Принято:

на педагогическом совете МКДОУ «Звездочка» пгт Славянка

Протокол № 3 от «25» 03. 2022 г.

Утверждаю:

Заведующий МКДОУ «Звездочка»

_____ М.Б. Борунова

Приказ № 12 от «25» 03. 2022 г

РЕКОМЕНДАЦИИ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

Содержание

Обозначения и сокращения
АТС – автоматическая телефонная станция
ИСПДн – информационная система персональных данных
МЭ – межсетевой экран
НСД – несанкционированный доступ
ОС – операционная система
ОТСС – основные технические средства связи
ПДн – персональные данные
ПЭМИН – побочные электромагнитные излучения и наводки
ПМВ – программно-математическое воздействие
СЗПДн – система защиты персональных данных

1. Термины и определения
В настоящем документе используются следующие термины и их определения:
Блокирование персональных данных – временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи. 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 к информации – возможность получения информации и ее использования.
Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.
Зона 1 – пространство вокруг аппаратных средств информационных систем персональных данных, на границе и за пределами которого уровень наведенного от аппаратных средств информационных систем персональных данных информативного сигнала в технических средствах, а также в посторонних проводах и линиях передачи информации, имеющих выход за пределы контролируемой зоны, не превышает нормированного значения.
Зона 2 – пространство вокруг аппаратных средств информационных систем персональных данных, на границе и за пределами которого напряженность электромагнитного поля информативного сигнала не превышает нормированного значения.
Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.
Информационная система персональных данных – 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, представления, распространения информации и способы осуществления таких

процессов и методов.
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 распространения 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.
Не декларированные возможности – функциональные возможности средств вычислительной техники и (или) программного обеспечения, 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, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по своим функциональному предназначению и техническим характеристикам.
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.
Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.
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, 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.
Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.
Программная закладка – скрытно внесенный в программное обеспечение функциональный объект, который при определенных условиях способен обеспечить несанкционированное программное воздействие. Программная закладка может быть реализована в виде вредоносной программы или программного кода.
Программное (программно-математическое) воздействие – несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.
Ресурс информационной системы – именованный элемент системного, прикладного

или аппаратного обеспечения функционирования информационной системы.
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.
Технические средства информационной системы персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (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.
Технический канал утечки информации – совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.
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.
Уполномоченное оператором лицо – лицо, которому на основании договора оператор поручает обработку персональных данных.
Целостность информации – состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право.

2. Общие положения

Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (далее – рекомендации) разработаны ФСТЭК России на основании Федерального закона от 27 июля 2006 г. No 152-ФЗ «О персональных данных» и постановления Правительства Российской Федерации от 17 ноября 2007 г. No 781 « Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» с учетом действующих нормативных документов ФСТЭК России по защите информации.
Рекомендации предназначены для использования при проведении работ по обеспечению безопасности персональных данных (ПДн) при их обработке в следующих информационных системах персональных данных (ИСПДн):
ИСПДн государственных органов, организующих и (или) осуществляющих обработку персональных данных, а также определяющих цели и содержание обработки персональных данных;
ИСПДн муниципальных органов, организующих и (или) осуществляющих обработку

персональных данных, а также определяющих цели и содержание обработки персональных данных;
ИСПДн юридических лиц, организующих и (или) осуществляющих обработку персональных данных, а также определяющих цели и содержание обработки персональных данных;
ИСПДн физических лиц, организующих и (или) осуществляющих обработку персональных данных, а также определяющих цели и содержание обработки персональных данных (за исключением случаев, когда последние используют указанные системы исключительно для личных и семейных нужд).
В рекомендациях рассматриваются вопросы обеспечения безопасности ПДн, оценки опасности угроз безопасности ПДн, применения способов, мер и средств защиты ПДн. Документ предназначен для использования операторами ИСПДн, специалистами по обеспечению безопасности информации, руководителями организаций, проводящих работы по обработке ПДн в ИСПДн.

3. Понятие информационной системы персональных данных. Классификация информационных систем персональных данных

В соответствии с Федеральным законом «О персональных данных» под информационной системой персональных данных понимается информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных. В настоящем документе рассматриваются только ИСПДн, в которых обработка данных осуществляется с использованием средств автоматизации.
Классификация ИСПДн осуществляется с учетом категорий и объема накапливаемых, обрабатываемых и распределяемых с их использованием ПДн
с целью установления методов и средств защиты, необходимых для обеспечения безопасности ПДн. Состав и функциональное содержание методов и средств защиты зависит от вида и степени ущерба, возникающего вследствие реализации угроз безопасности ПДн.
При этом ущерб возникает за счет неправомерного или случайного уничтожения, изменения, блокирования, копирования, распространения ПДн или от иных неправомерных действий с ними. В зависимости от объекта, причинение ущерба которому, в конечном счете, вызывается неправомерными действиями с ПДн, рассматриваются два вида ущерба: непосредственный и опосредованный.
Непосредственный ущерб связан с причинением физического, материального, финансового или морального вреда непосредственно субъекту ПДн. Он возникает за счет незаконного использования (в том числе распространения) ПДн или за счет несанкционированной модификации этих данных и может проявляться в виде:
нанесения вреда здоровью субъекта ПДн;
незапланированных и (или) непроизводительных финансовых или материальных затрат субъекта; потери субъектом свободы действий вследствие шантажа и угроз, осуществляемых с использованием ПДн; нарушения конституционных прав субъекта вследствие вмешательства в его личную жизнь путем осуществления контактов с ним по различным поводам без его на то согласия (например – рассылка персонифицированных рекламных предложений и т.п.).
Опосредованный ущерб связан с причинением вреда обществу и (или) государству вследствие нарушения нормальной деятельности экономических, политических, военных, медицинских, правоохранительных, социальных, кредитно-финансовых и иных государственных органов, органов местного самоуправления, муниципальных органов, организаций различных форм собственности за счет неправомерных действий с ПДн.
Классификация ИСПДн проводится государственными органами, муниципальными

органами, юридическими и физическими лицами, организующими и(или) осуществляющими обработку ПДн, а также определяющими цели и содержание обработки ПДн (операторами ИСПДн) в соответствии с Порядком проведения классификации информационных систем персональных данных, утвержденным приказом ФСТЭК России, ФСБ России и Мининформсвязи России от 13 февраля 2008 г. No55/86/20.
Классификация ИСПДн проводится на этапе их создания или в ходе их эксплуатации (для ранее введенных в эксплуатацию и (или) модернизируемых информационных систем) с целью установления методов и средств защиты информации, необходимых для обеспечения безопасности персональных данных.
Проведение классификации информационных систем включает в себя следующие этапы: сбор и анализ исходных данных по информационной системе;
присвоение информационной системе соответствующего класса и его документальное оформление.

При проведении классификации информационной системы учитываются следующие исходные данные:
категория обрабатываемых в информационной системе персональных данных – ХПД;
объем обрабатываемых персональных данных (количество субъектов персональных данных, персональные данные которых обрабатываются в информационной системе) – ХНПД; заданные оператором характеристики безопасности персональных данных, обрабатываемых в информационной системе; структура информационной системы; наличие подключений информационной системы к сетям связи общего пользования и (или) сетям международного информационного обмена; режим обработки персональных данных; режим разграничения прав доступа пользователей информационной системы; местонахождение технических средств информационной системы.
Определяются следующие категории обрабатываемых в информационной системе персональных данных (ХПД):
категория 1 – персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни;
категория 2 – персональные данные, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию, за исключением персональных данных, относящихся к категории 1;
категория 3 – персональные данные, позволяющие идентифицировать субъекта персональных данных;
категория 4 – обезличенные и (или) общедоступные персональные данные.
В зависимости от объема обрабатываемых в ИСПДн персональных данных ХНПД может принимать следующие значения:
1 – в информационной системе одновременно обрабатываются персональные данные более чем 100 000 субъектов ПДн или персональные данные субъектов ПДн в пределах субъекта Российской Федерации или Российской Федерации в целом;
2 – в информационной системе одновременно обрабатываются персональные данные от 1000 до 100 000 субъектов ПДн или персональные данные субъектов ПДн, работающих в отрасли экономики Российской Федерации, в органе государственной власти, проживающих в пределах муниципального образования;
3 – в информационной системе одновременно обрабатываются персональные данные менее чем 1000 субъектов ПДн или персональные данные субъектов ПДн в пределах конкретной организации.
По заданным оператором характеристикам безопасности персональных данных, обрабатываемых в информационной системе, информационные системы подразделяются на типовые и специальные информационные системы.
Типовые информационные системы – информационные системы, в которых требуется

обеспечение только конфиденциальности персональных данных.
Специальные информационные системы – информационные системы,
в которых вне зависимости от необходимости обеспечения конфиденциальности персональных данных требуется обеспечить хотя бы одну из характеристик безопасности персональных данных, отличную от конфиденциальности (защищенность от уничтожения, изменения, блокирования, а также иных несанкционированных действий).
К специальным информационным системам должны быть отнесены:
информационные системы, в которых обрабатываются персональные данные, касающиеся состояния здоровья субъектов ПДн;
информационные системы, в которых предусмотрено принятие на основании исключительно автоматизированной обработки персональных данных решений.

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ

ПОДЛИННОСТЬ ДОКУМЕНТА ПОДТВЕРЖДЕНА.
ПРОВЕРЕНО В ПРОГРАММЕ КРИПТОАРМ.

ПОДПИСЬ

Общий статус подписи:	Подпись верна
Сертификат:	00BE23600A3B08150EB5C58F3A5D8EFE59
Владелец:	RU, Приморский край, пгт Славянка, Заведующий, МУНИЦИПАЛЬНОЕ КАЗЕННОЕ ДОШКОЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ "ДЕТСКИЙ САД "ЗВЕЗДОЧКА" ПГТ СЛАВЯНКА ХАСАНСКОГО МУНИЦИПАЛЬНОГО РАЙОНА, 04372428951, 253100235390, certmgr@list.ru, Марина Борисовна, Борунова, Борунова Марина Борисовна
Издатель:	Казначейство России, Казначейство России, RU, г. Москва, Большой Златоустинский переулок, д. 6, строение 1, 1047797019830, 7710568760, 77 Москва, uc_fk@roskazna.ru
Срок действия:	Действителен с: 01.03.2022 15:33:00 UTC+10 Действителен до: 25.05.2023 14:42:00 UTC+10
Дата и время создания ЭП:	05.04.2022 10:58:32 UTC+10