УТВЕРЖДЕНА
приказом от 29.12.2017 г. № 274___

Инструкция о порядке резервирования и восстановления работоспособности технических средств, программного обеспечения, баз данных и средств защиты информации информационных систем персональных данных

Обозначения и сокращения

В настоящем документе применяются следующие обозначения и сокращения:

АВС – антивирусные средства

АРМ – автоматизированное рабочее место

БД – база данных

ВТСС – вспомогательные технические средства и системы

ИСПДн – информационная система персональных данных

ИБ – информационная безопасность

КЗ – контролируемая зона

ЛВС – локальная вычислительная сеть

МЭ – межсетевой экран

НСД – несанкционированный доступ

ОС – операционная система

ПДн – персональные данные

ПК – персональный компьютер

ПО – программное обеспечение

ПП – программный продукт

ПЭМИН – побочные электромагнитные излучения и наводки

СВТ – средства вычислительной техники

СЗИ – средство защиты информации

СЗПДн – система защиты персональных данных

СОВ – система обнаружения вторжений

ТС – технические средства

УБПДн – угрозы безопасности персональных данных

1.Общие положения

1.1. Настоящая инструкция о порядке резервирования и восстановления работоспособности технических средств, программного обеспечения, баз данных и средств защиты информации информационных систем персональных данных (далее – Инструкция) определяет действия, связанные с функционированием информационных систем персональных данных МАДОУ д/с №2 (далее – Учреждение), меры и средства поддержания непрерывности работы и восстановления работоспособности информационных систем персональных данных.

1.2. Целью настоящей Инструкции является превентивная защита элементов ИСПДн от потери защищаемой информации.

1.3. Задачами настоящей Инструкции являются:

- определение мер защиты от потери информации;
- определение действий для восстановления в случае потери информации.

1.4. Действие настоящей Инструкции распространяется на всех пользователей Учреждения, имеющих доступ к ресурсам ИСПДн, а также к основным системам обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций, в том числе:

- системы жизнеобеспечения ИСПДн;
- системы резервного копирования и хранения данных;
-системы обеспечения отказоустойчивости;
-системы контроля физического доступа.

1.5. Пересмотр настоящего документа осуществляется по мере необходимости.

1.6. Ответственным сотрудником за реагирование на инциденты безопасности, приводящие к потере защищаемой информации, является Администратор ИСПДн.

1.7. Ответственным сотрудником за контролем обеспечения мероприятий по предотвращению инцидентов безопасности, приводящих к потере защищаемой информации, назначается ответственный за обеспечение безопасности персональных данных.

2. Порядок реагирования на инциденты

2.1. В настоящей Инструкции под инцидентом понимается происшествие, связанное со сбоем в функционировании элементов ИСПДн, предоставляемых пользователям ИСПДн, а также потерей защищаемой информации.

2.2. Происшествие, вызывающее инцидент, может произойти:

- в результате непреднамеренных действий пользователей;
- в результате преднамеренных действий третьих лиц;
- в результате нарушения правил эксплуатации технических средств ИСПДн;
- в результате возникновения внештатных ситуаций и обстоятельств непреодолимой силы.

2.3. Все действия в процессе реагирования на инцидент должны документироваться Администратором ИСПДн и передаваться ответственному за обеспечение безопасности персональных данных в виде служебной записки.

2.4. В срок, не превышающий одного рабочего дня, должны быть приняты меры по восстановлению работоспособности. Предпринимаемые меры, по

3.Меры обеспечения непрерывности работы и восстановления ресурсов при возникновении инцидентов

3.1. Технические меры

3.1.1. К техническим мерам обеспечения непрерывной работы и восстановления относятся программные, аппаратные и технические средства и системы, используемые для предотвращения возникновения инцидентов, такие как:

- системы жизнеобеспечения;
- системы обеспечения отказоустойчивости;
- системы резервного копирования и хранения данных;
- системы контроля физического доступа.

3.1.2. Системы жизнеобеспечения ИСПДн включают:

- пожарные сигнализации и системы пожаротушения;
- системы вентиляции и кондиционирования;
- системы резервного питания.

3.1.3. Все помещения Учреждения, в которых располагаются элементы ИСПДн и средства защиты, должны быть оборудованы средствами пожарной сигнализации.

3.1.4. Для выполнения требований по эксплуатации (температура, относительная влажность воздуха) серверных компонентов ИСПДн в помещениях, где они установлены, должны применяться системы вентиляции и кондиционирования воздуха.

3.1.5. Для предотвращения потерь информации при кратковременном отключении электроэнергии все ключевые элементы ИСПДн, сетевое и коммуникационное оборудование, а также наиболее критичные рабочие станции должны подключаться к сети электропитания через источники бесперебойного питания. В зависимости от необходимого времени работы ресурсов после потери питания могут применяться следующие методы резервного электропитания:

- локальные источники бесперебойного электропитания с различным временем питания для защиты отдельных компьютеров;
- источники бесперебойного питания с дополнительной функцией защиты от скачков напряжения;
- дублированные системы электропитания в устройствах (серверы, концентраторы);
- резервные линии электропитания в пределах комплекса зданий;
- аварийные электрогенераторы.

3.1.6. Для защиты от отказов отдельных дисков серверов, осуществляющих обработку и хранение защищаемой информации, должны использоваться технологии RAID (кроме RAID-0), которые применяют дублирование данных, хранимых на дисках.

3.1.7. Также для обеспечения отказоустойчивости критичных компонентов ИСПДн при сбое в работе оборудования и их автоматической замены без простоев могут использоваться методы кластеризации.

3.1.8. Система резервного копирования и хранения данных, должна обеспечивать хранение защищаемой информации на твердом носителе (жестком диске и т.п.).

3.2 Организационные меры

3.2.1. Резервное копирование и хранение данных должно осуществляться на периодической основе:

- для обрабатываемых персональных данных – не реже раза в неделю;
- для технологической информации – не реже раза в месяц;
- эталонные копии программного обеспечения (операционные системы, штатное и специальное программное обеспечение, программные средства защиты), с которых осуществляется их установка на элементы ИСПДн – не возобновляемому (однократному, эталонному) резервному копированию, и каждый раз при внесении изменений в эталонные копии (выход новых версий).

3.2.2. Носители, на которые произведено резервное копирование, должны быть пронумерованы: номером носителя, датой проведения резервного копирования.

3.2.3. Носители должны храниться в специально отведенном месте, доступ посторонних лиц к которому ограничен. Должна быть обеспечена целостность резервных носителей.

3.2.4. Носители должны храниться не менее года для возможности восстановления данных.

4. Ответственность

Ответственность за поддержание установленного в настоящей Инструкции порядка проведения резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в информационных системах персональных данных возлагается на ответственного за обеспечение безопасности персональных данных.

УТВЕРЖДЕНА
приказом от 29.12.2017 г. № 274

Инструкция ответственного за организацию обработки и обеспечение безопасности персональных данных в информационных системах персональных данных

Обозначения и сокращения

В настоящем документе применяются следующие обозначения и сокращения:

АРМ – автоматизированное рабочее место

ИСПДн – информационная система персональных данных

ЛВС – локальная вычислительная сеть

МЭ – межсетевой экран

НСД – несанкционированный доступ

ОС – операционная система

ПДн – персональные данные

ПК – персональный компьютер

ПО – программное обеспечение

РД – руководящие документы

СЗИ – средство защиты информации

СЗПДн – система защиты персональных данных

1. Общие положения

1.1. Ответственный за организацию обработки и обеспечение безопасности персональных данных назначается приказом руководителя МАДОУ д/с №2 (далее – Учреждение).

1.2. Ответственный за организацию обработки и обеспечение безопасности персональных данных подчиняется непосредственно руководителю или лицу, замещающему руководителя.

1.3. Ответственный за организацию обработки и обеспечение безопасности персональных данных в своей работе руководствуется настоящей инструкцией, Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», законодательством РФ, руководящими и нормативными документами ФСТЭК России, ФСБ России, Роскомнадзора, а также регламентирующими документами Учреждения в области защиты персональных данных.

1.4. Ответственный за организацию обработки и обеспечение безопасности персональных данных является должностным лицом Учреждения, уполномоченным на внутренний контроль за соблюдением требований законодательства Российской Федерации при обработке персональных данных, в том числе требований к защите персональных данных, проведение работ по защите информации, содержащей персональные данные и поддержанию достигнутого уровня защиты персональных данных, обрабатываемых с использованием средств автоматизации и без использования таковых.

1.5. Ответственный за организацию обработки и обеспечение безопасности персональных данных должен иметь специальное рабочее место, размещенное в здании Учреждения так, чтобы исключить несанкционированный доступ к нему посторонних лиц и других пользователей.

1.6. На рабочем месте ответственного за организацию обработки и обеспечение безопасности персональных данных должны присутствовать средства физической защиты внешних электронных и бумажных носителей информации (личный сейф, железный шкаф).

1.7. Ответственный за организацию обработки и обеспечение безопасности персональных данных осуществляет методическое руководство сотрудников, допущенных к обработке ПДн, к техническим средствам информационной системы персональных данных (ИСПДн) и иной конфиденциальной информации, в вопросах обеспечения безопасности информации.

1.8. Требования ответственного за организацию обработки и обеспечение безопасности персональных данных, связанные с выполнением им своих должностных обязанностей, обязательны для исполнения всеми работниками Учреждения, имеющими доступ к ПДн и конфиденциальной информации.

1.9. Ответственный за организацию обработки и обеспечение безопасности персональных данных несет персональную ответственность за качество проводимых им работ по контролю действий пользователей при работе в ИСПДн, состояние и поддержание установленного уровня защиты ИСПДн.

1.10. Ответственный за организацию обработки и обеспечение безопасности персональных данных по согласованию с руководителем Учреждения для консультаций по выбору и реализации методов и способов защиты информации в информационной системе может привлекать организацию,

имеющую оформленную в установленном порядке лицензию на осуществление деятельности по технической защите конфиденциальной информации.

2. Обязанности ответственного

2.1. В рамках поставленных перед ответственным за организацию обработки и обеспечение безопасности персональных данных задач, на него возлагаются следующие функции:

- организовать предоставление субъекту персональных данных либо его представителю по запросу информацию об обработке его персональных данных;
- осуществлять внутренний контроль за соблюдением требований законодательства Российской Федерации при обработке персональных данных, в том числе требований к защите персональных данных;
- доводить до сведения лиц, допущенных к обработке персональных данных, положения законодательства РФ о персональных данных, нормативных правовых актов по вопросам обработки персональных данных, требований к защите персональных данных;
- организовать прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов;
- организовать получение обязательства о прекращении обработки персональных данных у лиц, непосредственно осуществляющих обработку персональных данных, в случае расторжения с ним договора (контракта);
- организовать получение согласия на обработку персональных данных у субъектов персональных данных (при необходимости);
- организовать разъяснение субъекту персональных данных юридические последствия отказа предоставления его персональных данных;
- проводить систематический анализ состояния защиты персональных данных по вопросам, входящим в его компетенцию;
- соблюдать правила использования персональных данных, порядок их учета и хранения, исключать доступ к ним посторонних лиц.

2.2. Ответственный за организацию обработки и обеспечение безопасности персональных данных обязан:

- знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, распоряжений, регламентирующих порядок действий по защите персональных данных;
- уточнять в установленном порядке обязанности пользователей и администраторов ИСПДн;
- контролировать неизменность состояния защищенности информационных систем обработки персональных данных;
- контролировать обработку ПДн без использования средств автоматизации согласно принятому в учреждении порядку обработки персональных данных без использования средств автоматизации и Положению об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденному Постановлением правительства РФ № 687 от 15 сентября 2008г;
- ответственный за организацию обработки и обеспечение безопасности персональных данных выполняет свои обязанности индивидуально или в составе рабочих групп, формируемых распоряжениями руководства Учреждения;

- при доступе или обработке персональных данных ответственному за организацию обработки и обеспечение безопасности персональных данных запрещается: использовать сведения, содержащие персональные данные, в неслужебных целях; передавать персональные данные по незащищенным каналам связи без использования сертифицированных средств криптографической защиты информации; снимать копии с документов и других носителей информации, содержащих персональные данные, или производить выписки из них, а равно использовать различные технические средства (видео- и звукозаписывающую аппаратуру) для фиксации сведений, содержащих персональные данные.

- ответственный за организацию обработки и обеспечение безопасности персональных данных, виновный в нарушении требований законодательства о защите персональных данных, в том числе допустившие разглашение персональных данных, несет персональную гражданскую, уголовную, административную, дисциплинарную и иную, предусмотренную законодательством ответственность.

Инструкция по организации антивирусной защиты

Обозначения и сокращения

В настоящем документе применяются следующие обозначения и сокращения:

АВЗ	– антивирусная защита
АРМ	– автоматизированное рабочее место
ИСПДн	– информационная система персональных данных
ОС	– операционная система
ПДн	– персональные данные
ПМВ	– программно-математическое воздействие
ПО	– программное обеспечение

1. Общие положения

1.1. Настоящая инструкция по организации антивирусной защиты (далее – Инструкция) определяет требования к организации защиты информации от разрушающего воздействия компьютерных вирусов в МАДОУ д/с №2 (далее – Учреждение), а также устанавливает ответственность сотрудников, эксплуатирующих и сопровождающих ИСПДн.

1.2. Целями защиты является противодействие угрозам несанкционированного уничтожения, блокирования, модификации, копирования информации или нейтрализации средств защиты информации.

1.3. В целях перекрытия всех возможных каналов проникновения вредоносных программ в ИСПДн антивирусное программное обеспечение должно применяться на автоматизированных рабочих местах, серверах, средствах межсетевого экранирования, прокси-серверах, почтовых шлюзах, мобильных технических средствах и иных точках доступа в информационную систему, подверженных заражению вредоносными программами через съемные носители информации или сетевые подключения, в том числе к сетям общего пользования (вложения электронной почты, веб- и другие сетевые сервисы).

1.4. К использованию в ИСПДн допускаются только лицензионные антивирусные средства, купленные у разработчиков (поставщиков) указанных средств и прошедшие в установленном порядке процедуру оценки соответствия требованиям по безопасности.

1.5. Установка, конфигурирование и управление средствами антивирусной защиты осуществляется ответственным за обеспечение безопасности персональных данных.

1.6. После установки и настройки средств АВЗ в обязательном порядке должно быть произведено тестирование системы АВЗ.

1.7. Ответственность за организацию и проведение мероприятий антивирусного контроля в соответствии с требованиями настоящей Инструкции возлагается на ответственного за обеспечение безопасности персональных данных.

1.8. Ответственность за ежедневный антивирусный контроль в процессе эксплуатации ИСПДн и своевременное информирование ответственного за обеспечение безопасности персональных данных в случае обнаружения действий вредоносных программ возлагается на пользователей ИСПДн.

2. Реализация антивирусной защиты

2.1. Ежедневно, при загрузке компьютеров, в автоматическом режиме должен проводиться антивирусный контроль всех электронных носителей информации ПДн.

Обязательной проверке в масштабе времени, близком к реальному, подлежат любые объекты (файлы) из внешних источников (съемных машинных носителей информации, сетевых подключений, в том числе к сетям общего пользования, и других внешних источников) при загрузке, открытии или исполнении таких файлов.

2.2. Настройка средств антивирусной защиты должна реализовывать следующие функции:

– непрерывный автоматический мониторинг информационного обмена в

– автоматическую проверку на наличие вредоносных программ или последствий ПМВ при импорте в ИСПДн всех программных модулей (прикладных программ), которые могут содержать вредоносные программы, по их типовым шаблонам и с помощью эвристического анализа;

– реализацию механизма автоматического блокирования обнаруженных вредоносных программ путем их удаления из программных модулей или уничтожения;

– автоматическую проверку критических областей АРМ и серверов, таких как системная память, загрузочные секторы дисков, объекты автозапуска, каталоги ОС «system» и «system32» при каждом запуске ОС;

– полную автоматическую проверку носителей информации всех АРМ и серверов не реже одного раза в неделю;

– оповещение в масштабе времени, близком к реальному, об обнаружении вирусов.

2.3. Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль. Периодические проверки электронных архивов должны проводиться не реже одного раза в месяц.

2.4. Устанавливаемое ПО должно быть предварительно проверено на наличие вирусов. Непосредственно после установки ПО, должна быть выполнена антивирусная проверка.

2.5. При возникновении подозрения на наличие вируса должна быть провести внеочередную антивирусную проверку АРМ.

3. Обновление базы данных признаков вредоносных программ

3.1. Обеспечение актуальности базы данных признаков вредоносных программ производится периодическим их обновлением. Получение базы данных должно происходить из доверенных источников.

3.2. Обновление должно происходить в автоматическом режиме с получением уведомлений о необходимости обновления и непосредственном обновлении базы данных.

3.3. Должен осуществляться контроль целостности обновлений базы данных признаков вредоносных программ.

4. Права и обязанности сотрудников

4.1. Ответственный за обеспечение безопасности персональных данных несет персональную ответственность за организацию и осуществление АВЗ.

4.2. Руководители отделов управления образования администрации г.Белгорода обязаны осуществлять постоянный контроль выполнения пользователями ИСПДн правил Инструкции.

4.3. Руководители отделов управления образования администрации г.Белгорода имеют право обращаться к ответственному за обеспечение безопасности персональных данных за оказанием методической и практической помощи в обеспечении АВЗ.

4.4. Пользователь ИСПДн обязан удостовериться, что на АРМ установлено и активно антивирусное ПО. В случае его отсутствия необходимо известить об этом ответственного за обеспечение безопасности персональных данных.

4.5. При подозрении на заражение вирусом или его обнаружении

выключением. После чего немедленно сообщить об этом ответственному за обеспечение безопасности персональных данных или руководителю отдела. Возобновление работы возможно лишь после полной нейтрализации угрозы.

4.6. Пользователь ИСПДн при работе со съемными носителями информации (flash-накопители, оптические диски, жесткие диски USB и т.д.) обязан перед началом работы осуществить их полную проверку на предмет наличия вредоносных программ.

4.7. Запрещается сохранять (скачивать) и открывать вложения из писем электронной почты от неизвестных отправителей. Если отправитель известен, то необходимо уточнить у него факт отправки письма лично, после чего сохранить вложение и перед открытием проверить антивирусом.

4.8. При появлении любых предупреждающих сообщений (сообщения об обнаружении вируса, истечения срока лицензии, о неактуальности базы данных признаков вредоносных программ) необходимо сообщить об этом ответственному за обеспечение безопасности персональных данных.

4.9. Пользователь ИСПДн, в случае служебной необходимости, имеет право обратиться к ответственному за обеспечение безопасности персональных данных с просьбой о временной приостановке активных компонентов и задач АВЗ.

5. Ответственность за нарушение требований инструкции

5.1. Каждый пользователь ИСПДн несет персональную ответственность за нарушение требований Инструкции.

5.2. Нарушение требований Инструкции является чрезвычайным происшествием и влечет за собой ответственность, предусмотренную действующим законодательством РФ.

Инструкция пользователя информационных систем персональных данных

Обозначения и сокращения

В настоящем документе применяются следующие обозначения и сокращения:

АРМ – автоматизированное рабочее место

ИСПДн – информационная система персональных данных

ЛВС – локальная вычислительная сеть

МЭ – межсетевой экран

НСД – несанкционированный доступ

ОС – операционная система

ПДн – персональные данные

ПК – персональный компьютер

ПМВ – программно-математическое воздействие

ПО – программное обеспечение

ПЭМИН – побочные электромагнитные излучения и наводки

РД – руководящие документы

САЗ – средства анализа защищенности

СЗИ – средство защиты информации

СЗПДн – система защиты персональных данных

СОВ – система обнаружения вторжений

УБПДн – угрозы безопасности персональных данных

1. Общие положения

1.1. Пользователь информационной системы персональных данных осуществляет обработку персональных данных.

1.2. Пользователем является каждый сотрудник МАДОУ д/с №2 (далее – Учреждение), участвующий, в рамках своих функциональных обязанностей, в процессах обработки информации, содержащей персональные данные, и имеющий доступ к аппаратным средствам, программному обеспечению и средствам защиты информации.

1.3. Пользователь несет персональную ответственность за свои действия.

1.4. Пользователь в своей работе руководствуется настоящей инструкцией, требованиями законодательства Российской Федерации, а также принятыми в Учреждении положениями, инструкциями и приказами.

1.5. Методическое руководство работой пользователя осуществляется ответственным за обеспечение безопасности персональных данных.

2. Обязанности пользователя ИСПДн

Пользователь обязан:

2.1. Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, положения о порядке обработки персональных данных и распоряжений, регламентирующих порядок действий по защите информации.

2.2. Выполнять на автоматизированном рабочем месте (АРМ) только те процедуры, которые определены для него должностными обязанностями.

2.3. Знать и соблюдать установленные требования по режиму обработки персональных данных, учету, хранению и передаче информации, обеспечению безопасности персональных данных, в соответствии с руководящими и организационно-распорядительными документами.

2.4. Хранить съемные носители персональных данных в сейфах (металлических шкафах), оборудованных внутренним замком и приспособлением для опечатывания замочных скважин или кодовым замком. В случае если на съемном машинном носителе персональных данных хранятся только персональные данные в зашифрованном с использованием СКЗИ виде, допускается хранение таких носителей вне сейфов.

2.5. Соблюдать требования парольной политики (раздел 3).

2.6. Соблюдать правила при работе в сетях общего доступа и (или) международного информационного обмена – Интернет и других (раздел 4).

2.7. Располагать экран монитора во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на ним информацией посторонними лицами; шторы на оконных проемах должны быть завешены (жалюзи закрыты) в случае, если есть возможность просмотра экрана монитора через окно.

2.8. В рабочее время помещение закрывать на замок и открывать только для санкционированного прохода.

2.9. Обо всех выявленных нарушениях необходимо сообщать ответственному за обеспечение безопасности персональных данных.

2.10. Для получения консультаций по вопросам работы и настройки элементов ИСПДн, необходимо обращаться к Администратору ИСПДн.

2.11. Пользователю запрещается:

- разглашать защищаемую информацию (отраженную в Перечне защищаемых информационных ресурсов и Перечне обрабатываемых персональных данных) третьим лицам;

- копировать защищаемую информацию на неучтенные внешние носители;

- самостоятельно устанавливать, тиражировать или модифицировать программное и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств;

- несанкционированно открывать общий доступ к ресурсам на своем автоматизированном рабочем месте (АРМ);

- подключать к АРМ и корпоративной информационной сети личные внешние носители и устройства;

- отключать (блокировать) средства защиты информации;

- обрабатывать на АРМ информацию, не имеющую отношения к трудовой деятельности и выполнять другие работы, не предусмотренные должностными обязанностями;

- сообщать (или передавать) посторонним лицам личные ключи и атрибуты доступа к ресурсам ИСПДн;

- бесконтрольно оставлять, либо передавать посторонним лицам ключи от помещения, в котором располагаются элементы ИСПДн;

- привлекать посторонних лиц для производства ремонта или настройки АРМ, без согласования с ответственным за обеспечение безопасности персональных данных.

2.12. При отсутствии визуального контроля за АРМ доступ к компьютеру должен быть немедленно заблокирован (например, для ОС Windows необходимо нажать комбинацию клавиш Ctrl+Alt+Del и выбрать опцию Блокировка).

2.13. В случае возникновения внештатных и аварийных ситуаций, необходимо принимать меры по реагированию с целью ликвидации их последствий.

3. Организация парольной защиты

3.1. Пароли доступа к ИСПДн выдаются пользователям ответственным за обеспечение безопасности персональных данных или создаются самостоятельно.

3.2. Полная плановая смена паролей в ИСПДн проводится не реже одного раза в 3 месяца.

3.3. Правила формирования пароля:

- пароль не должен содержать имя учетной записи пользователя или его часть;

- пароль должен состоять не менее, чем из 6 символов;

- в пароле должны присутствовать прописные и строчные буквы английского алфавита, цифры и специальные символы;

- запрещается использовать в качестве пароля простые пароли типа «123456», «qwerty» и т.д., а также свои имена и даты рождения, клички домашних животных, номера телефонов и другие пароли, которые можно подобрать, основываясь на информации о пользователе;

- запрещается выбирать пароли, которые уже использовались ранее.

3.4. Правила ввода пароля:

- ввод пароля должен осуществляться с учётом регистра, в котором пароль

- во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами или техническими средствами (видеокамеры и др.).

3.5. Правила хранения пароля:

- запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации, в том числе на предметах;

- запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем.

3.6. Лица, использующие паролирование, обязаны:

- четко знать и строго выполнять требования настоящей инструкции и других руководящих документов по парольной защите;

- своевременно сообщать лицу, ответственному за обеспечение безопасности персональных данных об утере, несанкционированном изменении паролей и несанкционированном изменении сроков действия паролей.

4. Правила работы в сетях общего доступа и (или) международного информационного обмена

4.1. Работа в сетях общего доступа и (или) международного информационного обмена (сети Интернет и других) (далее – Сеть) на элементах ИСПДн, должна проводиться при служебной необходимости.

4.2. При работе в Сети запрещается:

- осуществлять работу при отключенных средствах защиты (антивирус, межсетевой экран и других);

- передавать по Сети защищаемую информацию без использования средств шифрования;

- запрещается скачивать из Сети программное обеспечение и другие файлы, не связанные с исполнением служебных обязанностей, либо содержащие вредоносный код;

- запрещается сохранять (скачивать) и открывать вложения из писем электронной почты от неизвестных отправителей. Если отправитель известен, то необходимо уточнить у него факт отправки письма лично, после чего сохранить вложение и перед открытием проверить антивирусом;

- запрещается посещение сайтов сомнительной репутации (сайты, содержащие нелегально распространяемое ПО и другие);

запрещается нецелевое использование подключения к Сети.

Инструкция по организации защиты информации в информационных системах персональных данных

Термины и определения

Автоматизированная информационная система (АИС) – комплекс программных, технических, информационных, лингвистических, организационно-технологических средств и персонала, предназначенный для сбора, (первичной) обработки, хранения, поиска, (вторичной) обработки и выдачи данных в заданной форме (виде) в целях решения разнородных профессиональных задач пользователей системы.

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

Авторизация – предоставление доступа к защищаемому ресурсу в соответствии с уровнем полномочий.

Адаптивность – способность АИС изменяться для сохранения своих эксплуатационных показателей в заданных пределах при изменениях условий.

Администратор защиты информации – лицо, ответственное за выполнение мероприятий защиты информации, обрабатываемой техническими средствами.

Архивирование – 1) запись на отчуждаемый носитель данных информационного ресурса со специальным преобразованием в целях сокращения занимаемого ими места на носителе; 2) реализация процесса хранения резервных копий информационных ресурсов в целях исключения потери их функциональности.

Архивированная копия – копия ресурса, полученная путем его копирования с архивированием.

Архивная копия – копия ресурса, находящаяся на хранении в архиве, специальном хранилище.

Аутентификация – процесс проверки принадлежности субъекту доступа предъявленного им идентификатора; то есть проверка подлинности пользователя с помощью предъявляемого им идентификатора.

Аутентичность – свойство данных (информации), выражающееся в том, что они были созданы законными участниками информационного процесса, и что они не подверглись искажениям (случайным или преднамеренным).

Безопасность информации – состояние защищенности информации от внешних и внутренних угроз, характеризуемое способностью персонала, технических средств и информационных технологий обеспечить конфиденциальность, доступность и целостность информации при ее обработке.

Вредоносная программа – специальная компьютерная программа (троянская, вирус, червь, шпион и т.п.), последовательность инструкций или иной специальный код, предназначенные или приспособленные для

предусмотренного технологией авторизованной обработки информации воздействия на доступные этому средству ресурсы. На практике вредоносными программами признаются: компьютерные вирусы, черви, троянские программы, программы-маскировщики (руткиты), сканеры (эксплоиты) уязвимостей, программы-шпионы (spyware-программы).

Вскрытие корпуса устройства – разъем конструктивных деталей корпуса устройства, открывающий доступ к накопителю информации.

Данные – информация, представленная в виде, пригодном для обработки автоматическими средствами при возможном участии человека.

Дифференциальное (дифференцированное) копирование – копирование, при котором копируются только данные, измененные со времени последнего создания полной копии. Дифференциальные копии (архивы) имеют меньшие размеры и быстрее создаются. Для восстановления ресурса из дифференциальной копии необходима полная копия.

Документированная информация – зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель.

Доступ к информации – возможность получения информации и ее использования.

Доступность информации – состояние информации, характеризуемое способностью автоматизированной системы обеспечить беспрепятственный доступ к информации субъектов, имеющих на это полномочия.

Дублирование – создание (реализация для целей хранения) информационного ресурса аутентичного дублируемому ресурсу, на другом программно-аппаратном комплексе.

Живучесть АИС – свойство АИС, характеризуемое способностью выполнять установленный объем функций в условиях воздействий внешней среды и отказов компонентов системы в заданных пределах.

Защита информации – принятие правовых, организационных и технических мер, направленных на: обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении информации; соблюдение конфиденциальности информации ограниченного доступа и реализацию права на доступ к информации.

Идентификатор – уникальный признак субъекта или объекта доступа.

Идентификация – присвоение объектам и субъектам доступа идентификатора и/или проверка наличия предъявляемого идентификатора в перечне присвоенных идентификаторов.

Имя пользователя – идентификатор, представляющий последовательность символов установленного формата.

Инкрементное (инкрементальное) копирование – копирование, при котором копируются только данные, измененные со времени последнего создания полной или инкрементной копии. Инкрементные копии (архивы) имеют меньшие размеры и быстрее создаются. Для восстановления ресурса из инкрементной копии необходимы все предыдущие инкрементные копии и полная копия.

Информационно-телекоммуникационная сеть (корпоративная сеть передачи данных) – технологическая система, предназначенная для передачи по

линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

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

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

Контролируемая зона (КЗ) – пространство, в котором исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового допуска, и посторонних транспортных средств. Границей контролируемой зоны могут являться периметр охраняемой территории организации или ограждающие конструкции охраняемого здания или его части.

Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

Копирование – запись данных оригинала информационного ресурса или его фрагмента на съемный (отчуждаемый) носитель информации.

Копирование с архивированием – запись данных оригинала информационного ресурса или их фрагментов на съемный (отчуждаемый) носитель информации со специальным преобразованием данных в целях сокращения занимаемого ими места на носителе.

Копия ресурса – съемный (отчуждаемый) носитель информации (комплект однотипных носителей), содержащий информацию ресурса, аутентичную по состоянию на момент записи оригиналу (информации хранящейся в АИС).

Машинный носитель информации (носитель информации, носитель) – специальный вещественный энергонезависимый объект, предназначенный для записи на него информации и ее хранения (с возможностью последующего чтения) посредством средств вычислительной техники, или конструктивно законченное устройство, содержащее в своем составе такой объект.

Межсетевой экран – локальное или функционально распределенное программное (программно-аппаратное) средство, реализующее контроль пакетов, поступающих на компьютер и/или выходящих с него в рамках определенных протоколов.

Несанкционированный доступ к информации – 1) получение защищаемой информации субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации; 2) доступ к информации или ее носителям с нарушением установленных правил доступа к ним.

Носитель информации однократной записи – носитель информации, позволяющий в процессе эксплуатации однократно произвести полнообъемную (в размере полной заявленной производителем информационной емкости) запись информации.

Носитель информации ограниченного доступа – носитель информации, учтенный в «Журнале учета машинных носителей информации» и предназначенный для хранения информации ограниченного доступа (конфиденциальной информации).

Обработка информации в АС – совокупность операций (сбор, накопление, хранение, преобразование, отображение, выдача и т.п.) осуществляемых над информацией (сведениями, данными) с использованием средств АС.

Объект доступа – информационный ресурс автоматизированной системы, доступ к которому регламентирован.

Оригинал ресурса – информационный ресурс, хранящийся в АИС (в памяти аппаратно-программного комплекса).

Отчуждаемый носитель [информации] – см. съемный носитель.

Пароль – назначаемый (присваиваемый) аутентификатор пользователя, представляющий собой группу символов определенной длины, являющийся секретом пользователя и служащий для подтверждения принадлежности предъявленного идентификатора (имени пользователя) обращающемуся пользователю.

Парольная документация – документы, предназначенные для обеспечения функционирования системы аутентификации пользователей.

Перезаписываемый носитель информации – носитель информации, позволяющий многократно (более одного раза) производить полнообъемную (то есть в размере полной заявленной производителем информационной емкости) запись информации.

Полное копирование – копирование ресурса в полном объеме его данных.

Пользователь – субъект доступа, обращающийся к информационной системе в целях получения информации и/или воздействия на нее.

Предоставление информации – действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц.

Применение носителей информации – процессы учета, хранения, использования по назначению, списания и уничтожения носителей информации, то есть стадия жизненного цикла носителя информации от его приобретения до уничтожения (утилизации).

Профайл – объект операционной системы серверов iSeries (i5)(AS/400), описывающий уровень полномочий субъекта доступа.

Распространение информации – действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц.

Ресурс [информационный] – отдельный документ и отдельный массив документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах).

Системный администратор – лицо или подразделение, осуществляющее администрирование (техническое управление) вычислительной системой.

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

Примечание. Субъектом, осуществляющим несанкционированный доступ к защищаемой информации, может выступать: юридическое лицо; группа физических лиц, в том числе общественная организация; отдельное физическое лицо.

Съемный носитель [информации] – носитель информации, технология применения которого предусматривает его включение в работу автоматизированной системы и/или выключение из работы автоматизированной системы без ее остановки, а также носитель, извлекаемый из корпуса устройства без его (корпуса) вскрытия.

Тиражирование копии – размножение съемного (отчуждаемого) носителя (комплекта носителей) информации, содержащего копию ресурса, путем копирования этого носителя.

Тиражирование ресурса – запись ресурса (или его фрагмента) на съемный носитель с последующим их перемещением в целях обеспечения автоматизированной обработки вне Учреждения.

Угроза безопасности информации – совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации и/или несанкционированными и/или непреднамеренными воздействиями на нее.

Уровень полномочий – совокупность прав доступа субъекта доступа.

Устойчивость – комплексное свойство автоматизированной системы, характеризуемое ее живучестью, помехоустойчивостью и надежностью.

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

Энергонезависимый объект – объект, не требующий подвода энергии для обеспечения своих функций по хранению информации или содержащий автономный источник энергии.

1. Общие положения

1.1. Настоящая инструкция по организации защиты информации в информационных системах персональных данных (далее – Инструкция) определяет цели и основные задачи защиты информации информационных систем персональных данных, основные требования и единый порядок ее организации в МАДОУ д/с №2 (далее – Учреждение).

1.2. Нормативной базой Инструкции являются федеральное законодательство, нормативные правовые акты Президента Российской Федерации и Правительства Российской Федерации, а также нормативные документы Федеральной службы по техническому и экспортному контролю, Федеральной службы безопасности Российской Федерации.

2. Ответственность за нарушение безопасности информации

2.1. Инструкция является нормативным документом Учреждения, обязательным для выполнения (в части касающейся) всеми сотрудниками Учреждения.

2.2. Сотрудники, виновные в нарушении безопасности ИСПДн, могут быть привлечены к административной или уголовной ответственности в соответствии с действующим законодательством Российской Федерации.

3. Цель и задачи защиты информации

3.1. Целью защиты информации ИСПДн является достижение их безопасности, то есть состояния защищенности информации от внешних и внутренних угроз, характеризуемого способностью персонала, технических средств и информационных технологий обеспечить в процессе обработки ее конфиденциальность, целостность, доступность.

3.2. Защите подлежит вся циркулирующая в ИСПДн информация. Методы и меры защиты ресурсов определяются дифференцированно, исходя из их важности, особенностей реализации и использования. Защита общедоступной информации производится только в целях обеспечения ее целостности, доступности.

3.3. Цель защиты информации ИСПДн достигается решением следующих задач:

- реализация комплекса мер по предотвращению противоправного получения информации или ее несанкционированной передачи (распространения);
- своевременное обнаружение фактов несанкционированного доступа к информации и предотвращение неавторизованного (неполномочного) воздействия на информационные ресурсы;
- недопущение воздействия на технические средства обработки и хранения информации, нарушающего их функционирование;
- предупреждение неблагоприятных последствий нарушения порядка доступа к информации;
- обеспечение восстановления в приемлемые сроки информации после не предусмотренной технологией ее обработки, модификации, в том числе уничтожения.

4. Объекты и мероприятия защиты информации

4.1. Защите подлежат:

- техническое и программное обеспечение ИСПДн;
- информационно-телекоммуникационная сеть (КСПД);
- информационные ресурсы, представленные в виде носителей на различной физической основе, информативных физических полей, информационных массивов и баз данных;
- помещения, в которых размещаются носители или средства обработки защищаемой информации;
- все технические средства и системы, размещенные в помещениях, в которых обрабатывается (циркулирует) информация ограниченного доступа;
- система защиты информации.

4.2. Выполнение задач защиты информации в ИСПДн обеспечивается организацией эффективной системы защиты информации – комплексным применением организационных и технических (программно и аппаратно реализуемых) мероприятий:

- созданием системы нормативных (руководящих) документов по организации защиты;
- четким распределением ответственности по обеспечению защиты информации между должностными лицами и работниками;
- установлением персональной ответственности работников за обеспечение безопасности обрабатываемой информации;
- юридической защитой безопасности информации при ее предоставлении сторонним организациям;
- своевременным выявлением угроз безопасности информации и принятием соответствующих мер защиты;
- дифференцированием мер защиты в зависимости от степени угрозы и важности объекта защиты;
- комплексным применением программно и аппаратно реализованных средств защиты информации от несанкционированного доступа к ней и от специальных воздействий на информационные ресурсы в целях их уничтожения, искажения, блокирования или фальсификации;
- регламентированием порядка применения средств ввода-вывода информации и контролем его выполнения;
- содержанием актуальных резервных копий информационных ресурсов;
- применением прикладных программных продуктов, отвечающих требованиям обеспечения защиты информации;
- организацией контроля доступа в помещения и здания Учреждения, их охраной в нерабочее время;
- систематическим анализом безопасности информации и совершенствованием системы её защиты;
- эффективной противопожарной защитой;
- приданием мероприятиям защиты информации характера обязательных элементов производственного процесса, а требованиям по их исполнению – элементов производственной дисциплины;
- глубоким знанием и пониманием работниками требований безопасности информации.

4.3. Применение технических средств защиты информации в Учреждении

Используемые средства должны соответствовать требованиям всех указанных принципов.

4.4. Безопасность. Применяемые технические средства защиты должны иметь сертификат компетентных государственных органов (организаций):

- отсутствия деструктивного воздействия на защищаемую информацию или возможности их использования для такого воздействия;
- обеспечения требуемого уровня защищенности.

4.5. Правомочность. Для обеспечения защиты информации Учреждения используются лицензированные или свободно распространяемые программные средства.

4.6. Эффективность. Защита информации должна обеспечивать положительный результат, соотносимый с затратами ресурсов на ее реализацию.

5. Основные методы защиты информации

5.1. В Учреждении комплексно применяются организационные и технические методы защиты информации ИСПДн.

5.2. К числу основных организационных и технических мер защиты информации, применяемых в Учреждении, относятся:

- идентификация и аутентификация субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- защита машинных носителей информации;
- антивирусная защита;
- контроль (анализ) защищенности информации;
- защита технических средств;
- защита информационной системы, ее средств, систем связи и передачи данных;
- управление конфигурацией информационной системы и системы защиты персональных данных.

6. Руководство защитой информации

6.1. В Учреждении ответственность за организацию и выполнение мероприятий по обеспечению защиты информации в ИСПДн возлагается на руководителя Учреждения.

6.2. Методическое руководство, организация мероприятий по защите информации в ИСПДн, эксплуатация технических средств защиты, а также контроль безопасности информации возлагается на ответственного за обеспечение безопасности персональных данных (далее - администратор по защите информации).

6.3. Практическая реализация мероприятий по защите информации в ИСПДн осуществляется работниками в соответствии с их должностными полномочиями и обязанностями.

7. Задачи Учреждения и должностных лиц

7.1. Администратором ИСПДн обеспечивается:

- внедрение и сопровождение технических и программных (общесистемных и прикладных) средств, удовлетворяющих требованиям безопасности информации;

- выполнение процедур обеспечения целостности информации ИСПДн;

- включение в разрабатываемую проектную документацию ИСПДн разделов по защите информации;

- обеспечение устойчивости и адаптивности ИСПДн, организационной и информационной совместимости ее подсистем и элементов;

- отражение вопросов защиты информации в документации по приемке технологий и приложений в эксплуатацию и при организации фонда алгоритмов и программ Учреждения;

- выбор (разработка) программных средств, удовлетворяющих требованиям настоящей Инструкции и других нормативных документов по защите информации;

- обеспечение соответствия информационно-телекоммуникационной системы Учреждения требованиям безопасности информации;

- содержание фонда алгоритмов и программ Учреждения.

7.2. Администратором по защите информации обеспечивается:

- организация выполнения практических мероприятий по защите информации ИСПДн и информационно-телекоммуникационной сети Учреждения;

- разработка нормативных документов по обеспечению защиты информации;

- организация разграничения допуска и обеспечение доступа работников к защищаемой информации в соответствии с их правами;

- организация и обеспечение криптографической защиты информации;

- организация и обеспечение антивирусной защиты;

- организация защиты конфиденциальной информации от НСД;

- анализ состояния безопасности информации и выработка рекомендаций по совершенствованию системы защиты информации;

- учет защищаемых ресурсов, средств защиты и машинных носителей информации в Учреждении;

- контроль применения машинных носителей информации;

- контроль функционирования средств защиты информации;

- организация закупки средств защиты информации, а также услуг по обеспечению защиты информации в соответствии с бюджетом Учреждения;

- организация и выполнение работ по внедрению технических средств защиты информации;

- организация работ по аттестации ИСПДн, помещений, специальных исследований и специальных проверок технических средств;

- согласование технических решений при проектировании систем охранной и пожарной сигнализации, разграничения, контроля доступа и видеонаблюдения зданий (помещений), участие в приеме в эксплуатацию;

- выявление и блокирование каналов возможной утечки конфиденциальной информации.

8. Задачи пользователя

8.1. На пользователя средств и ресурсов ИСПДн возлагается:

- выполнение в объеме должностных полномочий и обязанностей требований нормативных (руководящих) документов по защите информации;

- соблюдение конфиденциальности информации, правил пользования

порядка их учета, хранения и уничтожения, исключение всеми имеющимися средствами доступа к конфиденциальной информации посторонних лиц;

- ознакомление только с той информацией (документами), содержащими конфиденциальную информацию, к которым получен доступ в силу исполнения прямых служебных обязанностей;

- защита целостности и доступности пользовательских информационных ресурсов;

- своевременное информирование непосредственного руководителя о возникновении предпосылок к нарушению конфиденциальности информации и о фактах нарушения, ставших ему известными;

- использование только программных продуктов, включенных в перечень разрешенного для использования прикладного программного обеспечения ИСПДн.

8.2. При работе с конфиденциальной информацией пользователю ЗАПРЕЩАЕТСЯ:

- использовать сведения конфиденциального характера в неслужебных целях, в разговорах с лицами, не имеющим отношения к этим сведениям, либо в других ситуациях, не связанных с выполнением служебных обязанностей;

- выносить документы и другие носители информации, содержащие сведения конфиденциального характера и выполнять работы, связанные со сведениями конфиденциального характера, вне служебных помещений Учреждения без разрешения руководителя

- использовать сведения конфиденциального характера при ведении переговоров в телефонной сети и по незащищенным каналам связи (в том числе передавать конфиденциальную информацию по электронной почте без применения средств криптографической защиты);

- использовать сведения конфиденциального характера в открытой переписке, статьях и выступлениях;

- снимать копии с документов и служебной информации, содержащей сведения конфиденциального характера, или производить выписки из них, а также использовать различные технические средства (фото-, видео-, и звукозаписывающую аппаратуру) для записей сведений конфиденциального характера без разрешения руководителя

- работать с неучтенными машинными носителями информации;

- записывать игровые и обучающие программы на любые служебные машинные носители информации;

- уничтожать, копировать или производить какие-либо действия над информацией, программным обеспечением, и базами данных других пользователей без разрешения руководителя, если это не определено функциональными обязанностями;

- хранить парольную документацию и личные карточки с паролями в открытом виде, в местах, доступных для обозрения (на дисплеях ПЭВМ, на рабочих столах и т.д.) другими работниками и посторонними лицами.

9. Задачи и мероприятия защиты информации от несанкционированного доступа

9.1. Цели защиты информации от несанкционированного доступа (далее – НСД) достигаются решением следующих задач:

- предотвращение неавторизованного (неполномочного) воздействия на информацию как в режиме реального времени (вторжение), так и посредством вредоносных программ (заражение, закладка);

- обеспечение возможности восстановления информации после непредусмотренной технологией обработки модификации, в том числе уничтожения;

- организация безопасного обращения носителей информации;

- недопущение несанкционированного проникновения в помещения и воздействия на технические средства обработки и хранения информации, нарушающего режимы их функционирования;

- минимизация возможности перехвата информации или ее съема посредством побочных излучений и полей.

9.2. Основными мероприятиями защиты информации от НСД и вредоносных программ в Учреждении являются:

- учет защищаемых ресурсов;

- минимизация перечня лиц, допущенных к защищаемой информации, и разграничение их прав доступа;

- авторизация пользователей информационных ресурсов и вычислительных средств;

- управление правами и привилегиями пользователей, разграничение доступа пользователей информационной системы на основе совокупности установленных в информационной системе правил разграничения доступа, а также обеспечивать контроль соблюдения этих правил;

- контроль конфигурации вычислительных средств и их программного обеспечения;

- организация учета и безопасного хранения носителей информации;

- сбор, запись, хранение и защиту информации о событиях безопасности в информационной системе и их анализ;

- организация защиты от вредоносных программ;

- обнаружение (предотвращение) вторжений в ИСПДн;

- создание и организация безопасного хранения резервных копий (дубликатов) информационных ресурсов ИСПДн;

- пропускная система допуска работников и посетителей в здания;

- ограничение доступа работников в помещения, в которых размещаются хранилища информации и средства ее обработки;

- создание контролируемых зон, оборудование зданий и помещений элементами и системами безопасности и контроля.

10. Средства защиты информации от несанкционированного доступа

10.1. Для обеспечения защиты информации от несанкционированного доступа и вредоносных программ применяются встроенные и специализированные технические (аппаратные и программные) средства защиты.

10.2. К встроенным средствам защиты относятся такие средства защиты, механизмы которых являются неотъемлемой частью функциональных программ (системных и прикладных) и реализуют их дополнительную функцию – обеспечение защиты обрабатываемой информации.

10.3. К специализированным средствам защиты относятся такие средства защиты, основным функциональным назначением которых является обеспечение

10.4. Встроенные и специализированные средства защиты могут использоваться совместно.

10.5. При организации защиты ИСПДн от несанкционированного доступа к информации и вредоносных программ учитывается фактор наличия в корпоративной сети вычислительной техники низкой производительности (морально устаревшей).

10.6. Основными специализированными средствами защиты, применяемыми для защиты от несанкционированного доступа к информации и вредоносных программ, являются:

- антивирусные комплексы;
- межсетевые защитные (фильтрующие) экраны;
- средства мониторинга состояния объектов защиты;
- средства авторизации пользователей;
- средства криптографической защиты информации;
- средства блокирования устройств и портов вычислительных систем;
- средства гарантированного уничтожения информации на носителях;
- средства охранной, пожарной сигнализации, видеоконтроля и контроля доступа.

11. Мероприятия защиты информации от несанкционированного доступа

11.1. Работа с персоналом

11.1.1. В целях придания мероприятиям защиты информации характера обязательных элементов производственного процесса Учреждения требования по обеспечению защиты информации от несанкционированного доступа и вредоносных программ вменяются в обязанность всем пользователям вычислительной техники.

11.1.2. Придание требованиям по исполнению мероприятий по защите информации в ИСПДн от несанкционированного доступа и вредоносных программ характера элементов производственной дисциплины обеспечивается включением их в должностные обязанности всех работников, а также взятием с каждого принимаемого на работу в Учреждение работника письменного обязательства о соблюдении конфиденциальности информации.

11.1.3. Понимание и знание работниками Учреждения требований политики безопасности информации обеспечивается:

– своевременным изучением работниками под подпись требований нормативных документов и корректировкой их функциональных и должностных инструкций;

– регулярным проведением с работниками занятий по вопросам защиты информации;

– приобщением обязательств о соблюдении конфиденциальности информации, к личным делам работников.

11.2. Оборудование помещений для размещения средств обработки информации

11.2.1. Средства обработки конфиденциальной информации размещаются в помещениях, оборудование которых обеспечивает предотвращение бесконтрольного использования размещенных средств, возможность хищения носителей информации, визуальную досягаемость для посторонних лиц

отображаемой информации. Помещения оборудуются прочными дверями с замками.

11.2.2. Допуск работников, в помещения, в которых размещены средства обработки информации ограниченного доступа, не связанных непосредственно с их обслуживанием и обработкой информации, производится в сопровождении ответственных за обработку информации работников.

приказом управления образования
администрации города Белгорода
от «___» _____ 2017г. № ___

Правила обработки персональных данных, устанавливающие процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, а также определяющие для каждой цели обработки персональных данных содержание обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, сроки их обработки и хранения, порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований

1. Общие положения

1.1. Настоящие правила обработки персональных данных, устанавливающие процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, а также определяющие для каждой цели обработки персональных данных содержание обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, сроки их обработки и хранения, порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований (далее – Правила) разработаны в соответствии с:

- статьей 24 Конституции Российской Федерации;
- главой 14 Трудового Кодекса Российской Федерации;
- Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- постановлением Правительства РФ от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».

1.2. Настоящие Правила устанавливают в МАДОУ д/с №2 (далее – Учреждение) процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, а также определяют:

- цели обработки персональных данных;

- содержание обрабатываемых персональных данных;
- сроки обработки и хранения персональных данных;
- порядок уничтожения персональных данных при достижении целей обработки или при наступлении иных законных оснований.

1.3. Настоящие Правила вступают в силу с момента их утверждения и действуют бессрочно, до замены их новыми. Все изменения в Правила вносятся приказом.

2. Цели обработки персональных данных

Обработка персональных данных осуществляется с целью:
- выполнения возложенных на Учреждение обязанностей;
- учета персональных данных сотрудников в связи с реализацией трудовых отношений.

3. Категории субъектов, персональные данные которых обрабатываются, сроки их обработки и хранения

3.1. Категории субъектов, персональные данные которых обрабатываются:
- сотрудники Учреждения;
- субъекты ПДн, не являющиеся сотрудниками Учреждения.

3.2. Персональные данные обрабатываются в сроки, обусловленные заявленными целями их обработки.

3.3. Обработка персональных данных прекращается по достижении заявленных целей или при наступлении иных законных оснований.

3.4. Определение сроков хранения осуществляется в соответствии с требованиями архивного законодательства Российской Федерации, в том числе в соответствии с перечнями типовых архивных документов с указанием сроков их хранения.

При использовании документов, содержащих персональные данные, срок обработки, в том числе хранения, устанавливается по максимальному сроку.

Обработка персональных данных без документально определенных и оформленных сроков обработки, в том числе хранения, не допускается.

4. Содержание обрабатываемых персональных данных

4.1. В соответствии с целями обработки Учреждение обрабатывает следующие персональные данные:

4.1.1. Персональные данные работников:
- фамилия, имя, отчество;
- должность.

4.1.2. Персональные данные граждан:
- фамилия, имя, отчество;
- адрес места жительства;
- адрес электронной почты.

5. Порядок уничтожения персональных данных при достижении целей обработки или при наступлении иных законных оснований

5.1. В случае достижения цели обработки персональных данных Учреждение обязано прекратить обработку персональных данных или обеспечить

ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Учреждения) и уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Учреждения) в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между Учреждением и субъектом персональных данных либо если Учреждение не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных федеральными законами Российской Федерации.

5.2. В случае отзыва субъектом персональных данных согласия на обработку его персональных данных Учреждение обязано прекратить их обработку или обеспечить прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению Учреждения) и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Учреждения) в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между Учреждением и субъектом персональных данных либо если Учреждение не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных федеральными законами Российской Федерации.

5.3. В случае выявления неправомерной обработки персональных данных, осуществляемой Учреждением или лицом, действующим по поручению Учреждения, Учреждение в срок, не превышающий трех рабочих дней с даты этого выявления, обязано прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных лицом, действующим по поручению Учреждения. В случае, если обеспечить правомерность обработки персональных данных невозможно, Учреждение в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, обязано уничтожить такие персональные данные или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных Учреждение обязано уведомить субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

5.4. В случае отсутствия возможности уничтожения персональных данных в течение срока, указанного в пунктах 5.1-5.3, Учреждение осуществляет блокирование таких персональных данных или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Учреждения) и обеспечивает уничтожение

персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

5.5. После уничтожения персональных данных Учреждение обязано уведомить о факте уничтожения субъекта персональных данных и, в случае если уничтожение произведено по запросу уполномоченного органа, указанный орган.

6. Процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных

6.1. К процедурам, направленным на выявление и предотвращение нарушений законодательства в сфере персональных данных и устранение таких последствий, относятся:

- реализация мер, направленных на обеспечение выполнения Учреждением своих обязанностей;
- выполнение предусмотренных законодательством обязанностей, возложенных на Учреждение;
- обеспечение личной ответственности сотрудников, осуществляющих обработку либо доступ к персональным данным;
- организация рассмотрения запросов субъектов персональных данных или их представителей и ответов на такие запросы;
- организация внутреннего контроля соответствия обработки персональных данных требованиям к защите, установленным действующим законодательством и локальными актами;
- сокращение объема обрабатываемых данных;
- стандартизация операций, осуществляемых с персональными данными;
- определение порядка доступа сотрудников Учреждения в помещения, в которых ведется обработка персональных данных;
- проведение необходимых мероприятий по обеспечению безопасности персональных данных и носителей персональных данных;
- проведение периодических проверок условий обработки персональных данных;
- повышение осведомленности сотрудников, имеющих доступ к персональным данным, путем ознакомления с положениями законодательства Российской Федерации, локальными актами и организации обучения;
- блокирование, внесение изменений и уничтожение персональных данных в предусмотренных действующим законодательством случаях;
- оповещение субъектов персональных данных в предусмотренных действующим законодательством случаях;
- разъяснение прав субъектам персональных данных в вопросах обработки и обеспечения безопасности персональных данных;
- публикация и обеспечение доступа неограниченному кругу лиц документов, определяющих политику в отношении обработки персональных данных.

6.2. Указанный перечень процедур может дополняться.

Приложение 1

Акт уничтожения персональных данных

«___» _____ 20__ г. г. Белгород № _____

Комиссия в составе:
председатель комиссии

_____

(Ф.И.О., должность)

члены комиссии

_____

(Ф.И.О., должность)

_____

(Ф.И.О., должность)

Уничтожила персональные данные:

№ п/п	Ф.И.О. субъекта персональных данных	Состав персональных данных	Основание для уничтожения	Дата
1.				
2.				
3.				
4.				
5.				

Председатель комиссии:

Должность _____ Ф.И.О

Члены комиссии:

Должность _____ Ф.И.О

Должность _____ Ф.И.О

Приказом от 29.12.2017 г №274

Правила работы с обезличенными данными в случае обезличивания персональных данных

Термины и определения

Деобезличивание – действия, в результате которых обезличенные данные принимают вид, позволяющий определить их принадлежность конкретному субъекту персональных данных, то есть становятся персональными данными.

Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

Обезличенные данные – это данные, хранимые в информационных системах в электронном виде, принадлежность которых конкретному субъекту персональных данных невозможно определить без дополнительной информации.

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.

Обработка обезличенных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации, с обезличенными данными, без применения их предварительного деобезличивания.

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

Атрибут персональных данных субъекта – элемент структуры персональных данных (параметр персональных данных). Атрибут имеет название и может иметь множество возможных количественных и качественных значений применительно к конкретным субъектам персональных данных.

Атрибут обезличенных данных субъекта – элемент структуры обезличенных данных (параметр обезличенных данных). Атрибут имеет название и может иметь множество возможных количественных и качественных значений.

Семантика атрибута персональных данных – смысловое значение названия атрибута, обозначения персональных данных

Семантика атрибута обезличенных данных – смысловое значение названия атрибута, обозначения обезличенных данных.

1. Общие положения

1.1. Настоящие правила работы с обезличенными данными в случае обезличивания персональных данных (далее – Правила) определяют методы и процедуры обезличивания персональных данных, а также порядок работы с обезличенными данными в МАДОУ д/с №2 (далее – Учреждение) и действуют постоянно.

1.2. Настоящие Правила разработаны в соответствии с постановлением Правительства Российской Федерации от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», приказом Роскомнадзора от 5 сентября 2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных».

1.3. Свойства обезличенных данных:

- полнота – сохранение всей информации о персональных данных конкретных субъектов или группах субъектов, которая имелась до обезличивания;
- структурированность – сохранение структурных связей между обезличенными данными конкретного субъекта или группы субъектов, соответствующих связям, имеющимся до обезличивания;
- релевантность – возможность обработки запросов по обработке персональных данных и получения ответов в одинаковой семантической форме;
- семантическая целостность – соответствие семантики атрибутов обезличенных данных семантике соответствующих атрибутов персональных данных при их обезличивании;
- применимость – возможность обработки персональных данных без предварительного деобезличивания всего объема записей о субъектах;
- анонимность – невозможность однозначной идентификации субъектов данных, полученных в результате обезличивания, без применения дополнительной информации.

2. Методы обезличивания

2.1. К методам обезличивания относятся:

- метод введения идентификаторов – замена части персональных данных, позволяющих идентифицировать субъекта, их идентификаторами и созданием таблицы соответствия;
- метод изменения состава или семантики – изменение состава или семантики персональных данных путем замены результатами статистической обработки, преобразования, обобщения или удаления части сведений;

- метод декомпозиции – разделение множества (массива) персональных данных на несколько подмножеств (частей) с последующим раздельным хранением подмножеств;

- метод перемешивания – перестановка отдельных значений или групп значений атрибутов персональных данных в массиве персональных данных.

2.2. Применение того или иного метода обезличивания позволит получить обезличенные данные, обладающие различными свойствами, что даст возможность осуществлять все виды обработки персональных данных.

2.3. В каждом конкретном случае необходимо применять метод, который гарантирует свойства, необходимые для решения конкретных задач обработки.

2.4. Результаты сопоставления свойства обезличенных данных с методами обезличивания приведены в Таблице 1.

Таблица 1

Соответствие методов обезличивания свойствам обезличенных данных

Метод обезличивания / **Свойства обезличенных данных**	**Введение идентификаторов**	**Изменение состава и семантики**	**Декомпозиция**	**Перемешивание**
Полнота	+	+/–	+	+
Структурированность	+	+	+	+
Релевантность	+/–	+	+	+
Семантическая целостность	+	+/–	+	+
Применимость	+	+	+	+
Анонимность	+/–	+	+/–	+
+ безусловное наличие свойства; +/– условное наличие свойства				

3. Процедуры обезличивания

Процедура обезличивания обеспечивает практическую реализацию метода обезличивания и задается своим описанием.

3.2. Процедура реализации метода введения идентификаторов

3.2.1. Каждому значению идентификатора должно соответствовать одно значение атрибута и каждому значению атрибута должно соответствовать одно значение идентификатора.

3.2.2. Таблицы соответствия (дополнительные данные) создаются для каждого атрибута персональных данных, значения которых заменяются идентификаторами.

3.2.3. При обезличивании персональные данные в исходном множестве заменяются идентификаторами согласно таблице соответствия. Деобезличивание достигается обратной заменой идентификаторов на значения персональных данных по таблице соответствия.

3.2.4. На этапе реализации процедуры обезличивания определяются

- перечень таблиц соответствия (перечень атрибутов, для которых происходит замена значений идентификаторами);

- правила вычисления идентификаторов - наборов символов, однозначно соответствующих значениям атрибутов персональных данных субъекта;

- объемы таблицы соответствия - количество строк таблицы соответствия, содержащих идентификатор и соответствующее ему значение.

3.2.5. В качестве атрибутов, значения которых заменяются идентификаторами, как правило, выбираются атрибуты, однозначно идентифицирующие субъекта персональных данных.

3.2.6. Количество идентификаторов и объем таблиц соответствия, как правило, равны исходному количеству субъектов персональных данных. Возможны случаи, когда идентификатор вычисляется в зависимости от значения соответствующего атрибута.

3.2.7. Таблицы соответствия должны быть доступны ограниченному числу сотрудников.

3.2.8. Программное обеспечение, реализующее процедуру, должно обеспечивать внесение изменений и поддержку актуальности таблиц соответствия.

3.3. Процедура реализации метода изменения состава или семантики

3.3.1. Процедура реализации метода должна содержать правила удаления либо замены значений персональных данных субъектов на новые значения, вычисляемые по заданным правилам.

3.3.2. При замене значений атрибутов на новые требуется устанавливать правила обратной замены, если это необходимо для деобезличивания.

3.3.3. На этапе реализации процедуры обезличивания необходимо определить следующие параметры:

- перечень атрибутов персональных данных, подлежащих удалению;

- перечень атрибутов персональных данных, подлежащих замене на новые значения;

правила вычисления значений для замены (обратной замены) персональных данных субъектов.

3.3.4. Программная реализация процедуры должна обеспечить возможность внесения изменений и дополнений в состав обезличенных данных, динамическое вычисление значений для замены при занесении новых субъектов, проверку и поддержку актуальности данных.

3.4. Процедура реализации метода декомпозиции

3.4.1. Процедура реализации метода по заданному правилу (алгоритму) производит разделение исходного массива персональных данных на несколько частей, каждая из которых содержит заданный набор атрибутов всех субъектов. Сведения, содержащиеся в каждой части, не позволяют идентифицировать субъектов персональных данных.

3.4.2. Деобезличивание осуществляется по заданному набору связей (используются таблицы связей, являющиеся дополнительными данными) между раздельно хранимыми частями.

3.4.3. На этапе реализации процедуры обезличивания необходимо определить следующие параметры:

- перечень атрибутов, составляющих подмножества персональных данных;
- таблицы связей между подмножествами персональных данных;
- адреса хранения подмножеств персональных данных.

3.4.4. Правила разделения исходного массива данных определяются таким образом, чтобы каждая из раздельно хранимых частей не содержала сведений, позволяющих однозначно идентифицировать субъекта персональных данных.

3.4.5. Программная реализация процедуры должна обеспечивать согласованное внесение изменений и дополнений во все подмножества и таблицы связей, поиск данных о субъекте во всех подмножествах, поддержку актуальности таблиц связей, проверку полноты данных (согласование подмножеств).

3.5. Процедура реализации метода перемешивания

3.5.1. Метод перемешивания реализуется путем перемешивания отдельных значений или групп значений атрибутов субъектов персональных данных между собой.

3.5.2. Перемешивание проводится по установленному правилу.

3.5.3. Деобезличивание достигается с использованием процедуры, обратной процедуре перемешивания.

3.5.4. Для реализации процедуры необходимо определить алгоритм перемешивания и его параметры.

3.5.5. На этапе реализации процедуры обезличивания необходимо определить следующие параметры:

- набор параметров алгоритма перемешивания (дополнительные данные для обезличивания/деобезличивания);
- значения параметров алгоритма перемешивания (дополнительные данные для обезличивания/деобезличивания).

3.5.6. Выбор параметров перемешивания зависит от алгоритма перемешивания, требуемой стойкости к атакам, и объема обезличиваемых персональных данных.

3.5.7. Программная реализация процедуры должна обеспечивать возможность внесения изменений и дополнений в состав обезличенных данных, добавление новых пользователей, поддержку актуальности данных и возможность повторного перемешивания с новыми параметрами без предварительного деобезличивания.

4. Организация обработки обезличенных данных

4.1. При использовании процедуры обезличивания не допускается совместное хранение персональных данных и обезличенных данных.

4.2. Обезличивание персональных данных должно производиться перед внесением их в информационную систему.

4.3. Учреждение вправе обрабатывать обезличенные данные, полученные от третьих лиц.

4.4. В процессе обработки обезличенных данных, при необходимости, может проводиться деобезличивание. После обработки персональные данные, полученные в результате такого деобезличивания, уничтожаются

4.5. Обработка персональных данных до осуществления процедур обезличивания и после выполнения операций деобезличивания должна осуществляться в соответствии с действующим законодательством Российской Федерации с применением мер по обеспечению безопасности персональных данных.

4.6. Обработка обезличенных данных должна осуществляться с использованием технических и программных средств, соответствующих форме представления и хранения данных.

4.7. Хранение и защиту дополнительной (служебной) информации, содержащей параметры методов и процедур обезличивания/деобезличивания, следует обеспечить в соответствии с внутренними процедурами защиты конфиденциальной информации. При этом должно обеспечиваться исполнение установленных правил доступа пользователей к хранимым данным, резервного копирования и возможности актуализации и восстановления хранимых данных.

4.8. Процедуры обезличивания/деобезличивания должны встраиваться в процессы обработки персональных данных как их неотъемлемый элемент, а также максимально эффективно использовать имеющуюся инфраструктуру, обеспечивающую обработку персональных данных.

5. Правила работы с обезличенными данными

5.1. При обработке обезличенных данных следует:

- обеспечить соответствие процедур обезличивания/деобезличивания персональных данных требованиям к обезличенным данным и методам обезличивания;
- обеспечить соответствие процедур обезличивания/деобезличивания условиям и целям обработки персональных данных;
- убедиться, что при реализации процедур обезличивания/ деобезличивания, а также при последующей обработке обезличенных данных не нарушаются права субъекта персональных данных.

5.2. В случае, если обработка обезличенных данных была поручена третьим лицом, следует соблюдать все требования, предъявляемые этим лицом.

5.3. При хранении обезличенных данных следует:

- организовать раздельное хранение обезличенных данных и дополнительной (служебной) информации о выбранном методе реализации процедуры обезличивания и параметрах процедуры обезличивания;
- обеспечивать конфиденциальность дополнительной (служебной) информации о выбранном методе реализации процедуры обезличивания и параметрах процедуры обезличивания.

5.4. При передаче вместе с обезличенными данными информации о выбранном методе реализации процедуры обезличивания и параметрах процедуры обезличивания следует обеспечить конфиденциальность канала (способа) передачи данных.

5.5.В ходе реализации процедуры деобезличивания следует:

- реализовать все требования по обеспечению безопасности получаемых персональных данных при автоматизированной обработке на средствах вычислительной техники, участвующих в реализации процедуры деобезличивания и обработке деобезличенных данных;

- обеспечить обработку и защиту деобезличенных данных в соответствии с требованиями Федерального закона от 26 июня 2006 г. № 152-ФЗ «О персональных данных».

6. Рекомендации по выбору методов обезличивания

6.1. При выборе методов и процедур обезличивания следует руководствоваться целями и задачами обработки персональных данных.

6.2. Обезличивание персональных данных, обработка которых осуществляется с разными целями, может осуществляться разными методами.

6.3. Возможно объединение различных методов обезличивания в одну процедуру.

6.4. При выборе метода и процедуры обезличивания следует учитывать:

- объем персональных данных, подлежащих обезличиванию;
- форму представления данных;
- область обработки обезличенных данных;
- способы хранения обезличенных данных;
- применяемые меры по обеспечению безопасности данных.

6.5. В Таблице 2 приведены рекомендации по выбору метода обезличивания в зависимости от класса решаемых задач.

Таблица 2

Сопоставление задач обработки методам обезличивания

Класс задач	**Задачи обработки**	**Метод обезличивания**
Статистическая обработка и статистические исследования персональных данных	– осуществление обработки по заявленным параметрам; – проведение исследований по заданным параметрам субъектов.	– перемешивание; – декомпозиция; – изменение состава или семантики.
Сбор и хранение персональных данных	– внесение персональных данных субъектов в информационную систему на основе анкет, заявлений и прочих документов.	– перемешивание; – декомпозиция; – введение идентификаторов.
Обработка поисковых запросов (поиск данных о субъектах и поиск субъектов по известным данным)	– поиск информации о субъектах; – печать и выдача субъектам документов в установленной форме, содержащих персональные данные; – выдача справок, выписок, уведомлений по запросам субъектов или уполномоченных органов.	– перемешивание; – декомпозиция; - введение идентификаторов
Актуализация персональных данных	– внесение изменений в существующие записи о	– перемешивание; – декомпозиция;

	субъектах на основе обращений субъектов, решений судов и других уполномоченных органов; – внесение изменений в существующие записи о субъектах на основе исследований, выполнения своих функций или требований законодательства РФ.	– введение идентификаторов.
Интеграция данных	– поиск информации о субъектах; – передача данных смежным организациям.	– перемешивание; – декомпозиция; – введение идентификаторов.
Ведение учета субъектов персональных данных	– прием анкет, заявлений; – ведение учета персональных данных в соответствии с функциями органа.	– перемешивание; – декомпозиция; – введение идентификаторов.