

Российская Федерация
Тюменская область
Ханты-Мансийский автономный округ - Югра
Департамент образования и молодежной политики
Ханты-Мансийского автономного округа - Югры
казенное общеобразовательное учреждение
Ханты-Мансийского автономного округа – Югры
«Сургутская школа с профессиональной подготовкой
для обучающихся с ограниченными возможностями здоровья»

ПРИКАЗ

«26» августа 2016 г.

№ 346

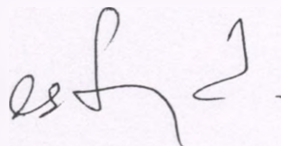
Об утверждении
Положения «По обеспечению
безопасности персональных
данных при обработке в
автоматизированной системе»

На основании письма № 10-Исх-6852 от 28.07.2016 г. Департамента образования и молодежной политики Ханты-Мансийского автономного округа-Югры, в целях обеспечения безопасности персональных данных КОУ «Сургутская школа с профессиональной подготовкой».

ПРИКАЗЫВАЮ:

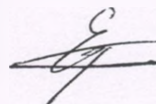
1. Утвердить Положение «по обеспечению безопасности персональных данных при обработке в автоматизированной системе казенного общеобразовательного учреждения Ханты-Мансийского автономного округа – Югры «Сургутская школа с профессиональной подготовкой для обучающихся с ограниченными возможностями здоровья».
2. Контроль за исполнением приказа оставляю за собой.

Директор



В.А. Цыганкова

Визы:
Техник



С.М. Ермаков

Рассылка:

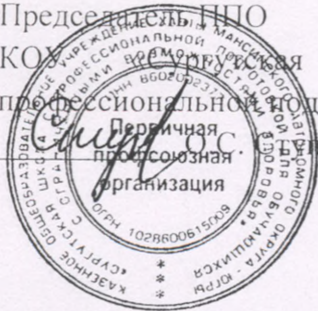
в дело – 1 экз.,

зам. директора по УПРИБ – 1 экз.,

СОГЛАСОВАНО:

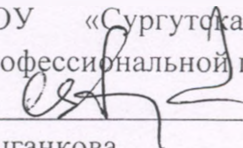
Председатель ЦПО

КОУ «Сургутская школа с профессиональной подготовкой» филиал



УТВЕРЖДЕНО:

Приказом директора
КОУ «Сургутская школа с профессиональной подготовкой»


В.А.

Цыганкова

приказ № 346 от 26 августа 2016 г.

ПРИНЯТО:

Педагогическим советом

№ 1 от 25 августа 2016 г.

КОУ «Сургутская школа с профессиональной подготовкой»

Положение

по обеспечению безопасности персональных данных при обработке в автоматизированной системе казенного общеобразовательного учреждения
Ханты-Мансийского автономного округа – Югры
«Сургутская школа с профессиональной подготовкой
для обучающихся с ограниченными возможностями здоровья»

г. Сургут, 2016 г.

1. Общие положения

Настоящее Положение определяет порядок и правила организации и проведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, в которых обработка данных осуществляется с использованием средств автоматизации (далее - ИСПДн) в КОУ «Сургутская школа с профессиональной подготовкой» (далее - Учреждение).

Работы по обеспечению безопасности ПДн при их обработке в информационных системах являются неотъемлемой частью работ по созданию информационных систем.

При обработке ПДн в информационной системе должно быть обеспечено:

- проведение мероприятий, направленных на предотвращение несанкционированного доступа (далее - НСд) к ПДн и (или) передачи их лицам, не имеющим права доступа к такой информации;
- своевременное обнаружение фактов НСд к ПДн;
- недопущение воздействия на технические средства автоматизированной обработки ПДн, в результате которого может быть нарушено их функционирование;
- возможность незамедлительного восстановления ПДн, модифицированных или уничтоженных вследствие НСд к ним;
- постоянный контроль за обеспечением уровня защищенности ПДн.

Мероприятия по обеспечению безопасности ПДн при их обработке в ИСПДн включают в себя:

- определение угроз безопасности ПДн при их обработке, формирование на их основе модели угроз;
- разработку на основе модели угроз системы защиты ПДн, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты ПДн, предусмотренных для соответствующего класса ИСПДн;
- установку и ввод в эксплуатацию СЗПДн в соответствии с эксплуатационной и технической документацией;
- обучение лиц, использующих СЗПДн, применяемые в ИСПДн, правилам работы с ними;
- учет применяемых СЗПДн, эксплуатационной и технической документации к ним, носителей ПДн;
- контроль за соблюдением условий использования СЗПДн, предусмотренных эксплуатационной и технической документацией;
- разбирательство и составление заключений по фактам несоблюдения условий хранения носителей ПДн, СЗПДн, которые могут привести к нарушению конфиденциальности ПДн или другим нарушениям, приводящим к снижению уровня защищенности ПДн, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;
- описание системы защиты ПДн.

2. Общий порядок организации работ по защите ПДн при их обработке в ИСПДн

2.1. Под организацией обеспечения безопасности ПДн при их обработке в ИСПДн понимается формирование совокупности мероприятий, осуществляемых на всех стадиях жизненного цикла ИСПДн, согласованных по цели, задачам, месту и времени, направленных на предотвращение (нейтрализацию) и парирование угроз безопасности ПДн в ИСПДн, на восстановление нормального функционирования ИСПДн после нейтрализации угрозы, с целью минимизации как непосредственного, так и опосредованного ущерба от возможной реализации таких угроз.

Обеспечение безопасности ПДн при их обработке в ИСПДн должно проводиться путем выполнения комплекса организационных и технических мероприятий (применения технических средств) в рамках системы (подсистемы) защиты ПДн, развертываемой в ИСПДн в процессе ее создания или модернизации.

2.2. Порядок организации обеспечения безопасности ПДн в ИСПДн должен предусматривать:

- оценку обстановки;
- обоснование требований по обеспечению безопасности ПДн и формулирование задач защиты ПДн;
- разработку замысла обеспечения безопасности ПДн;
- выбор целесообразных способов (мер и средств) защиты ПДн в соответствии с задачами и замыслом защиты;

- решение вопросов управления обеспечением безопасности ПДн в динамике изменения обстановки и контроля эффективности защиты;
- обеспечение реализации принятого замысла защиты;
- планирование мероприятий по защите ПДн;
- организацию и проведение работ по созданию системы защиты персональных данных в рамках разработки (модернизации) ИСПДн, в том числе с привлечением специализированных сторонних организаций к разработке и развертыванию СЗПДн или ее элементов в ИСПДн, а также решение основных задач взаимодействия, определение их задач и функций на различных стадиях создания и эксплуатации ИСПДн;

- разработку документов, регламентирующих вопросы организации обеспечения безопасности ПДн и эксплуатации СЗПДн в ИСПДн;

- развертывание и ввод в опытную эксплуатацию СЗПДн в ИСПДн;

- доработку СЗПДн по результатам опытной эксплуатации.

2.3. Оценка обстановки является этапом, во многом определяющим эффективность решения задач обеспечения безопасности ПДн. Она основывается на результатах комплексного обследования ИСПДн, в ходе которого, прежде всего, проводится определение защищаемой информации и ее категорирование по важности.

2.4. При оценке обстановки определяется необходимость обеспечения безопасности ПДн от угроз:

- уничтожения, хищения аппаратных средств ИСПДн, и (или) носителей информации путем физического доступа к элементам ИСПДн;

- утечки информации по каналам побочных электромагнитных излучений и наводок (ПЭМИН);

- перехвата информации при передаче по проводным (кабельным) линиям связи;

- хищения, несанкционированной модификации или блокирования информации за счет НСд с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий);

- воспрепятствования функционированию ИСПДн путем преднамеренного электромагнитного воздействия на ее элементы;

- непреднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.

2.5. При оценке обстановки должна учитываться степень ущерба, который может быть причинен в случае неправомерного использования соответствующих ПДн.

2.6. Обоснование требований по обеспечению безопасности ПДн, обрабатываемых в ИСПДн, проводится в соответствии с нормативными и методическими документами уполномоченных федеральных органов исполнительной власти, обязательными к применению стандартами.

2.7. При выборе способов обеспечения безопасности ПДн, обрабатываемых в ИСПДн, необходимо определить организационные меры и технические (аппаратные, программные и программно-аппаратные) средства защиты. При выборе технических средств защиты следует использовать сертифицированные СЗПДн.

2.8. Решение вопросов управления обеспечением безопасности ПДн в динамике изменения обстановки и контроля эффективности защиты является важным аспектом поддержания требуемого уровня безопасности ПДн.

К основным вопросам управления относятся:

- распределение функций управления доступом к данным и их обработкой между должностными лицами;

- определение порядка изменения правил доступа к ПДн;

- определение порядка изменения правил доступа к резервируемым информационным и аппаратным ресурсам;

- определение порядка действий должностных лиц в случае возникновения нештатных ситуаций;

- определение порядка проведения контрольных мероприятий и действий по его результатам.

2.9. Контроль заключается в проверке выполнения требований нормативных документов по защите информации, а также в оценке обоснованности и эффективности, принятых мер. Он может

проводиться Учреждением или на договорной основе сторонними организациями, имеющими лицензии на деятельность по технической защите конфиденциальной информации.

2.10. Решение основных вопросов обеспечения защиты ПДн должно предусматривать подготовку кадров, выделение необходимых финансовых и материальных средств, закупку и разработку программного и аппаратного обеспечения.

2.11. При подготовке документации по вопросам обеспечения безопасности ПДн при их обработке в ИСПДн и эксплуатации СЗПДн в обязательном порядке разрабатываются:

- положение по организации и проведению работ по обеспечению безопасности ПДн при их обработке в ИСПДн;
- требования по обеспечению безопасности ПДн при обработке в ИСПДн;
- должностные инструкции персоналу ИСПДн в части обеспечения безопасности ПДн при их обработке в ИСПДн;
- рекомендации (инструкции) по использованию программных и аппаратных средств защиты информации.

2.12. Испытания СЗПДн проводятся в процессе развертывания и ввода в опытную эксплуатацию ИСПДн в соответствии с частным техническим заданием. Заключение по результатам испытаний должно содержать вывод о степени соответствия СЗПДн заданным требованиям по обеспечению безопасности ПДн.

3. Организационная структура системы обеспечения безопасности персональных данных при их обработке в ИСПДн и обязанности должностных лиц

3.1. Систему обеспечения безопасности персональных данных при их обработке в ИСПДн образуют:

- ответственный за защиту персональных данных и техническую защиту информации в ИСПДн, он же администратор безопасности ИСПДн в Учреждении;
- сотрудники Учреждения (пользователи ИСПДн), доступ которых к персональным данным, обрабатываемым в информационных системах, необходим для выполнения служебных (трудовых) обязанностей.

4. Обязанности должностных лиц, эксплуатирующих ИСПДн, в части обеспечения безопасности ПДн при их обработке в ИСПДн

4.1. Администратор безопасности ИСПДн обязан:

- знать правила эксплуатации используемых в ИСПДн средств защиты информации (в том числе криптографических), средств антивирусной защиты, правила резервирования и восстановления общего и специального программного обеспечения, а также баз ПДн;
- осуществлять резервирование и восстановление общего и специального программного обеспечения, а также баз ПДн;
- контролировать обновление общего и специального программного обеспечения ИСПДн в соответствии с эксплуатационной документацией;
- генерировать, распределять и выдавать личные пароли пользователям ИСПДн;
- проводить первичный инструктаж пользователей ИСПДн в части эксплуатации СЗПДн;
- осуществлять контроль настроек СЗПДн в соответствии с эксплуатационной документацией на них и установленными правилами разграничения доступа;
- осуществлять периодический контроль электронных журналов СЗПДн, антивирусной защиты и систем управления базами ПДн.

4.2. Пользователи ИСПДн, должны:

- соблюдать требования по обеспечению безопасности ПДн;
- знать правила эксплуатации СЗПДн, используемых в ИСПДн (проверяется администратором безопасности ИСПДн в форме зачетного практического занятия);
- строго соблюдать технологию обработки ПДн и правила эксплуатации СЗПДн;
- сообщать администратору безопасности ИСПДн о ставших им известными попытках посторонних лиц получить доступ к техническим средствам ИСПДн;
- немедленно уведомлять администратора безопасности ИСПДн о фактах утраты носителей ПДн, личных идентификаторов, ключей от помещений, личных печатей и о других фактах, которые могут привести к разглашению защищаемых ПДн;

- сдать личный идентификатор при увольнении или отстранении от исполнения служебных обязанностей.

5. Порядок разбирательства и составления заключений по фактам несоблюдения условий хранения носителей ПДн, использования СЗПДн и нарушения порядка предоставления ПДн, которые могут привести к нарушению конфиденциальности ПДн или другим нарушениям, разработка и принятие мер по предотвращению возможных опасных последствий подобных нарушений

5.1. При обнаружении нарушений порядка предоставления ПДн пользователям, ИСПДн незамедлительно приостанавливается до выявления причин нарушений и устранения этих причин.

5.2. Основаниями для приостановки обработки ПДн в ИСПДн и проведения разбирательства являются:

- предоставление ПДн в нарушение установленных правил;
- допуск к ИСПДн лица, не имеющего на то разрешения;
- утрата носителя ПДн;
- нарушение правил хранения носителей ПДн;
- нарушение правил эксплуатации СЗПДн;
- нарушение правил парольной защиты;
- нарушение правил защиты от программно-математических воздействий (антивирусной защиты);
- нарушение правил резервирования и восстановления общего и специального программного обеспечения, а также баз ПДн;
- выявление несанкционированного внесения изменений в состав технических средств ИСПДн;
- выявления других фактов НСД в ИСПДн, в т.ч. нарушения физического доступа в помещение (оставление без присмотра) где ведется обработка ПДн в нарушении установленных правил.

5.3. Разбирательство проводится администратором безопасности информации в ИСПДн с привлечением пользователя ИСПДн.

5.4. В ходе разбирательства составляется заключение, в котором отражается:

- состав группы проводившей разбирательство;
- период времени, в который проводилось разбирательство;
- основание для проведения разбирательства;
- факты, выявленные в ходе разбирательства и имеющие значение в определении наличия нарушений конфиденциальности ПДн или нарушений правил использования СЗПДн, а также иные факты, которые могут привести к нарушению конфиденциальности ПДн или к снижению уровня защищенности ПДн;
- вывод о значимости нарушений, их причинах и виновных, допустивших данные нарушения;
- рекомендации по совершенствованию обеспечения безопасности ПДн, исключающие в дальнейшем подобные нарушения.

5.5. Заключение передать директору.

6. Мероприятия по техническому обеспечению безопасности ПДн при их обработке в ИСПДн

6.1. В интересах технического обеспечения безопасности ПДн при их обработке в ИСПДн в зависимости от класса информационной системы должны быть реализованы следующие мероприятия:

- мероприятия по защите от НСД к ПДн при их обработке в ИСПДн;
- мероприятия по защите информации от утечки по техническим каналам.

6.2. В состав мероприятий по защите ПДн при их обработке в ИСПДн от НСД и неправомерных действий входят следующие мероприятия:

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

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

- защита информации при межсетевом взаимодействии ИСПДн;
- антивирусная защита;
- обнаружение вторжений.

6.3. Мероприятия по защите ПДн реализуются в рамках подсистем:

- управления доступом;
- регистрации и учета;
- обеспечения целостности;
- антивирусной защиты;
- обнаружения вторжений.

Термины и 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, характеризующееся 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 уграждение, 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 описанному 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 определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

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, контролирующего 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, заблокировать, уничтожить информацию или уничтожить и модифицировать программное обеспечение информационной системы персональных данных и (или) заблокировать 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.

Учреждение - учреждения здравоохранения, социальной сферы, труда и занятости.

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).

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 ТКУИ - технические каналы утечки информации УБПДн - угрозы безопасности персональных данных