



МУНИЦИПАЛЬНОЕ ОБРАЗОВАНИЕ ГОРОД НОЯБРЬСК
МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ДОШКОЛЬНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ «РОМАШКА»
МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ ГОРОД НОЯБРЬСК

(МБДОУ «РОМАШКА»)

П Р И К А З

01.09.2017г.

№ 92/1-од

**О назначении ответственного за обработку и обеспечение безопасности
персональных данных**

В целях исполнения Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», Постановления Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»,

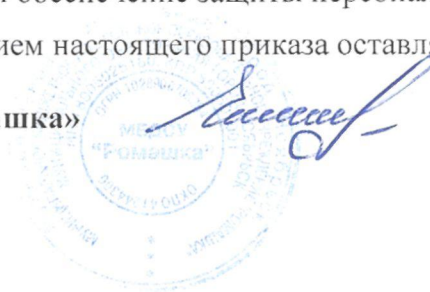
п р и к а з ы в а ю:

1. Назначить ответственным за обработку и обеспечение защиты персональных данных в информационной системе (ИС) МБДОУ «Ромашка» Лучиц Асию Адигамовну (специалист по кадрам).
2. Осуществлять доступ лица, ответственного за обработку персональных данных, к обрабатываемым персональным данным.
3. Утвердить и внедрить инструкцию ответственного за организацию обработки и обеспечения безопасности персональных данных (приложение № 1).
4. Утвердить и внедрить инструкцию пользователей, осуществляющих обработку данных в ИС (приложение № 2).
5. Определить периодичность мероприятий по обеспечению безопасности персональных данных при их обработке в ИС.
6. Осуществлять регистрацию обращений субъектов персональных данных в Журнале учета обращений субъектов персональных данных о выполнении их законных прав.
7. Контроль за соблюдением требований по защите информации возложить на ответственного за обработку и обеспечение защиты персональных данных.
8. Контроль за выполнением настоящего приказа оставляю за собой.

Заведующий МБДОУ «Ромашка»

И.В.Егорова

в дело 03-05
01.09.2017г.



**Инструкция ответственного за организацию обработки и обеспечение
безопасности персональных данных в
Муниципальном бюджетном дошкольном образовательном учреждении «Ромашка»
муниципального образования город Ноябрьск**

1. Общие положения

1.1. Данная Инструкция определяет основные обязанности, права ответственного лица за организацию обработки и обеспечение безопасности персональных данных (ответственного за защиту информации) (далее – Ответственный) Муниципального бюджетного дошкольного образовательного учреждения «Ромашка» муниципального образования город Ноябрьск (далее – Организация).

1.2. Ответственный является штатным работником Организации и назначается приказом руководителя Организации.

1.3. Ответственный отвечает за организацию и состояние процесса обработки информации ограниченного доступа в информационных системе (далее – информационная система), в том числе персональных данных.

1.4. Решение вопросов организации обработки и обеспечения защиты информации, обрабатываемой в информационной системе, входит в прямые трудовые обязанности Ответственного.

1.5. Ответственный отвечает за поддержание необходимого уровня безопасности объектов защиты, является уполномоченным на проведение соответствующих работ.

1.6. Ответственный в своей работе руководствуется Федеральным законом от 27.07.2006

№ 152-ФЗ «О персональных данных», постановлениями Правительства, руководящими и нормативными документами ФСТЭК России, а также другими нормативно-правовыми актами, действующими на территории Российской Федерации, настоящей Инструкцией и иными регламентирующими документами Организации.

1.7. Требования Ответственного, связанные с выполнением им своих трудовых обязанностей, обязательны для исполнения всеми работниками, имеющими санкционированный доступ к защищаемой информации.

1.8. Ответственный обладает правами доступа к любым носителям информации Организации.

2. Термины и определения

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

2.2. Администратор безопасности информации – пользователь, уполномоченный выполнять некоторые действия (имеющий полномочия) по администрированию (управлению) системой защиты информации в соответствии с установленной ролью.

2.3. Безопасность информации [данных] – состояние защищенности информации [данных], при котором обеспечены ее [их] конфиденциальность, доступность и целостность.

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

2.5. Доступность информации [ресурсов информационной системы] – состояние информации [ресурсов информационной системы], при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно.

2.6. Защищаемая информация – информация, для которой обладателем информации

определены характеристики ее безопасности.

2.7. Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

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

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

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

2.11. Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

2.12. Носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

2.13. 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.

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

2.15. Пользователь – лицо, которому разрешено выполнять некоторые действия (операции) по обработке информации в информационной системе или использующее результаты ее функционирования.

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

2.17. Средство защиты информации – техническое, программное, программно-техническое средство, предназначенное или используемое для защиты информации.

2.18. Техническое средство – аппаратное или программно-аппаратное устройство, осуществляющее формирование, обработку, передачу или прием информации в информационной системе.

3. Обязанности ответственного

Ответственный обязан:

3.1. Обеспечивать выполнение режимных и организационных мероприятий на месте эксплуатации информационной системы, а также следить за выполнением требований по условиям размещения средств вычислительной техники и их сохранностью.

3.2. Знать и предоставлять администратору безопасности информации изменения к списку лиц, доступ которых к информации ограниченного доступа необходим для выполнения трудовых обязанностей.

3.3. Проводить инструктаж и консультации пользователей информационной системы по соблюдению режима конфиденциальности.

3.4. Участвовать в определении полномочий пользователей информационной системы (оформлении разрешительной системы доступа), минимально необходимых им для выполнения трудовых обязанностей.

3.5. Организовывать периодический контроль пользователей по соблюдению ими режима конфиденциальности, правил работы со съемными машинными носителями информации, выполнению организационных мер по защите информации, а также принимать участие в проведении проверок уполномоченными структурами.

3.6. Взаимодействовать с администратором безопасности информации по вопросам обеспечения и выполнения требований обработки персональных данных.

3.7. Контролировать осуществление мероприятий по установке и настройке средств защиты.

3.8. Организовывать работы по плановому контролю работоспособности технических средств защиты информации, охраны объекта, средств защиты информации от несанкционированного доступа.

3.9. Контролировать периодическое резервное копирование баз данных и сопутствующей защищаемой информации.

3.10. По указанию руководства своевременно и точно отражать изменения в локальных нормативно-правовых актах по управлению средствами защиты информации в информационной системе и по правилам обработки информации ограниченного доступа.

3.11. Знать перечень и условия обработки персональных данных в Организации.

3.12. Знать перечень установленных в подразделении технических средств, входящих в состав информационной системы, и перечень задач, решаемых с их использованием.

3.13. Обеспечивать соблюдение работниками утвержденного порядка проведения работ по установке и модернизации аппаратных и программных средств компьютеров и серверов из состава информационной системы.

3.14. Осуществлять контроль за порядком учета, создания, хранения и использования машинных (выходных) документов, содержащих защищаемую информацию.

3.15. При выявлении возможных каналов неправомерного вмешательства в процесс функционирования информационной системы и осуществления несанкционированного доступа к защищаемой информации и техническим средствам из состава информационной системы подразделения, сообщать о них руководителю Организации.

3.16. Инструктировать работников по вопросам обеспечения информационной безопасности и правилам работы с применяемыми средствами защиты информации.

3.17. Знать законодательство РФ о персональных данных, следить за его изменениями.

3.18. Проводить разбирательства и составление заключений по фактам несоблюдения условий хранения носителей защищаемой информации, нарушения правил работы с документами, содержащими персональные данные, или по другим нарушениям, которые могут привести к снижению уровня защищенности персональных данных.

3.19. Выполнять иные мероприятия, требуемые нормативными документами по защите информации.

4. Права ответственного

Ответственный имеет право:

4.1. Требовать от всех пользователей информационной системы выполнения установленной технологии обработки персональных данных, инструкций и других нормативных правовых документов по обеспечению безопасности информации.

4.2. Инициировать блокирование доступа работников к защищаемой информации, если это необходимо для предотвращения нарушения режима защиты информации.

4.3. Участвовать в разработке мероприятий по совершенствованию системы защиты информации.

4.4. Инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения информационной безопасности, несоблюдения

условий хранения носителей защищаемой информации, нарушения правил работы с документами, содержащими персональные данные, несанкционированного доступа, утраты, порчи защищаемых носителей информации и технических средств из состава информационной системы или по другим нарушениям, которые могут привести к снижению уровня информационной безопасности.

4.5. Обращаться к руководителю подразделения с предложением о приостановке процесса обработки персональных данных или отстранению от работы пользователя в случаях нарушения установленной технологии обработки персональных данных или нарушения режима конфиденциальности.

4.6. Подавать свои предложения по совершенствованию мер защиты информации, разработке и принятии мер по предотвращению возможных опасных последствий нарушений, приводящих к снижению уровня информационной безопасности.

5. Действия при обнаружении попыток несанкционированного доступа

5.1. К попыткам несанкционированного доступа относятся:

5.1.1. сеансы работы в информационной системе незарегистрированных пользователей, пользователей, нарушивших установленную периодичность доступа, или срок действия полномочий которых истек, или превышающих свои полномочия по доступу к данным;

5.1.2. действия постороннего лица, пытающегося получить доступ (или уже получившего доступ) к информационной системе, при использовании учетной записи администратора или другого пользователя, методом подбора пароля, использования пароля, разглашенного владельцем учетной записи или любым другим методом.

5.2. При выявлении факта несанкционированного доступа Ответственный обязан:

5.2.1. по возможности пресечь дальнейший несанкционированный доступ к защищаемой информации;

5.2.2. доложить руководителю Организации служебной запиской о факте несанкционированного доступа, его результате (успешный, неуспешный) и предпринятых действиях;

5.2.3. известить руководителя структурного подразделения, в котором работает пользователь, от имени учетной записи которого была осуществлена попытка несанкционированного доступа, о факте несанкционированного доступа;

5.2.4. известить администратора безопасности информации о факте несанкционированного доступа.

6. Ответственность

6.1. Ответственный несет персональную ответственность за:

6.1.1. соблюдение требований настоящей Инструкции;

6.1.2. правильность и объективность принимаемых решений;

6.1.3. качество и своевременность проводимых им работ по обеспечению безопасности информации;

6.1.4. за все действия, совершенные от имени его учетной записи в информационной системе, если с его стороны не было предпринято необходимых действий для предотвращения несанкционированного использования его учетной записи.

6.2. Ответственный при нарушении норм, регулирующих получение, обработку и защиту информации ограниченного доступа, несет дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством Российской Федерации.

Инструкция пользователя информационной системы, осуществляющих обработку данных в ИС

1. Общие положения

1.1. Настоящий документ разработан в соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», а также другими нормативными документами по безопасности информации, и определяет порядок обеспечения информационной безопасности при проведении работ пользователями информационной системы (далее – информационная система; ИС) Муниципального бюджетного дошкольного образовательного учреждения «Ромашка» муниципального образования город Ноябрьск (далее – Организация).

1.2. Субъектами доступа к ресурсам ИС являются администратор безопасности информации (далее – АБИ), пользователи и обслуживающий персонал.

1.3. Обрабатываемая в ИС информация содержит сведения, составляющие персональные данные (далее – ПДн).

1.4. Пользователи получают свои права на доступ к ресурсам ИС через АБИ.

1.5. Пользователи имеют право письменно вносить предложения по изменению и дополнению данной Инструкции.

1.6. Изменения и дополнения к данной Инструкции утверждаются в установленном порядке.

2. Термины и определения

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

2.2. Администратор безопасности информации – пользователь, уполномоченный выполнять некоторые действия (имеющий полномочия) по администрированию (управлению) системой защиты информации в соответствии с установленной ролью.

2.3. Безопасность информации [данных] – состояние защищенности информации [данных], при котором обеспечены ее [их] конфиденциальность, доступность и целостность.

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

2.5. Доступность информации [ресурсов информационной системы] – состояние информации [ресурсов информационной системы], при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно.

2.6. Защищаемая информация – информация, для которой обладателем информации определены характеристики ее безопасности.

2.7. Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

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

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

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

2.11. Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

2.12. Носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

2.13. 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.

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

2.15. Пользователь – лицо, которому разрешено выполнять некоторые действия (операции) по обработке информации в информационной системе или использующее результаты ее функционирования.

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

2.17. Средство защиты информации – техническое, программное, программно-техническое средство, предназначенное или используемое для защиты информации.

2.18. Техническое средство – аппаратное или программно-аппаратное устройство, осуществляющее формирование, обработку, передачу или прием информации в информационной системе.

3. Обязанности

Пользователь обязан:

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

3.2. Выполнять на АРМ только те процедуры, которые определены технологическим процессом обработки информации ограниченного доступа.

3.3. Знать и соблюдать установленные требования к обработке информации ограниченного доступа, учету и хранению носителей информации, обеспечению информационной безопасности, а также руководящих и организационно-распорядительных документов.

3.4. Соблюдать требования парольной политики в соответствии с «Инструкцией по организации парольной защиты».

3.5. Получить уникальное имя и персональный идентификатор (при его наличии) от администратора безопасности информации. Пользователь обязан помнить и соблюдать в тайне свои имена и пароли, не допускается их запись на каких-либо носителях в целях напоминания.

3.6. Во время работы располагать экран монитора так, чтобы затруднить посетителям просмотр отображаемой информации. Жалюзи на окнах должны быть закрыты.

3.7. При возникновении подозрения на наличие вредоносного программного обеспечения (частые ошибки в работе программ, появление посторонних графических и звуковых эффектов, искажения данных, неконтролируемое пропадание файлов, появление сообщений о системных ошибках, замедление работы компьютера и т.п.) самостоятельно или вместе с АБИ провести внеочередной антивирусный контроль своего автоматизированного рабочего места (далее – АРМ). При самостоятельном проведении антивирусного контроля – уведомить о результатах АБИ для определения им факта наличия или отсутствия вредоносного программного обеспечения.

3.8. В случае появления информационного окна средства антивирусной защиты, сигнализирующем об обнаружении вредоносного программного обеспечения:

3.8.1. приостановить обработку данных;

3.8.2. немедленно поставить в известность о факте обнаружения вредоносного программного обеспечения АБИ, владельца зараженных файлов, а также смежные структурные подразделения, использующие эти файлы в работе;

3.8.3. совместно с владельцем файлов, зараженных вредоносным программным обеспечением, провести анализ необходимости дальнейшего их использования;

3.8.4. произвести лечение или уничтожение зараженных файлов (для выполнения требований данного пункта привлечь АБИ).

3.9. Немедленно вызывать АБИ и поставить в известность руководителя структурного подразделения при обнаружении:

3.9.1. нарушений целостности пломб (наклеек, нарушения или несоответствии номеров печатей) на аппаратных средствах АРМ или иных фактов совершения в его отсутствие попыток несанкционированного доступа к защищаемому АРМ;

3.9.2. несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств АРМ;

3.9.3. отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию АРМ, выхода из строя или неустойчивого функционирования узлов АРМ или периферийных устройств (дисководов, принтера и т.п.), а также перебоев в системе электроснабжения;

3.9.4. некорректного функционирования установленных на АРМ технических средств защиты;

3.9.5. непредусмотренных отводов кабелей и подключенных к АРМ дополнительных устройств.

3.10. При утере или подозрении на утечку своего имени, пароля и персональных идентификаторов пользователь должен немедленно сообщить об этом АБИ.

3.11. Обо всех выявленных нарушениях, связанных с информационной безопасностью Организации, а так же для получения консультаций по вопросам информационной безопасности, необходимо обратиться к АБИ.

3.12. При отсутствии визуального контроля за рабочей станцией доступ к компьютеру должен быть немедленно заблокирован. Для этого необходимо нажать одновременно комбинацию клавиш <Ctrl><Alt> и выбрать опцию <Блокировка>.

3.13. Принимать меры по реагированию в случае возникновения внештатных ситуаций и аварийных ситуаций с целью ликвидации их последствий в пределах возложенных на него функций.

3.14. Пользователям запрещается:

- разглашать защищаемую информацию посторонним лицам;
- копировать защищаемую информацию на неучтенные внешние носители;

- самостоятельно устанавливать, тиражировать или модифицировать программное и аппаратное обеспечение, изменять установленный порядок функционирования технических и программных средств;
- подключать к рабочей станции и корпоративной информационной сети личные внешние носители и мобильные устройства;
- отключать (блокировать) средства защиты информации;
- выполнять на АРМ работы, не предусмотренные технологическим процессом обработки информации;
- сообщать (или передавать) посторонним лицам параметры своей учетной записи (имя, персональный идентификатор (при его наличии) и пароль) в ИС;
- оставлять без присмотра и передавать другим лицам персональный идентификатор;
- привлекать посторонних лиц для ремонта или настройки АРМ без согласования с ответственным за защиту информации;
- оставлять без присмотра свое АРМ, не активизировав блокировку доступа, или оставлять свое АРМ включенным по окончании работы;
- умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к нарушению безопасности информации.

4. Порядок работы пользователя с ресурсами ИС

4.1. Начало работы на АРМ

При включении АРМ необходимо дождаться завершения загрузки и готовности системы защиты информации (далее – СЗИ) и операционной системы (далее – ОС) к идентификации пользователя. Идентификация пользователя осуществляется по уникальному имени и паролю с использованием персонального идентификатора, если таковой предусмотрен комплектацией СЗИ. Для получения доступа к ресурсам ИС пользователь должен приложить к считывателю персональный идентификатор (при его наличии) и ввести с клавиатуры свой пароль. Если после ввода пароля СЗИ выдаст сообщение об ошибке, пользователь должен обратиться к АБИ.

4.2. Завершение работы на АРМ

По окончании работы пользователь должен либо завершить штатными средствами сеанс своей работы (без выключения АРМ), либо завершить работу АРМ стандартным способом (при этом выключить АРМ).

4.3. Требования к распечатыванию информации

Все распечатываемые документы должны быть учтены. Бракованные бумажные носители и черновики документов должны быть уничтожены.

При отсутствии пользователя на рабочем месте либо в присутствии лиц, не имеющих допуска к ресурсам ИС, все документы, содержащие защищаемую информацию, должны быть недоступны для просмотра и иного их использования.

5. Организация парольной защиты

5.1. Личные пароли доступа к элементам ИС выдаются пользователям администратором безопасности информации или создаются самостоятельно.

5.2. Полная плановая смена паролей в ИС проводится не реже одного раза в 4 месяца.

5.3. Правила формирования пароля:

- пароль должен состоять не менее чем из 6 символов;
- в пароле должны присутствовать символы из числа прописных и строчных букв английского алфавита от А до Z; десятичных цифр (от 0 до 9);

символы, не принадлежащие алфавитно-цифровому набору (например, !, \$, #, %);

- запрещается использовать в качестве пароля имя учетной записи, простые пароли типа «123», «111», «qwerty» и им подобные, а так же имена и даты рождения пользователей ИС и их родственников, клички домашних животных, номера автомобилей, телефонов и другие пароли, которые можно вычислить, основываясь на информации о пользователе;
- запрещается использовать в качестве пароля один и тот же повторяющийся символ, либо повторяющуюся комбинацию из нескольких символов;
- запрещается использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, 1234567 и т.п.);
- запрещается выбирать пароли, которые уже использовались ранее.

5.4. Правила ввода пароля:

- ввод пароля должен осуществляться с учетом регистра, в котором пароль был задан;
- во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами.

5.5. Правила хранения пароля:

- запрещается записывать пароли на бумаге, в файле и других носителях информации, в том числе на предметах;
- запрещается сообщать другим пользователям личный пароль и/или регистрировать их в системе под своей учетной записью.

5.6. Лица, использующие паролирование, обязаны:

- четко знать и строго выполнять требования настоящей Инструкции и других руководящих документов по паролированию;
- своевременно сообщать АБИ об утере, компрометации, несанкционированном изменении паролей и несанкционированном изменении сроков действия паролей.

6. Ответственность

6.1. Пользователь несет персональную ответственность за:

- сохранность носителей информации и содержащейся на них информации (в рабочее время);
- соблюдение требований данной Инструкции, неправомерное использование ресурсов ИС и за все действия, совершенные от имени его учетной записи в ИС, если с его стороны не было предпринято необходимых действий для предотвращения несанкционированного использования его учетной записи.

6.2. За разглашение информации ограниченного доступа и нарушение порядка работы со средствами ИС, содержащими такую информацию, работники могут быть привлечены к гражданской, уголовной, административной, дисциплинарной и иной предусмотренной законодательством Российской Федерации ответственности.