АДМИНИСТРАЦИЯ ГОРОДА БЕЛГОРОДА

УПРАВЛЕНИЕ ОБРАЗОВАНИЯ

ПРИКАЗ

«30» марта 2017 г. № 465

О введении в действие документов, регламентирующих мероприятия по ЗПДн

В целях обеспечения защиты персональных данных, обрабатываемых в информационных системах персональных данных **п р и к а з ы в а ю :**

1. Утвердить и ввести в действие следующие организационно-распорядительные документы по защите персональных данных:

1.1. Инструкцию администратора информационных систем персональных данных (прилагается).

1.2. Инструкцию о порядке резервирования и восстановления работоспособности технических средств, программного обеспечения, баз данных и средств защиты информации информационных систем персональных данных (прилагается).

1.3. Инструкцию ответственного за организацию обработки и обеспечение безопасности персональных данных в информационных системах персональных данных (прилагается).

1.4. Инструкцию по организации антивирусной защиты (прилагается).

1.5. Инструкцию пользователя информационных систем персональных данных (прилагается).

1.6. Инструкцию по организации защиты информации в информационных системах персональных данных (прилагается).

1.7. Положение об обработке персональных данных (прилагается).

1.8. 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 (прилагается).

1.9. Правила работы с обезличенными данными в случае обезличивания персональных данных (прилагается).

1.10. Регламент по учету, хранению и уничтожению машинных носителей персональных данных (прилагается).

1.11. Журнал поэкземплярного учета криптосредств, эксплуатационной и технической документации к ним (прилагается).

1.12. Журнал технический (аппаратный) (прилагается).

1.13. Журнал учета выдачи идентификаторов и паролей (прилагается).

1.14. Журнал учета мероприятий по контролю защиты персональных данных (прилагается).

1.15. Журнал учета машинных носителей информации (прилагается).

1.16. Журнал учета резервного копирования информационных ресурсов (прилагается).

1.17. Журнал учёта обращений субъектов персональных данных и их законных представителей (прилагается).

2. Обеспечить ознакомление всех сотрудников с утвержденными документами в соответствии с их должностными обязанностями.

3. Контроль за исполнением настоящего приказа возложить на заместителя руководителя управления образования администрации г. Белгорода А.Ю.Ковалева.

Руководитель управления образования
администрации г. Белгорода **И.А.Гричаникова**

О.В.Пашкова
32-47-20

УТВЕРЖДЕНА
приказом управления образования
администрации города Белгорода
от «30» марта 2017 г. № 465

Инструкция администратора 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

Роскомнадзор - Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций

САЗ - система анализа защищенности

СЗИ - средства защиты информации

СЗПДн - система (подсистема) защиты персональных данных

СОВ - система обнаружения вторжений

УБПДн - угрозы безопасности персональных данных

ФСТЭК - Федеральная служба по экспортному и техническому контролю

ФСБ - Федеральная служба безопасности

1. Общие положения

1.1. Администратор ИСПДн управления образования администрации г. Белгорода (далее - Администратор) назначается приказом руководителя управления образования администрации г. Белгорода.

1.2. Администратор в своей работе руководствуется настоящей инструкцией, требованиями законодательства РФ, руководящими и нормативными документами ФСТЭК России и ФСБ России, Роскомнадзора, а также принятыми в организации положениями, инструкциями, приказами.

1.3. Администратор отвечает за обеспечение устойчивой работоспособности элементов ИСПДн и СЗИ при обработке ПДн.

1.4. Методическое руководство работой Администратора осуществляется ответственным за организацию обработки и обеспечение безопасности ПДн.

2. Обязанности администратора ИСПДн

Администратор обязан:

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

2.2. Участвовать в контрольных и тестовых испытаниях и проверках элементов ИСПДн.

2.3. Уточнять в установленном порядке обязанности пользователей и администраторов ИСПДн.

2.4. Анализировать состояние защиты ИСПДн и ее отдельных подсистем.

2.5. Контролировать неизменность состояния защищенности информационных систем обработки персональных данных.

2.6. Контролировать физическую сохранность средств и оборудования ИСПДн.

2.7. Контролировать исполнение пользователями ИСПДн введенного режима безопасности, а также правильность работы с элементами ИСПДн и средствами защиты.

2.8. Контролировать исполнение пользователями парольной политики.

2.9. Периодически представлять руководству отчет о состоянии защиты ИСПДн, о нештатных ситуациях на объектах ИСПДн и допущенных пользователями нарушениях установленных требований по защите информации.

2.10. В случае отказа работоспособности технических средств и программного обеспечения ИСПДн, в том числе средств защиты, принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.

2.11. Принимать меры по реагированию, в случае возникновения нештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий.

2.12. Обеспечивать установку, настройку и своевременное обновление элементов ИСПДн:

- программного обеспечения АРМ и серверов (операционные системы, прикладное и специальное ПО);
- антивирусного ПО;
- аппаратных средств;
- аппаратных и программных средств защиты.

2.13. Обеспечивать работоспособность элементов ИСПДн и локальной вычислительной сети.

2.14. Осуществлять еженедельное резервное копирование информации, содержащей ПДн.

2.15. Осуществлять контроль за порядком учета, создания, хранения и использования резервных и архивных копий массивов данных, машинных (выходных) документов.

2.16. Обеспечивать функционирование и поддержку работоспособности средств защиты информации, либо по согласованию с руководителем привлекать для этого организацию, имеющую оформленную в установленном порядке лицензию на осуществление деятельности по технической защите конфиденциальной информации.

2.17. В случае отказа работоспособности технических средств и программного обеспечения элементов ИСПДн, в том числе средств защиты информации, принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.

2.18. Проводить периодический контроль работоспособности элементов ИСПДн в пределах возложенных на него функций.

2.19. В случае необходимости хранить, осуществлять прием и выдачу персональных паролей пользователей, осуществлять контроль за правильностью использования персонального пароля пользователями ИСПДн.

2.20. Информировать ответственного за организацию обработки и обеспечение безопасности персональных данных о фактах нарушения установленного порядка работ и попытках несанкционированного доступа к информационным ресурсам ИСПДн.

2.21. Требовать прекращения обработки информации, как в целом, так и для отдельных пользователей, в случае выявления нарушений установленного порядка работ или нарушения функционирования ИСПДн или средств защиты информации.

2.22. Обеспечивать строгое выполнение требований по обеспечению безопасности информации при организации обслуживания технических средств и отправке их в ремонт. При проведении технического обслуживания и ремонта запрещается передавать ремонтным организациям узлы и блоки с элементами накопления и хранения информации.

2.23. Присутствовать при выполнении технического обслуживания элементов ИСПДн сторонними физическими лицами и организациями.

2.24. В случае возникновения нештатных и аварийных ситуаций принимать меры по реагированию с целью их предотвращения либо ликвидации их последствий.

УТВЕРЖДЕНА
приказом управления образования
администрации города Белгорода
от «30» марта 2017 г. № 465

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 управления образования администрации г. Белгорода (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 возможности, должны согласовываться с вышестоящим руководством.

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 управления образования
администрации города Белгорода
от «30» марта 2016 г. № 465

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 управления образования администрации г. Белгорода (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.

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

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 управлении образования администрациит г. Белгорода (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 ИСПДн с целью выявления программно-математического воздействия;

– 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 пользователь ИСПДн должен приостановить работу на АРМ с последующим его

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.

УТВЕРЖДЕНА
приказом управления образования
администрации города Белгорода
от «30» марта 2017 г. № 465

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 управления образования администрации г. Белгорода (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 был задан;

- 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.

УТВЕРЖДЕНА
приказом управления образования
администрации города Белгорода
от «30» марта 2017 г. № 465

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 несанкционированного запуска на вычислительном средстве в целях не

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 управлении образования администрации г.Белгорода (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;
- организацией выполнения отделами управления образования администрации г.Белгорода, должностными лицами и работниками требований нормативных документов по защите 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;
- проведением аттестации ИСПДн на соответствие требованиям по защите информации, установленными государственными регуляторами;
- 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 основано на принципах безопасности, правомочности и эффективности. 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;
- регистрация событий безопасности;
- 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 носителями (документами), содержащими конфиденциальную информацию, 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 отдела управления образования администрации г.Белгорода;
- 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 своего структурного подразделения;
- 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 отдела управления образования

администрации г.Белгорода, 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:

- разграничение прав доступа к информации;
- 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 безопасности информации.

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.

11.1.4. Ответственность за своевременное доведение требований нормативных (руководящих) документов до работников, проведения занятий по вопросам защиты информации возлагается на руководителей отделов управления образования администрации г.Белгорода.

11.1.5. Ответственность за организацию занятий с работниками возлагается на руководителя Учреждения.

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 и устройствами для опечатывания или устройствами, гарантирующими надежное их закрытие и контроль вскрытия.

11.2.2. Помещения, в которых размещаются средства обработки информации, оборудуются аппаратурой обеспечения требуемого температурно-влажностного режима.

11.2.3. При использовании автоматизированной системы контроля и управления доступом в технологические помещения применяются электромеханические нормально закрытые замки или электромагнитные замки с резервируемым питанием.

11.2.4. Помещения цокольного, первого, последнего этажей, помещения других этажей, примыкающие к карнизам, балконам, пожарным лестницам, должны иметь три рубежа технической охраны или прочные распашные металлические решетки и два рубежа охраны. В случае сдачи здания Учреждения на пульт централизованного наблюдения (ПЦН), необходимо руководствоваться требованиями вневедомственной охраны по оборудованию техническими средствами.

11.2.5. По окончании рабочего времени закрытые помещения сдаются под охрану установленным в Учреждении порядком.

11.2.6. 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.

11.3. Учет ресурсов и авторизация пользователей

11.3.1. Защищаемые ресурсы Учреждения определяются «Перечнем защищаемых информационных ресурсов», который утверждается руководителем Учреждения.

11.3.2. Доступ к защищаемому ресурсу ИСПДн обеспечивается минимально необходимому для выполнения производственных задач числу сотрудников, определяемому «Матрицей доступа к информационной системе персональных данных».

11.3.3. «Матрицей доступа к информационной системе персональных данных» определяются разрешенные режимы работы пользователей и уровни доступа.

11.3.4. Авторизация пользователей и информационных ресурсов производится на основании положительных результатов аутентификации. Не допускается авторизация неаутентифицированных пользователей.

11.3.5. По возможности используется двухфакторная аутентификация пользователей. Двухфакторная аутентификация организуется в первую очередь при организации доступа к конфиденциальной информации.

11.4. Межсетевые экраны

11.4.1. Межсетевые экраны в Учреждении применяются как для ограничения или запрещения доступа узлов (хостов) внешней сети к устройствам внутренней сети, так и для ограничения доступа узлов внутренней сети к сервисам внешней сети, а также для защиты и изоляции приложений, сервисов и устройств во внутренней сети от нежелательного трафика.

11.4.2. Межсетевой экран устанавливается в «разрыв» канала связи между внутренней сетью Учреждения и внешней информационно-телекоммуникационной сетью или между сегментами внутренней сети и контролирует (фильтрует) весь проходящий через него трафик.

11.4.3. Фильтрация трафика организуется, как правило, в соответствии с разрешительным принципом, то есть путем явного указания разрешенного для пропускания трафика и блокирования всего остального.

11.4.4. Устройства с выходом в Интернет располагаются в сегменте сети, отделенном от устройств, выход которых в Интернет запрещен, межсетевым экраном.

11.4.5. Допускается в целях ограждения узлов (сегментов) ЛВС от нежелательного внутреннего сетевого трафика использование фильтрации в соответствии с запретительным принципом, при котором межсетевым экраном не пропускается только соответствующий правилу трафик.

11.4.6. Для сокрытия схемы внутренней сети от внешнего наблюдателя используется прокси-сервер или предоставляемый межсетевым экраном режим трансляции сетевых адресов, позволяющий подменять IP-адреса пакетов, проходящих через него.

12. Защита активного сетевого оборудования и рабочих станций

12.1. В целях контроля конфигурации средств вычислительной техники для каждого хоста (узла) сети фиксируется состав устройств и программного обеспечения на момент ввода его в эксплуатацию и все изменения, вносимые в процессе эксплуатации.

12.2. Учет состояния средств вычислительной техники ведется вручную или с использованием специальных программных продуктов.

12.3. Защищаемые компьютеры настраиваются на обеспечение:

- защиты входа в настройку базовой системы ввода-вывода (BIOS) паролем;
- использования в качестве первого загрузочного устройства накопителя на жестком магнитном диске;
- исключения входа в систему без пароля;
- отсутствия привилегий администратора системы у остальных пользователей вычислительного средства;
- отсутствия консоли восстановления системы.

12.4. В целях исключения бесконтрольного вскрытия корпус компьютера опечатывается путем соединения разъемных деталей специальными легко разрываемыми наклейками или пломбируется.

12.5. Диски горячей замены серверов или закрывающие доступ к ним панели также опечатываются.

12.6. Использование функций вывода информации всех, не требующихся для непосредственного выполнения функций автоматизированного рабочего места, устройств рабочей станции блокируется с помощью специального программного обеспечения. При отсутствии программных средств защиты блокировка портов производится контрольными наклейками.

12.7. Для защиты рабочих станций применяются программно-аппаратные средства, обеспечивающие защиту устройств и информационных ресурсов от несанкционированного доступа посредством выполнения контрольных процедур: аутентификации пользователя, проверки целостности программных средств компьютера.

12.8. Доступ в помещения с активным сетевым оборудованием ограничивается.

13. Системы безопасности зданий (помещений)

13.1. В целях защиты от несанкционированного доступа к информации в Учреждении определена контролируемая зона.

13.2. Охрана контролируемой зоны организуется в целях предотвращения доступа в нее посторонних лиц, а также создания надежных препятствий для несанкционированного проникновения в помещения Учреждения и хранилища носителей информации.

13.3. В целях повышения эффективности охраны здания, при необходимости, помещения Учреждения оборудуются системами безопасности:

- системой пожарной сигнализации;
- системой охранной сигнализации.

13.4 Охранная сигнализация

13.4.1. Охранная сигнализация предназначается для обеспечения своевременного выявления попыток несанкционированного проникновения в помещения и выдачи сигнала тревоги в случае несанкционированного проникновения в помещение, находящееся под охраной.

13.4.2. Охранная сигнализация должна обеспечить надежное и быстрое срабатывание извещателей с достаточной для принятия немедленных мер локализацией места проникновения, самодиагностику и возможность работы от автономного источника электроэнергии.

13.4.3. Системой охранной сигнализации обязательно оборудуются:

- все входы в здание, в том числе запасные, чердачные люки и вентиляционно-технологические проемы;
- помещения, в которых размещаются средства обработки и хранения информации ограниченного доступа (конфиденциальной информации);
- помещения, в которых размещаются хранилища носителей информации ограниченного доступа;
- помещение администратора по защите информации.

13.5. Пожарная сигнализация

13.5.1. Здания Учреждения оборудуются системами пожарной сигнализации в целях своевременного обнаружения очага возгорания и своевременного принятия мер по тушению пожара.

13.5.2. Пожарная сигнализация должна обеспечить надежное и быстрое срабатывание извещателей с достаточной для принятия немедленных мер по локализации места возникновения пожара, самодиагностику и возможность работы от автономного источника электроэнергии.

13.5.3. При повседневном режиме электроснабжения система пожарной сигнализации должна функционировать круглосуточно (непрерывно).

13.5.4. Устанавливаемое оборудование и сети систем должны быть безопасны при эксплуатации для лиц, соблюдающих правила обращения с ними.

14. Авторизация пользователей

14.1. К работе с защищаемым ресурсом допускается только определенный круг пользователей, в соответствии с должностными инструкциями.

14.2. Идентификация пользователя производится присвоением ему имени пользователя (код пользователя) – уникальной символьной последовательности.

14.3. Аутентификация пользователя производится посредством сравнения предъявляемого ими аутентификатора с аутентификатором, поставленным в однозначное соответствие предъявленному идентификатору (имени пользователя).

14.4. В качестве аутентификатора пользователя ИСПДн используется пароль (случайная уникальная символьная последовательность) или сертификат, которые вводятся в ПК с клавиатуры или считываются из индивидуального аутентификатора.

14.5. Аутентификация пользователя выполняется при:

- входе в систему;
- обращении к ресурсам.

14.6. Авторизация пользователей производится при положительном результате аутентификации.

14.7. Смена аутентификаторов, вводимых с клавиатуры, выполняется один раз в три месяца. Смена аутентификаторов, которые хранятся и предъявляются системе аутентификации посредством устройств аутентификации индивидуального пользования, производится не реже, чем один раз в год.

14.8. Технические мероприятия авторизации пользователей обеспечиваются выполнением следующих организационных мероприятий:

- актуализация перечня защищаемых информационных ресурсов;
- актуализация документов по допуску и обеспечению соответствующего доступа пользователей к защищаемым ресурсам;
- распределение ответственности за выполнение мероприятий по защите информации между должностными лицами, организующими и реализующими технические мероприятия;
- назначение администраторов защиты (безопасности) информации.

14.9. Пользователям предоставляются минимально необходимые для выполнения производственных задач права доступа к информации. Ответственность за обоснованность предоставляемых пользователям прав возлагается на руководителей отделов управления образования администрации г.Белгорода.

15. Действия при компрометации аутентификатора или парольной информации

15.1. Под компрометацией аутентификатора понимается: утрата электронного аутентификатора, разглашение PIN-кода электронного аутентификатора или иная ситуация, которая дает основание для предположения о нарушении конфиденциальности пароля или PIN-кода устройства аутентификации (неявная компрометация).

15.2. При выявлении факта компрометации аутентификатора пользователь незамедлительно обязан: при разглашении PIN-кода электронного аутентификатора сменить PIN-код; в остальных случаях – сообщить о факте выявления непосредственному руководителю и администратору по защите информации.

15.3. В случае выявления факта компрометации аутентификатора пользователя администратор по защите информации обязан немедленно заблокировать учетную запись пользователя, аутентификатор которого скомпрометирован.

15.4. Расследование факта компрометации проводится комиссией, назначаемой руководителем Учреждения. В состав комиссии обязательно включается администратор по защите информации.

15.5. Результаты работы комиссии оформляются актом. Акт утверждается руководителем Учреждения.

15.6. Выдача пользователю нового аутентификатора производится по указанию руководителя Учреждения.

УТВЕРЖДЕНО
приказом управления образования
администрации города Белгорода
от «30» марта 2017г. № 465

Положение об обработке персональных данных

Термины и определения

Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.

Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

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

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.

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.

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

Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Трансграничная передача персональных данных – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

Уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в

информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

1. Общие положения

1.1. Настоящее положение об обработке персональных данных (далее – Положение) разработано в соответствии с Конституцией Российской Федерации, Гражданским кодексом Российской Федерации, Трудовым кодексом Российской Федерации, Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», Постановлением Правительства РФ от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Постановлением Правительства РФ от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

1.2. Цель настоящего Положения – определение единого порядка обработки персональных данных в управлении образования администрации города Белгорода (далее – Учреждение); обеспечение прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты права на неприкосновенность частной жизни, личную и семейную тайну; установление ответственности лиц, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.

1.3. Область действия настоящего Положения включает в себя:

- все процессы обработки персональных данных как с использованием средств автоматизации, так и без использования таковых;
- все структурные подразделения Учреждения;
- все информационные системы Учреждения, в которых происходит обработка персональных данных.

1.4. Настоящее Положение вступает в силу с момента его утверждения и действует бессрочно до замены его новым Положением.

1.5. Все изменения в Положение вносятся приказом.

1.6. Все работники Учреждения должны быть ознакомлены с настоящим Положением под роспись.

2. Цели обработки персональных данных

Обработка персональных данных осуществляется в целях: реализации трудовых отношений; обеспечения соблюдения законов Российской Федерации и иных нормативных правовых актов; содействия в трудоустройстве, обучении и продвижении работника по службе; осуществления расчета заработной платы и иных выплат и удержаний; осуществления платежей и переводов в интересах работника.

3. Состав обрабатываемых персональных данных

Для достижения заявленных в п.2 целей Учреждение обрабатывает персональные данные граждан, состоящих в трудовых отношениях с Учреждением. Состав обрабатываемых персональных данных определен в

«Перечне обрабатываемых персональных данных», утвержденных руководителем Учреждения.

4. Действия, осуществляемые с персональными данными

4.1. Действия или совокупность действий (операций) с персональными данными: сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (распространение, предоставление, доступ), блокирование, удаление, уничтожение.

4.2. Персональные данные субъектов, не являющихся сотрудниками.

5. Цели обработки персональных данных

Обработка персональных данных осуществляется в целях выполнения возложенных на Учреждение функций.

6. Состав обрабатываемых персональных данных

Для достижения заявленных в п.2 целей Учреждение обрабатывает персональные данные граждан, не являющихся сотрудниками Учреждения. Состав обрабатываемых персональных данных определен в «Перечне обрабатываемых персональных данных», утвержденных руководителем Учреждения.

7. Действия, осуществляемые с персональными данными

7.1. Действия или совокупность действий (операций) с персональными данными: сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (распространение, предоставление, доступ), блокирование, удаление, уничтожение.

7.2. Обработка персональных данных.

8. Общие положения

8.1. При обработке персональных данных должны обеспечиваться точность персональных данных, их достаточность и актуальность по отношению к целям обработки персональных данных.

8.2. При обнаружении неточных или неполных персональных данных производится их уточнение и актуализация.

8.3. В Учреждении на основании «Перечня сведений конфиденциального характера», утвержденного Указом Президента Российской Федерации 6 марта 1997 г. № 188, определен и утвержден «Перечень защищаемых информационных ресурсов» и «Перечень обрабатываемых персональных данных».

8.4. Специальные категории персональных данных не обрабатываются.

8.5. Биометрические персональные данные не обрабатываются.

8.6. Обработка специальных категорий персональных данных и биометрических персональных данных возможна только с письменного согласия субъекта персональных данных.

8.7. Трансграничная передача персональных данных не осуществляется.

8.8. Обработка персональных данных в целях продвижения товаров, работ, услуг путем осуществления прямых контактов с потенциальным потребителем не осуществляется. В случае принятия решения об обработке персональных данных в целях продвижения товар, работ, услуг необходимо предварительно получить согласие субъекта персональных данных и прекратить по его требованию.

8.9. Обработка персональных данных осуществляется в смешанном режиме, как с использованием средств автоматизации, так и без использования таковых.

8.10. При обработке персональных данных Учреждение руководствуется принципами:

- обеспечение законности целей и способов обработки персональных данных;
- соответствие целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных;
- соответствие объема и характера обрабатываемых персональных данных, а также способов обработки персональных данных целям обработки;
- отсутствия избыточных персональных данных по отношению к заявленным целям;
- использования раздельных баз данных для несовместимых целей обработки персональных данных.

8.11. Обработка персональных данных осуществляется на законной и справедливой основе.

8.12. Обработка персональных данных допускается в следующих случаях:

- с согласия субъекта персональных данных;
- для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей;
- для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, в том числе в случае реализации оператором своего права на уступку прав (требований) по такому договору, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем;
- для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;
- для осуществления прав и законных интересов Учреждения или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;
- для осуществления правосудия, исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве;
- в случае, когда доступ неограниченного круга лиц к персональным данным субъекта предоставлен самим субъектом персональных данных, либо по его просьбе;
- в случае, когда персональные данные подлежат опубликованию или обязательному раскрытию в соответствии с федеральным законом;
- в статистических или иных исследовательских целях, при условии обязательного обезличивания персональных данных.

8.13. Правовыми основаниями для обработки являются:
- Конституция Российской Федерации;
- Трудовой кодекс Российской Федерации.

9. Сбор персональных данных

9.1. Все персональные данные Учреждение получает от субъекта персональных данных.

9.2. Обработка персональных данных осуществляется с согласия субъекта персональных данных.

9.3. Обработка персональных данных без согласия субъекта персональных данных допускается в случаях, предусмотренных Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

9.4. Персональные данные могут быть получены Учреждением от лица, не являющегося субъектом персональных данных, при условии предоставления оператору подтверждения наличия оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

9.5. Если персональные данные были получены не от субъекта персональных данных, то Учреждение уведомляет субъекта персональных данных об осуществлении обработки его персональных данных и получает от него письменное согласие. Согласия субъекта на получение его персональных данных от третьих лиц не требуется в случаях, установленных Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

9.6. Если согласие на обработку персональных данных получено от представителя субъекта персональных данных, то полномочия данного представителя на дачу согласия от имени субъекта персональных данных проверяются Учреждением.

9.7. Если предоставление персональных данных является обязательным в соответствии с федеральным законом, Учреждение разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные.

9.8. Учреждение проверяет достоверность предоставляемых сведений, сверяя полученные данные с имеющимися у субъекта персональных данных документами.

10. Накопление персональных данных

10.1. Накопление персональных данных происходит в результате деятельности Учреждения.

10.2. Учреждение накапливает персональные данные следующими способами:
- копирование оригиналов документов;
- внесение сведений в учетные формы (на бумажные носители и в базы данных);
- получение оригиналов документов.

11. Хранение персональных данных

11.1. Хранение персональных данных осуществляется в форме, позволяющей определить субъекта персональных данных не дольше, чем этого требуют цели их обработки.

11.2. Персональные данные хранятся на бумажных и электронных носителях.

11.3. Хранение персональных данных, обработка которых осуществляется в целях, не совместимых между собой, осуществляется на разных материальных носителях и(или) в разных базах данных.

11.4. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

12. Обработка персональных данных без использования средств автоматизации

12.1. Согласно п. 1 Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденного Постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687, обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

12.2. При обработке персональных данных без использования средств автоматизации должны выполняться следующие требования:

- персональные данные должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях персональных данных, в специальных разделах или на полях форм (бланков);
- при фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы;
- для каждой категории персональных данных должен использоваться отдельный материальный носитель;
- лица, осуществляющие обработку персональных данных без использования средств автоматизации, должны быть проинформированы о факте обработки ими персональных данных, обработка которых осуществляется без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки.

12.3. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных, должны соблюдаться следующие условия:

- типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, имя (наименование) и адрес оператора, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными

данными, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки персональных данных;

- типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации;

- типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;

- типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

12.4. При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных, в частности:

- при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных;

- при необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

12.5. Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, - путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными.

12.6. В случае ведения журнала (реестра, книги), содержащего персональные данные, необходимые для однократного пропуска субъекта персональных данных на территорию, на которой находится Учреждение, или в иных аналогичных целях должны соблюдаться следующие условия:

- необходимость ведения такого журнала (реестра, книги) должна быть предусмотрена актом, содержащим сведения о цели обработки персональных данных, способы фиксации и состав информации, запрашиваемой у субъектов персональных данных, перечень лиц (поименно или по должностям), имеющих доступ к материальным носителям и ответственных за ведение и сохранность журнала (реестра, книги), сроки обработки персональных данных, а также сведения о порядке пропуска субъекта персональных данных на территорию без

подтверждения подлинности персональных данных, сообщенных субъектом персональных данных;

- копирование содержащейся в таких журналах (реестрах, книгах) информации не допускается;

- персональные данные каждого субъекта персональных данных могут заноситься в такой журнал (книгу, реестр) не более одного раза в каждом случае пропуска субъекта персональных данных на территорию.

13. Доступ к персональным данным

13.1. Доступ к персональным данным имеют сотрудники Учреждения, которым персональные данные необходимы в связи с исполнением ими трудовых обязанностей.

13.2. Доступ к персональным данным предоставляется в объеме, необходимом для выполнения сотрудниками конкретных трудовых обязанностей.

13.3. В случае, если на основании заключенных договоров доступ к персональным данным должны иметь юридические или физические лица, то с ними подписывается соглашение о неразглашении конфиденциальной информации.

13.4. Процедура оформления доступа к персональным данным включает в себя:

- ознакомление сотрудника с настоящим Положением под роспись;

- прохождение обучения правилам обработки и обеспечению безопасности персональных данных;

- ознакомление сотрудника с локальными актами, регламентирующими обработку и защиту персональных данных, под роспись;

- подписание сотрудником обязательства о неразглашении конфиденциальной информации;

- включение пользователя в перечни на доступ к персональным данным.

13.5. Права доступа могут предоставляться на постоянной или разовой основе.

Основанием для оформления сотруднику прав доступа к персональным данным на постоянной основе является факт назначения сотрудника на должность, где для выполнения трудовых обязанностей необходим доступ к персональным данным.

Основанием для оформления сотруднику прав доступа к персональным данным на разовой основе является выполнение служебного задания, в рамках которого сотруднику потребуется доступ к персональным данным.

14. Передача персональных данных

14.1. Учреждение может передавать персональные данные субъектов государственным органам (Федеральной налоговой службе, Пенсионному Фонду, Федеральной службе судебных приставов, Министерству внутренних дел) в рамках осуществления последними своих полномочий и функций, а также банкам, страховым компаниям в строгом соответствии с требованиями законодательства Российской Федерации.

14.2. Передача персональных данных должна осуществляться в составе и объеме, минимально необходимых для достижения целей, в которых передаются персональные данные.

14.3. Обработка персональных данных третьем лицом возможна с согласия субъекта персональных данных, на основании заключенного с этим лицом договора.

14.4. Лицо, осуществляющее обработку персональных данных по поручению Учреждения, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные действующим законодательством РФ в области защиты персональных данных.

14.5. Должны быть определены действия (операции) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, а также цели обработки персональных данных.

14.6. В договоре должна быть указана обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечить безопасность персональных данных при их обработке.

14.7. Персональные данные, передаваемые третьему лицу, могут быть использованы лишь в целях, для которых они были переданы.

14.8. Третье лицо, осуществляющее обработку персональных данных, не обязано получить согласие субъекта персональных данных на обработку его персональных данных.

14.9. Учреждение несет ответственность перед субъектом персональных данных за действия третьего лица, осуществляющего обработку персональных данных по его поручению.

15. Прекращение обработки и уничтожение персональных данных

15.1. Обработка персональных данных прекращается или обеспечивается её прекращение, если обработка персональных данных осуществляется другим лицом, действующим по поручению Учреждения, а персональные данные уничтожаются в сроки, установленные Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», в случаях, если иное не установлено законом:

- по истечению установленного срока обработки;
- по достижению заявленных целей обработки или при утрате необходимости в их достижении;
- по требованию субъекта персональных данных, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки;
- при отзыве субъектом персональных данных согласия на обработку персональных данных.

15.2. Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

15.3. Учреждение может заключать договоры с третьими лицами на оказание услуг по уничтожению материальных носителей персональных данных. При этом Учреждение и третье лицо в соответствии с условиями договора

соблюдают все правила для обеспечения конфиденциальности уничтожаемых данных.

16. Отзыв согласия на обработку персональных данных

16.1. В случае отзыва субъектом персональных данных согласия на обработку его персональных данных Учреждение прекращает их обработку и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожает их 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.

16.2. В случае отзыва субъектом персональных данных согласия на обработку персональных данных Учреждение вправе продолжить обработку персональных данных без согласия субъекта персональных данных при наличии оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

17. Конфиденциальность персональных данных

17.1. В соответствии с «Перечнем сведений конфиденциального характера», утвержденным Указом Президента Российской Федерации от 06 марта 1997 г. № 188, персональные данные являются конфиденциальной информацией.

17.2. Для персональных данных, не являющихся обезличенными или общедоступными, обеспечивается конфиденциальность.

18. Взаимодействие с субъектами персональных данных

18.1. В соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» на Учреждение, как оператора персональных данных, возлагается обязанность своевременно реагировать на обращения и запросы субъектов персональных данных.

18.2. При взаимодействии с субъектами персональных данных обеспечивается соблюдение их прав в соответствии с законодательством Российской Федерации.

18.3. Взаимодействие с субъектом персональных данных при реализации права субъекта на доступ к его персональным данным, а также ограничение таких прав осуществляется с соблюдением требований ст. 14 Федерального Закона от 27 июля 2006 года № 152-ФЗ «О персональных данных».

18.4. Взаимодействие с субъектами персональных данных определяется «Правилами рассмотрения запросов субъектов персональных данных или их представителей», утвержденными руководителем Учреждения.

19. Обезличивание персональных данных

19.1. Учреждение может осуществлять обезличивание персональных данных.

19.2. Обезличивание персональных данных проводится в статистических или иных исследовательских целях, а также по достижению целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено законом.

19.3. Для обезличивания могут применяться методы, определенные Методическими рекомендациями по применению приказа Роскомнадзора от 5 сентября 2013 года № 996 «Об утверждении требований и методов по обезличиванию персональных данных»:

- метод введения идентификаторов;
- метод изменения состава или семантики;
- метод декомпозиции;
- метод перемешивания.

19.4. Методы и процедуры обезличивания персональных данных, а также правила работы с обезличенными данными определяются «Правилами работы с обезличенными данными в случае обезличивания персональных данных», утвержденными руководителем Учреждения.

20. Права и обязанности Учреждения

20.1. При работе с персональными данными лица, допущенные к обработке этих данных, в процессе выполнения служебных обязанностей должны обеспечивать:

- проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и передачи их лицам, не имеющим права доступа к такой информации;
- своевременное обнаружение фактов несанкционированного доступа к персональным данным;
- недопущение воздействия на технические средства информационной системы, в результате которого может быть нарушено их функционирование и целостность данных;
- возможность восстановления персональных данных, модифицированных или уничтоженных в результате несанкционированного доступа к ним;
- постоянный контроль за обеспечением безопасности персональных данных.

20.2. В Учреждении составляется план проведения и организуется обучение персонала по вопросам работы и обеспечения защиты персональных данных в информационных системах персональных данных, определяется ответственность сотрудников за нарушения при работе с персональными данными, порядок их взаимодействия с субъектами персональных данных.

21. Права и обязанности субъекта персональных данных

21.1. В соответствии с главой 3 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» субъект персональных данных имеет право на получение сведений, касающихся обработки его персональных данных Учреждением, а именно:

- подтверждение факта обработки персональных данных Учреждением;
- правовые основания и цели обработки персональных данных;

- цели и применяемые Учреждением способы обработки персональных данных;

- наименование и местонахождение Учреждения, сведения о лицах (за исключением работников Учреждения), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Учреждением или на основании федерального закона;

- обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;

- сроки обработки персональных данных, в том числе сроки их хранения;

- порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных»;

- информацию об осуществленной или о предполагаемой трансграничной передаче данных;

- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Учреждения, если обработка поручена или будет поручена такому лицу;

- иные сведения, предусмотренные Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» или другими федеральными законами.

21.2. Субъект персональных данных вправе требовать от Учреждения уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

21.3. Субъект персональных данных имеет право заявить возражение против принятия в его отношении решений, порождающих юридические последствия на основе исключительно автоматизированной обработки персональных данных.

21.4. Субъект персональных данных имеет право отозвать согласие на обработку его персональных данных. В случае отзыва субъектом персональных данных согласия на обработку персональных данных Учреждение вправе продолжить обработку персональных данных без согласия субъекта персональных данных при наличии оснований, указанных в Федеральном законе от 27 июля 2006 года № 152-ФЗ «О персональных данных».

21.5. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами.

21.6. Если субъект персональных данных считает, что Учреждение осуществляет обработку его персональных данных с нарушением требований Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие Учреждения в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

21.7. Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

21.8. Субъект персональных данных обязан предоставлять достоверные персональные данные и своевременно сообщать об изменениях в них.

21.9. Запрос субъекта персональных данных должен содержать сведения, установленные Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» и быть удостоверен одним из следующих способов:

- собственноручной подписью субъекта персональных данных или его законного представителя;
- электронной подписью (в случае направления электронного закона).

22. Меры, направленные на обеспечение безопасности персональных данных

22.1. Меры по обеспечению безопасности персональных направлены на защиту персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении персональных данных.

22.2. Обеспечение безопасности достигается применением необходимых и достаточных мер, а именно:

- определен перечень информационных систем персональных данных;
- определены угрозы безопасности персональных данных при их обработке в информационных системах персональных данных;
- применены правовые, организационные и технические меры по обеспечению безопасности персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных;
- производится оценка эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационных систем персональных данных;
- производится учет машинных носителей персональных данных;
- производится восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- обеспечивается сохранность носителей персональных данных;

устанавливаются правила доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечена регистрация и учет всех действий, совершаемых с персональными данными в информационной системе персональных данных;

- осуществляется контроль за принимаемыми мерами по обеспечению безопасности персональных данных;
- назначен ответственный за организацию обработки персональных данных;
- изданы документы, определяющие политику в отношении обработки персональных данных, локальные акты по вопросам обработки персональных данных, а также локальные акты, устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;
- осуществляется внутренний контроль соответствия обработки персональных данных Федеральному закону от 27 июля 2006 года № 152-ФЗ «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике

Учреждения в отношении обработки персональных данных, а также локальным актам;

- произведена оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения требований Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», определено соотношение вреда и принимаемых мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных»;

- работники Учреждения, непосредственно осуществляющие обработку персональных данных, ознакомлены с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику Учреждения в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, а также прошли обучение.

23. Ответственность за нарушение требований законодательства

23.1. Сотрудники Учреждения, обрабатывающие персональные данные, и лица, которым Учреждение поручает обработку персональных данных, несут гражданскую, уголовную, административную и иную, предусмотренную законодательством Российской Федерации, ответственность за нарушение режима защиты и обработки персональных данных.

23.2. За неисполнение или ненадлежащее исполнение сотрудниками Учреждения возложенных на них обязанностей по соблюдению установленного порядка обработки персональных данных Учреждение вправе применять предусмотренные Трудовым кодексом Российской Федерации дисциплинарные взыскания.

23.3. Сотрудники Учреждения, получающие доступ к обрабатываемым персональным данным, несут персональную ответственность за конфиденциальность полученной информации.

Приложение 1

Типовая форма согласия на обработку персональных данных

Я, _____

(фамилия, имя, отчество)

проживающий (ая) по адресу: _____

(адрес места жительства)

_____

паспорт _____

(номер, серия, кем и когда выдан)

_____

в соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» предоставляю управлению образования администрации города Белгорода, расположенному по адресу: г.Белгород, ул.Попова 25а, свое согласие на обработку персональных данных в целях:

_____

Перечень персональных данных, в отношении которых дается согласие, включает:

_____

_____

Действия с персональными данными включают: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение.
Обработка персональных данных производится в смешанном режиме.
Согласие действует бессрочно и может быть отозвано в соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

_____	_____	_____
(дата)	*(подпись)*	*(Ф.И.О.)*

Приложение 2

Типовая форма разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные

В соответствии с требованиями Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» обязанность предоставления субъектом персональных данных установлена _____

(реквизиты и наименование нормативных правовых актов)

В случае отказа субъекта предоставить свои персональные данные, управлению образования администрации города Белгорода не сможет на законных основаниях осуществлять такую обработку, что приведет к следующим юридическим последствиям _____

_____

(перечисляются юридические последствия для субъекта персональных данных, то есть случаи возникновения, изменения или прекращения личных либо имущественных прав граждан или случаи иным образом затрагивающие его права, свободы и законные интересы)

В соответствии с законодательством в области персональных данных субъект персональных данных имеет право:

- на получение сведений о управлении образования администрации города Белгорода, о месте его нахождения, о наличии у него своих персональных данных, а также на ознакомление с персональными данными;
- требовать уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав;
- на получение при обращении или при направлении запроса информации, касающейся обработки своих персональных данных;
- на обжалование действия или бездействия управлению образования администрации города Белгорода в уполномоченный орган по защите прав субъектов персональных данных.

_____	_____	_____
(дата)	*(подпись)*	*(Ф.И.О.)*

Приложение 3

Отзыв согласия на обработку персональных данных

Я, _____

(фамилия, имя, отчество)

проживающий (ая) по адресу: _____

(адрес места жительства)

_____

паспорт _____

(номер, серия, кем и когда выдан)

_____

Прошу вас прекратить обработку моих персональных данных в связи с:

_____

(указать причину)

_____

_____

_____

_____

начиная с «___» _____ 20__ г.

_____	_____	_____
(дата)	*(подпись)*	*(Ф.И.О.)*

Приложение 4

Типовое обязательство о неразглашении информации, содержащей персональные данные

Я, _____

(фамилия, имя, отчество)

Исполняющий (ая) должностные обязанности по замещаемой должности: _____

_____

(должность, наименование структурного подразделения)

предупрежден (а), что на период исполнения должностных обязанностей мне будет предоставлен допуск к информации, содержащей персональные данные.

Настоящим добровольно принимаю на себя обязательства:

- не передавать и не разглашать третьим лицам информацию, содержащую персональные данные, которая мне станет известна в связи с исполнением должностных обязанностей;
- в случае попытки третьих лиц получить от меня информацию, содержащую персональные данные, сообщить об этом непосредственному руководителю, а также лицу, ответственному за обеспечение безопасности персональных данных;
- не использовать информацию, содержащую персональные данные, с целью получения выгоды;
- выполнять требования нормативных правовых актов, регламентирующих вопросы защиты персональных данных;
- в случае расторжения договора (контракта) и (или) прекращения права на допуск к информации, содержащей персональные данные, не разглашать и не передавать третьим лицам известную мне информацию, содержащую персональные данные.

Я предупрежден (а), что нарушение данного обязательства является основанием для привлечения к административной, уголовной или иной ответственности в соответствии с законодательством Российской Федерации.

_____	_____	_____
(дата)	*(подпись)*	*(Ф.И.О.)*

УТВЕРЖДЕНЫ
приказом управления образования
администрации города Белгорода
от «30» марта 2017г. № 465

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 управлении образования администрации города Белгорода (далее – Учреждение) процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, а также определяют:

- цели обработки персональных данных;
- категории субъектов, персональные данные которых обрабатываются;
- 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.

УТВЕРЖДЕНЫ
приказом управления образования
администрации города Белгорода
от «30» марта 2017г. № 465

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 управлении образования администрации города Белгорода (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 следующие параметры:

- 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 субъектах на основе обращений субъектов, решений судов и других уполномоченных органов; – внесение изменений в существующие записи о	– перемешивание; – декомпозиция; – введение идентификаторов.

	субъектах на основе исследований, выполнения своих функций или требований законодательства РФ.	
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.

УТВЕРЖДЕН
приказом управления образования
администрации города Белгорода
от «30» марта 2017г. № 465

Регламент по учету, хранению и уничтожению машинных носителей персональных данных

1. Общие положения

1.1. Настоящий регламент по учету, хранению и уничтожению машинных носителей персональных данных (далее–Регламент) определяет единый порядок учета, хранения, выдачи, применения, передачи и транспортировки носителей информации в управлении образования города Белгорода (далее–Учреждение).

1.2. Регламент является обязательным для выполнения (в части касающейся) всеми работниками Учреждения.

2. Организация учета машинных носителей информации

2.1. Применение в Учреждении носителей информации подлежит контролю. Все используемые съемные носители подлежат регистрации ответственным за обеспечение безопасности персональных данных (далее–администратор по защите информации). Применение незарегистрированных носителей информации ограниченного доступа и незарегистрированных съёмных носителей информации запрещается.

2.2. Приобретенные носители информации перед использованием передаются администратору по защите информации для регистрации.

2.3. Все поступающие от сторонних организаций носители информации подвергаются проверке на наличие вирусов на специально выделенном компьютере. При обнаружении на носителе зараженного и не поддающегося лечению файла дальнейшее использование носителя не допускается.

2.4. Ответственность за организацию применения носителей информации в Учреждении возлагается на руководителя.

2.5. На администратора по защите информации возлагаются обязанности по регистрации, хранению и выдаче носителей, ведению учетной документации и уничтожение носителей в установленном порядке.

3. Порядок учета носителей информации

3.1. Основной учет носителей в Учреждении производится в «Журнале учета машинных носителей информации».

3.2. При регистрации носителей информации ограниченного доступа в графе 5 «Журнала учета машинных носителей информации» делается пометка «конфиденциально», а при регистрации носителей ключевой (парольной) информации – «ключ».

3.3. Все журналы учета носителей информации включаются в номенклатуру дел. Листы журналов нумеруются, прошиваются и опечатываются с нанесением

заверяющей надписи с указанием количества листов, использованной печати и подписью лица, выполнившего регистрацию.

3.4. Учетный номер наносится на носитель информации способом, обеспечивающим сохранность маркировки в процессе эксплуатации носителя и не приводящим носитель в негодность. Номер заверяется специальным штампом или подписью лица, ответственного за учет носителей.

3.5. Принятие мер по обеспечению сохранности (читаемости) учетного номера носителя информации возлагается на работника, осуществляющего его эксплуатацию или хранение.

4. Хранение носителей информации

4.1. Хранение носителей информации осуществляется в условиях, исключающих утрату их функциональности и хранимой информации из-за влияния внешних полей, излучений и иных неблагоприятных факторов, а также несанкционированный доступ к информации ограниченного доступа.

4.2. Носители информации ограниченного доступа хранятся в сейфах (металлических шкафах с надежными замками) в условиях необходимого температурно-влажностного режима в помещениях с ограниченным доступом персонала.

4.3. В сейфах (или в непосредственной близости от них) размещаются средства эвакуации носителей в случае пожара или иных стихийных бедствий. Средства эвакуации (ящики или прочные мешки) носителей информации ограниченного доступа оснащаются приспособлениями для опечатывания.

4.4. Эвакуация носителей информации ограниченного доступа производится в места, исключающие бесконтрольный доступ к ним или их хищение.

4.5. Порядок хранения носителей конфиденциальной информации, предназначенных к списанию (уничтожению), в том числе нечитаемых вследствие выхода из строя из-за неисправности (износа), аналогичен порядку хранения действующих носителей конфиденциальной информации.

5. Особенности применения носителей информации

5.1. Ремонт носителей информации ограниченного доступа вне Учреждения запрещается (в том числе ремонт или замена носителей, вышедших из строя в течение гарантийного срока).

5.2. Носители информации ограниченного доступа подлежат маркировке. Маркировка производится путем нанесения на корпус, или нерабочую поверхность пометки «конфиденциально».

5.3. К эксплуатации в составе вычислительного средства, предназначенного для обработки информации ограниченного доступа, допускаются только зарегистрированные носители информации ограниченного доступа.

5.4. Накопители на жестких магнитных дисках

5.4.1. Получение пользователями носителей информации ограниченного доступа на жестких магнитных дисках, входящих в комплект средств вычислительной техники (далее – СВТ), оформляется записью в «Журнале учета машинных носителей информации».

5.4.2. Факт выхода из строя накопителя информации ограниченного доступа на жестких дисках устанавливается комиссией в составе администратора ИСПДн, администратора по защите информации и пользователя СВТ, в состав которого входит накопитель.

5.4.3. Заключение комиссии о выходе из строя носителя информации ограниченного доступа на жестких магнитных дисках оформляется «Актом технической экспертизы состояния носителя информации ограниченного доступа», утверждаемым руководителем Учреждением или лицом его замещающим (приложение 1).

5.4.4. В акте в обязательном порядке указываются:

- время, место и основание составления акта;
- идентификационные данные накопителя и укомплектованного им средства вычислительной техники;
- характеристики накопителя;
- место установки средства вычислительной техники;
- характер записанной информации;
- проявления неисправности и метод определения неработоспособности носителя;
- вывод о выходе носителя из строя и причинах невозможности передачи его в ремонт сторонней организации;
- рекомендации по уничтожению информации ограниченного доступа;
- рекомендации по списанию носителя.

5.4.5. При необходимости изъятия накопителя из состава СВТ, находящегося на гарантийном обслуживании, составляется односторонний «Акт вскрытия гарантийного СВТ», с уведомлением гарантийной организации или представлением ей экземпляра (копии) акта.

5.4.6. Неисправный накопитель заменяется исправным носителем конфиденциальной информации, после чего соответствующие отметки делаются в «Журнале учета машинных носителей информации», а СВТ опечатывается.

5.4.7. «Акт технической экспертизы состояния носителя информации ограниченного доступа» является основанием для изъятия из эксплуатации или оформления списания носителя с баланса Учреждения (если носитель информации является основным средством) и уничтожения.

5.4.8. В случае необходимости передачи в ремонт средства вычислительной техники, вышедшего из строя не из-за неисправности входящего в его состав носителя информации ограниченного доступа, накопитель из устройства изымается и заменяется другим, не являющимся носителем информации ограниченного доступа.

5.4.9. Изъятое устройство передается (возвращается) по «Журналу учета машинных носителей информации» на хранение лицу, ответственному за учет и хранение носителей информации в Учреждении.

5.4.10. По возвращении СВТ из ремонта изъятый ранее носитель информации ограниченного доступа при необходимости устанавливается в присутствии ответственного за учет и хранение носителей обратно с оформлением соответствующей записи в «Журнале учета машинных носителей информации».

5.4.11. Возвращение арендованных СВТ, имеющих в своем составе носители информации ограниченного доступа, производится после замены носителей на аналогичные модели или гарантированного уничтожения

информации на них, если условиями аренды не предусмотрено возвращение СВТ без носителя информации.

5.5 Оптические носители.

5.5.1. Учетный номер оптического носителя информации наносится несмываемыми чернилами на его нерабочую поверхность или наклеиваемую на него специальную этикетку и заверяется подписью администратора по защите информации. Допускается наклеивание на носитель только специальной этикетки для оптических носителей, исключающей нарушение его балансировки и не препятствующих его движению в приводе.

5.5.2. На нерабочей поверхности носителя (этикетке) может также указываться дополнительная информация, используемая в процессе его применения.

5.5.3. Оптические носители хранятся в местах, защищенных от попадания прямых солнечных лучей, в конвертах или специальных коробках, обеспечивающих сохранность рабочей поверхности носителя от загрязнения и механических повреждений.

6. Выдача, передача и транспортировка носителей информации

6.1. Выдача носителей информации пользователям производится под роспись в «Журнале учета машинных носителей информации».

6.2. Допускается выдача по одной записи комплекта (нескольких носителей одного типа) оптических носителей (или гибких магнитных дисков), не предназначенных для записи информации ограниченного доступа.

6.3. Передача носителя информации ограниченного доступа в другое учреждение производится с оформлением сопроводительного письма и фиксируется в «Журнале учета машинных носителей информации».

6.4. В сопроводительном письме указывается количество передаваемых носителей, а также тип, учетный номер, серийный (заводской) номер и, при необходимости, другая информация.

6.5. При транспортировке носителей информации ограниченного доступа необходимо обеспечить условия, исключающие утрату или несанкционированный доступ к информации.

7. Контроль применения носителей информации

7.1. Контроль наличия носителей информации, правил и условий их хранения осуществляется посредством периодических проверок руководителем Учреждения, администратором по защите информации Учреждения и пользователями.

7.2. Порядок и периодичность текущего контроля носителей в Учреждении определяется руководителем Учреждения.

7.3. Ежегодно (в ноябре-декабре) проверка наличия и состояния носителей информации проводится комиссией, назначаемой распоряжением по Учреждению.

7.4. Проверке подлежат: соответствие количества учтенных носителей фактическому, наличие и состояние учетной документации, соответствие

серийных (заводских) и учетных номеров, условия хранения и использования носителей.

7.5. В «Журнале учета машинных носителей информации» после сверки имеющихся в графе 12 записей на наличие соответствующих документов в графе 13 проставляется подпись председателя комиссии и дата.

7.6. В процессе проверки также оценивается (при необходимости) техническое состояние предлагаемых к списанию носителей и вырабатываются соответствующие рекомендации.

7.7. Результаты проверки наличия носителей информации и порядка их применения оформляются актом. Акт проверки подлежит утверждению руководителем Учреждения.

7.8. По каждому случаю утраты носителя информации ограниченного доступа или несанкционированного доступа к нему распоряжением руководителя Учреждения назначается служебное расследование.

7.9. Целью работы комиссии является установление обстоятельств, условий и причин возникновения инцидента, виновных лиц и выработка предложений по устранению причин и способствующих инциденту условий, а также по минимизации возможного ущерба.

7.10. Расследование производится не позднее, чем в течение 14 дней с момента выявления факта утраты носителя или несанкционированного доступа к нему. Результаты расследования оформляются актом, подписываемым членами комиссии и утверждаемым руководителем Учреждения.

7.11. Носители информации ограниченного доступа многократной записи в случае выхода из строя, а носители однократной записи при миновании необходимости хранимой на них информации, подлежат списанию в соответствии с действующими правилами списания категории материальных средств, к которой они отнесены, и последующему уничтожению.

7.12. Основанием для списания с баланса Учреждения носителей информации ограниченного доступа на жестких дисках – «Акт технической экспертизы состояния носителя информации ограниченного доступа».

7.13. Уничтожение носителя, состоящего на балансе Учреждения как основного средства, производится после утверждения акта о его списании.

7.14. Уничтожение носителей информации производится в присутствии членов комиссии, назначаемой распоряжением руководителя Учреждения, способом, исключающим возможность восстановления хранившейся на носителе информации.

7.15. Факт уничтожения носителя оформляется актом. Акт об уничтожении носителя информации хранится у лица, ответственного за учет и хранение машинных носителей информации (приложение 2).

Приложение 1

Акт технической экспертизы состояния носителя информации ограниченного доступа

Комиссия в составе: председателя _____

и членов комиссии: _____

составила настоящий акт на предмет технического состояния следующего носителя информации:

Идентификационные данные (характеристики) накопителя и укомплектованного им средства вычислительной техники	Инвент. №	Место установки СВТ	Характер записанной информации
1	2	3	4

Комиссия установила, что носитель информации является *неработоспособным*

(указываются проявления неисправности и метод определения неработоспособности носителя)

Вывод:

1. Носитель информации *подлежит* / *не подлежит* передаче в ремонт

(указывается наименование сторонней организации или причина невозможности передачи носителя для ремонта)

2. Носитель информации *подлежит* / *не подлежит* уничтожению

(указывается способ уничтожения)

Рекомендации по списанию носителя информации _____

Председатель комиссии (подпись) _____
(расшифровка подписи)

Члены комиссии: (подпись) _____
(расшифровка подписи)

(подпись) _____
(расшифровка подписи)

Приложение 2

Акт уничтожения носителей информации

Основание: приказ

_____

_____

Комиссия в составе: председателя

_____

и членов комиссии:

_____

_____

произвела наружный осмотр и сверила с данными регистрационного учета следующие носители информации:

№ п/п	Тип носителя	Учетный номер носителя	Серийный (заводской) номер носителя

в количестве _____ штук, списанные в соответствии с актом от

(число прописью)

_____ по причине непригодности к дальнейшему использованию, и свидетельствует об их уничтожении способом _____

_____ в присутствии всех членов комиссии.

(способ уничтожения)

Председатель комиссии (подпись) _____
(расшифровка подписи)

Члены комиссии: (подпись) _____
(расшифровка подписи)

(подпись) _____
(расшифровка подписи)

УТВЕРЖДЕН
приказом управления образования
администрации города Белгорода
от «30» марта 2017г. № 465

Управление образования администрации города Белгорода

ЖУРНАЛ
поэкземплярного учета крипто средств, эксплуатационной и технической документации к ним

Начат «____» _____ 20___ г.
Окончен «____» _____ 20___ г.
На _____ листах

№ п/п	Наименование СКЗИ	Регистрационный номер СКЗИ	Номер экземпляра	Отметка о получении		Отметка о выдаче	
				От кого получены	Дата и номер сопроводительного письма	Ф.И.О. пользователя	Дата и расписка в получении
1	2	3	4	5	6	7	8

Отметка о подключении (установке) СКЗИ			Отметка об изъятии СКЗИ из аппаратных средств ИСПДн			Примечание
Ф.И.О. сотрудников органа криптографической защиты, пользователя СКЗИ, произведших подключение (установку)	Дата подключения (установки) и подписи лиц, произведших подключение (установку)	Номера аппаратных средств, в которые установлены или к которым подключены СКЗИ	Дата изъятия (уничтожения)	Ф.И.О. сотрудников органа криптографической защиты, пользователя СКЗИ, производивших изъятие (уничтожение)	Номер акта или расписка об уничтожении	
9	10	11	12	13	14	15

УТВЕРЖДЕН
приказом управления образования
администрации города Белгорода
от «30» марта 2017г. № 465

Управление образования администрации города Белгорода

ЖУРНАЛ
технический (аппаратный)

Начат «____» _____ 20___ г.
Окончен «____» _____ 20___ г.
На _____ листах

№ п\п	Дата	Тип и серийные номера используемых СКЗИ	Записи по обслуживанию СКЗИ	Используемые криптоключи			Отметка об уничтожении		Примечание
				Тип ключевого документа	Серийный, криптографический номер и номер экземпляра ключевого документа	Номер разового ключевого носителя или зоны СКЗИ, в которую введены криптоключи	Дата	Подпись пользователя СКЗИ	

УТВЕРЖДЕН
приказом управления образования
администрации города Белгорода
от «30» марта 2017г. № 465

Управление образования администрации города Белгорода

ЖУРНАЛ
учета выдачи идентификаторов и паролей

Начат «____» _____ 20___ г.
Окончен «____» _____ 20___ г.
На _____ листах

№ п/п	Номер парольной карточки	Идентификационный номер электронного ключа	Регистрация выдачи электронных ключей					Отметка в обратном приеме		
			Должность	Ф. И. О.	Дата получения	Роспись в получении	Ф. И. О. выдавшего	Дата приема	Роспись принявшего	Номер акта о списании
1	2	3	4	5	6	7	8	9	10	11

УТВЕРЖДЕН
приказом управления образования
администрации города Белгорода
от «30» марта 2017г. № 465

Управление образования администрации города Белгорода

ЖУРНАЛ
учета мероприятий по контролю защиты персональных данных

Начат «____» _____ 20___ г.
Окончен «____» _____ 20___ г.

На _____ листах

№ п\п	Название проведенного мероприятия	Дата проведенного мероприятия	Исполнитель мероприятия	Результат

УТВЕРЖДЕН
приказом управления образования
администрации города Белгорода
от «30» марта 2017г. № 465

Управление образования администрации города Белгорода

ЖУРНАЛ
учета машинных носителей информации

Начат «____» _____ 20___ г.
Окончен «____» _____ 20___ г.

На _____ листах

№ п/п	Учетный номер	Дата постановки на учет	Тип носителя	Метка категории носителя	Заводской или инв. №	Емкость носителя	Откуда поступил	Инв. № ПК, в который установлен НЖМД	Расписка пользователя о получении носителя	Расписка в обратном приеме	Отметка о снятии с учета, номер документа	Отметка о выполнении ежегодной проверки
1	2	3	4	5	6	7	8	9	10	11	12	13

УТВЕРЖДЕН
приказом управления образования
администрации города Белгорода
от «30» марта 2017г. № 465

Управление образования администрации города Белгорода

ЖУРНАЛ
учета обращений субъектов персональных данных и их законных представителей

Начат «____» _____ 20___ г.
Окончен «____» _____ 20___ г.

На _____ листах

№ п\п	Сведения о запрашивающем лице	Краткое содержание обращения	Отметка о предоставлении информации или отказе в ее предоставлении	Дата передачи или отказа в предоставлении информации	Подпись ответственного	Примечание
1	2	3	4	5	6	7

УТВЕРЖДЕН
приказом управления образования
администрации города Белгорода
от «30» марта 2017г. № 465

Управление образования администрации города Белгорода

ЖУРНАЛ
учета резервного копирования информационных ресурсов

Начат «____» _____ 20___ г.
Окончен «____» _____ 20___ г.
На _____ листах

№ п/п	Дата проведения резервного копирования/восстановления	Наименование резервной копии	Наименование информационной системы / базы данных	Номер носителя	Ф.И.О., подпись ответственного
1	2	3	4	5	6