Приложение 5

к приказу Отдела образования

администрации Сусанинского

муниципального района

Костромской области

от 18 января 2016 г. N 10

**Правила**

**работы с информационными системами Отдела образования администрации Сусанинского муниципального района Костромской области**

**1.** О**бщие положения**

1.1. Настоящие Правила определяют основные принципы безопасной работы автоматизированных информационных систем Отдела образования и обработки конфиденциальной информации сотрудниками Отдела образования (Приложение 1.)

1.2. Целью данного документа является формализация требований, предъявляемых к сотрудникам, по обеспечению режима безопасности конфиденциальной информации, циркулирующей в информационных системах, в том числе при обработке персональных данных.

1.3. Правила разработаны в соответствии с требованиями Федеральных законов РФ от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», от 27.07.2006 № 152-ФЗ «О персональных данных», постановлений Правительства РФ от 01.11.2012 № 1119 «Об утверждении Требований к защите персональных данных при их обработке в информационных системах персональных данных», от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и иных нормативных актов.

**2. Основные термины и определения**

**Автоматизированное рабочее место пользователя** (далее АРМ) - персональный компьютер с предустановленным системным, прикладным и антивирусным программным обеспечением (далее ПО), в том числе предназначенным для защиты информации ограниченного распространения.

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

**Информационные ресурсы** - программное обеспечение, документы и массивы документов расположенные, хранящиеся и обрабатываемые в информационных системах;

**Интернет** - всемирная система объединённых компьютерных сетей, построенная на использовании протокола IP и маршрутизации пакетов данных (телекоммуникационная сеть общего пользования);

**Пользователь** - сотрудник, допущенный к работе на автоматизированном рабочем месте и использующий для исполнения своих должностных обязанностей средства вычислительной техники;

**Персональный компьютер (далее ПК)** - компьютер, с предустановленным системным, прикладным и антивирусным ПО и предназначенный для эксплуатации одним пользователем, то есть для личного использования;

**Электронная почта** - технология и предоставляемые ею услуги по пересылке и получению электронных сообщений (называемых «письма» или «электронные письма») по распределённой (в том числе глобальной) компьютерной сети;

**Flash-карта** - разновидность твердотельной полупроводниковой энергонезависимой перезаписываемой памяти (один из видов электронных носителей информации).

**3. Общие правила работы на АРМ**

3.1. В целях исполнения своих служебных обязанностей, сотруднику Отдела образования (пользователю) на период работы предоставляется автоматизированное рабочее место с предустановленным лицензионным системным, прикладным и антивирусным программным обеспечением, имеющим сертификаты соответствия по безопасности.

Для организации доступа пользователя к информационным ресурсам АИС его АРМ подключается к локальной вычислительной сети (далее ЛВС). Установку и настройку АРМ, а также подключение ПК к ЛВС выполняет Администратор безопасности.

3.2. Допуск пользователя к АРМ осуществляется по устной заявке заведующего Отделом образования (либо его заместителя) на основании утвержденного Перечня должностей, имеющих право доступа к обработке конфиденциальной информации, в том числе персональных данных.

Доступ пользователя к работе на АРМ осуществляется на основании индивидуальной учетной записи (Логин + Пароль). Пользователь обязан использовать пароль в соответствии со следующими требованиями:

- длина пароля должна быть не менее 8 символов;

- пароль должен состоять из строчных и прописных букв, а также небуквенных символов (т.е. цифр, знаков пунктуации, специальных символов);

- пароль не должен быть легко угадываемым (не должен включать повторяющуюся последовательность каких-либо символов (например, "11111111", "абвгдеё" и т.п.), пароль не должен включать в себя легко подбираемые сочетания символов (имена, фамилии, даты рождения знакомых, наименования городов и улиц, клички домашних животных и т.п.), а также общепринятые сокращения (ЭВМ, ЛВС и т.п.).

3.3. Пользователь обеспечивает безопасное хранение пароля, исключающее возможность его утери или разглашения. Срок использования пароля составляет не более 90 дней. При смене пароля новое значение должно отличаться от предыдущего не менее чем в трёх-четырёх позициях.

3.4. При необходимости оставить рабочее место, даже на короткое время, пользователь должен заблокировать доступ к АРМ, нажав одновременно Ctrl + Alt + Delete, и принять иные меры по ограничению доступа к отображаемой на экране монитора информации

3.5. При использовании телекоммуникационных возможностей сети общего пользования Интернет пользователи обязаны выполнять следующие требования:

- использовать ресурсы Интернет только для выполнения своих служебных обязанностей;

- не посещать ресурсы Интернет, содержащие материалы противозаконного, экстремистского или неэтичного характера, а также использовать доступ к социальным сетям Интернет и развлекательным сайтам;

- не размещать в сети Интернет информацию служебного характера, о её сотрудниках и решаемых задачах, если это не связано с выполнением служебных обязанностей; - не использовать Интернет для несанкционированной передачи (выгрузки) или получения (загрузки) видео-, аудио- и информационных материалов, защищенных авторским правом;

3.6. При работе с электронной почтой пользователи должны соблюдать следующие требования:

- запрещается использовать возможности электронной почты для отправки сообщений противозаконного (террористического, экстремистского или враждебного характера), а также содержащего в себе информацию неэтичного содержания;

- при получении электронных сообщений из незнакомого источника и/или сомнительного содержания не следует открывать файлы, вложенные в сообщение, так как они с большой долей вероятности могут содержать вирусы. Такие сообщения необходимо удалять;

-не отвечать на подозрительные письма и, тем более, сообщать любые данные о себе и сотрудниках.

3.7. По окончании рабочего времени при отсутствии служебной необходимости пользователь обесточивает АРМ и другую оргтехнику во избежание выхода её из строя и в целях обеспечения противопожарной безопасности.

3.8. В случае подозрения на компрометацию пароля доступа необходимо немедленно изменить пароль и проинформировать об этом своего непосредственного руководителя.

В процессе эксплуатации АРМ пользователям ЗАПРЕЩАЕТСЯ:

3.9. Открывать корпус системного блока и вносить изменения в конфигурацию ПК; 3.10. Без получения санкции руководителя и администратора безопасности изменять настройки программного обеспечения и параметры доступа к информационным ресурсам; 3.11. Отключать и изменять параметры настройки в установленное антивирусное программное обеспечение и иные средства защиты информации;

3.12. Подключать к АРМ неучтенные внешние запоминающие устройства (активное сетевое оборудование, незарегистрированные Flash-карты. НЖМД, смартфоны, фотоаппараты и т.д.), если это не связано с исполнением должностных обязанностей сотрудника;

3.13. Умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты для организации несанкционированного доступа к обрабатываемым информационным ресурсам. При обнаружении такого рода ошибок необходимо информировать своего непосредственного руководителя и администратора безопасности;

3.14. Осуществлять действия направленные на преодоление систем безопасности, получение несанкционированного доступа к ресурсам информационной сети и перехват информации, циркулирующей в ИС;

3.15. Оставлять оборудование АРМ, переносные компьютеры и средства хранения информации без личного присмотра, в случаях, если это может привести к их краже;

При наличии риска хищения ПК и (или) средств хранения информации, необходимо принять меры по их минимизации (например, убирать переносной компьютер на обеденный перерыв и после завершения рабочего дня в закрывающийся на ключ шкаф, не оставлять незакрытым помещение, в котором находится оборудование информационной системы, использовать замки для переносных компьютеров);

3.16. Осуществлять обработку конфиденциальной информации на ПК, не оснащенном принятыми в Отделе образования средствами защиты информации, а также в присутствии лиц, не имеющих права доступа к данной информации, если при этом указанные лица могут ознакомиться с обрабатываемой информацией;

3.17. Записывать и хранить конфиденциальную информацию на неучтённых носителях информации (Flash-карта, CD-диск, носимый HDD и т.п), а также оставлять без личного присмотра на рабочем месте или где бы то ни было носители информации и распечатки, содержащие подобную информацию;

3.18. Допускать к работе на ПК лиц, не имеющих прав доступа к информационным ресурсам.

**4. Порядок работы с информационной системой**

4.1. При работе с программными и техническими средствами, входящими в состав АРМ и информационной системы, пользователь обязан выполнять установленные правила их эксплуатации. За неисполнение установленных правил он несёт персональную ответственность.

4.2. Отдел образования оставляет за собой право протоколировать и контролировать действия сотрудников при обработке конфиденциальной информации обрабатываемой в информационной системе.

4.3. Пользователи не имеют права предпринимать попыток получения доступа к закрытым информационным ресурсам, не получив официального разрешения на доступ к ним.

4.4. Пользователи не должны разглашать сведения о содержании информации, ставшей известной им в ходе выполнения должностных обязанностей, а также о процедурах и технической реализации защиты информации, принятых в департаменте.

4.5. В целях повышения эффективности служебной деятельности для обмена открытыми информационными ресурсами (обновления программных продуктов, инструкции, правила и т.п.) между пользователями могут использоваться съёмные материальные носители информации (Flash-карты, переносные жесткие диски, иные устройства записи и чтения), зарегистрированные и учтённые по Журналу учёта съемных носителей информации.

4.6. Выдача сотрудникам и учёт материальных носителей информации осуществляется сотрудником, ответственным за организацию работы по защите персональных данных, по Журналу учёта съёмных носителей информации.

**5. Ответственность за нарушение порядка**

5.1. Ответственность за неисполнение требований настоящей Инструкции возлагается на всех сотрудников, являющихся пользователями информационной системы департамента.

5.2. Сотрудник, нарушивший требования данной Инструкции, может быть подвергнут дисциплинарному наказанию в соответствии с законодательством Российской Федерации (уголовный, налоговый, гражданский, трудовой Кодексы и иное законодательство).

Приложения: 1. Перечень информационных систем персональных данных,

используемых в Отделе образования администрации Сусанинского муниципального района Костромской области

2. Инструкция администратора безопасности АИС.

3. Инструкция по проведению антивирусного контроля на автоматизированном рабочем месте (АРМ).

4. Инструкция по резервному копированию информации и восстановлению работоспособности ИС

Приложение 1

к правилам работы

с информационными системами

Отдела образования

**Перечень информационных систем персональных данных,**

**используемых в Отделе образования**

**администрации Сусанинского муниципального района Костромской области**

1. Программа "1С:Предприятие - КАМИН: расчет заработной платы для бюджетных учреждений".

Приложение 2

к правилам работы

с информационными системами

Отдела образования

**Инструкция администратора безопасности АИС**

**1. Общие положения**

1.1. Настоящая Инструкция разработана на основании действующих нормативных документов и определяет общие функции, права и обязанности администратора безопасности по вопросам обеспечения информационной безопасности при обработке персональных данных и иной конфиденциальной информации с использованием средств автоматизации, входящих в состав автоматизированных информационных систем (далее – АИС)

1.2. Администратор безопасности (далее - Администратор) в своей работе руководствуется настоящей Инструкцией, внутренними нормативными документами и требованиями законодательства в сфере защиты информации ограниченного доступа.

1.3. Администратор безопасности назначается из числа сотрудников Оператора персональных данных, имеющих соответствующую квалификацию и опыт работы с оборудованием и программным обеспечением информационных систем. Администратор безопасности является ответственным должностным лицом организации и обеспечивает правильное использование и функционирование установленного системного и прикладного программного обеспечения, средств технической защиты информации (далее по тексту - СЗИ) от несанкционированного доступа (далее по тексту - НСД), а также поддержание достигнутого уровня защиты АИС и её ресурсов на этапах эксплуатации и модернизации.

1.4. Администратор безопасности имеет рабочее место, размещаемое в выделенном помещении, оборудованном средствами физической защиты в которое исключается несанкционированный доступ посторонних лиц. Рабочее место Администратора подключается к ЛВС, оборудуется средствами удаленного контроля используемых информационных ресурсов и местами хранения конфиденциальных документов.

1.5. Требования Администратора безопасности к сотрудникам, связанные с выполнением ими своих должностных обязанностей, обязательны для исполнения всеми пользователями АИС.

1.6. Администратор безопасности осуществляет плановый и периодический контроль действий пользователей при работе в АИС, определяет текущее состояние и поддерживает установленный уровень защиты конфиденциальной информации.

**2. Администратор безопасности в своей деятельности имеет право:**

2.1. Знать и выполнять требования действующих в организации нормативных и руководящих документов по защите информации, а также внутренних Инструкций регламентирующих работу с конфиденциальной информацией.

2.2. Оказывать содействие в установке и настройке автоматизированных рабочих мест сотрудников Отдела образования, а также осуществлять сопровождение работы установленного системного и прикладного программного обеспечения и средств защиты информации.

2.3. Организовывать доступ пользователей к ресурсам автоматизированной информационной системы в соответствии с Перечнем должностей, имеющих право доступа к обработке конфиденциальной информации, на основании письменных заявок, утверждаемых руководителем организации.

2.4. Уточнять в установленном порядке обязанности пользователей ИС при обработке на автоматизированном рабочем месте (АРМ) конфиденциальных сведений, в том числе персональных данных, являющихся объектами защиты.

2.5. Осуществлять резервное копирование критичных для работы Отдела образования информационных ресурсов, обеспечивая их защиту и целостность.

2.6. Принимать участие в реализации плановых мероприятий по защите конфиденциальной информации, в том числе персональных данных, циркулирующих в АИС.

2.7. Оказывать помощь пользователям ИСПДн в части консультирования по вопросам введенного режима защиты персональных данных.

2.8. Анализировать состояние принятых в организации мер защиты конфиденциальной информации, в том числе выявлять попытки несанкционированного доступа к ресурсам ИС и совершенствовать методы защиты от угроз информационной безопасности.

2.9. Вести журнал учёта событий, регистрируемых средствами защиты, с целью выявления возможных нарушений или попыток несанкционированного доступа.

2.10. Своевременно вносить коррективы в список пользователей информационных ресурсов и матрицу доступов к персональным данным при приеме на работу и увольнении сотрудников. Удалять учётные записи пользователей ИС на доступ к информационным ресурсам в течение суток после подписания Обходного листа либо получения информации от руководителей подразделений об увольнении сотрудника.

2.11. В соответствии с планом внутренних проверок состояния обработки и защиты конфиденциальной информации в том числе персональных данных, на регулярной основе осуществлять контроль:

- за соблюдением сотрудниками требований действующих нормативных и руководящих документов, регламентирующих обработку конфиденциальной информации; - за осуществлением неизменности и целостности программной среды АИС (системное и прикладное ПО), средств антивирусной защиты и межсетевого экранирования, их параметров и режимов;

- за наличием и возможным использованием на автоматизированных рабочих местах вредоносных программ и иного нелицензионного ПО, не связанного с выполнением функциональных задач;

- за соблюдением пользователями принятого в организации режима парольной политики и порядка использования учётных записей на доступ к информационным ресурсам;

- за состоянием допуска пользователей к работе с ресурсами АИС и изменением прав доступа к защищаемой конфиденциальной информации, в том числе персональным данным;

- за выполнением правил учёта, использования и хранения электронных носителей конфиденциальной информации;

- за соблюдением сроков смены паролей доступа к ресурсам АИС и выполнением рекомендаций по выбору наиболее безопасных Паролей;

- за поддержанием установленного порядка обновления антивирусных баз и антивирусной защиты информационных ресурсов;

- за наличием и целостностью пломб (печатей, специальных защитных знаков) на корпусах системных блоков АРМ, обрабатывающих информацию ограниченного доступа; - за сроками действия сертификатов и лицензий эксплуатируемого оборудования и ПО;

2.12. В случаях отказа работоспособности технических средств и программного обеспечения ИСПДн, в том числе средств защиты, принимать меры по своевременному восстановлению и выявлению причин, приведших к отказу работоспособности, а также недопущения доступа посторонних лиц к конфиденциальной информации.

2.13. Периодически (не реже одного раза в полугодие) представлять руководству организации отчёт о состоянии защиты конфиденциальной информации, о нештатных ситуациях на объектах АИС, о работе сотрудников в сетях общего пользования, в том числе в Интернет, и допущенных пользователями нарушениях требований по защите информации, предусмотренных руководящими документами.

**3. Администратор безопасности обязан:**

3.1. Принимать необходимые меры по обеспечению безаварийного функционирования и работоспособности автоматизированных средств обработки информации, системного и прикладного ПО, СЗИ от НСД в пределах, возложенных на него функций;

3.2. Проводить инструктаж пользователей правилам работы на АРМ, с установленными СКЗИ и СЗИ от НСД;

3.3. Докладывать заведующему Отделом образования или лицу, исполняющему его обязанности, о фактах и попытках несанкционированного доступа к конфиденциальной информации, о неправомерных действиях пользователей или иных лиц, приводящих к нарушению требований безопасности информации.

3.5. Вносить изменения в документацию ИС в соответствии с требованиями нормативных документов в части, касающейся СЗИ от НСД;

3.6. Проводить работу по выявлению возможных каналов утечки конфиденциальной информации, вести их учёт и принимать меры к их устранению;

3.7. Регистрировать факты нарушений требований режима безопасности и организовывать проведение расследований по возникшим инцидентам информационной безопасности.

3.8. Блокировать учётные записи пользователей на АРМ в случае окончания срока действия сертификата соответствия ФСТЭК России, ФСБ России на любое СЗИ, из используемых в ИСПДн, до момента его продления. В случае непродления сертификата соответствия на СЗИ администратор обязан поставить в известность орган по аттестации, проводивший аттестацию ИСПДн, для принятия дальнейшего совместного решения.

3.9. Контролировать действия пользователей при уничтожении и затирании информации записанной на электронных носителях (накопителях) информации.

**4. Администратор безопасности имеет право:**

4.1. Запрашивать и получать необходимую информацию от структурных подразделений Отдела образования для планирования и организации работ по защите конфиденциальной информации.

4.2. Требовать от сотрудников Отдела образования - пользователей ИСПДн соблюдения установленных технологий обработки информации и выполнения требований руководящих документов.

4.3. Инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения информационной безопасности, доступа к информационным ресурсам, утраты, порчи защищаемой информации и технических компонентов автоматизированной системы.

4.4. Требовать от руководителей структурных подразделений департамента прекращения работы сотрудников в автоматизированной информационной системе при несоблюдении ими установленной технологии обработки информации или невыполнения требований по безопасности.

4.5. Вносить на рассмотрение руководства предложения по совершенствованию технических мер защиты.

**5. Администратор безопасности несёт ответственность:**

5.1. За разглашение конфиденциальных сведений организации (в том числе - персональных данных работников и должностных лиц контрагентов, используемых способов и методов защиты информационных ресурсов), ставших ему известными по роду своей деятельности.

5.2. За умышленное причинение материального ущерба, повлекшее отказ в работе оборудования корпоративной информационной системы, - в пределах, определенных действующим трудовым, уголовным и гражданским законодательством РФ.

Приложение 3

к правилам работы

с информационными системами

Отдела образования

**Инструкция**

**по проведению антивирусного контроля на автоматизированном рабочем месте (АРМ)**

1. Настоящая Инструкция предназначена для администратора безопасности и пользователей, обрабатывающих персональные данные с использованием средств автоматизации.

2. В целях обеспечения защиты автоматизированной информационной системы от программных закладок и программно-математического воздействия на обрабатываемые конфиденциальные данные на автоматизированных рабочих местах (АРМ) производится антивирусный контроль.

3. Ответственность за поддержание установленного в настоящей Инструкции порядка проведения антивирусного контроля возлагается на администратора безопасности.

4. К установке и использованию в автоматизированной информационной системе и на АРМ разрешаются только лицензионные антивирусные средства, имеющие сертификат ФСТЭК.

5. На АРМ пользователя запрещается установка прикладного программного обеспечения, не связанного с выполнением функций, предусмотренных технологическим процессом обработки информации на АРМ.

6. Пользователи АРМ при работе с информацией (ПО, БД, файлы) записанной на электронных носителях информации (Flash-карты, CD-диски, дискеты и т.п.) обязаны перед началом работы осуществить их проверку на предмет отсутствия компьютерных вирусов.

7. Ярлык для запуска антивирусной программы должен быть вынесен на "Рабочий стол" операционной системы.

8. Обновление вирусных баз осуществляется ежедневно путём скачивания и установки антивирусных баз с сервера производителя антивирусного ПО.

Посредством настроек антивирусного средства и организации доступа к серверам разработчика антивирусного средства обновление можно выполнять в автоматическом режиме без участия пользователя АРМ. При невозможности настроить доступ АРМ к серверам обновлений разработчика антивирусного средства Администратор информационной безопасности один раз в неделю производит установку пакетов.

9. При обнаружении компьютерного вируса в процессе эксплуатации АРМ либо сканирования съёмных электронных носителей информации пользователь обязан немедленно поставить об этом в известность администратора безопасности и прекратить какие-либо действия, связанные с обработкой конфиденциальной информации на АРМ.

10. По факту заражения АРМ компьютерным вирусом администратор безопасности производит «лечение» зараженных файлов путём выбора соответствующего пункта меню антивирусной программы, после чего вновь проводит антивирусный контроль файловой системы и обрабатываемых данных на АРМ. По результатам заражения АИС администратор безопасности проводит служебное расследование.

11. При обнаружении не поддающегося лечению вируса, администратор безопасности обязан удалить инфицированный файл в соответствующую папку антивирусного пакета, и проверить работоспособность АРМ. В случае отказа работоспособности АРМ - произвести восстановление и настройки соответствующего операционного и прикладного программного обеспечения.

12. О всех фактах заражения АИС и АРМ вредоносным программным обеспечением администратор безопасности обязан проинформировать ответственного за организацию обработки персональных данных либо заведующего Отделом образования.

Приложение 4.

к правилам работы

с информационными системами

Отдела образования

**Инструкция**

**по резервному копированию информации и восстановлению работоспособности ИС**

**1. Общие положения.**

1.1. В целях предупреждения возможности неблагоприятных последствий и обеспечения защиты важной или критичной для обеспечения работоспособности автоматизированных информационных систем информации от её случайного либо умышленного уничтожения, модификации или хищения, а также обеспечения её сохранности необходимо создавать её резервные копии.

1.2. Настоящая Инструкция разработана в соответствии с требованиями Федеральных законов от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации» и от 27.07.2006 № 152-ФЗ «О персональных данных», постановлений Правительства РФ от 15.09.2008 № 687 «Об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» и от 01.11.2012 № 1119 «Об утверждении Требований к защите персональных данных при их обработке в информационных системах персональных данных» и иных нормативных документов и определяет общие правила резервирования обрабатываемых данных, в том числе при обработке информации ограниченного распространения (обработка персональных данных и иной конфиденциальной информации).

1.3. При осуществлении резервирования (резервного копирования) данных пользователи в своей работе руководствуется настоящей Инструкцией, иными внутренними нормативными документами и требованиями законодательства в сфере защиты информации ограниченного доступа.

1.4. Резервирование данных проводится для обеспечения восстановления работоспособности автоматизированных информационных систем (АИС), вызванной сбоями в работе либо отказами аппаратного и программного обеспечения, чрезвычайными обстоятельствами, ошибками пользователей и (или) иными внешними воздействиями, ведущими к полной или частичной утрате информации.

1.5. Требования настоящей Инструкции, связанные с резервным копированием критичной информации обязательны для исполнения всеми сотрудниками (пользователями), обрабатывающими такую информацию.

1.6. Администратор безопасности Отдела образования осуществляет плановый и периодический контроль действий пользователей по обеспечению резервного копирования критически важных для обеспечения работоспособности АИС данных (информация о серийных номерах лицензионного ПО, настройках и т.п.).

**2. Термины и определения**

**Автоматизированная информационная система (АИС)** - взаимосвязанная совокупность данных, оборудования, программных средств, персонала, реализующая информационную технологию выполнения установленных функций, предназначенных для сбора, обработки, распределения, хранения, выдачи (предоставления) информации (по ГОСТ 34.003).

**Критичная информация** - любая важная информация, а также системное и прикладное программное обеспечение, утрата которых может привести к перебоям либо отказу в работе автоматизированной информационной системы и затруднению (либо невозможности) исполнения служебных обязанностей.

**Резервное копирование** - сохранение текущего состояния информации (системы) без обязательного сохранения предыдущего.

**Съемный носитель информации** - носитель информации, предназначенный для автономного хранения информации вне зависимости от места записи и использования (НЖМД, CD-DVD-диск, Flash-накопитель и т.п).

**Гарантированное хранение** - хранение, обеспечивающее целостность информации, определяемую требованиями федерального законодательства и внутренними организационно-распорядительными документами Отдела образования.

**3. Информация, подлежащая резервированию**

В целях скорейшего восстановления работоспособности автоматизированной ИС и исключения неблагоприятных последствий вызванных отказами в её работе либо утратой критичной информации в Отделе образования определен перечень информационных ресурсов, системного и прикладного ПО, подлежащих резервному копированию (Приложение 1), в который включен:

3.1. Персональные данные работников организации, обрабатываемые с использованием средств автоматизации и прикладного программного обеспечения в бухгалтерии.

3.2. Инсталляции системного и прикладного ПО, используемого для защиты и обработки критичной информации, персональных данных и иной конфиденциальной информации.

**4. Порядок резервирования данных**

Организация обеспечения резервного копирования обрабатываемой критичной информации, в том числе персональных данных, возложена на руководителей структурных подразделений Отдела образования, в которых она обрабатывается (одного из его сотрудников).

4.1. Обязательному резервному копированию и гарантированному хранению подлежит информация, указанная в Приложении 1.

4.2. В качестве носителей, на которые осуществляется резервное копирование информации, в зависимости от сохраняемых информационных ресурсов, используются:

- папки на сетевом диске Отдела образования;

- накопители на жестких магнитных носителях АРМ пользователей, физически разнесенные с накопителями, где происходит обработка критичной информации; - перезаписываемые или не перезаписываемые диски (CD, DVD, Blu-Ray).

4.3. К носителям, на которые производится резервное копирование предъявляются следующие требования:

4.4.1. Наличие достаточного объема свободного дискового пространства либо свободной памяти для обеспечения надежного хранения резервных копий;

4.4.2. Носитель должен периодически проходить полную проверку целостности (не реже одного раза в 6 месяцев);

4.4.3. Носитель должен быть учтён по Журналу учёта электронных носителей с указанием наименования, информационной емкости, ответственного за его эксплуатацию сотрудника;

4.4.4. К носителю должен быть ограничен физический доступ посторонних лиц, в том числе по сети. Его хранение осуществляется в местах с ограниченным доступом (запираемый шкаф, сейф и т.п.);

4.4.5. Ход выполнения установленных требований соблюдения установленных правил хранения и доступа, целостности ячеек памяти и работоспособности осуществляется на регулярной основе в соответствии с планом проведения внутренних проверок.

4.5. Период сохранения резервных копий определяется комиссионно, исходя из целесообразности обеспечения гарантированного сохранения тех или иных информационных ресурсов (частота внесения изменений в данные, критичность их утраты и т.п.) и производится по окончании рабочего времени ежеквартально, ежегодно с сохранением информации за указанный период + 1 день.

**5. Учёт материальных носителей резервных копий**

5.1. В целях обеспечения сохранности резервируемой в Отделе образования ведётся журнальный учёт электронных носителей, на которых сохраняются резервные копии критичной информации. Журнал учёта электронных носителей информации (Приложение 2) ведётся ответственным за организацию работы с персональными данными.

5.2. Сотрудник структурного подразделения Отдела образования, отвечающий за резервное копирование критичной информации, обязан зарегистрировать электронный носитель по Журналу учёта и в дальнейшем хранить его в недоступном для посторонних лиц месте (запираемом шкафу, сейфе или иных защищенных местах хранения).

5.3. Уничтожение электронных носителей с резервными копиями (при необходимости) производится членами экспертной комиссии Отдела образования на основании принятого ими решения в соответствии с установленным порядком ( «Положение об экспертной комиссии»)

**6. Порядок восстановления работоспособности ИС**

6.1. В случае потери (уничтожения, модификации) критичной информации пользователь информационных ресурсов ИСПДн либо ответственный работник обязан сообщить руководителю структурного подразделения о факте происшедшего сбоя в работе информационной системы, в результате которого произошла утрата данных. При этом сотрудник сообщает о возможных признаках сопутствующих отказу в работе АИС и принимает незамедлительные меры по восстановлению утраченной информации в кратчайший срок.

6.2. При потере критичной информации хранящейся на сетевом диске локальной информационной системы восстановление производится при участии администратора безопасности Отдела образования.

6.3. По итогам происшедшего инцидента с утратой критичной информации в целях предотвращения подобных фактов в дальнейшем администратором безопасности проводится разбирательство с выявлением причин инцидента и лиц, допустивших нарушение.

**7. Ответственность за нарушение установленного порядка резервирования данных**

7.1. Персональная ответственность за обеспечение безопасного хранения критичной информации пользователя в соответствии с установленным порядком возлагается на ответственных работников, обрабатывающих эту информацию.

7.2. Ответственность за обеспечение резервного копирования критичной информации, обрабатываемой и сохраняемой в ИСПДн, возлагается на руководителя и ответственных работников подразделений.

7.3. Хранение резервных копий и инсталляций эксплуатируемого ПО, серийных номеров и регистрационных кодов возлагается на администратора безопасности.

7.4. Нарушение требований настоящей Инструкции влечёт за собой дисциплинарную ответственность в соответствии с трудовым законодательством РФ.

7.5. К лицам, нарушившим установленный порядок резервирования критичной информации, обеспечения сохранности и уничтожения электронных носителей информации ограниченного доступа, вследствие которых произошло нанесение материального ущерба организации, могут быть приняты меры по возмещению убытков и компенсации морального вреда1.

Приложение: 1. Перечень критичных информационных ресурсов;

2. Форма журнала учёта электронных носителей информации

1 Требование о возмещении убытков не может быть удовлетворено в случае предъявления его лицом, не принимавшим мер по соблюдению установленного порядка резервирования или нарушившим установленные законодательством Российской Федерации требования о защите информации, если принятие этих мер и соблюдение таких требований являлись обязанностями данного лица.

Приложение 1.

к инструкции по резервному

копированию информации и

восстановлению работоспособности ИС

ПЕРЕЧЕНЬ

критичных информационных ресурсов, подлежащих резервному копированию

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № п/п | Наименование информационного ресурса | Подразделение (сотрудник) ответственное за резервирование | Период резервирования | Носитель |
| 1. | Программа "1С:Предприятие - КАМИН: расчет заработной платы для бюджетных учреждений". | Григоренко О.Н. | ежеквартально | Жесткий диск гл. бухгалтера |
| 2. | Системное ПО | Администратор безопасности | При установке | DVD-диск |
| 3. | Прикладное ПО | Администратор безопасности | При установке | DVD-диск |

Приложение 2.

к инструкции по резервному

копированию информации и

восстановлению работоспособности ИС

**Типовая форма**

**журнала учета съемных носителей персональных данных**

Начат "\_\_\_" \_\_\_\_\_ 20\_\_ года на \_\_\_\_\_\_ листах

Окончен "\_\_\_" \_\_\_\_\_ 20\_\_ года

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Должность и Ф.И.О., ответственного за хранение Подпись

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| №  п/п | Регистрационный номер/дата | Тип/ёмкость машинного носителя персональных данных | Номер экземпляра/  количество экземпляров | Место установки (использования)/дата установки | Ответственное должностное лицо (ФИО) | Расписка в получении (ФИО, подпись, дата) | Расписка в обратном приеме (ФИО, подпись, дата) | Место хранения машинного носителя персональных данных | Сведения об уничтожении машинных носителей персональных данных, стирании информации (подпись, дата) |
| 1 |  |  |  |  |  |  |  |  |  |
| 2 |  |  |  |  |  |  |  |  |  |
| 3 |  |  |  |  |  |  |  |  |  |