения.

Автоматизированная система – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Аутентификация отправителя данных – подтверждение того, что отправитель полученных данных соответствует заявленному.

Безопасность персональных данных – состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

Биометрические персональные данные – сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность, включая фотографии, отпечатки пальцев, образ сетчатки глаза, особенности строения тела и другую подобную информацию.

Блокирование персональных данных – временное прекращение сбора, систематизации, накопления, использования, распространения, персональных данных, в том числе их передачи.

Вирус (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

Вспомогательные технические средства и системы – технические средства и системы, не предназначенные для передачи, обработки и хранения персональных данных, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки персональных данных или в помещениях, в которых установлены информационные системы персональных данных.

Доступ в операционную среду компьютера (информационной системы персональных данных) – получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ.

Доступ к информации – возможность получения информации и ее использования.

Закладочное устройство – элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации).

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

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

Информативный сигнал – электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация (персональные данные) обрабатываемая в информационной системе персональных данных.

Информационная система персональных данных (ИСПДн) – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

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

Источник угрозы безопасности информации – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

Контролируемая зона – пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

Межсетевой экран – локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

Нарушитель безопасности персональных данных – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных.

Неавтоматизированная обработка персональных данных – обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

Недекларированные возможности – функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

Носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Обезличивание персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

Обработка персональных данных – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Общедоступные персональные данные – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

Оператор (персональных данных) – государственный орган, муниципальный орган, юридическое или физическое лицо, организующее и (или) осуществляющее обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

Технические средства информационной системы персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

Перехват (информации) – неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

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

Побочные электромагнитные излучения и наводки – электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

Политика «чистого стола» – комплекс организационных мероприятий, контролирующих отсутствие записывания на бумажные носители ключей и атрибутов доступа (паролей) и хранения их вблизи объектов доступа.

Пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Программная закладка – код программы, преднамеренно внесенный в программу с целью осуществить утечку, изменить, блокировать, уничтожить информацию или уничтожить и модифицировать программное обеспечение информационной системы персональных данных и (или) блокировать аппаратные средства.

Программное (программно-математическое) воздействие – несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

Раскрытие персональных данных – умышленное или случайное нарушение конфиденциальности персональных данных.

Распространение персональных данных – действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

Ресурс информационной системы – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

Специальные категории персональных данных – персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья и интимной жизни субъекта персональных данных.

Средства вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Субъект доступа (субъект) – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Технический канал утечки информации – совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

Трансграничная передача персональных данных – передача персональных данных оператором через Государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства.

Угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

Уничтожение персональных данных – действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

Утечка (защищаемой) информации по техническим каналам – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

Уязвимость – слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации.

Целостность информации – способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

2 Обозначения и сокращения

АВС – антивирусные средства
АРМ – автоматизированное рабочее место
ВТСС – вспомогательные технические средства и системы
ИСПДн – информационная система персональных данных
КЗ – контролируемая зона
ЛВС – локальная вычислительная сеть
МЭ – межсетевой экран
НСД – несанкционированный доступ
ОС – операционная система
ПДн – персональные данные
ПМВ – программно-математическое воздействие
ПО – программное обеспечение
ПЭМИН – побочные электромагнитные излучения и наводки
САЗ – система анализа защищенности
СЗИ – средства защиты информации
СЗПДн – система (подсистема) защиты персональных данных
СОВ – система обнаружения вторжений
ТКУ И – технические каналы утечки информации
УБПДн – угрозы безопасности персональных данных

3 Введение

Настоящая Политика информационной безопасности (далее – Политика) Муниципального казённого учреждения «Центр обеспечения деятельности образовательных организаций» (далее – Учреждения) является официальным документом.

Политика разработана в соответствии с целями, задачами и принципами обеспечения безопасности персональных данных.

Политика разработана в соответствии с требованиями Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и Постановления Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», на основании:

- Приказа Федеральной службы по техническому и экспортному контролю (ФСТЭК России) от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- «Типовых требований по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденных руководством 8 Центра ФСБ России 21.02.2008 г. № 149/6/6-662.

В Политике определены требования к персоналу ИСПДн, степень ответственности персонала, структура и необходимый уровень защищенности, статус и должностные обязанности сотрудников, ответственных за обеспечение безопасности персональных данных в ИСПДн Учреждения.

4 Общие положения

Целью настоящей Политики является обеспечение безопасности объектов защиты Учреждения от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности ПДн (УБПДн).

Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

Информация и связанные с ней ресурсы должны быть доступны для авторизованных пользователей. Должно осуществляться своевременное обнаружение и реагирование на УБПДн.

Должно осуществляться предотвращение преднамеренных или случайных, частичных или полных несанкционированных модификаций или уничтожения данных.

Состав объектов защиты представлен в Перечне персональных данных, обрабатываемых в ИСПДн.

5 Область действия

Требования настоящей Политики распространяются на всех сотрудников Учреждения (штатных, временных, работающих по контракту и т.п.), а также всех прочих лиц (подрядчики, аудиторы и т.п.).

6 Система защиты персональных данных

Система защиты персональных данных (СЗПДн), строится на основании:

– *Перечня персональных данных, обрабатываемых в ИСПДн;*

– *Акта обследования ИСПДн;*

– *Модели угроз безопасности персональных данных при их обработке в ИСПДн;*

– *Руководящих документов ФСТЭК и ФСБ России.*

На основании этих документов определяется необходимый уровень защищенности ПДн каждой ИСПДн Учреждения. На основании анализа актуальных угроз безопасности ПДн, описанного в *Модели угроз*, делается заключение о необходимости использования технических средств и организационных мероприятий для обеспечения безопасности ПДн. Выбранные необходимые мероприятия отражаются в *Плане по приведению ИСПДн в соответствие требованиям ФЗ «О персональных данных»*.

Для каждой ИСПДн должен быть составлен список используемых технических средств защиты, а так же программного обеспечения, участвующего в обработке ПДн, на всех элементах ИСПДн:

- АРМ пользователей;

- СУБД;

- каналы передачи в сети общего пользования и (или) международного обмена, если по ним передаются ПДн.

В зависимости от уровня защищенности ИСПДн и актуальных угроз, СЗПДн может включать следующие технические средства:

- антивирусные средства для рабочей станции пользователя;

- модуль доверенной загрузки;

- средства межсетевого экранирования;

- средства криптографической защиты информации, при передаче защищаемой информации по каналам связи.

Так же в список должны быть включены функции защиты, обеспечиваемые штатными средствами обработки ПДн операционными системами (ОС), прикладным ПО и специальными комплексами, реализующими средства защиты. Список функций защиты может включать:

- управление и разграничение доступа пользователей;

- регистрацию и учет действий с информацией;

- обеспечивать целостность данных;

- производить обнаружения вторжений.

Список используемых технических средств отражается в *Техническом паспорте информационной системы персональных данных*. Список используемых средств должен поддерживаться в актуальном состоянии. При изменении состава технических средств защиты или элементов ИСПДн, соответствующие изменения должны быть внесены в Технический паспорт и утверждены руководителем Управления или лицом, ответственным за обеспечение безопасности ПДн.

7 Требования к подсистемам СЗПДн

СЗПДн включает в себя следующие меры:

– идентификация и аутентификация субъектов доступа и объектов доступа;

– управление доступом субъектов доступа к объектам доступа;

– ограничение программной среды;

– защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные;

– регистрация событий безопасности;

– антивирусная защита;

– обнаружение вторжений;

– контроль (анализ) защищенности персональных данных;

– обеспечение целостности информационной системы и персональных данных;

– обеспечение доступности персональных данных;

– защита технических средств;

– защита информационной системы, ее средств, систем связи и передачи данных;

– выявление инцидентов и реагирование на них;

– управление конфигурацией информационной системы и системы защиты персональных данных.

Подсистемы СЗПДн имеют различный функционал в зависимости от уровня защищенности ИСПДн, определенного в *Акте определения уровня защищенности персональных данных в ИСПДн*.

7.1 Идентификация и аутентификация субъектов доступа и объектов доступа

Меры по идентификации и аутентификации субъектов доступа и объектов доступа должны обеспечивать присвоение субъектам и объектам доступа уникального признака (идентификатора), сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверку принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности).

7.2 Управление доступом субъектов доступа к объектам доступа

Меры по управлению доступом субъектов доступа к объектам доступа должны обеспечивать управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных в информационной системе правил разграничения доступа, а также обеспечивать контроль за соблюдением этих правил.

7.3 Ограничение программной среды

Меры по ограничению программной среды должны обеспечивать установку и (или) запуск только разрешенного к использованию в информационной системе программного обеспечения или исключать возможность установки и (или) запуска запрещенного к использованию в информационной системе программного обеспечения.

7.4 Защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные

Меры по защите машинных носителей персональных данных (средств обработки (хранения) персональных данных, съемных машинных носителей персональных данных) должны исключать возможность несанкционированного доступа к машинным носителям и хранящимся на них персональным данным, а также несанкционированное использование съемных машинных носителей персональных данных.

7.5 Регистрация событий безопасности

Меры по регистрации событий безопасности должны обеспечивать сбор, запись, хранение и защиту информации о событиях безопасности в информационной системе, а также возможность просмотра и анализа информации о таких событиях и реагирование на них.

7.6 Антивирусная защита

Меры по антивирусной защите должны обеспечивать обнаружение в информационной системе компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.

7.7 Обнаружение вторжений

Меры по обнаружению (предотвращению) вторжений должны обеспечивать обнаружение действий в информационной системе, направленных на несанкционированный доступ к информации, специальные воздействия на информационную систему и (или) персональные данные в целях добывания, уничтожения, искажения и блокирования доступа к персональным данным, а также реагирование на эти действия.

7.8 Контроль (анализ) защищенности персональных данных

Меры по контролю (анализу) защищенности персональных данных должны обеспечивать контроль уровня защищенности персональных данных, обрабатываемых в информационной системе, путем проведения систематических мероприятий по анализу защищенности информационной системы и тестированию работоспособности системы защиты персональных данных.

7.9 Обеспечение целостности информационной системы и персональных данных

Меры по обеспечению целостности информационной системы и персональных данных должны обеспечивать обнаружение фактов несанкционированного нарушения целостности информационной системы и содержащихся в ней персональных данных, а также возможность восстановления информационной системы и содержащихся в ней персональных данных.

7.10 Обеспечение доступности персональных данных

Меры по обеспечению доступности персональных данных должны обеспечивать авторизованный доступ пользователей, имеющих права по доступу, к персональным данным, содержащимся в информационной системе, в штатном режиме функционирования информационной системы.

7.11 Защита технических средств

Меры по защите технических средств должны исключать несанкционированный доступ к стационарным техническим средствам, обрабатывающим персональные данные, средствам, обеспечивающим функционирование информационной системы, и в помещения, в которых они постоянно расположены, защиту технических средств от внешних воздействий, а также защиту персональных данных, представленных в виде информативных электрических сигналов и физических полей.

7.12 Защита информационной системы, ее средств, систем связи и передачи данных

Меры по защите информационной системы, ее средств, систем связи и передачи данных должны обеспечивать защиту персональных данных при взаимодействии информационной системы или ее отдельных сегментов с иными информационными системами и информационно-телекоммуникационными сетями посредством применения архитектуры информационной системы и проектных решений, направленных на обеспечение безопасности персональных данных.

7.13 Выявление инцидентов и реагирование на них

Меры по выявлению инцидентов и реагированию на них должны обеспечивать обнаружение, идентификацию, анализ инцидентов в информационной системе, а также принятие мер по устранению и предупреждению инцидентов.

7.14 Управление конфигурацией информационной системы и системы защиты персональных данных

Меры по управлению конфигурацией информационной системы и системы защиты персональных данных должны обеспечивать управление изменениями конфигурации информационной системы и системы защиты персональных данных, анализ потенциального воздействия планируемых изменений на обеспечение безопасности персональных данных, а также документирование этих изменений.

8 Пользователи ИСПДн

В ИСПДн Учреждения можно выделить следующие группы пользователей, участвующих в обработке и хранении ПДн:

- Ответственный за обеспечение безопасности персональных данных;
- Администратор безопасности ИСПДн;
- Оператор АРМ;
- Программист-разработчик ИСПДн.

Разрешительная система доступа пользователей к информационным ресурсам ИСПДн оформляется в виде *Матрицы доступа сотрудников к защищаемым персональным данным, содержащимся в информационной системе персональных данных*, утверждаемой руководителем Учреждения, и реализуется с помощью средств защиты от несанкционированного доступа. Матрица доступа должна отражать полномочия пользователей по выполнению конкретных действий в отношении информационных ресурсов ИСПДн (чтение, запись, модификация, передача).

8.1 Ответственный за обеспечение безопасности персональных данных

Ответственный за обеспечение безопасности персональных данных – сотрудник Учреждения, ответственный за организацию работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Ответственный за обеспечение безопасности персональных данных обладает следующим уровнем доступа и знаний:

- обладает полной информацией о перечне персональных данных и технических средств, входящих в информационные системы персональных данных;
- обладает полной информацией о списке лиц, доступ которых к персональным данным, обрабатываемым в информационных системах, необходим для выполнения служебных (трудовых) обязанностей;
- обладает полной информацией о текущем состоянии защищенности ИСПДн Учреждения;
- имеет доступ ко всем программным и аппаратным средствам обработки информации и данным ИСПДн;
- имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн;
- имеет доступ ко всем помещениям, где ведется обработка персональных данных.

8.2 Администратор безопасности ИСПДн

Администратор безопасности – сотрудник Учреждения, ответственный за настройку, внедрение и сопровождение ИСПДн, функционирование СЗПДн, включая обслуживание и настройку административной, серверной и клиентской компонент. Обеспечивает функционирование подсистемы управления доступом ИСПДн и уполномочен осуществлять предоставление и разграничение доступа конечного пользователя (Оператора АРМ) к элементам, хранящим персональные данные.

Администратор безопасности обладает следующим уровнем доступа и знаний:

- обладает полной информацией о системном и прикладном программном обеспечении ИСПДн;
- обладает полной информацией о технических средствах и конфигурации ИСПДн;
- имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн;
- обладает правами конфигурирования и административной настройки технических средств ИСПДн;
- имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн;
- не имеет прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных).

Администратор безопасности уполномочен:

- реализовывать политики безопасности в части настройки СКЗИ, межсетевых экранов и систем обнаружения атак, в соответствии с которыми пользователь (Оператор АРМ) получает возможность работать с элементами ИСПДн;
- осуществлять аудит средств защиты;
- устанавливать доверительные отношения своей защищенной сети с сетями других Учреждений.

8.3 Оператор АРМ

Оператор АРМ – сотрудник Учреждения, осуществляющий обработку ПДн. Обработка ПДн включает: возможность просмотра ПДн, ввод ПДн в ИСПДн, корректировка ПДн, формирование справок и отчетов по информации, полученной из ИСПДн. Оператор не имеет полномочий для управления подсистемами обработки данных и СЗПДн.

Оператор ИСПДн обладает следующим уровнем доступа и знаний:

- обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству ПДн;
- может использовать конфиденциальные данные, к которым имеет доступ, для выполнения служебных обязанностей.

8.4 Программист-разработчик ИСПДн

Программисты-разработчики (поставщики) прикладного программного обеспечения, обеспечивающие его сопровождение на защищаемом объекте. К данной группе могут относиться как сотрудники Учреждения, так и сотрудники сторонних организаций.

Лицо этой категории:

- обладает информацией об алгоритмах и программах обработки информации на ИСПДн;
- обладает возможностями внесения ошибок, недекларированных возможностей, программных закладок, вредоносных программ в программное обеспечение ИСПДн на стадии ее разработки, внедрения и сопровождения;

- может располагать любыми фрагментами информации о топологии ИСПДн и технических средствах обработки и защиты ПДн, обрабатываемых в ИСПДн.

9 Требования к персоналу по обеспечению защиты ПДн

Все сотрудники Учреждения, являющиеся пользователями ИСПДн, должны четко знать и строго выполнять установленные правила и обязанности по доступу к защищаемым объектам и соблюдению принятого режима безопасности ПДн.

При вступлении в должность нового сотрудника непосредственный начальник подразделения, в которое он поступает, обязан организовать его ознакомление с должностной инструкцией и необходимыми документами, регламентирующими требования по защите ПДн, а также обучение навыкам выполнения процедур, необходимых для санкционированного использования ИСПДн.

Сотрудник должен быть ознакомлен со сведениями настоящей Политики, принятых процедур работы с элементами ИСПДн и СЗПДн.

Сотрудники Учреждения, использующие технические средства аутентификации, должны обеспечивать сохранность идентификаторов (электронных ключей) и не допускать НСД к ним, а так же возможность их утери или использования третьими лицами. Пользователи несут персональную ответственность за сохранность идентификаторов.

Сотрудники Учреждения должны следовать Инструкции по организации парольной защиты.

Сотрудники Учреждения должны выполнять требования Инструкции пользователя ИСПДн.

При работе с ПДн в ИСПДн сотрудники Учреждения обязаны обеспечить отсутствие возможности просмотра ПДн третьими лицами с мониторов АРМ.

Сотрудники Учреждения должны быть проинформированы об угрозах нарушения режима безопасности ПДн и ответственности за его нарушение. Они должны быть ознакомлены с утвержденной формальной процедурой наложения дисциплинарных взысканий на сотрудников, которые нарушили принятые политику и процедуры безопасности ПДн.

Сотрудники обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы ИСПДн, могущих повлечь за собой угрозы безопасности ПДн, а также о выявленных ими событиях, затрагивающих безопасность ПДн, руководству подразделения и лицу, отвечающему за немедленное реагирование на угрозы безопасности ПДн.

9.1 Должностные обязанности пользователей ИСПДн

Должностные обязанности пользователей ИСПДн описаны в следующих документах:

- Инструкция ответственного за обеспечение безопасности персональных данных;
- Инструкция администратора безопасности ИСПДн;
- Инструкция пользователя ИСПДн.

10 Ответственность сотрудников ИСПДн Учреждения

В соответствии со ст. 24 Федерального закона Российской Федерации от 27 июля 2006 г. №152-ФЗ «О персональных данных» лица, виновные в нарушении требований данного Федерального закона, несут предусмотренную законодательством Российской Федерации ответственность.

Действующее законодательство РФ позволяет предъявлять требования по обеспечению безопасной работы с защищаемой информацией и предусматривает ответственность за нарушение установленных правил эксплуатации ЭВМ и систем, неправомерный доступ к информации, если эти действия привели к уничтожению, блокированию, модификации информации или нарушению работы ЭВМ или сетей (статьи 272, 273 и 274 УК РФ).

Ответственный за обеспечение безопасности персональных данных и администратор безопасности несут ответственность за все действия, совершенные от имени их учетных записей или системных учетных записей, если не доказан факт несанкционированного использования учетных записей.

При нарушениях сотрудниками Учреждения – пользователями ИСПДн правил, связанных с безопасностью ПДн, они несут ответственность, установленную действующим законодательством Российской Федерации.

Приведенные выше требования нормативных документов по защите информации должны быть отражены в Положениях о подразделениях Учреждения, осуществляющих обработку ПДн в ИСПДн, и должностных инструкциях сотрудников Учреждения.

Необходимо внести в Положения о подразделениях Учреждения, осуществляющих обработку ПДн в ИСПДн, сведения об ответственности их руководителей и сотрудников за разглашение и несанкционированную модификацию (искажение, фальсификацию) ПДн, а также за неправомерное вмешательство в процессы их автоматизированной обработки.

11 Список использованных источников

Основными нормативно-правовыми и методическими документами, на которых базируется настоящая Политика, являются:

1 Федеральный Закон № 152-ФЗ от 27.07.2006 г. «О персональных данных» (далее – ФЗ «О персональных данных»), устанавливающий основные принципы и условия обработки ПДн, права, обязанности и ответственность участников отношений, связанных с обработкой ПДн.

2 Постановление Правительства РФ № 1119 от 01.11.2012 г. «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

3 «Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», утвержденное Постановлением Правительства РФ № 687 от 15.09.2008 г.

4 «Требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных», утвержденные Постановлением Правительства РФ № 512 от 06.07.2008 г.

5 Нормативно-методические документы Федеральной службы по техническому и экспертному контролю Российской Федерации (далее - ФСТЭК России) по обеспечению безопасности ПДн при их обработке в ИСПДн:

5.1 Приказ Федеральной службы по техническому и экспортному контролю (ФСТЭК России) от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

5.2 Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утв. Зам. директора ФСТЭК России 15.02.2008г.

5.3 Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утв. Зам. директора ФСТЭК России 15.02.2008 г.

Приложение 13
от «31» декабря 2013г.
№54-п

Инструкция
по порядку учета и хранения машинных носителей конфиденциальной информации (персональных данных) в администрации Пушкинского района Санкт-Петербурга

1. Общие положения

1.1. Настоящая Инструкция разработана в соответствии с Федеральным законом № 149-ФЗ от 27.07.2006 «Об информации, информационных технологиях и о защите информации», ГОСТ Р ИСО/МЭК 17799-2015 «Практические правила управления информационной безопасностью» и другими нормативными правовыми актами, и устанавливает порядок использования машинных носителей конфиденциальной информации (персональных данных), предоставляемых администрацией Пушкинского района Санкт-Петербурга(далее - администрация Пушкинского района) для использования в информационных системах администрации.
1.2. Действие настоящей Инструкции распространяется на сотрудников администрации Пушкинского района Санкт-Петербурга, подрядчиков и третью сторону.

2. Основные термины, сокращения и определения

2.1 Администратор ИС – технический специалист, обеспечивает ввод в эксплуатацию, поддержку и последующий вывод из эксплуатации ПО и оборудования вычислительной техники.
2.2 АРМ – автоматизированное рабочее место пользователя (ПК с прикладным ПО) для выполнения определенной производственной задачи.
2.3 ИБ – информационная безопасность – комплекс организационно-технических мероприятий, обеспечивающих конфиденциальность, целостность и доступность информации.
2.4 ИС – информационная система – система, обеспечивающая хранение, обработку, преобразование и передачу информации с использованием компьютерной и другой техники.
2.5 Машинный носитель информации – материальный носитель, используемый для записи, хранения и воспроизведения информации, обрабатываемых с помощью средств вычислительной техники.
2.6 Паспорт ПК – документ, содержащий полный перечень оборудования и программного обеспечения АРМ.
2.7 ПК – персональный компьютер.
2.8 ПО – программное обеспечение вычислительной техники.
2.9 ПО вредоносное – ПО или изменения в ПО, приводящие к нарушению конфиденциальности, целостности и доступности критичной информации.

2.10 ПО коммерческое – ПО сторонних производителей (правообладателей). Предоставляется в пользование на возмездной (платной) основе.
2.11 Пользователь – сотрудник администрации Пушкинского района, использующий мобильные устройства и машинные носители информации для выполнения своих служебных обязанностей.

3. Порядок использования машинных носителей конфиденциальной информации (персональных данных)(далее- машинные носители информации)

3.1. Под использованием машинных носителей информации в ИС администрации Пушкинского района понимается их подключение к инфраструктуре ИС с целью обработки, приема/передачи информации между ИС и машинными носителями информации.
3.2. В ИС допускается использование только учтенных машинных носителей информации, которые являются собственностью администрации Пушкинского района и подвергаются регулярной ревизии и контролю.
3.3. К предоставленным администрацией Пушкинского района машинным носителям информации предъявляются те же требования ИБ, что и для стационарных АРМ (целесообразность дополнительных мер обеспечения ИБ определяется администраторами ИС).
3.4.Машинные носители информации предоставляются сотрудникам администрации Пушкинского района по инициативе руководителей структурных подразделений в случаях:
- необходимости выполнения вновь принятым сотрудником своих должностных обязанностей;
- возникновения у сотрудника администрации Пушкинского района производственной необходимости.

4. Порядок учета, хранения и обращения с машинными носителями информации, твердыми копиями и их утилизации.

4.1. Все находящиеся на хранении и в обращении машинные носители информации в администрации Пушкинского района подлежат учёту.
4.2. Каждый машинных носитель информации с записанной на нем информацией должен иметь этикетку, на которой указывается его уникальный учетный номер.
4.3. Учет и выдачу машинных носителей информации осуществляет администратор ИС. Факт выдачи машинного носителя информации фиксируется в журнале учета машинных носителей информации.
4.4. Сотрудники администрации Пушкинского района могут получать машинный носитель от уполномоченного сотрудника для выполнения работ на конкретный срок. При получении делаются соответствующие записи в журнале учета.
По окончании работ пользователь сдает машинный носитель информации для хранения уполномоченному сотруднику, о чем делается соответствующая запись в журнале учета.
4.5. При использовании сотрудниками машинных носителей информации необходимо:
4.5.1. Соблюдать требования настоящей Инструкции.
4.5.2. Использовать машинные носители информации исключительно для выполнения своих служебных обязанностей.

4.5.3. Ставить в известность администраторов ИС о любых фактах нарушения требований настоящей Инструкции.
4.5.4. Бережно относиться к машинным носителям информации.
4.5.5. Обеспечивать физическую безопасность машинных носителей информации всеми разумными способами, в том числе хранением носителя в сейфе.
4.5.6. Извещать администраторов ИС о фактах утраты (кражи) машинных носителей информации.
4.6. При использовании машинных носителей информации запрещено:
4.6.1. Использовать машинные носители информации в личных целях.
4.6.2. Передавать машинные носители информации другим лицам (за исключением администраторов ИС).
4.6.3. Хранить машинные носители информации вместе с носителями открытой информации, на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам;
4.6.4. Выносить машинные носители информации из служебных помещений для работы с ними на дому либо в других помещениях (местах).
4.7. Любое взаимодействие (обработка, прием, передача информации), инициированное сотрудником администрации Пушкинского района между ИС и неучтенными (личными) носителями информации, рассматривается как несанкционированное (за исключением случаев оговоренных с администраторами ИС заранее). Администратор ИС оставляет за собой право блокировать или ограничивать использование машинных носителей информации.
4.8. Информация об использовании сотрудником администрации Пушкинского района машинных носителей информации в ИС протоколируется и, при необходимости, может быть предоставлена ответственному лицу за организацию обработки персональных данных в администрации Пушкинского района.
4.9. В случае выявления фактов несанкционированного и/или нецелевого использовании машинных носителей информации инициализируется служебная проверка, проводимая комиссией, состав которой утвержден главой администрации Пушкинского района.
4.10. По факту выясненных обстоятельств составляется акт расследования инцидента и передается главе администрации Пушкинского района для принятия мер согласно действующему законодательству.
4.11. Информация, хранящаяся на машинных носителях информации, подлежит обязательной проверке на отсутствие вредоносного ПО.
4.12. При отправке или передаче информации адресатам на машинные носители информации записываются только предназначенные адресатам данные. Отправка информации адресатам на машинных носителях информации осуществляется в порядке, установленном для документов для служебного пользования.
4.13. Вынос машинных носителей информации для непосредственной передачи адресату осуществляется только с письменного разрешения руководителя структурного подразделения.
4.14. В случае утраты или уничтожения машинных носителей информации либо разглашении содержащихся в них сведений, об этом немедленно ставится в известность руководитель соответствующего структурного подразделения. По факту утраты носителя составляется акт. Соответствующие отметки вносятся в журналы учета машинных носителей информации.

4.15.Машинные носители информации, пришедшие в негодность, или отслужившие установленный срок, подлежат уничтожению. Уничтожение машинных носителей информации осуществляется уполномоченной комиссией. По результатам уничтожения машинных носителей информации составляется акт по прилагаемой форме.
4.16. В случае увольнения или перевода сотрудника в другое структурное подразделение, предоставленные ему машинные носители информации изымаются.

5.Ответственность

5.1. Сотрудники, нарушившие требования настоящей Инструкции, несут ответственность в соответствии с действующим законодательством.

Приложение к Инструкции
по порядку учета и хранению
машинных
носителейконфиденциальной
информации (персональных данных)

Акт
об уничтожении (машинных, бумажных)носителей конфиденциальной информации (персональных данных)

Комиссия в составе:
Председатель – _____
Члены комиссии – _____

провела отбор (машинных, бумажных) носителей персональных данных и установила, что в соответствии с требованиями руководящих документов по защите информации
_____ информация, записанная на них в процессе эксплуатации, подлежит гарантированному уничтожению:

№ п/п	Дата	Тип носителя	Регистрационный номер носителя ПДн	Кол-во	Примечание

Всего (машинных, бумажных) носителей
_____
(цифрами и прописью)

На указанных носителях персональные данные уничтожены путем
_____.
(стирания на устройстве гарантированного уничтожения информации и т.п.)

Перечисленные материальные носители ПДн уничтожены путем
_____.
(разрезания, сжигания, механического уничтожения и т.п.)
Председатель комиссии: _____ /_____/
Члены комиссии: _____ /_____/

Примечание:

1. Акт составляется раздельно на каждый способ уничтожения машинных носителей.
2. Все листы акта, а также все произведенные исправления и дополнения в акте заверяются подписями всех членов комиссии.

Утверждаю
директор МОУ «СОШ № 39»
_____А.Н. Кузнецова
Дата_____

Учет, хранение и уничтожение машинных носителей содержащих персональные данные, и порядок обращения с ними в МОУ «СОШ №39»

1. Общие положения

1.1. Настоящий порядок, определяет организационно-техническое обеспечение процессов обращения и порядок учёта, маркировки, хранения, передачи другим лицам, ремонта, технического обслуживания и уничтожения носителей содержащих персональные данные.

1.2. Действие установленного порядка распространяется на всех должностных лиц.

1.3. Ответственность за исполнение настоящего порядка возлагается на лицо, ответственное за защиту информации.

2. Машинные носители информации (персональных данных)

2.1. Машинные носители информации - изделия и устройства, предназначенные для записи и обработки информации входящие в состав средств вычислительной техники (СВТ), а также для хранения и перемещения записанной информации на внешние носители информации.

Виды МНИ:

- жесткие магнитные диски;
- гибкие магнитные диски;
- оптические и магнитооптические диски;
- устройства долговременной электронной памяти (флешь-память);

Типы МНИ:

а) съемные носители информации, устанавливаются и/или подключаются к СВТ на время сеанса работы пользователя, а по окончанию его отключаются и хранятся в определенном хранилище;

б) несъемные носители информации в процессе работы пользователя не снимаются и не изымается из состава СВТ автоматизированной системы и находится там постоянно.

3. Порядок обращения с машинными носителями содержащие персональные данные

3.1. Все МНИ подлежат обязательному учету в «Журнале учета машинных носителей защищаемых информационных ресурсов» (Приложение № 1).

3.2. Ответственность за ведение журнала возлагается на ответственного за защиту информации.

3.3. Выдача МНИ фиксируется в документе «Журнал учета машинных носителей защищаемых информационных ресурсов» и подтверждается подписью

пользователя.

3.4. Все МНИ должны маркироваться и содержать учетный номер, дату ввода в эксплуатацию, наименование органа исполнительной власти Ленинградской области (владельца МНИ).

МНИ содержащие биометрические персональные данные должны позволять идентифицировать информационную систему персональных данных, в которую была осуществлена запись биометрических персональных данных, а также оператора, осуществившего такую запись.

3.5. Съемные носители информациимаркируются этикеткой, закрепленной на лицевой стороне носителя.

3.6. Несъёмные носители информации учитываются отдельно и (или) в составе СВТ. При этом маркируется сам носитель или корпус СВТ, в состав которого входит носитель.

3.7. СВТ в состав которого входит МНИ, вскрывается в присутствии Ответственного за защиту информациии должностного лица эксплуатирующего данное СВТ.

4. Правила хранение носителей защищаемых информационных ресурсов

4.1. При хранении МНИ должны соблюдаться условия, обеспечивающие сохранность информации, и исключающие к ним несанкционированный доступ, хищение, подмену и уничтожение.

4.2. Хранение и использование МНИ должно осуществляться в условиях, соответствующих техническим условиям изготовителя и не более установленного срока эксплуатации.

4.3. Необходимо обеспечивать раздельное хранение материальных носителей персональных данных, обработка которых осуществляется в различных целях, а также носителей персональных данных от носителей, содержащих иную защищаемую информацию.

4.4. Для хранения носителей информации используются хранилища (сейфы, металлические шкафы, и т.п.), оборудованные внутренними замками с двумя или более дубликатами ключей и приспособлениями для опечатывания замочных скважин или кодовыми замками.

В случае если на съемном МНИ хранятся только данные в зашифрованном с использованием средств криптографической защиты информации (СКЗИ) виде, допускается хранение таких носителей в служебных помещениях вне сейфов (металлических шкафов).

4.5. МНИ с резервными копиями защищаемой информации не выдаются для работы обычным пользователям и служат только для восстановления в случае аварии или поломки основного МНИ. МНИ с резервными копиями рекомендуется хранить в отдельном хранилище.

4.6. В случае если на основании договора, хранение носителей поручено другому лицу, существенным условием такого договора является обязанность обеспечения таким лицом безопасности переданной ему защищаемой информации.

5. Порядок уничтожения носителей защищаемых информационных ресурсов

5.1. МНИ подлежат уничтожению в следующих случаях:

- достижения целей обработки информации или в случае утраты необходимости в их достижении, для носителей, уничтожение информации на которых невозможно без уничтожения самого носителя;
- выхода из строя, повреждение МНИ, в результате которого невозможно осуществлять корректную обработку информации с использованием данного носителя;
- возникновения иных обстоятельств, в результате которых необходимо уничтожить носители, содержащие защищаемую информацию.

5.2. Уничтожение осуществляется ответственным за защиту информации, с составлением акта об уничтожении МНИ, которые хранятся не менее трех лет.

5.3. Вышедшие из строя МНИ ремонту не подлежат. Такие носители уничтожаются методом разборки и физического разрушения.

5.4. Уничтожение МНИ должно обеспечивать полное физическое и невосстановимое уничтожение информации, содержащейся на таких носителях.

6. Права и обязанности работников при обращении с носителями защищаемых информационных ресурсов

6.1. Запрещается выносить носители из служебных помещений (за пределы контролируемой зоны) для работы с ними на дому, в гостиницах, общественном транспорте и т.д.

6.2. Права на перемещение МНИ за пределы контролируемой зоны предоставлено только тем лицам, которым оно необходимо для выполнения своих должностных обязанностей (функции).

6.3. Запрещается принимать и передавать МНИ без соответствующего разрешения и оформления в установленном порядке.

6.4. Должностное лицо, осуществляющее работу с МНИ, обязано работать только с вверенными ему МНИ. Самовольная передача МНИ другим лицам запрещается.

6.5. Запрещается хранить МНИ на рабочих столах, либо оставлять их без присмотра.

6.6. Руководители подразделений, в которых осуществляется работа с МНИ, должны пресекать действия, которые могут привести к хищению или разрушению носителей.

6.7. О фактах утраты носителей немедленно должен быть поставлен в известность ответственный за защиту информации.

Приложение № 1

Журнал учета машинных носителей защищаемых информационных ресурсов

Учетный номер	Регистрационный номер	Вид (съемный/несъемный)	Тип носителя (магнитный, оптический и т.п.)	Дата поступления	Расписка в получении (ФИО, подпись, дата)	Расписка в обратном приеме (ФИО, подпись, дата)	Место хранения (№ помещения)	Дата и номер акта об уничтожении	Примечание
1	2	3	4	5	6	7	8	9	10

Приложение №11
к приказу «наименование организации»
«О вводе в действие комплекта
организационно-распорядительной документации
по организации обработки и защите информации в ИС»
от « ___ » _____ 20___ г. № ____

ИНСТРУКЦИЯ
по защите машинных носителей информации

1. ВВЕДЕНИЕ
   1.1. Настоящая инструкция определяет порядок учета, хранения, выдачи, уничтожения и ограничения использования машинных носителей информации в организации «наименование» (далее – Организация).
   1.2. Машинный носитель информации (далее МНИ) – это материальный носитель, используемый для передачи и хранения защищаемой информации (в том числе персональных данных) в электронном виде. Машинные носители информации делятся на съемные и несъемные носители.
      1.2.1. Несъемные машинные носители информации являются частью автоматизированного рабочего места (далее АРМ) или сервера и в процессе эксплуатации не предполагают демонтаж.
      1.2.2. К съемным носителям относятся любые технические устройства, предназначенные для запоминания информации, оперативно подключаемые к АРМ или серверу в целях записи на них информации из памяти АРМ (или сервера) или считывания с них информации в память АРМ (или сервера).

2. УЧЕТ МАШИННЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ
   2.1. Все используемые в информационной системе (далее ИС) машинные носители информации подлежат учёту.
   2.2. Учет, хранение и выдачу носителей информации осуществляет администратор безопасности. При увольнении администратора безопасности составляется акт приема-сдачи учетных документов и носителей.
   2.3. Учет всех видов и типов носителей информации производится в Журнале учета машинных носителей информации (ПРИЛОЖЕНИЕ №1 к настоящей Инструкции).
   2.4. На несъемную часть носителей ИС наносится уникальный в пределах Организации учетный номер.

3. ВЫДАЧА МАШИННЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ

3.1. Пользователи ИС получают учтенный носитель от администратора безопасности, для выполнения работ на конкретный срок.

3.2. При получении пользователем носителя информации делается соответствующая запись в Журнале учета машинных носителей информации.

3.3. По окончании работ или установленного срока использования пользователь ИС сдает носитель информации администратору безопасности, о чем делается соответствующая запись в Журнале учета машинных носителей информации.

4. ИСПОЛЬЗОВАНИЕ МАШИННЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ

4.1. На машинные носители информации записываются исключительно информация и программные средства обработки информации, содержащейся в ИС.

4.2. Носители информации, допускающие повторную запись информации, проходят процедуру многократной перезаписи общедоступной информации перед повторным использованием или ремонтом с целью гарантированного уничтожения остаточной информации. Процедуру перезаписи организует и контролирует администратор безопасности.

4.3. Вынос учтенных носителей информации за пределы установленных мест обработки информации допустим только с письменного разрешения администратора безопасности.

4.4. Передача носителей, содержащих информацию, которая обрабатывается в ИС сторонним организациям или третьим лицам производится по приказу руководителя Организации через администратора безопасности. Администратор безопасности производит в этом случае необходимые отметки в Журнале учета машинных носителей информации.

5. ХРАНЕНИЕ МАШИННЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ

5.1. Хранение МНИ осуществляется в условиях, препятствующих несанкционированному ознакомлению с информацией, копированию, изменению или уничтожению информации, содержащейся на машинных носителях.

5.2. МНИ хранятся в служебных помещениях, в отведенных для этих целей хранилищах, исключающих несанкционированный доступ к ним.

5.3. ЗАПРЕЩАЕТСЯ хранить носители информации на рабочих столах, оставлять их без присмотра, передавать на хранение третьим лицам.

6. ДЕЙСТВИЯ ПРИ УТРАТЕ И ПОРЧЕ МНИ

6.1. В случае утраты или порчи пользователем МНИ, содержащих обрабатываемую в ИС информацию, немедленно ставится в известность администратор безопасности. Администратор безопасности вносит соответствующую запись в журнал учета машинных носителей информации.

6.2. По факту утраты или порчи машинных носителей информации администратор безопасности проводит служебное расследование в установленном порядке.

6.3. Носители, пришедшие в негодность или с истекшим сроком эксплуатации, подлежат уничтожению в установленном порядке.

7. УНИЧТОЖЕНИЕ МАШИННЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ

7.1. Уничтожение машинных носителей информации организует администратор безопасности с составлением Акта уничтожения машинных носителей информации.

7.2. Уничтожение носителей информации производится способом, гарантирующим невозможность восстановления информации, содержавшейся на носителе. Такими способами являются: механическое, электрическое, электромагнитное, химическое или термическое воздействие на носитель, применение специального программного обеспечения для уничтожения информации на носителе. Способ уничтожения выбирается администратором безопасности в зависимости от типа носителя и возможностей Организации.

8. ОГРАНИЧЕНИЯ И ОТВЕТСТВЕННОСТЬ

8.1. Всем пользователям ИС запрещено использовать учтенные машинные носители информации для личных целей.

8.2. Пользователям запрещено передавать носители информации кому-либо, осуществлять учет, хранение и выдачу носителей информации, обрабатываемой в ИС. Передача носителей информации осуществляется в порядке, предусмотренном п. 4.5 и п. 4.6 настоящей Инструкции.

8.3. Любое взаимодействие (чтение, запись информации, запуск программного обеспечения) между техническими средствами ИС, СЗИ и неучтенными носителями информации запрещено.

8.4. В случае выявления фактов утраты, несанкционированного и (или) нецелевого использования учтенных носителей информации, использования неучтенных

(личных) носителей информации в ИС назначается служебное расследование. По результату расследования и по представлению администратора безопасности, руководитель Организации принимает решение о привлечении пользователя ИС к ответственности согласно локальным нормативным актам Организации и действующему законодательству.

8.5. Сотрудники Организации, несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей предусмотренных настоящей Инструкцией, в пределах, определенных действующим законодательством Российской Федерации.

9. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

9.1. Пользователи ИС должны быть предупреждены об ответственности за невыполнение требований настоящей Инструкции и ознакомлены с Инструкцией до начала работы в ИС.

9.2. Обязанность ознакомления пользователей ИС с настоящей Инструкцией лежит на администраторе безопасности.

10. НОРМАТИВНЫЕ И ПРАВОВЫЕ ДОКУМЕНТЫ

10.1. Приказ ФСТЭК России от 18.02.2013 года №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

10.2. Приказ ФСТЭК России от 23.03.2017 года №49 «О внесении изменений в состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденные приказом федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. № 21, и в требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, утвержденные приказом федеральной службы по техническому и экспортному контролю от 14 марта 2014 г. № 31».

10.3. Постановление Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Директор Ф.И.О.

ПРИЛОЖЕНИЕ № 1
к Инструкции «По защите
машинных носителей информации»

ЖУРНАЛ
учета машинных носителей информации.

Начат: «___» _____ 20__ г.

Окончен: «___» _____ 20__ г.

1	2	3	4	5	6	7	8
Учетный / заводской номер	Наименование (марка) носителя	Вид носителя (съемный /несъемный)	Место установки (для несъемных носителей)	Ф.И.О. лица, эксплуатирующего носитель	Дата получения съемного носителя и подпись	Дата возврата съемного носителя и подпись администратора	Отметка об уничтожении носителя
инв. № 1000013	*USB flash drive Transcend JF V30/2Gb*	*съемный*	*нет*	*Иванов И.И.*	*01.01.2017_____(Иванов И.И.)*	*12.06.2017 _____(Сидоров И.И.)*	*уничтожен 20.06.2017*

ПРАВИЛА

по формированию и ведению журнала учета машинных носителей персональных данных.

ФОРМИРОВАНИЕ ЖУРНАЛА.

Журнал формируется из стандартных листов формата А4 в альбомной ориентации:
Обложка журнала изготавливается на отдельном листе.
Все листы журнала, за исключением листов обложки, нумеруются.
Все листы журнала, вместе с обложкой сшиваются.

ВЕДЕНИЕ ЖУРНАЛА.

Перед началом использования журнала на лицевой стороне обложки указывается номер журнала по номенклатуре дел (журналов) на текущий год и дата начала ведения журнала.
Графы журнала заполняются следующим образом:
Графа 1 – учетный или заводской номер носителя (**например – инв. № 1000013**) .
Графа 2 – наименование носителя (**например – USB flash drive Transcend JF V30/2Gb.**).
Графа 3 – указывается съемный или несъемный носитель (**например – съемный**).
Графа 4 – для несъемных носителей указывается АРМ пользователя.
Графа 5 – ФИО пользователя (**например – Иванов И.И.**).
Графа 6 – дата получения носителя и подпись пользователя безопасности (**например – 01.01.2017_____(Иванов И.И.)**).
Графа 7 – дата возврата носителя и подпись администратора безопасности (**например – 12.06.2017 _____(Сидоров И.И.))**
Графа 8 – отметку делает администратор безопасности после уничтожения носителя (**например – уничтожен 20.06.2017**).
Все записи в журнале делаются четко и разборчиво. В случае если вносимые данные не помещаются на одной строке (в одной ячейке), то используется несколько строк.

УТВЕРЖДАЮ
Директор КГКУ
«Региональный центр оценки качества
образования»

_____В.Ф. Макуха

« ___ » _____ 20___ г.

АКТ № _____

уничтожения машинных носителей информации

г. Хабаровск « ___ » _____ 20___ г.

Проведен отбор машинных носителей информации и установлено, что информация, записанная на них в процессе эксплуатации, в соответствии с действующим законодательством Российской Федерации, подлежит уничтожению:

№ п/п	Дата	Тип носителя	Регистрационный номер носителя

Всего носителей _____
(цифрами и прописью количество)

На указанных носителях информация уничтожена путем

_____

(стирания на устройстве гарантированного уничтожения информации и т.п.)

Перечисленные носители уничтожены путем

_____.

(механического уничтожения, сжигания и т.п.)

Администратор безопасности:

_____ _____

(ФИО) (подпись)

Приложение № _
к приказу от «__» _____ 2017 г. №_____

ПРАВИЛА
обращения с машинными носителями информации в информационных системах Полное наименование организации

1. Общие положения

1.1. Настоящие правила рассматривают вопросы защиты машинных носителей информации в информационных системах Полное наименование организации (далее – ИС Краткое наименование организации) от несанкционированного доступа к ним, уничтожения, а также неразрешенного раскрытия, модификации, удаления информации на них.

1.2. В качестве машинных носителей информации в настоящей инструкции рассматриваются:

- машинные носители информации, встроенные в корпус средств вычислительной техники (накопители на жестких дисках),
- съемные машинные носители информации (перечислить тип),
- портативные вычислительные устройства, имеющие встроенные носители информации.

1.3. Под использованием машинных носителей информации в ИС Краткое наименование организации понимается их подключение к инфраструктуре ИС Краткое наименование организации с целью обработки, приема/передачи информации между информационной системой и носителями информации.

1.4. Данные правила обязательны для применения во всех подразделениях Краткое наименование организации, в которых обрабатывается информация ограниченного доступа (в том числе персональные данные), не содержащая сведения, составляющие государственную тайну.

2. Использование машинных носителей информации

2.1. В ИС Краткое наименование организации допускается использование только учтенных машинных носителей информации, которые являются собственностью Краткое наименование организации и подвергаются регулярной ревизии и контролю.

2.2. Машинные носители информации предоставляютсясотрудникам Краткое наименование организации по инициативе начальника структурного подразделения в случаях:

- необходимости выполнения вновь принятым сотрудником своих должностных обязанностей;
- возникновения у сотрудника Краткое наименование организации производственной необходимости.

2.3. При использовании сотрудниками машинных носителей информации необходимо:

2.3.1. Использовать машинные носители информации исключительно для выполнения своих служебных обязанностей.

2.3.2. Ставить в известность Ответственного за защиту информации в Краткое наименование организации о любых фактах нарушения требований настоящих правил.

2.3.3. Бережно относиться к машинным носителям информации.

2.3.4. Обеспечивать физическую безопасность машинных носителей информации.

2.3.5. Извещать Ответственного за защиту информации о фактах утраты (кражи) машинных носителей информации.

2.3.6. Перед началом работы с машинными носителями информации пользователь обязан проверять их на наличие вредоносных программ (вирусов) с помощью штатных антивирусных программ. В случае обнаружения вирусов, пользователь обязан действовать в соответствии с «Инструкцией по антивирусной защите».

2.4. При использовании машинных носителей информации запрещено:

2.4.1. Использовать машинные носители информации в личных целях.

2.4.2. Передавать носители информации другим лицам (за исключением администратора информационной безопасности).

2.4.3. Оставлять машинные носители информации без присмотра или передавать на хранение другим лицам;

2.4.4. Выносить машинные носители информации из служебных помещений для работы с ними на дому и т. д.

2.5. Ответственность за подключение машинных носителей информации, не учтенных соответствующим образом, не прошедших проверку, несет пользователь, подключивший данное устройство.

3. Хранение и учёт машинных носителей информации

3.1. Все находящиеся на хранении и в обращении машинные носители информации в Краткое наименование организации подлежат обязательному учёту. На каждый машинный носитель должна наноситься маркировка, позволяющая его идентифицировать.

3.2. Регистрацию машинных носителей информации осуществляет Ответственный за защиту информации в Журнале регистрации, учета и выдачи машинных носителей информации (далее – Журнал регистрации) путем занесения регистрационного или иного номера с указанием пользователя или группы пользователей, которым разрешен доступ к машинным носителям информации.

3.3. Учет выдачи машинных носителей информации ведётся Ответственным за обработку и защиту информации в Журнале регистрации, в котором указывается маркировка носителя, дата, время, фамилия, имя и отчество должностного лица, получившего средство, его роспись.

3.4. сотрудники Краткое наименование организации получают учтенный машинный носитель от Ответственного за обработку и защиту информации для выполнения работ на конкретный срок. При получении делаются соответствующие записи в Журнале регистрации. По окончании работ пользователь сдает машинный носитель для хранения Ответственному за защиту информации, о чем делается соответствующая запись в журнале регистрации.

3.5. При поступлении нового машинного носителя информации, который будет использоваться в ИС Краткое наименование организации, Ответственный за защиту информации регистрирует его в Журнале регистрации. Перед использованием новый машинный носитель информации в обязательном порядке должен пройти антивирусную проверку (при наличии технической возможности).

3.6. При передаче средств вычислительной техники (далее – СВТ) ИС Краткое наименование организации сторонним организациям для проведения ремонтно-восстановительных или иных работ, несъемные машинные носители (накопители на жестких дисках) изымаются из состава СВТ.

3.7. В случае возврата машинного носителя информации в Журнале регистрации Ответственным за защиту информации проставляется отметка о возврате с указанием даты, времени возврата, личных подписей передающей и принимающей стороны.

3.8. В случае увольнения или перевода сотрудника в другое структурное подразделение предоставленные машинные носители информации изымаются.

3.9. Хранить машинные носители информации нужно вдали от источников электромагнитного излучения и тепла.

4. Ликвидация машинных носителей информации и уничтожение (стирание) информации на машинных носителях

4.1. В случае утраты или уничтожения машинных носителей информации немедленно ставятся в известность начальник соответствующего структурного подразделения и Ответственный и защиту информации. На утраченные носители составляется акт (приложение 1). Соответствующие отметки вносятся в Журнал регистрации.

4.2. Машинные носители информации, пришедшие в негодность или отслужившие установленный срок, должны быть уничтожены без возможности восстановления с составлением Акта уничтожения машинных носителей информации (по прилагаемой форме) и последующей регистрацией в Журнале регистрации. Уничтожение машинных носителей осуществляется комиссией.

4.3. В Краткое наименование организации обеспечивается уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) информации:

4.3.1. Уничтожение (стирание) информации на машинных носителях исключает возможность восстановления защищаемой информации при передаче машинных носителей между пользователями, в сторонние организации для ремонта или утилизации. Уничтожению (стиранию) подлежит информация, хранящаяся на цифровых и нецифровых, съемных и несъемных машинных носителях информации.

4.3.2. В ИС Краткое наименование организации используются следующие меры по уничтожению (стиранию) информации на машинных носителях, исключающие возможность восстановления защищаемой информации:

– перезапись уничтожаемых (стираемых) файлов случайной битовой последовательностью, удаление записи о файлах, обнуление журнала файловой системы

или полная перезапись всего адресного пространства машинного носителя информации случайной битовой последовательностью с последующим форматированием.

4.4. Ответственный за обработку и защиту информации обеспечивает регистрацию и контроль действий по удалению защищаемой информации и уничтожению машинных носителей информации путем составления соответствующих актов, и занесением в Журнал регистрации.

5. Ответственность

5.1. Ответственность за выполнение правил эксплуатации машинных носителей информации при выполнении непосредственных работ со средствами несут пользователи ИС Краткое наименование организации.

5.2. Контроль выполнения установленных правил эксплуатации и регистрацию и учёт машинных носителей информации осуществляет ответственный за защиту информации.

Приложение 1

Типовые формы актов

«УТВЕРЖДАЮ»

_____

«___» _____ 2017 г.

АКТ

уничтожения машинных носителей информации

Комиссия, наделенная полномочиями приказом _____ от №___ в составе:

_____

(должности, ФИО)

провела отбор машинных носителей информации, не подлежащих дальнейшему хранению:

№ п/п	Дата	Учетный номер машинного носителя	Примечание

Всего машинных носителей_____(цифрами и прописью)

На машинных носителях уничтожена вся информация путем:

_____

_____

_____.

Перечисленные машинные носители уничтожены

_____

путем (сжигания, измельчения, плавления и другое),

_____

Председатель комиссии:

Члены комиссии: _____ _____ *(подпись)*

_____ _____ *(подпись)*

_____ _____ *(подпись)*

_____ _____ *(подпись)*

«___» _____ 2017 г.

«УТВЕРЖДАЮ»

_____

«___» _____ 2017 г.

АКТ

утери машинных носителей информации

Комиссия, наделенная полномочиями приказом _____ от №___ в составе:

_____

(должности, ФИО)

постановила считать следующие машинные носители информации утерянными:

№ п/п	Дата	Учетный номер машинного носителя	Примечание

Всего машинных носителей _____(цифрами и прописью)

На машинных носителях хранилась следующая информация:

_____

_____

Носители были утеряны _____(дата) при следующих обстоятельствах:

_____

_____

_____

Председатель комиссии:

Члены комиссии: _____ _____
(подпись)

_____ _____
(подпись)

_____ _____
(подпись)

_____ _____
(подпись)

«___» _____ 2017 г.

«УТВЕРЖДАЮ»

_____

«___» _____ 2017 г.

АКТ

уничтожения информации на машинных носителей информации

Комиссия, наделенная полномочиями приказом _____ от №___ в составе:

_____

(должности, ФИО)

провела удаление информации, хранящейся на машинных носителях:

№ п/п	Дата	Учетный номер машинного носителя	Перечень защищаемой информации, удаленный с машинного носителя

На машинных носителях уничтожена перечисленная информация путем:

_____

_____

_____.

Председатель комиссии: _____ _____
(подпись)

Члены комиссии: _____ _____
(подпись)

_____ _____
(подпись)

_____ _____
(подпись)

«___» _____ 2017 г.

Лист ознакомления

с Правилами обращения с машинными носителями информации информационных системах Полное наименование организации

№ п/п	Дата ознакомления	ФИО сотрудников	Подпись сотрудников
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			
11.			
12.			
13.			
14.			
15.			
16.			
17.			
18.			
19.			
20.			