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

ОСНОВНЫЕ МЕРОПРИЯТИЯ ПО ОРГАНИЗАЦИИ И ТЕХНИЧЕСКОМУ ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОБРАБАТЫВАЕМЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

Содержание

Обозначения и сокращения
АВС – антивирусные средства
ВПр – вредоносная программа
ИСПДн – информационная система персональных данных
КЗ – контролируемая зона
МЭ – межсетевой экран
НДВ – недекларированные возможности
НСД – несанкционированный доступ
ПДн – персональные данные
ПМВ – программно-математическое воздействие
ПО – программное обеспечение
ПЭВМ – персональная электронно-вычислительная машина
ПЭМИН – побочные электромагнитные излучения и наводки
САЗ – система анализа защищенности
СЗИ – средства защиты информации
СЗПДн – система (подсистема) защиты персональных данных
СОВ – система обнаружения вторжений

1. Термины и определения
В настоящем документе используются следующие термины и их определения:
Безопасность персональных данных – состояние защищенности персональных данных, при котором обеспечиваются их конфиденциальность, доступность и целостность при их обработке в информационных системах персональных данных.
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 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.
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.
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.
Контролируемая зона – пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.
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.
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 – 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

2.1. Настоящий документ разработан на основе Федерального закона от 27 июля 2006 г. No 152-ФЗ «О персональных данных» и в соответствии с «Положением об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденным постановлением Правительства Российской Федерации от 17 ноября 2007 г. No 781, с целью совершенствования методического обеспечения деятельности в данной области государственных и муниципальных органов, юридических и физических лиц, организующих и (или) осуществляющих обработку персональных данных (ПДн), определяющих цели и содержание обработки ПДн (операторов), а также заказчиков и разработчиков информационных систем персональных данных (ИСПДн) при решении ими задач по обеспечению безопасности ПДн.
2.2. Обеспечение безопасности ПДн при их обработке в ИСПДн достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным

данным, результатом которого могут стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иные несанкционированные
действия.
Мероприятия по обеспечению безопасности ПДн формулируются в зависимости от класса ИСПДн, определяемого с учетом возможного возникновения угроз безопасности жизненно важным интересам личности, общества и государства.
2.3. Положения настоящего документа не распространяются на ИСПДн, обрабатывающие ПДн, отнесенные в установленном порядке к сведениям, составляющими государственную тайну. Порядок и содержание мероприятий по защите информации, содержащей сведения, составляющие государственную тайну, определяются в соответствии с нормативными и методическими документами в области защиты государственной тайны.
2.4. Настоящий документ является методическим документом, определяющим мероприятия по организации и техническому обеспечению безопасности ПДн (не криптографическими методами) при их обработке в ИСПДн, в интересах решения задач: проведения мероприятий, направленных на предотвращение несанкционированного доступа к ПДн и (или) передачи их лицам, не имеющим права доступа к такой информации; своевременного обнаружения фактов несанкционированного
доступа (НСД) к ПДн; недопущения воздействия на технические средства автоматизированной обработки ПДн, в результате которого может быть нарушено их функционирование; возможности незамедлительного восстановления ПДн, модифицированных или уничтоженных вследствие НСД к ним; постоянного контроля за обеспечением уровня защищенности ПДн.
Обеспечение безопасности ПДн с использованием криптографических методов в настоящем документе не рассматривается. Порядок организации и обеспечения указанных работ определяется в соответствии с нормативными документами Федеральной службы безопасности Российской Федерации.
2.5. Настоящий документ применяется для обеспечения безопасности ПДн при их обработке в ИСПДн следующих видов:
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).
2.6. Работы по обеспечению безопасности ПДн при их обработке
в ИСПДн являются неотъемлемой частью работ по созданию ИСПДн. Результатом этих работ должно являться создание системы (подсистемы) защиты персональных данных ИСПДн.
2.7. Для обеспечения безопасности ПДн при их обработке в ИСПДн осуществляется защита речевой информации и информации, обрабатываемой техническими средствами, а также информации, представленной в виде информативных электрических сигналов, физических полей, носителей на бумажной, магнитной, оптической и иной основе, в виде информационных массивов и баз данных в ИСПДн.

2.8. Основными мероприятиями по организации и техническому обеспечению безопасности ПДн в ИСПДн являются:
мероприятия по организации обеспечения безопасности ПДн, включая классификацию ИСПДн; мероприятия по техническому обеспечению безопасности ПДн при их обработке в ИСПДн, включающие мероприятия по размещению, специальному оборудованию, охране и организации режима допуска в помещения, где ведется работа с ПДн, мероприятия по закрытию технических каналов утечки ПДн при их обработке в информационных системах, мероприятия по защите ПДн от несанкционированного доступа и определению порядка выбора средств защиты ПДн при их обработке в ИСПДн.
2.9. При обработке ПДн в ИСПДн возможно возникновение угроз безопасности ПДн, включающих совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к ПДн.
Модель угроз применительно к конкретной ИСПДн разрабатывается в соответствии с «Методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» на основе «Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных».
Выявление и учет угроз безопасности ПДн в конкретных условиях составляют основу для планирования и осуществления мероприятий, направленных на обеспечение безопасности ПДн при их обработке в ИСПДн.
3. Основные мероприятия по организации обеспечения безопасности персональных данных
3.1. Под организацией обеспечения безопасности ПДн при их обработке в ИСПДн понимается формирование и реализация совокупности согласованных по цели, задачам, месту и времени организационных и технических мероприятий, направленных на минимизацию ущерба от возможной реализации угроз безопасности ПДн.
3.2. Обязанности по реализации необходимых организационных и технических мероприятий для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения ПДн, а также иных неправомерных действий с ними, возлагаются на оператора.
Для разработки и осуществления мероприятий по организации и обеспечению безопасности ПДн при их обработке в ИСПДн оператором или уполномоченным им лицом должно назначаться структурное подразделение или должностное лицо (работник), ответственное за обеспечение безопасности ПДн.
3.3. Технические и программные средства, используемые для обработки ПДн в ИСПДн, должны удовлетворять установленным в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.
Средства защиты информации, применяемые в ИСПДн, в установленном порядке проходят процедуру оценки соответствия, включая сертификацию на соответствие требованиям по безопасности информации.
3.4. Обеспечение безопасности ПДн осуществляется путем выполнения комплекса организационных и технических мероприятий, реализуемых в рамках создаваемой системы (подсистемы) защиты персональных данных (СЗПДн). Структура, состав и основные функции СЗПДн определяются исходя из класса ИСПДн. СЗПДн включает организационные меры и технические средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки ПДн), а также используемые в информационной системе информационные технологии.
3.5. Рекомендуются следующие стадии создания СЗПДн:
предпроектная стадия, включающая предпроектное обследование ИСПДн, разработку

технического (частного технического) задания на ее создание;
стадия проектирования (разработки проектов) и реализации ИСПДн, включающая разработку СЗПДн в составе ИСПДн;
стадия ввода в действие СЗПДн, включающая опытную эксплуатацию и приемо-сдаточные испытания средств защиты информации, а также оценку соответствия ИСПДн требованиям безопасности информации.
3.6. На предпроектной стадии по обследованию ИСПДн рекомендуются следующие мероприятия: устанавливается необходимость обработки ПДн в ИСПДн;
определяется перечень ПДн, подлежащих защите от НСД;
определяются условия расположения ИСПДн относительно границ контролируемой зоны (КЗ); определяются конфигурация и топология ИСПДн в целом и ее отдельных компонентов, физические, функциональные и технологические связи как внутри этих систем, так и с другими системами различного уровня и назначения;
определяются технические средства и системы, предполагаемые к использованию в разрабатываемой ИСПДн, условия их расположения, общесистемные и прикладные программные средства, имеющиеся и предлагаемые к разработке;
определяются режимы обработки ПДн в ИСПДн в целом и в отдельных компонентах;
определяется класс ИСПДн;

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 10:37:55 UTC+10