

ПРИНЯТО
На Педагогическом совете № 1
МБДОУ «Детский сад № 210»
Протокол № от 24.08.2016г.

«УТВЕРЖДАЮ»
Заведующий МБДОУ
«Детский сад № 210»
Н.В.Мартынова
Приказ № 97/О от 09.09.2016г



ПОЛОЖЕНИЕ
по организации и проведению работ по обеспечению
безопасности персональных данных при их обработке в
информационных системах персональных данных
муниципального бюджетного дошкольного
образовательного учреждения «Детский сад № 210»

г. Нижний Новгород
2016 год

1. Термины, определения и сокращения

1.1. 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.

1.2. Блокирование персональных данных - временное прекращение сбора, систематизации, накопления, использования, распространения и передачи персональных данных.

1.3. 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.

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

1.5. Доступ к персональным данным - возможность получения персональных данных и их использования.

1.6. Защита информации от несанкционированного доступа (защита от НСД) или воздействия - деятельность, направленная на предотвращение получения информации заинтересованным субъектом (или воздействия на информацию) с нарушением установленных прав или правил.

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

1.8. Информация - сведения (сообщения, данные) независимо от формы их представления.

1.9. Информационная система персональных данных (ИСПДн) - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

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

1.11. 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.

1.12. Машинный носитель информации - любое техническое устройство, предназначенное для фиксации, хранения, накопления, преобразования и передачи компьютерной информации (дискеты, компакт-диски, жесткие диски, USB-устройства и т.п.).

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

- 1.14. Несанкционированный доступ (НСД) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационной системой.
- 1.15. Обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.
- 1.16. Объект доступа - единица информационного ресурса информационной системы персональных данных, доступ к которой регламентируется правилами разграничения доступа.
- 1.17. Оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.
- 1.18. Персональные данные (ПДн) - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).
- 1.19. Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.
- 1.20. Программная закладка - код программы, преднамеренно внесенный в программу с целью осуществить утечку, изменить, блокировать, уничтожить персональные данные или уничтожить и модифицировать программное обеспечение информационной системы персональных данных и (или) блокировать аппаратные средства.
- 1.21. Санкционированный доступ к персональным данным - доступ к персональным данным, не нарушающий правила разграничения доступа.
- 1.22. Система защиты информации от НСД (СЗИ НСД) – комплекс организационных мер и программно-технических (в том числе криптографических) средств защиты информации от несанкционированного доступа (несанкционированных действий с ней) в информационной системе персональных данных.
- 1.23. Средства вычислительной техники (СВТ) – совокупность программных и технических элементов систем обработки персональных данных, способных функционировать самостоятельно или в составе других систем.
- 1.24. Субъект доступа - лицо или процесс, действия которого регламентируются правилами разграничения доступа.
- 1.25. Технический канал утечки информации - совокупность носителя персональных данных (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.
- 1.26. 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 информационных системах персональных данных.

1.27. Шифровальные (криптографические) средства - аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты информации при передаче по каналам связи и (или) для защиты информации от несанкционированного доступа при ее обработке и хранении.

1.28. Шифрование - способ преобразования открытой информации в закрытую, и обратно. Применяется для хранения важной информации в ненадежных источниках или передачи её по незащищенным каналам связи.

1.29. Электронная подпись - информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

2. Общие положения

2.1. Настоящее положение определяет цели, задачи, содержание, порядок организации и выполнения мероприятий по защите персональных данных (далее ПДн) в ходе её обработки в информационных системах персональных данных (далее ИСПДн) МБДОУ «Детский сад № 210» (далее *организации*).

2.2. Положение разработано в соответствии с Федеральным законом от 27 июля 2006 года №149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27 июля 2006 года №152-ФЗ «О персональных данных», постановлением Правительства РФ от 01 ноября 2012 года №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказом Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 года № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», приказом Федеральной службы по техническому и экспортному контролю от 18 февраля 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», а так же другими принятыми нормативно-методическими и организационно-распорядительными документами по обеспечению безопасности информации.

2.3. Должностные лица, осуществляющие обработку персональных данных, а также организующие эксплуатацию (разработку) информационных систем персональных данных, несут персональную ответственность за соблюдение требований настоящего Положения.

2.4. Защита ПДн, обрабатываемой в ИСПДн, является составной частью работ по созданию и эксплуатации ИСПДн и должна осуществляться в установленном настоящим Положением порядке во взаимосвязи с другими мерами по защите информации.

2.5. Технические и программные средства, применяемые в целях защиты информации в ходе ее обработки в ИСПДн должны иметь сертификат соответствия по требованиям безопасности информации, выданный уполномоченным органом.

2.6. Проведение любых работ по созданию и эксплуатации ИСПДн без принятия необходимых мер по защите информации, определенных настоящим Положением, не допускается.

2.7. Требования настоящего Положения не распространяются на информационные системы, обрабатывающие информацию, отнесенную в установленном порядке к сведениям, составляющим государственную тайну.

2.8. Финансирование мероприятий по обеспечению безопасности ПДн, при их обработке в ИСПДн осуществляется за счет средств сметы расходов *организации*.

2.9. Изменения в текст настоящего Положения вносятся порядком, предусмотренным для его утверждения.

3. Замысел обеспечения безопасности персональных данных

3.1. Цели защиты ПДн состоят в обеспечении:

- конфиденциальности информации (защите от утечки, разглашения информации ограниченного доступа);
- целостности информации (защите информации от искажения и уничтожения);
- доступности информации (защите от блокировки доступа к информации пользователей).

3.2. Защита ПДн обеспечивается реализацией комплекса программно-аппаратных средств и организационных мероприятий по противодействию потенциальным угрозам, которые направлены на объект защиты и могут нанести ущерб.

3.3. В качестве основных угроз безопасности ПДн в ходе её обработки в ИСПДн *организации* необходимо рассматривать:

- хищение, модификация или блокирование информации за счет несанкционированного доступа с применением программно-аппаратных и программных средств;
- уничтожение, хищение аппаратных средств информационной системы, носителей информации путем физического доступа к элементам информационной системы;
- просмотр информации с экранов дисплеев и других средств ее отображения;
- непреднамеренные действия персонала и нарушение безопасности функционирования ИСПДн и средств защиты информации в их составе из-за сбоев в программном обеспечении, а также угроз антропогенного и стихийного характера.

3.4. Конкретная ИСПДн, как объект защиты, характеризуется своей совокупностью угроз, зависящей от структурно-функциональных характеристик ИСПДн, условий в которых создается или функционирует система. Каждая ИСПДн имеет уязвимости, используя которые могут быть реализованы угрозы и нарушена защита.

3.5. Основной целью мероприятий по защите ПДн, обрабатываемых в ИСПДн, является снижение риска и исключения возможности получения ущерба в условиях действия преднамеренных и непреднамеренных угроз информационной безопасности, а также минимизации возможного ущерба в случае утечки информации, содержащей персональные данные, и ожидаемых затрат на достижение поставленной цели.

4. Организация и проведение работ по обеспечению безопасности информации ограниченного доступа

4.1. Обязанности должностных лиц

4.1.1. Ответственность за безопасность ПДн в подразделениях *организации* и общее руководство организацией работ по защите ПДн возлагается на *руководителя организации*.

4.1.2. Оперативное руководство организацией работ и координацию деятельности по защите ПДн возлагается на ответственного за обеспечение безопасности информации на объектах вычислительной техники, назначаемого приказом *руководителя организации*.

4.1.3. Ответственность за правильную организацию работ, соблюдение требований по защите ПДн при их обработке в ИСПДн, ведение организационно-распорядительной документации на ИСПДн возлагается на руководителей подразделений (управлений, отделов, секторов), осуществляющих в своей деятельности обработку ПДн на средствах вычислительной техники.

4.1.4. На каждом автоматизированном рабочем месте ИСПДн назначается должностное лицо ответственное за безопасность ПДн на данном рабочем месте.

4.1.5. Для своевременной разработки и осуществления необходимых мероприятий по защите ПДн в ИСПДн назначается администратор безопасности ИСПДн. Обязанности и права администратора безопасности отражаются в «Инструкция администратору безопасности».

4.1.6. Должностные лица, осуществляющие обработку ПДн в ИСПДн, несут персональную ответственность за выполнение установленных правил и требований по обеспечению безопасности ПДн. **Обязанности и права пользователей информационной системы отражаются в «Инструкция пользователя ИСПДн».**

4.1.7. **Должностные инструкции руководителей соответствующих** уровней и ответственных исполнителей, занимающихся обработкой персональных данных в ИСПДн, должны быть приведены в соответствие с требованиями законодательства Российской Федерации по защите персональных данных.

4.2. Порядок допуска сотрудников к обработке ПДн в ИСПДн

4.2.1. Перечень должностных лиц, допущенных к обработке ПДн в ИСПДн (допущенных к работе), а также перечень должностных лиц, допущенных к техническому обслуживанию аппаратных и программных средств информационной системы, утверждается *руководителя организации*.

4.2.2. Нахождение посторонних лиц в помещении, где расположена ИСПДн (ее элементы) допускается только в присутствии допущенных лиц.

4.3. Требования к помещению, размещению аппаратных средств ИСПДн и учету машинных носителей информации

4.3.1. Организация охраны и допуска в помещения, где эксплуатируется ИСПДн, должны исключать возможность неконтролируемого проникновения или пребывания в помещениях посторонних лиц, не имеющих права доступа в помещения, а так же обеспечить сохранность ПДн.

4.3.2. Требования к режиму охраны помещений, в том числе правила допуска работников и посетителей в рабочее и нерабочее время, устанавливается правовым актом.

4.3.3. Входные двери помещений, в которых располагаются аппаратные средства ИСПДн, а также машинные носители информации должны оборудоваться замками, гарантирующими надежное закрытие помещений в нерабочее время, в них также могут устанавливаться кодовые и электронные замки.

4.3.4. Уборка помещений должна производиться под контролем сотрудников, имеющих самостоятельный доступ в помещения и постоянно в них работающих в соответствии с утвержденным перечнем указанных лиц.

4.3.5. При обнаружении несанкционированного проникновения в помещение пользователь ИСПДн обязан немедленно сообщить о происшедшем ответственному за эксплуатацию ИСПДн. По данному происшествию проводится расследование с обязательным составлением акта.

4.3.6. Для исключения просмотра (с экранов дисплеев и др. средств отображения информации) видовой информации посторонними лицами помещение необходимо оборудовать шторами либо жалюзи.

4.3.7. При проведении технического обслуживания и ремонта аппаратных средств ИСПДн запрещается передавать ремонтным и обслуживающим организациям узлы и блоки с элементами накопления и хранения ПДн.

4.3.8. Машинные носители информации (дискеты, компакт-диски, жесткие диски, USB-устройства и т.п.), содержащие ПДн и/или используемые в ИСПДн, подлежат обязательному учету путем их маркировки с занесением учетных данных в журнал учета машинных носителей информации. Машинные носители информации маркируются следующим образом:

- На компакт-дисках (DVD, CD и др.) учетный номер проставляется на лицевой стороне диска специальным маркером.
- На магнитных дискетах размером 3,5 дюйма учетный номер проставляется на их корпусе.
- На жестком магнитном диске учетный номер проставляется на корпусе. Жесткий магнитный диск учитывается отдельно (в случае съемной конструкции) или в составе системного блока (СБ) автоматизированного рабочего места. В случае учета в составе СБ, на корпус СБ (в удобное для просмотра место) наклеивается бирка с указанием учетного номера, типа, модели машинного носителя, его объема, серийного номера жесткого магнитного диска.
- На носителях информации типа USB Flash-носители на корпус наклеивается бирка с указанием учетного номера носителя и его серийного номера.
- Бирки, по возможности, не должны закрывать заводские номера машинных носителей информации.

4.3.9. Журнал учета машинных носителей информации ИСПДн ведется в подразделениях, в которых производится обработка персональных данных.

4.3.10. Хранение съемных машинных носителей информации осуществляется в условиях, исключающих их хищение либо несанкционированное копирование или уничтожение содержащейся на них информации (запираемый ящик, запираемый шкаф, сейф и пр.).

4.3.11. Машинные носители информации, пришедшие в негодность, подлежат уничтожению с составлением Акта об уничтожении.

4.4. Организация работ по подготовке и вводу в эксплуатацию ИСПД

4.4.1. Действующие и проектируемые ИСПДн подразделений *организации*, обрабатывающие персональные данные, подлежат классификации (категорированию). Классификация проводится специальной комиссией, назначаемой *руководителем организации*.

4.4.2. Категорирование ИСПДн включает в себя следующие этапы:

4.4.2.1. Сбор и анализ исходных данных по информационной системе:

- наименование ИСПДн;
- цель обработки персональных данных;
- категория персональных данных;
- объем обрабатываемых в информационной системе персональных данных;
- принадлежность персональных данных (персональные данные сотрудников оператора или персональные данные не относятся к сотрудникам оператора).

4.4.2.2. Для каждой ИСПДн проводится анализ угроз безопасности персональных данных, по итогам которого определяются актуальные угрозы и составляется модель угроз безопасности ПДн.

4.4.2.3. Исходя из исходных данных, модели угроз безопасности ПДн проводится классификация (категорирование) ИСПДн.

4.4.3. На основании классификации (категорирования) ИСПДн и модели угроз безопасности ПДн определяется состав и содержание мер по обеспечению безопасности персональных данных, выполнение которых необходимо для обеспечения безопасности персональных данных при обработке в ИСПДн и нейтрализации актуальных угроз.

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

- назначение комиссии для проведения обследования и классификации (категорирования) ИСПДн;
- определение перечня ПДн, подлежащих обработке на объектах вычислительной техники;
- определение перечня информационных систем персональных данных в *организации*;
- определение перечня должностных лиц, допущенных к обработке ПДн;
- назначение ответственных лиц;
- приведение должностных инструкции руководителей соответствующих уровней и ответственных исполнителей, занимающихся обработкой персональных данных в информационных системах персональных данных в соответствие с требованиями законодательства Российской Федерации по защите персональных данных;
- разработка разрешительной системы доступа к защищаемым ресурсам;
- определение актуальных угроз безопасности ПДн при их обработке в ИСПДн;
- применение требуемых средств защиты информации прошедших в установленном порядке процедуру оценки соответствия, обеспечивающих нейтрализацию актуальных угроз безопасности;

- организация учёта машинных носителей информации используемых в ИСПДн и ведение журнала учета машинных носителей;
- утверждение технологического процесса обработки ПДн в ИСПДн;
- определение порядка, правил и инструкций по обработке и защите ПДн (инструкции администратору безопасности, пользователю, по антивирусной защите, инструкции по учету, выдаче и хранению машинных носителей информации);
- принятие мер для обеспечения возможности незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;
- разработка требований по обеспечению безопасности эксплуатации средств криптографической защиты информации (далее СКЗИ) и организация учета СКЗИ и ключевых документов в случае использования этих средств для защиты ПДн;
- разработка других необходимых нормативно правовых актов по вопросам обработки и защиты персональных данных и поддержание имеющихся в актуальном состоянии (Рекомендуемый базовый перечень документов - Приложение №1);
- проведение оценки эффективности реализованных мер по обеспечению безопасности персональных данных в ИСПДн;
- ввод ИСПДн в эксплуатацию приказом *руководителя организации*.

4.4.5. В случае модификации информационной системы проводится уточнение исходных данных, категории информационной системы, а также подлежит уточнению модель угроз безопасности ПДн.

4.5. **Обеспечение безопасности в ходе осуществления межсетевое взаимодействия, порядок обмена информацией со сторонними организациями.**

4.5.1. При межсетевом взаимодействии обеспечение безопасности ПДн достигается следующими методами:

- межсетевое экранирование с целью управления доступом, фильтрации сетевых пакетов и трансляции сетевых адресов для скрывания структуры информационной системы;
- обнаружение вторжений в информационную систему, нарушающих или создающих предпосылки к нарушению установленных требований по обеспечению безопасности информации ограниченного доступа;
- анализ защищенности информационных систем, предполагающий применение специализированных программных средств (сканер безопасности);
- защита информации при ее передаче по каналам связи (шифрование, VPN);
- использование средств антивирусной защиты.

4.5.2. В случае использования средств криптографической защиты информации для защиты ПДн должны выполняться требования «Инструкции по обеспечению безопасности эксплуатации средств криптографической защиты информации» и вестись журнал учета СКЗИ и выдачи ключевых документов.

5. Планирование работ по защите информации и контролю

5.1. Работа по защите ПДн в подразделениях проводится в рамках выполнения ежегодного плана мероприятий по защите ПДн, утверждаемого руководителем.

5.2. В разделе план работ по защите информации в части обеспечения безопасности ПДн должны быть отражены следующие мероприятия:

- выполнение решений Федеральной службы по техническому и экспортному контролю Российской Федерации
- уточнение перечня угроз безопасности ПДн;
- уточнение категории (класса) ИСПДн;
- аттестация (декларирование) ИСПДн на соответствие требованиям безопасности ПДн;
- разработка, корректировка и поддержание в актуальном состоянии организационно-распорядительных документов;
- проверка соответствия принимаемых мер защиты информации в ИСПДн требованиям руководящих документов в области безопасности информации;
- периодическое обследование аппаратных и программных средств ИСПДн, средств защиты информации;
- проведение занятий с сотрудниками по требованиям обеспечения безопасности информации.

6. Контроль состояния защиты персональных данных

6.1. Контроль состояния защиты ПДн - комплекс организационных и технических мероприятий, которые организуются и осуществляются в целях выявления и предотвращения утечки информации по техническим каналам, исключения или существенного затруднения несанкционированного доступа к информации, хищения технических средств и носителей информации, предотвращения специальных программно-технических воздействий, вызывающих нарушение целостности информации или работоспособности информационных систем.

6.2. Основными задачами контроля являются:

- проверка выполнения установленных норм и требований по защите ПДн в эксплуатируемых ИСПДн;
- уточнение возможных технических каналов утечки информации, несанкционированного доступа к ней и программно-технических воздействий на аппаратные и программные элементы ИСПДн;
- оценка достаточности и эффективности принимаемых мер по защите ПДн;
- проверка надлежащего использования средств защиты информации;
- оперативное принятие мер по пресечению нарушений требований защиты ПДн;
- разработка предложений по устранению (ослаблению) угроз безопасности ПДн, обрабатываемых в ИСПДн.

7. Порядок привлечения сторонних организаций к работам по обеспечению безопасности информации ограниченного доступа

7.1. С целью выполнения комплекса (отдельных видов) работ по защите ПДн, разработке и эксплуатации (модернизации) ИСПДн, разработке и внедрению системы защиты информации, а также проведения контроля достаточности и эффективности принимаемых мер защиты требованиям безопасности ПДн *организация* может заключать договора с организациями-лицензиатами ФСТЭК России и ФСБ России в области оказания услуг по защите конфиденциальной информации.

При заключении договора необходимо учитывать требование Заказчика к Исполнителю о соблюдении последним условий конфиденциальности сведений, ставших ему известными в ходе исполнения договора.