

МУНИЦИПАЛЬНОЕ ОБРАЗОВАНИЕ

ХАНТЫ-МАНСИЙСКИЙ РАЙОН

Ханты-Мансийский автономный округ – Югра

**АДМИНИСТРАЦИЯ ХАНТЫ-МАНСИЙСКОГО РАЙОНА**

**Р А С П О Р Я Ж Е Н И Е**

от 30.07.2019 № 756-р

*г. Ханты-Мансийск*

О внесении изменений в распоряжение

администрации Ханты-Мансийского

района от 16.04.2014 № 552-р

«Об организации работ по обеспечению

безопасности персональных данных

при их обработке, в том числе

в информационных системах

персональных данных в администрации

Ханты-Мансийского района»

На основании статьи 32 Устава Ханты-Мансийского района:

1. Внести в распоряжение администрации Ханты-Мансийского района от 16.04.2014 № 552-р «Об организации работ по обеспечению безопасности персональных данных при их обработке, в том числе
в информационных системах персональных данных в администрации Ханты-Мансийского района» следующие изменения:

1.1. Приложение 1 изложить в новой редакции:

«Приложение 1

к распоряжению администрации

Ханты-Мансийского района

от 16.04.2014 № 552-р

Инструкция

администратора информационной безопасности в администрации

Ханты-Мансийского района

Обозначения и сокращения:

АРМ – автоматизированное рабочее место;

ИБ – информационная безопасность;

МИСПДн – муниципальная информационная система персональных данных;

ОС – операционная система;

ОТСС – основные технические средства и системы;

ПДн – персональные данные;

ПЭВМ – персональная электронно-вычислительная машина;

СЗИ – средства защиты информации;

ПО – программное обеспечение;

МНИ – машинные носители информации;

ИС – информационная система.

I. Общие положения

1.1. Настоящая инструкция определяет обязанности, права
и ответственность администратора информационной безопасности (далее – администратор ИБ) информационных систем персональных данных администрации Ханты-Мансийского района (далее – Учреждение).

1.2. Используемые основные понятия:

Оператор – администрация Ханты-Мансийского района, органы администрации Ханты-Мансийского района, 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.

Субъект персональных данных – физическое лицо, которое прямо или косвенно определено или определяемо с помощью персональных данных.

Администратор информационной безопасности – должностное лицо, ответственное за обеспечение безопасности ПДн (конфиденциальности, целостности и доступности) в процессе их обработки в МИСПДн.

1.3. Администратор ИБ назначается распоряжением Оператора
из числа сотрудников Оператора.

1.4. Администратор информационной безопасности осуществляет контроль выполнения организационных и технических мероприятий
по обеспечению безопасности информации в МИСПДн администрации Ханты-Мансийского района.

1.5. Администратор ИБ в своей деятельности руководствуется действующим законодательством Российской Федерации, локальными актами Оператора по обеспечению безопасности персональных данных и другой защищаемой информации, а также настоящей инструкцией.

1.6. Методическое руководство и контроль за работой администратора информационной безопасности осуществляется ответственным за организацию обработки персональных данных и другой защищаемой информации в Учреждении.

II. Особенности организации работы в ИС

Администратор информационной безопасности должен знать, что МИСПДн в Учреждении относятся к многопользовательским ИС с разными правами доступа пользователей к ресурсам. Группы пользователей, работающих в МИСПДн: администратор информационной безопасности, пользователи ИС. Данные группы пользователей имеют права доступа к ресурсам ИС в соответствии с разрешительной системой доступа персонала к сведениям конфиденциального характера в МИСПДн.

III. Обязанности

администратора информационной безопасности

3.1. Администратор информационной безопасности должен:

3.1.1. Знать требования нормативных, правовых, методических документов в области обеспечения безопасности информации и организационно-распорядительные документы в части, его касающейся.

3.1.2. Знать перечень обрабатываемых ПДн, состав, структуру, назначение и выполняемые задачи МИСПДн.

3.1.3. Знать состав ОТСС МИСДПн Учреждения и контролировать их соответствие техническому паспорту на МИСДПн. Вести учет изменений аппаратно-программной конфигурации (архив заявок, на основании которых были произведены данные изменения).

3.1.4. Уметь пользоваться средствами защиты информации и осуществлять их непосредственное администрирование.

3.1.5. Контролировать процесс управления (заведения, активации, блокирования, уничтожения) учетными записями пользователей ИС, в т.ч. ИС органов администрации Ханты-Мансийского района, в состав которых входит центральный сегмент Учреждения:

проверять соответствие прав доступа пользователей к ИС в соответствии с задачами, решаемыми пользователями и взаимодействующими с ней ИС;

контролировать назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы;

проверять отсутствие в ИС учетных записей уволенных (отстраненных) пользователей;

осуществлять управление учетными записями пользователей при изменении сведений о пользователях, их ролях, обязанностях, полномочиях, ограничениях.

3.1.6. Контролировать неизменность настроек средств защиты информации:

настройки средств защиты информации должны препятствовать передаче защищаемой информации через сеть Интернет и (или) другие информационно-телекоммуникационные сети международного информационного обмена по незащищенным линиям связи;

средства защиты информации должны ограничивать доступ к ИС
при 5 неудачных попытках входа в ИС;

на BIOS ПЭВМ должен быть установлен пароль;

должен быть запрещен доступ к ИС до прохождения процедур идентификации и аутентификации;

должен обеспечиваться запрет удаленного доступа к ИС.

3.1.7. Осуществлять организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах МИСПДн и контроль за действиями пользователей при работе с паролями в соответствии с Инструкцией по организации парольной защиты в информационных системах персональных данных администрации Ханты-Мансийского района.

3.1.8. Контролировать запрет использования в ИС технологий беспроводного доступа и мобильных технических средств (кроме съемных машинных носителей информации).

3.1.9. Контролировать отсутствие доступа к ИС со стороны пользователей информационных систем сторонних организаций.

3.1.10. Контролировать установку на АРМ ИС ПО с целью отсутствия в составе АРМ ИС стороннего ПО, не связанного с задачами, решаемыми пользователями в ИС.

3.1.11. Контролировать появление новых функциональных обновлений (добавляющих функционал или решающих проблему с функциональностью) ПО в соответствии с Инструкцией по управлению обновлениями программного обеспечения.

3.1.12. Вести учет машинных носителей с защищаемой информацией.

3.1.13. Вести журнал учета лиц, допущенных к работе с персональными данными в МИСПДн.

3.1.14. Обеспечивать уничтожение (стирание) защищаемой информации с машинных носителей АРМ ИС при их передаче в сторонние организации для ремонта или утилизации либо контролировать процесс уничтожения (стирания). Уничтожение защищаемой информации должно исключать возможность восстановления защищаемой информации.

3.1.15. Контролировать регистрацию в информационной системе следующих событий безопасности:

входа (выхода), а также попытки входа субъектов доступа в информационную систему и загрузки (остановки) операционной системы:

даты (время) входа/выхода в систему (из системы) или загрузки/останова операционной системы, результат попытки входа (успешная или неуспешная), результат попытки загрузки (останова) операционной системы (успешная или неуспешная), идентификатор, предъявленный при попытке доступа;

подключения машинных носителей информации и вывода

информации на носители информации:

даты и время подключения машинных носителей информации
и вывода информации на носители информации, логическое имя (номер) подключаемого машинного носителя информации, идентификатора субъекта доступа, осуществляющего вывод информации на носитель информации;

запуска (завершения) программ и процессов (заданий, задач), связанных с обработкой защищаемой информации:

даты и время запуска, имя (идентификатор) программы (процесса, задания), идентификатор субъекта доступа (устройства), запросившего программу (процесс, задание), результат запуска (успешный, неуспешный);

попыток доступа программных средств к защищаемым АРМ ИС доступа:

даты и время попытки доступа к защищаемому файлу с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), спецификацию защищаемого файла (логическое имя, тип);

попыток удаленного доступа:

дату и время попытки удаленного доступа с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), используемый протокол доступа, используемый интерфейс доступа и (или) иную информацию о попытках удаленного доступа к информационной системе.

3.1.16. Контролировать права на доступ к информации о событиях безопасности: доступ должен предоставляться исключительно администраторам ИС, обеспечивающим функционирование ИС, а также администратору информационной безопасности.

3.1.17. Обеспечивать постоянный контроль за выполнением пользователями МИСПДн установленного комплекса мероприятий по обеспечению безопасности информации и соблюдения действующего законодательства в области информационной безопасности, а также организационно-распорядительных документов Оператора в части обеспечения безопасности информации.

3.1.18. Требовать от пользователей ИС и выполнять самому требования Инструкции по установке, модификации, ремонту, техническому обслуживанию и восстановлению работоспособности программного обеспечения и аппаратных средств в муниципальных информационных системах персональных данных администрации Ханты-Мансийского района и вести «Журнал учета нештатных ситуаций и выполнения профилактических и ремонтных работ, установки, модификации программных и аппаратных средств на автоматизированных рабочих местах».

3.1.19. Контролировать порядок учета, создания, хранения и использования резервных и архивных копий массивов данных, машинных (выходных) документов.

3.1.20. Осуществлять управление средствами антивирусной защиты,

в т.ч. на АРМ, входящих в состав ИС органов администрации, включенных в домен администрации. Проводить мероприятия по организации антивирусной защиты в соответствии с Инструкцией по организации антивирусной защиты в информационных системах персональных данных администрации Ханты-Мансийского района.

3.1.21. Контролировать использование пользователями только учтенных съемных носителей. После того, как цель переноса информации на носители достигнута (переданы третьим лицам и т.п.), информация незамедлительно удаляется с носителей.

3.1.22. Контролировать настройки ОС и СЗИ АРМ пользователей.

3.1.23. Проводить инструктаж пользователей по правилам работы с используемыми средствами и системами защиты информации.

3.1.24. Устанавливать права доступа пользователей к информационным и техническим ресурсам ИС в соответствии с принятой и утвержденной разрешительной системой доступа.

3.1.25. Следить за изменением программной среды МИСПДн и полномочиями пользователей.

3.1.26. Своевременно вносить изменения в разрешительную систему доступа, перечни лиц, имеющих право доступа в помещения размещения ОТСС МИСПДн, и перечни лиц, имеющих право доступа к обработке защищаемой информации, технический паспорт на МИСПДн.

3.1.27. Инициировать внеплановый пересмотр частной модели угроз в предусмотренных для этого случаях.

3.1.28. Хранить дистрибутивы СЗИ, производить при необходимости восстановление программной среды СЗИ или настройки защитных механизмов операционной системы и привилегий пользователей по доступу к ресурсам ИС. При необходимости для данных мероприятий привлекать других технических специалистов.

3.1.29. Фиксировать и пресекать невыполнение пользователями ИС требований или норм нормативно-методических документов и организационно-распорядительных документов по обеспечению безопасности информации.

3.1.30. При получении информации о фактах нарушения политики и правил безопасности, в т.ч. пользователями ИС органов администрации, в состав которых входит центральный сегмент Учреждения, а также попыток реализации внешними нарушителями атак, в том числе с использованием методов социальной инженерии – немедленно докладывать ответственному за организацию обработки ПДн, при необходимости – администратору информационной безопасности органа администрации, инициировать проведение служебной проверки (при нарушениях со стороны ответственного за организацию обработки ПДн докладывать необходимо непосредственно вышестоящему руководству), регистрировать в журнале учета инцидентов ИБ.

3.1.31. Не реже 1 раза в месяц просматривать журналы регистрации событий СЗИ в соответствии с Инструкцией о порядке проверки электронного журнала обращений к информационным системам персональных данных администрации Ханты-Мансийского района
на предмет выявления подключения неучтенных носителей, попыток НСД
и т.п.

3.1.32. Требовать от пользователей ИС и выполнять самому порядок пропускного и внутриобъектового режима в здании.

3.1.33. Контролировать отсутствие в составе ПО АРМ, входящих в ИС, средств разработки и отладки программ.

3.1.34. Реагировать на поступление в ИС спама (в случае присутствия данной информации в журналах событий межсетевого экрана) путем блокирования атакующего хоста.

3.1.35. Выполнять мероприятия по еженедельному резервному копированию защищаемой информации в соответствии с Инструкцией по организации резервирования и восстановления программного обеспечения и баз персональных данных в муниципальных информационных системах персональных данных администрации Ханты-Мансийского района.

3.1.36. Знать эксплуатационную документацию на применяемые СЗИ. Устанавливать и эксплуатировать СЗИ в соответствии с документацией.

3.1.37. Хранить документацию и дистрибутивы СЗИ в соответствии с техническими условиями. Компакт-диск с программным обеспечением СЗИ должен упаковываться согласно требованиям, предусмотренным для оптических носителей.

3.1.38. Поддерживать настройки СЗИ, соответствующие требованиям нормативных документов по безопасности информации и протоколу аттестационных испытаний, при этом система должна реализовывать в совокупности на каждой АРМ ИС функции, необходимые для выполнения требований по защите от НСД для ИС.

3.1.39. Контролировать срок действия сертификатов соответствия на СЗИ или технической поддержки производителем СЗИ и обеспечить продление.

3.1.40. Вести и актуализировать информацию об имеющихся защищенных объектах информатизации, а также о составе средств защиты информации (ведение реестра).

3.1.41. Участвовать в работе комиссий по проведению периодического контроля за обеспечением уровня защищенности информации, обрабатываемой в МИСПДн.

3.1.42. Вести календарь событий информационной безопасности, анализировать и реагировать на события безопасности:

срока ежегодного контроля;

срока истечения аттестата;

срока истечения лицензии ПО;

срока истечения лицензии СЗИ.

3.2. При исключении пользователя ИС из перечня лиц, имеющих доступ к ИС, администратору информационной безопасности необходимо до момента доведения до сотрудника информации о прекращении его работы в ИС лишить пользователя возможности доступа к защищаемой информации.

3.3. Администратору информационной безопасности запрещается:

3.3.1. Фиксировать учетные данные пользователя (пароли, идентификаторы, ключи и др.) на твердых носителях, а также сообщать их кому бы то ни было, кроме самого пользователя.

3.3.2. Раскрывать информацию об организации СЗИ ИС и любую информацию, которая может создать предпосылки для возникновения канала утечки информации или создания угрозы безопасности информации.

IV. Права администратора информационной безопасности

4.1. Администратор информационной безопасности имеет право:

4.1.1. Требовать от пользователей ИС соблюдения установленных технологий обработки информации, выполнения нормативно-методических документов в области безопасности информации и организационно-распорядительных документов на ИС.

4.1.2. Вносить предложения непосредственному руководителю по совершенствованию системы защиты информации в ИС.

4.1.3. Взаимодействовать с системным администратором в рамках выполнения работ по техническому обслуживанию ИС.

4.1.4. Взаимодействовать с ответственным за организацию обработки персональных данных и ответственным за эксплуатацию МИСПДн по вопросам обработки и обеспечения безопасности ПДн.

V. Ответственность

Администратор информационной безопасности несет ответственность в соответствии с действующим законодательством Российской Федерации за разглашение сведений ограниченного распространения, ставших известными ему по роду деятельности, а также за недобросовестное выполнение обязательств по обеспечению безопасности персональных данных и другой защищаемой информации.

VI. Порядок продления сроков действия сертификатов

соответствия на средства защиты информации, программные

средства контроля защищенности информации

 от несанкционированного доступа

1. Администратор информационной безопасности контролирует актуальность сертификатов соответствия средств защиты информации. Заблаговременно, до окончания срока действия сертификата соответствия, который указан в копии сертификата, а также в Государственном реестре сертифицированных средств защиты информации в Системе сертификации средств защиты информации по требованиям безопасности информации
№ РОСС RU.0001.01БИ00, связывается с производителем, с целью получения информации о продлении сертификата соответствия
или осуществлении технической поддержки продукта производителем.».

1.2. Приложения 5, 6 изложить в новой редакции:

«Приложение 5

к распоряжению администрации

Ханты-Мансийского района

от 16.04.2014 № 552-р

ИНСТРУКЦИЯ

по организации антивирусной защиты

в информационных системах персональных данных

администрации Ханты-Мансийского района

I. Общие требования

1. Настоящая инструкция определяет требования к организации антивирусной защиты информационных систем персональных данных (далее – ИСПДн) от разрушающего воздействия вирусов и вредоносных программ и устанавливает ответственность руководителя и работников структурных подразделений, эксплуатирующих и сопровождающих ИСПДн, за их выполнение. Инструкция распространяется на все ИСПДн, существующие и вновь разрабатываемые в администрации района. Для отдельных ИСПДн могут быть разработаны свои инструкции, учитывающие особенности работы ИСПДн.

2. Используемые термины:

Оператор – администрация Ханты-Мансийского района, органы администрации Ханты-Мансийского района, 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;

администратор информационной безопасности – должностное лицо, ответственное за обеспечение безопасности персональных данных (далее – ПДн) (конфиденциальности, целостности и доступности) в процессе их обработки в ИСПДн.

3. К использованию в ИСПДн допускаются только лицензионные антивирусные средства, централизованно закупленные у разработчиков (поставщиков) указанных средств.

4. Установка и настройка средств антивирусного контроля

осуществляется администратором информационной безопасности в ИСПДн или специально назначенным лицом в соответствии с руководствами по применению конкретных антивирусных средств.

II. Применение средств антивирусного контроля

1. При загрузке АРМ в автоматическом режиме должен проводиться антивирусный контроль служб операционной системы, исполняемых приложений, находящихся в автозагрузке, реестра операционной системы.

2. Полному антивирусному контролю автоматизированные рабочие места (АРМ) Оператора должны подвергаться не реже одного раза в неделю.

3. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), информация на съемных носителях информации (магнитных, оптических дисках, флэш-накопителях и т.п.). Разархивирование и контроль входящей информации необходимо проводить непосредственно после ее приема. Возможно применение другого способа антивирусного контроля входящей информации, обеспечивающего аналогичный уровень эффективности контроля. Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

Должна быть проведена настройка антивирусной защиты от вирусов-макросов. Макросы позволяют выполнять любой вредоносный код (скачивание и выполнение файла). Необходимо отключить макросы в Microsoft Office. В антивирусном средстве должна быть включена проактивная защита от макросов.

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

5. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов и других вредоносных программ. Непосредственно после установки (изменения) программного обеспечения администратором информационной безопасности в ИСПДн должна быть выполнена антивирусная проверка на защищаемых серверах и пользовательских АРМ ИСПДн.

6. При возникновении подозрения на наличие вируса либо вредоносной программы (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) работник структурного подразделения самостоятельно или вместе с администратором информационной безопасности в ИСПДн должен провести внеочередной антивирусный контроль своего АРМ.

7. В случае обнаружения при проведении антивирусной проверки зараженных вирусами либо вредоносными программами файлов работник

структурного подразделения обязан:

приостановить работу в ИСПДн;

немедленно поставить в известность о факте обнаружения зараженных вирусом файлов руководителя структурного подразделения и администратора информационной безопасности в ИСПДн, владельца зараженных файлов, а также смежные подразделения, использующие эти файлы в работе;

совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;

провести лечение или уничтожение зараженных файлов.

8. Обновление антивирусных баз осуществляется в автоматическом режиме из доверенных серверов обновлений разработчика.

В случае возникновения ошибок при автоматическом обновлении средств антивирусной защиты (появлении диалоговых окон, сообщений об ошибке) пользователь ИС сообщает данную информацию администратору информационной безопасности. Администратор информационной безопасности еженедельно осуществляет проверку статистики обновлений баз сигнатур, обновляет базу вручную в случае необходимости.

III. Ответственность

1. Ответственность за проведение мероприятий антивирусного контроля в подразделениях и соблюдение требований настоящей Инструкции возлагается на администратора информационной безопасности в ИСПДн и всех работников, являющихся пользователями ИСПДн.

Приложение 6

к распоряжению администрации

Ханты-Мансийского района

от 16.04.2014 № 552-р

ИНСТРУКЦИЯ

по организации резервирования и восстановления

программного обеспечения и баз персональных данных

в информационных системах персональных данных

администрации Ханты-Мансийского района

I. Общие положения

 1. Настоящая инструкция разработана с целью обеспечения возможности оперативного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

2. Инструкция определяет правила и объемы резервирования, а также

порядок восстановления работоспособности ИСПДн администрации района.

3. Используемые термины:

администратор информационной безопасности – должностное лицо, ответственное за обеспечение безопасности персональных данных (далее – ПДн) (конфиденциальности, целостности и доступности) в процессе их обработки в информационных системах персональных данных (далее – ИСПДн).

II. Резервируемое программное обеспечение

и базы персональных данных

 1. В ИСПДн резервированию подлежит:

общее программное обеспечение (операционная система и программные драйверы устройств (принтеры, мониторы, видеокарты и т.п.), поставляемые с компонентами автоматизированных рабочих мест (далее – АРМ), входящими в состав ИСПДн);

прикладное программное обеспечение, используемое для обработки персональных данных (средства обработки текстов и таблиц, специализированные программы и т.п.);

базы персональных данных (тестовые и табличные файлы, а также файлы баз данных специализированных программ);

программное обеспечение средств защиты информации, в том числе средств антивирусной защиты;

виртуальные вычислительные системы (виртуальные машины).

III. Порядок резервирования и хранения резервных копий

 1. Резервирование общего и прикладного программного обеспечения, программного обеспечения виртуальной инфраструктуры, а также программного обеспечения средств защиты информации обеспечивается путем хранения у администратора информационной безопасности в ИСПДн машинных носителей информации, содержащих дистрибутивы данного программного обеспечения.

 2. Машинные носители информации обновлений общего и прикладного программного обеспечения, а также программного обеспечения средств защиты информации должны также храниться у администратора информационной безопасности в ИСПДн.

 3. Допускается хранение машинных носителей прикладного программного обеспечения и машинных носителей с обновлениями к нему в структурных подразделениях, эксплуатирующих ИСПДн.

 4. Резервирование баз ПДн, а также текстовых и табличных файлов, содержащих ПДн, допускается только на учтенные установленным порядком машинные носители информации.

5. Резервирование осуществляется администратором

информационной безопасности еженедельно на дисковое хранилище данных. Контроль успешности резервирования проводится после окончания резервирования путем просмотра отчетов специализированного программного обеспечения резервирования и восстановления. Контроль данных, копируемых на съемные машинные носители информации, проводится путем проверки возможности открытия файлов, баз ПДн.

 6. Резервные носители персональных данных хранятся в структурных подразделениях, эксплуатирующих ИСПДн, в порядке, предусмотренном для носителей информации ПДн.

 7. К резервному носителю ПДн должна быть приложена учетная карточка, в которой делаются отметки о дате резервирования.

 8. Резервные носители персональных данных не могут быть переданы за пределы структурных подразделений, эксплуатирующих ИСПДн.

 9. Копирование информации с резервных носителей ПДн, за исключением случая восстановления работоспособности ИСПДн, запрещается.

10. Резервное копирование виртуальных машин осуществляется путем снятия образов виртуальных машин.

IV. Порядок восстановления работоспособности ИСПДн

1. Восстановление работоспособности ИСПДн осуществляется в случаях сбоев, отказов и аварий технических средств и систем ИСПДн, а также ее программного обеспечения.

2. Данные работы осуществляются администратором информационной безопасности в ИСПДн в соответствии с эксплуатационной документацией на программное обеспечение до полного восстановления работоспособности.

3. В случае необходимости привлечения для восстановления работоспособности ИСПДн представителей сторонних организаций должна быть обеспечена невозможность их ознакомления с персональными данными. Ответственность за выполнение данного требования возлагается на администратора информационной безопасности в ИСПДн
и руководителя структурного подразделения, обеспечивающего ее эксплуатацию.».

2. Контроль за выполнением распоряжения возложить на первого заместителя главы Ханты-Мансийского района.

И.о. главы Ханты-Мансийского района Р.Н.Ерышев