

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 11.01.2019 № 8-р

*г. Ханты-Мансийск*

Об организации работ по обеспечению

безопасности персональных данных

при их обработке, в том числе

в муниципальных информационных

системах персональных данных

В соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ   
«О персональных данных», постановлениями Правительства Российской Федерации 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 принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», с целью организации работ по обеспечению безопасности персональных данных, в том числе при их обработке в муниципальных информационных системах персональных данных:

1. Утвердить инструкции:

о порядке работы пользователей муниципальных информационных систем персональных данных в части обеспечения безопасности персональных данных при их обработке в муниципальных информационных системах персональных данных администрации Ханты-Мансийского района (далее – МИСПДн) (приложение 1);

о порядке работы со средствами криптографической защиты информации администрации Ханты-Мансийского района (приложение 2);

по работе с инцидентами информационной безопасности   
(приложение 3).

по ведению журнала учета хранилищ (приложение 4);

по ведению журнала учета инцидентов информационной безопасности (приложение 5);

по ведению журнала учета передачи персональных данных (приложение 6);

по ведению журнала периодического тестирования средств защиты информации (приложение 7);

по ведению журнала учета проверок электронных журналов обращений к информационным системам персональных данных (приложение 8);

по ведению журнала учета резервного копирования и восстановления данных (приложение 9);

по ведению журнала поэкземплярного учета криптосредств, эксплуатационной и технической документации к ним, ключевых документов (приложение 10);

по ведению журнала учета нештатных ситуаций в муниципальных информационных системах персональных данных, выполнения профилактических работ, установки и модификации программных средств на автоматизированных рабочих местах (приложение 11).

2. Назначить администратором средств криптографической защиты информации (далее – СКЗИ, криптосредства) специалиста по защите информации II категории управления по информационным технологиям администрации Ханты-Мансийского района.

3. Утвердить перечень пользователей СКЗИ (приложение 12). Сотрудникам, допущенным к работе со СКЗИ, при работе со СКЗИ руководствоваться инструкцией о порядке работы со СКЗИ администрации Ханты-Мансийского района (приложение 2).

4. Администратору СКЗИ при работе с СКЗИ руководствоваться инструкцией о порядке работы со СКЗИ администрации Ханты-Мансийского района (приложение 2), а также приказом ФСБ России   
от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных (далее – ПДн) при их обработке в муниципальных информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

5. Назначить ответственных за эксплуатацию МИСПДн:

МИСПДн «АМБА Зарплата»: Боричко Надежду Владимировну – эксперта I категории управления по учету и отчетности;

МИСПДн «МАИС ЗАГС»: Новицкую Ильмиру Михайловну – начальника отдела ЗАГС;

МИСПДн «Опека», «Аист»: Дьяченко Светлану Григорьевну – начальника отдела опеки и попечительства;

МИСПДн «Учет обращений граждан»: Сагирову Ольгу Александрову – консультанта отдела организационной и контрольной работы;

МИСПДн «Комиссия по делам несовершеннолетних»: Буракову Марину Николаевну – начальника отдела по организации работы комиссии по делам несовершеннолетних и защите их прав;

МИСПДн «Административная комиссия»: Безукладникова Владимира Викторовича – секретаря административной комиссии.

6. Утвердить перечень сотрудников администрации Ханты-Мансийского района, доступ которых к ПДн, обрабатываемым в МИСПДн, необходим для выполнения должностных обязанностей (приложение 13), и допустить их к обработке ПДн в МИСПДн.

В дальнейшем основанием для допуска и прекращения допуска сотрудника к обработке ПДн является распоряжение администрации Ханты-Мансийского района о зачислении нового работника в штат администрации Ханты-Мансийского района и увольнении работника соответственно.

Лицам, допущенным к обработке ПДн в МИСПДн, в обязательном порядке подписать обязательство о неразглашении информации, содержащей ПДн.

7. Сотрудникам администрации Ханты-Мансийского района при определении ПДн, подлежащих обработке и защите в МИСПДн, руководствоваться распоряжением администрации Ханты-Мансийского района «Об утверждении перечня муниципальных информационных систем персональных данных и перечня персональных данных, обрабатываемых в муниципальных информационных системах персональных данных».

8. Признать утратившими силу распоряжения администрации Ханты-Мансийского района:

от 09.12.2016 № 1204-р «Об организации работ по обеспечению безопасности персональных данных при их обработке, в том числе в муниципальных информационных системах персональных данных»;

от 26.11.2018 № 1130-р «О внесении изменений в распоряжение администрации Ханты-Мансийского района от 09.12.2016 № 1204-р   
«Об организации работ по обеспечению безопасности персональных данных при их обработке, в том числе в муниципальных информационных системах персональных данных».

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

Глава Ханты-Мансийского района К.Р.Минулин

Приложение 1

к распоряжению администрации

Ханты-Мансийского района

от 11.01.2019 № 8-р

ИНСТРУКЦИЯ  
о порядке работы пользователей  
муниципальных информационных систем персональных данных  
в части обеспечения безопасности персональных данных  
при их обработке в муниципальных информационных системах персональных данных администрации Ханты-Мансийского района

(далее – МИСПДн)

1. Настоящая инструкция определяет порядок действий пользователей МИСПДн в части обеспечения безопасности персональных данных (далее – ПДн) при их обработке в МИСПДн.

2. Допуск пользователей для работы за автоматизированным рабочим местом (далее – АРМ) осуществляется на основании утверждаемого списка сотрудников, доступ которых к персональным данным, обрабатываемым в муниципальных информационных системах персональных данных, необходим для выполнения служебных обязанностей.

3. Пользователь МИСПДн имеет право в отведенное ему время решать поставленные задачи в соответствии с полномочиями доступа к ресурсам МИСПДн. При этом для хранения информации, содержащей ПДн, разрешается использовать только машинные носители информации, учтенные в журнале учета машинных носителей информации, использующихся для обработки, хранения, транспортировки информации.

4. Пользователь несет ответственность за правильность включения и выключения АРМ, входа в систему и все действия при работе в МИСПДн.

5. Вход пользователя в систему может осуществляться по выдаваемому ему электронному идентификатору или по персональному паролю.

6. Запись информации, содержащей ПДн, осуществляется пользователем МИСПДн только на учтенные съемные машинные носители информации, использующиеся в МИСПДн для обработки, хранения, транспортировки информации.

7. При работе со съемными машинными носителями информации пользователь каждый раз перед началом работы обязан проверить их на отсутствие вирусов и иных вредоносных программ с использованием антивирусных средств, установленных на АРМ. В случае обнаружения вирусов либо вредоносных программ пользователь МИСПДн обязан немедленно прекратить их использование и действовать в соответствии с требованиями инструкции по организации антивирусной защиты.

8. Каждый сотрудник, обрабатывающий ПДн в рамках своих служебных обязанностей, в процессах обработки ПДн в МИСПДн и имеющий доступ к АРМ, программному обеспечению и данным МИСПДн, несет персональную ответственность за свои действия и обязан:

8.1. Строго соблюдать установленные соответствующими инструкциями правила обеспечения безопасности информации МИСПДн.

8.2. Знать и строго выполнять правила работы со средствами защиты информации, установленными на АРМ.

8.3. Хранить в тайне свой пароль (пароли). Выполнять требования инструкции по организации парольной защиты в полном объеме.

8.4. Хранить в установленном порядке свое индивидуальное устройство идентификации (ключ) и другие реквизиты в сейфе (металлическом шкафу).

8.5. Выполнять требования инструкции по организации антивирусной защиты в полном объеме.

8.6. Немедленно известить администратора информационной безопасности в случае утери индивидуального устройства идентификации (ключа) или при подозрении компрометации личных ключей и паролей, а также при обнаружении:

фактов совершения в его отсутствие попыток несанкционированного доступа (далее – НСД) к АРМ;

несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации АРМ МИСПДн;

отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию АРМ, выхода из строя или неустойчивого функционирования компонентов АРМ, а также перебоев в системе электроснабжения;

некорректного функционирования установленных на АРМ технических средств защиты;

непредусмотренных отводов кабелей и подключенных устройств.

9. Пользователю АРМ категорически запрещается:

использовать компоненты программного и аппаратного обеспечения АРМ в неслужебных целях;

самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств МИСПДн или устанавливать дополнительно любые программные и аппаратные средства, не предусмотренные перечнем программного обеспечения, разрешенного к установке;

записывать и хранить конфиденциальную информацию (содержащую ПДн) на неучтенных машинных носителях информации (гибких магнитных дисках, флеш-накопителях и т.п.);

оставлять включенным без присмотра АРМ, не активизировав средства защиты от НСД;

оставлять без личного присмотра на рабочем месте или в ином месте свое персональное устройство идентификации, машинные носители и распечатки, содержащие ПДн;

умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению кризисной ситуации;

размещать средства МИСПДн так, чтобы существовала возможность визуального считывания с них информации.

Приложение 2

к распоряжению администрации

Ханты-Мансийского района

от 11.01.2019 № 8-р

ИНСТРУКЦИЯ  
о порядке работы со средствами криптографической защиты информации  
администрации Ханты-Мансийского района

1. Общие положения

* 1. Настоящая инструкция определяет порядок организации и обеспечения функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну (далее – криптосредство), в случае их использования для обеспечения безопасности персональных данных при их обработке в муниципальных информационных системах персональных данных (далее – информационная система).
  2. Пользователь – лицо, участвующее в эксплуатации криптосредства или использующее результаты его функционирования.
  3. Режимные помещения – помещения, где установлены криптосредства или хранятся ключевые документы к ним.
  4. Шифровальные (криптографические) средства – криптосредства:
     1. Средства шифрования – аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты информации при передаче по каналам связи и (или) для защиты информации от несанкционированного доступа (далее – НСД) при ее обработке и хранении.
     2. Средства имитозащиты – аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты от навязывания ложной информации.
     3. Средства электронной цифровой подписи (далее – ЭЦП) – аппаратные, программные и аппаратно-программные средства, обеспечивающие на основе криптографических преобразований реализацию хотя бы одной из следующих функций: создание ЭЦП с использованием закрытого ключа ЭЦП, подтверждение с использованием открытого ключа ЭЦП подлинности ЭЦП, создание закрытых и открытых ключей ЭЦП.
     4. Средства кодирования – средства, реализующие алгоритмы криптографического преобразования информации с выполнением части преобразования путем ручных операций или с использованием автоматизированных средств на основе таких операций.
     5. Средства изготовления ключевых документов (независимо от вида носителя ключевой информации).
     6. Ключевые документы (независимо от вида носителя ключевой информации).

2. Обязанности пользователей криптосредств

2.1. Пользователи криптосредств обязаны:

2.1.1. Не разглашать информацию, к которой они допущены, в том числе сведения о криптосредствах, ключевых документах к ним и других мерах защиты.

2.1.2. Соблюдать требования к обеспечению безопасности персональных данных, требования к обеспечению безопасности криптосредств и ключевых документов к ним.

2.1.3. Сообщать о ставших им известными попытках посторонних лиц получить сведения об используемых криптосредствах или ключевых документах к ним.

2.1.4. Немедленно уведомлять администратора информационной безопасности о фактах утраты или недостачи криптосредств, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к разглашению защищаемых персональных данных.

2.1.5. Сдать криптосредства, эксплуатационную и техническую документацию к ним, ключевые документы в соответствии с порядком, установленным настоящей инструкцией, при увольнении или отстранении от исполнения обязанностей, связанных с использованием криптосредств.

3. Порядок обращения с криптосредствами и криптоключами к ним.

Мероприятия при компрометации криптоключей

3.1. При необходимости передачи по техническим средствам связи служебных сообщений ограниченного доступа, касающихся организации и обеспечения функционирования криптосредств, указанные сообщения необходимо передавать только с использованием криптосредств. Передача по техническим средствам связи криптоключей не допускается, за исключением специально организованных систем с децентрализованным снабжением криптоключами.

3.2. Криптосредства, используемые для обеспечения безопасности персональных данных при их обработке в информационных системах, подлежат учету с использованием индексов или условных наименований и регистрационных номеров.

3.3. Перечень индексов, условных наименований и регистрационных номеров криптосредств определяется Федеральной службой безопасности Российской Федерации.

3.4. Используемые или хранимые криптосредства, эксплуатационная и техническая документация к ним, ключевые документы подлежат поэкземплярному учету. При этом программные криптосредства должны учитываться совместно с аппаратными средствами, с которыми осуществляется их штатное функционирование. Если аппаратные или аппаратно-программные криптосредства подключаются к системной шине или к одному из внутренних интерфейсов аппаратных средств, то такие криптосредства учитываются также совместно с соответствующими аппаратными средствами.

3.5. Единицей поэкземплярного учета ключевых документов считается ключевой носитель многократного использования, ключевой блокнот. Если один и тот же ключевой носитель многократно используют для записи криптоключей, то его каждый раз следует регистрировать отдельно.

3.6. Все полученные экземпляры криптосредств, эксплуатационной и технической документации к ним, ключевых документов должны быть выданы под расписку в соответствующем журнале поэкземплярного учета пользователям криптосредств, несущим персональную ответственность за их сохранность.

3.7. Если эксплуатационной и технической документацией к криптосредствам предусмотрено применение разовых ключевых носителей или криптоключи вводят и хранят (на весь срок их действия) непосредственно в криптосредствах, то такой разовый ключевой носитель или электронная запись соответствующего криптоключа должны регистрироваться в техническом (аппаратном) журнале, ведущемся непосредственно пользователем криптосредств. В техническом (аппаратном) журнале отражают также данные об эксплуатации криптосредств и другие сведения, предусмотренные эксплуатационной и технической документацией. В иных случаях технический (аппаратный) журнал на криптосредства не заводится (если нет прямых указаний о его ведении в эксплуатационной или технической документации к криптосредствам).

3.8. Передача криптосредств, эксплуатационной и технической документации к ним, ключевых документов допускается только между пользователями криптосредств и (или) администратором средств криптографической защиты информации под расписку в соответствующих журналах поэкземплярного учета. Такая передача между пользователями криптосредств должна быть санкционирована администратором средств криптографической защиты информации.

3.9. Пользователи криптосредств хранят инсталлирующие криптосредства носители, эксплуатационную и техническую документацию к криптосредствам, ключевые документы в шкафах (ящиках, хранилищах) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

3.10. Пользователи криптосредств предусматривают также раздельное безопасное хранение действующих и резервных ключевых документов, предназначенных для применения в случае компрометации действующих ключевых документов.

3.11. Аппаратные средства, с которыми осуществляется штатное функционирование криптосредств, а также аппаратные и аппаратно-программные криптосредства должны быть оборудованы средствами контроля за их вскрытием (опечатаны, опломбированы). Место опечатывания (опломбирования) криптосредств, аппаратных средств должно быть таким, чтобы его можно было визуально контролировать. При наличии технической возможности на время отсутствия пользователей криптосредств указанные средства необходимо отключать от линии связи и убирать в опечатываемые хранилища.

3.12. Эксплуатационную и техническую документацию к криптосредствам допускается пересылать заказными или ценными почтовыми отправлениями.

3.13. Уничтожение криптоключей (исходной ключевой информации) может производиться путем физического уничтожения ключевого носителя, на котором они расположены, или путем стирания (разрушения) криптоключей (исходной ключевой информации) без повреждения ключевого носителя (для обеспечения возможности его многократного использования).

3.14. Криптоключи (исходную ключевую информацию) стирают по технологии, принятой для соответствующих ключевых носителей многократного использования (дискет, компакт-дисков (CD-ROM), Data Key, Smart Card, Touch Memory и т.п.). Непосредственные действия по стиранию криптоключей (исходной ключевой информации), а также возможные ограничения на дальнейшее применение соответствующих ключевых носителей многократного использования регламентируются эксплуатационной и технической документацией к соответствующим криптосредствам, а также указаниями организации, производившей запись криптоключей (исходной ключевой информации).

3.15. Ключевые носители уничтожают путем нанесения им неустранимого физического повреждения, исключающего возможность их использования, а также восстановления ключевой информации. Непосредственные действия по уничтожению конкретного типа ключевого носителя регламентируются эксплуатационной и технической документацией к соответствующим криптосредствам, а также указаниями организации, производившей запись криптоключей (исходной ключевой информации).

3.16. Бумажные и прочие сгораемые ключевые носители, а также эксплуатационная и техническая документация к криптосредствам уничтожаются путем сжигания или с помощью любых бумагорезательных машин.

3.17. Пригодные для дальнейшего использования узлы и детали аппаратных средств общего назначения, не предназначенные специально для аппаратной реализации криптографических алгоритмов или иных функций криптосредств, а также совместно работающее с криптосредствами оборудование (мониторы, принтеры, сканеры, клавиатура и т.п.), разрешается использовать после уничтожения криптосредств без ограничений. При этом информация, которая может оставаться в устройствах памяти оборудования (например, в принтерах, сканерах), должна быть надежно удалена (стерта).

3.18. Ключевые документы должны быть уничтожены в сроки, указанные в эксплуатационной и технической документации к соответствующим криптосредствам. Если срок уничтожения эксплуатационной и технической документацией не установлен, то ключевые документы должны быть уничтожены не позднее 10 суток после вывода их из действия (окончания срока действия). Факт уничтожения оформляется в соответствующих журналах поэкземплярного учета. В эти же сроки с отметкой в техническом (аппаратном) журнале подлежат уничтожению разовые ключевые носители и ранее введенная и хранящаяся в криптосредствах или иных дополнительных устройствах ключевая информация, соответствующая выведенным из действия криптоключам; хранящиеся в криптографически защищенном виде данные следует перешифровать на новых криптоключах.

3.19. Разовые ключевые носители, а также электронные записи ключевой информации, соответствующей выведенным из действия криптоключам, непосредственно в криптосредствах или иных дополнительных устройствах уничтожаются пользователями этих криптосредств самостоятельно под расписку в техническом (аппаратном) журнале.

3.20. Ключевые документы уничтожаются администратором средств криптографической защиты информации под расписку в соответствующих журналах поэкземплярного учета, а уничтожение большого объема ключевых документов может быть оформлено актом.

3.21. Уничтожение по акту производит комиссия в составе не менее двух человек из числа лиц, допущенных к пользованию криптосредств. В акте указывается, что уничтожается и в каком количестве. В конце акта делается итоговая запись (цифрами и прописью) о количестве наименований и экземпляров уничтожаемых ключевых документов, инсталлирующих криптосредства носителей, эксплуатационной и технической документации. Исправления в тексте акта должны быть оговорены и заверены подписями всех членов комиссии, принимавших участие в уничтожении. О проведенном уничтожении делаются отметки в соответствующих журналах поэкземплярного учета.

3.22. Криптоключи, в отношении которых возникло подозрение в компрометации, а также действующие совместно с ними другие криптоключи необходимо немедленно вывести из действия, если иной порядок не оговорен в эксплуатационной и технической документации к криптосредствам. В чрезвычайных случаях, когда отсутствуют криптоключи для замены скомпрометированных, допускается по решению администратора средств криптографической защиты информации использование скомпрометированных криптоключей. В этом случае период использования скомпрометированных криптоключей должен быть максимально коротким, а защищаемая информация как можно менее ценной.

3.23. О нарушениях, которые могут привести к компрометации криптоключей, их составных частей или передававшихся (хранящихся) с их использованием персональных данных, пользователи криптосредств обязаны сообщать администратору средств криптографической защиты информации.

3.24. Осмотр ключевых носителей многократного использования посторонними лицами не следует рассматривать как подозрение в компрометации криптоключей, если при этом исключалась возможность их копирования (чтения, размножения).

3.25. В случаях недосдачи, непредъявления ключевых документов, а также неопределенности их местонахождения принимаются срочные меры к их розыску.

3.26. Мероприятия по розыску и локализации последствий компрометации ключевых документов организует и осуществляет администратор СКЗИ.

Приложение 3

к распоряжению администрации

Ханты-Мансийского района

от 11.01.2019 № 8-р

ИНСТРУКЦИЯ

по работе с инцидентами информационной безопасности

Обозначения и сокращения:

Администрация – администрация Ханты-Мансийского района;

ИБ – информационная безопасность;

ПДн – персональные данные;

МИСПДн – муниципальная информационная система персональных данных;

СЗИ – средства защиты информации;

ОРД – организационно-распорядительная документация.

Ответственность за выявление инцидентов ИБ и реагирование на них в администрации возлагается на администратора информационной безопасности.

Администратор информационной безопасности имеет полномочия инициировать проведение служебных проверок (ходатайствовать о наложении дисциплинарного взыскания перед главой Ханты-Мансийского района) по фактам нарушения установленных требований обеспечения информационной безопасности, несанкционированного доступа, утраты, порчи защищаемой информации.

Администратор информационной безопасности обязан вести журнал учета инцидентов ИБ (событий, действий, повлекших за собой риски безопасности защищаемой информации и создающих предпосылки к нарушению критериев безопасности информации). Сюда относятся нарушения пользователями положений организационно-распорядительных документов, установленных порядков и технологии работы в МИСПДн, разглашение защищаемой информации и любые действия, направленные на это, не антропогенные инциденты (сбои ПО, стихийные бедствия).

В журнале в свободной форме описывается инцидент с указанием следующих данных:

даты и времени;

причин (умышленные и неумышленные действия, не антропогенные инциденты и т.п.) и описания инцидента и задействованных лиц;

информации о последствиях;

информации о возможных последствиях (экономические убытки (в связи с заменой СЗИ, повторной аттестацией; временные и трудозатраты на устранение последствий, нарушение работы пользователей, ущерб субъектам ПДн и юридические последствия для администрации и т.п.).

Журнал с данным отчетом об инциденте предоставляется на ознакомление ответственному за организацию обработки ПДн для принятия мер по предотвращению рецидива (возникновения повторного инцидента).

В случае возникновения рецидива со стороны пользователя или администратора информационной безопасности по ходатайству ответственного за организацию обработки ПДн главой Ханты-Мансийского района накладывается дисциплинарное взыскание.

Сокрытие нарушений и инцидентов ИБ, вызванных любыми должностными лицами администрации, является грубым нарушением трудовой дисциплины. Сокрытие нарушений и инцидентов ИБ, вызванных действиями администратора информационной безопасности и ответственным за организацию обработки ПДн, является грубейшим нарушением дисциплины и при выяснении данного факта должно строго наказываться.

Любой сотрудник должен согласовывать следующие действия с администратором информационной безопасности:

замена прикладного оборудования (мышь, клавиатура, принтер, монитор);

установка дополнительного ПО;

изменение сетевых настроек рабочего места;

замена, изменение любой аппаратной части рабочего места.

Ответственный за организацию обработки ПДн не может требовать от администратора информационной безопасности действий, направленных на нарушение настоящего руководства и других организационно-распорядительных документов по защите процесса обработки ПДн администрации, требовать сокрытия инцидентов ИБ, вызванных любыми должностными лицами, требовать сообщения ему паролей на СЗИ и нарушения установленного разграничения прав по допуску к информационным ресурсам, установленным матрицей доступа к информационным.ресурсам.МИСПДн.

Приложение 4

к распоряжению администрации

Ханты-Мансийского района

от 11.01.2019 № 8-р

ИНСТКУЦИЯ

по ведению журнала учета хранилищ

Назначение: журнал учета хранилищ ведется с целью учета хранения сведений конфиденциального характера и защиты их от несанкционированного доступа. Под хранилищем подразумеваются помещения, сейфы, шкафы и пр. В хранилищах хранятся: бумажные носители персональных данных, резервные копии персональных данных, съемные носители персональных данных, средства защиты информации, в том числе криптографической, техническая и эксплуатационная документация на информационные системы персональных данных, другие сведения конфиденциального характера.

Ответственное лицо за ведение: администратор безопасности информации в муниципальных информационных системах персональных данных.

Общепринятые сокращения: сокращения в журнале отсутствуют.

Место хранения: журнал хранится в личном сейфе администратора безопасности информации в муниципальных информационных системах персональных данных.

Порядок заполнения:

в столбцах журнала указывается следующая информация:

№ 1: номер, идущий по порядку;

№ 2: регистрационный (учетный) номер хранилища – не указывается в случаях, когда в виде хранилища выступает помещение;

№ 3: вид хранилища – помещение, сейф, шкаф и пр.;

№ 4: дата постановки на учет – дата принятия решения об определении хранилища для хранения сведений конфиденциального характера;

№ 5: фамилия и подпись принявшего (ответственного), дата – лица, ответственного за сохранность сведений в хранилище и за доступ к хранилищу;

№ 6: место расположения (номер помещения);

№ 7: дата и номер акта о выводе из эксплуатации – дата принятия решения о прекращении хранения сведений конфиденциального характера в хранилище;

№ 8: примечание.

Периодичность заполнения: журнал заполняется по мере поставки на учет хранилищ.

Срок хранения: 5 лет (п. 230 приказа Министерства культуры Российской Федерации от 25.09.2010 № 558 «Об утверждении Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения»).

Приложение 5

к распоряжению администрации

Ханты-Мансийского района

от 11.01.2019 № 8-р

ИНСТКУЦИЯ

по ведению журнала учета инцидентов информационной безопасности

Назначение: журнал учета инцидентов информационной безопасности ведется с целью учета и регистрации событий инцидентов информационной безопасности.

Ответственное лицо за ведение: администратор безопасности информации в муниципальных информационных системах персональных данных.

Общепринятые сокращения: сокращения в журнале отсутствуют.

Место хранения: журнал хранится в личном сейфе администратора безопасности информации в муниципальных информационных системах персональных данных.

Порядок заполнения:

в столбцах журнала указывается следующая информация:

№ 1: номер, идущий по порядку;

№ 2: дата инцидента;

№ 3: №, дата справки или акта по результатам расследования или краткое содержание инцидента;

№ 4: ФИО проверяющего;

№ 5: подпись проверяющего.

Периодичность заполнения: журнал заполняется по мере выявления инцидента информационной безопасности.

Срок хранения: 5 лет (п. 217 приказа Министерства культуры Российской Федерации от 25.09.2010 № 558   
«Об утверждении Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения»).

Журнал учета инцидентов информационной безопасности

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № п/п | Дата инцидента | №, дата справки или акта по результатам расследования или краткое содержание инцидента | ФИО проверяющего | Подпись проверяющего |
| 1 | 2 | 3 | 4 | 5 |
|  |  |  |  |  |

Приложение 6

к распоряжению администрации

Ханты-Мансийского района

от 11.01.2019 № 8-р

ИНСТКУЦИЯ

по ведению журнала учета передачи персональных данных

Назначение: журнал учета передачи персональных данных ведется с целью защиты прав субъектов персональных данных при осуществлении передачи их персональных данных третьим лицам.

Ответственное лицо за ведение: ответственный за обработку персональных данных в органе администрации Ханты-Мансийского района.

Общепринятые сокращения: сокращения в журнале отсутствуют.

Место хранения: журнал хранится в личном сейфе ответственного за обработку персональных данных в органе администрации Ханты-Мансийского района.

Порядок заполнения: журнал заполняется в тех случаях, когда передача возможна только с согласия субъекта персональных данных, при этом согласие от субъекта не было получено раннее. При этом оператор не освобождается от обязанности взять от субъекта указанное согласие.

В столбцах журнала указывается следующая информация:

№ 1: номер, идущий по порядку;

№ 2: сведения о запрашивающем лице – физическом или юридическом;

№ 3: состав запрашиваемых персональных данных – перечень персональных данных;

№ 4: цель получения персональных данных – цель с указанием правового обоснования;

№ 5: отметка о передаче или отказе в передаче персональных данных – с указанием причин отказа;

№ 6: дата передачи/отказа в передаче персональных данных;

№ 7: подпись запрашивающего лица – для подтверждения факта такого запроса.

Периодичность заполнения: журнал заполняется в тех случаях, когда передача возможна только с согласия субъекта персональных данных, при этом согласие от субъекта не было получено раннее.

Срок хранения: 5 лет (п. 258 приказа Министерства культуры Российской Федерации от 25.09.2010 № 558   
«Об утверждении Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения»).

Журнал

учета передачи персональных данных

| №  п/п | Сведения о запрашивающем лице | Состав запрашиваемых персональных данных | Цель получения персональных данных | Основание для передачи персональных данных | Дата передачи/отказа в передаче персональных данных | Подпись исполнителя/  исполнителей | Подпись руководителя органа администрации  Ханты-Мансийского района |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 1. |  |  |  |  |  |  |  |

Приложение 7

к распоряжению администрации

Ханты-Мансийского района

от 11.01.2019 № 8-р

ИНСТКУЦИЯ

по ведению журнала периодического тестирования средств защиты информации

Назначение: журнал периодического тестирования средств защиты информации ведется с целью контроля уровня защищенности персональных данных при их обработке в информационных системах персональных данных.

Ответственное лицо за ведение: администратор безопасности информации в информационных системах персональных данных.

Общепринятые сокращения:

средство защиты информации – СЗИ;

несанкционированный доступ – НСД.

Место хранения: журнал хранится в личном сейфе администратора безопасности информации в информационных системах персональных данных.

Порядок заполнения: журнал заполняется по мере проведения работ по тестированию СЗИ.

В столбцах журнала указывается следующая информация:

№ 1: номер, идущий по порядку;

№ 2: наименование средства защиты информации от НСД или криптосредства;

№ 3: регистрационные номера СЗИ от НСД или криптосредства;

№ 4: дата проведения тестирования;

№ 5: фамилия и подпись ответственного лица, проводившего тестирование – администратора безопасности информации в информационных системах персональных данных, за исключением отдельных случаев, когда проведение тестирования данным лицом невозможно;

№ 6: наименование теста (при отсутствии – указание проверяемых мер защиты), используемые средства для проведения теста (программные, программно-аппаратные средства анализа защищенности);

№ 7: результат тестирования (успешный/неуспешный), в случае неуспешного тестирования в обязательном порядке заполняются комментарии с указанием причин отрицательных результатов тестирования;

№ 8: дата очередного тестирования: в случае отрицательных результатов тестирования – незамедлительно по результатам исправления недостатков в работе СЗИ, в случае положительных результатов тестирования – дата следующего ежегодного тестирования всех СЗИ либо ввиду обоснованных причин в следующем квартале.

Периодичность заполнения: тестирование всех средств защиты информации – не менее одного раза в год, выборочное тестирование средств защиты информации – не менее одного раза в квартал.

Срок хранения: 10 лет (п. 224 приказа Министерства культуры Российской Федерации от 25.09.2010 № 558   
«Об утверждении Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения»).

Журнал

периодического тестирования средств защиты информации

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| № п/п | Наименование средства защиты информации от НСД или криптосредства | Регистрационные номера СЗИ от НСД или криптосредства | Дата тестирования | Фамилия и подпись ответственного лица, проводившего тестирование | Наименование теста, используемые средства для проведения теста | Результат тестирования (успешный/неуспешный), комментарий | Дата очередного тестирования |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

Приложение 8

к распоряжению администрации

Ханты-Мансийского района

от 11.01.2019 № 8-р

ИНСТКУЦИЯ

по ведению журнала учета проверок электронных журналов обращений к информационным системам персональных данных

Назначение: журнал учета проверок электронных журналов обращений к информационным системам персональных данных ведется с целью выявления фактов несанкционированного доступа к информационным системам персональных данных или нарушения их функционирования.

Ответственное лицо за ведение: администратор безопасности информации в информационных системах персональных данных.

Общепринятые сокращения: информационная система персональных данных – МИСПДн.

Место хранения: журнал хранится в личном сейфе администратора безопасности информации в информационных системах персональных данных.

Порядок заполнения: журнал обращений должен заполняться с использованием информации, полученной от средств операционной системы, или с помощью дополнительного программного обеспечения (средств защиты информации). При заполнении журнала учитываются требования инструкции о порядке проверки электронного журнала обращений к информационным системам персональных данных.

В столбцах журнала указывается следующая информация:

№ 1: номер, идущий по порядку;

№ 2: дата проверки;

№ 3: наименование МИСПДн, компьютера, технического средства;

№ 4: наименование проверяемого журнала – операционной системы либо средства защиты информации;

№ 5: выявленные нарушения требований безопасности, нештатные ситуации – с указанием причин возникновения;

№ 6: подпись администратора безопасности информации в МИСПДн;

№ 7: примечание.

Периодичность заполнения: проверки всех МИСПДн проводятся не менее одного раза в год, выборочные – не менее одного раза в квартал.

Срок хранения: 3 года по истечении срока хранения учтенных журналов (п. 261 приказа Министерства культуры Российской Федерации от 25.09.2010 № 558 «Об утверждении Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения»).

Журнал

учета проверок электронных журналов обращений к информационным системам персональных данных

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| №  п/п | Дата проверки | Наименование МИСПДн, компьютера, технического средства | Наименование проверяемого журнала | Выявленные нарушения требований безопасности, нештатные ситуации | Подпись администратора безопасности | Примечание |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

Приложение 9

к распоряжению администрации

Ханты-Мансийского района

от 11.01.2019 № 8-р

ИНСТКУЦИЯ

по ведению журнала резервного копирования и восстановления данных

Назначение: журнал резервного копирования и восстановления данных ведется с целью определения категории информации, подлежащей обязательному резервному копированию, процедуры резервирования данных для последующего восстановления работоспособности информационных систем при полной или частичной потере информации, вызванной сбоями или отказами аппаратного или программного обеспечения, ошибками пользователей, чрезвычайными обстоятельствами.

Ответственное лицо за ведение: администратор безопасности информации в информационных системах персональных данных.

Общепринятые сокращения: информационная система персональных данных – МИСПДн.

Место хранения: журнал хранится в личном сейфе администратора безопасности информации в информационных системах персональных данных.

Порядок заполнения: журнал должен заполняться по мере выполнения процедур резервного копирования с указанием конкретных резервируемых данных и аппаратных средств, а также полного или частичного восстановления данных.

В столбцах журнала указывается следующая информация:

№ 1: дата проведения резервного копирования/восстановления;

№ 2: наименование резервной копии;

№ 3: наименование информационной системы/базы данных;

№ 4: Ф.И.О., подпись ответственного.

Периодичность заполнения: проверки всех МИСПДн проводятся не менее одного раза в год, выборочные –   
не менее одного раза в квартал.

Срок хранения: 10 лет (п. 224 приказа Министерства культуры Российской Федерации от 25.09.2010 № 558   
«Об утверждении Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения»).

Журнал учета резервного копирования и восстановления данных

|  |  |  |  |
| --- | --- | --- | --- |
| Дата проведения резервного копирования/восстановления | Наименование резервной копии | Наименование информационной системы/базы данных | Ф.И.О., подпись ответственного |
|  |  |  |  |

Приложение 10

к распоряжению администрации

Ханты-Мансийского района

от 11.01.2019 № 8-р

ИНСТКУЦИЯ

по ведению журнала поэкземплярного учета криптосредств, эксплуатационной и технической документации к ним, ключевых документов

Назначение: журнал поэкземплярного учета криптосредств, эксплуатационной и технической документации к ним, ключевых документов ведется с целью учета криптосредств согласно требованиям законодательства Российской Федерации, а также расследования инцидентов в случае несанкционированного доступа к указанным средствам.

Ответственное лицо за ведение: администратор безопасности информации в муниципальных информационных системах персональных данных.

Общепринятые сокращения: средство криптографической защиты информации – СКЗИ.

Место хранения: журнал хранится в личном сейфе администратора безопасности информации в муниципальных информационных системах персональных данных.

Порядок заполнения: журнал заполняется в случаях получения, установки, изъятия криптосредств, а также эксплуатационной и технической документации к ним, ключевых документов.

В столбцах журнала указывается следующая информация:

№ 1: номер, идущий по порядку;

№ 2: наименование криптосредства, эксплуатационной и технической документации к ним, ключевых документов – указывается полное наименование;

№ 3: регистрационные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов – указываются реквизиты и учетные номера;

№ 4: номера экземпляров (криптографические номера) ключевых документов (учетный номер ключевого носителя, на который записан закрытый ключ подписи и/или ключ шифрования);

№ 5: отметка о получении. От кого получены – наименование организации, осуществляющей поставку/передачу криптосредства;

№ 6: отметка о получении. Дата и номер сопроводительного письма о передаче/получении криптосредства;

№ 7: отметка о выдаче. Ф.И.О. пользователя криптосредств – сотрудника, использующего криптосредство в работе;

№ 8: отметка о выдаче, дата и расписка в получении сотрудника, использующего криптосредство в работе;

№ 9: отметка о подключении (установке) СКЗИ. Ф.И.О. пользователя криптосредств, производившего подключение (установку) – администратора безопасности информации в муниципальных информационных системах персональных данных;

№ 10: отметка о подключении (установке) СКЗИ. Дата подключения (установки) и подписи лиц, произведших подключение (установку) – администратора безопасности информации в муниципальных информационных системах персональных данных;

№ 11: отметка о подключении (установке) СКЗИ. Номера аппаратных средств, в которые установлены или к которым подключены криптосредства – номер кабинета, инвентарный либо серийный номер автоматизированного рабочего места;

№ 12: отметка об изъятии СКЗИ из аппаратных средств, уничтожении ключевых документов. Дата изъятия (уничтожения);

№ 13: отметка об изъятии СКЗИ из аппаратных средств, уничтожении ключевых документов. Ф.И.О. пользователя СКЗИ, производившего изъятие (уничтожение) – администратора безопасности информации в информационных системах персональных данных;

№ 14: отметка об изъятии СКЗИ из аппаратных средств, уничтожении ключевых документов. Номер акта или расписка об уничтожении – в случае большого количества СКЗИ составляется акт об уничтожении, иначе расписка;

№ 15: примечание – в поле указывается дополнительная информация о получении, установке или изъятии криптосредств (при необходимости), в обязательном порядке в случае компрометации либо утере криптосредств.

Периодичность заполнения: журнал заполняется по мере получения, установки, изъятия криптосредств.

Срок хранения: 5 лет (п. 231 приказа Министерства культуры Российской Федерации от 25.09.2010 № 558   
«Об утверждении Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения»).

Журнал

поэкземплярного учета криптосредств, эксплуатационной и технической документации к ним, ключевых документов (лист 1)

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| № п/п | Наименование криптосредства, эксплуатационной и технической документации к ним, ключевых документов | Регистрационные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов | Номера экземпляров (криптографические номера) ключевых документов | Отметка о получении | | Отметка о выдаче | |
| от кого получены | дата и номер сопроводительного письма | Ф.И.О. пользователя криптосредств | дата и расписка в получении |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|  |  |  |  |  |  |  |  |

Журнал

поэкземплярного учета криптосредств, эксплуатационной и технической документации к ним, ключевых документов (лист 2)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Отметка о подключении (установке) СКЗИ | | | Отметка об изъятии СКЗИ из аппаратных средств, уничтожении ключевых документов | | | Примечание |
| Ф.И.О. пользователя криптосредств, производившего подключение (установку) | дата подключения (установки) и подписи лиц, произведших подключение (установку) | номера аппаратных средств, в которые установлены или к которым подключены криптосредства | дата изъятия (уничтожения) | Ф.И.О. пользователя СКЗИ, производившего изъятие (уничтожение) | номер акта или расписка об уничтожении |
| 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

Приложение 11

к распоряжению администрации

Ханты-Мансийского района

от 11.01.2019 № 8-р

ИНСТКУЦИЯ

по ведению журнала учета нештатных ситуаций в муниципальных информационных системах персональных данных, выполнения профилактических работ, установки и модификации программных средств

на автоматизированных рабочих местах

Назначение: журнал учета нештатных ситуаций в муниципальных информационных системах персональных данных, выполнения профилактических работ, установки и модификации программных средств на автоматизированных рабочих местах ведется с целью разбирательств нештатных ситуаций, а также контроля за выполнением профилактических работ, установки и модификации программных средств.

Ответственное лицо за ведение: администратор безопасности информации в муниципальных информационных системах персональных данных.

Общепринятые сокращения: автоматизированное рабочее место – АРМ.

Место хранения: журнал хранится в личном сейфе администратора безопасности информации в муниципальных информационных системах персональных данных.

Порядок заполнения: в столбцах журнала указывается следующая информация:

№ 1: номер, идущий по порядку;

№ 2: дата возникновения нештатной ситуации (выполнения работ);

№ 3: краткое описание выполненной работы (нештатной ситуации) – с указанием предпосылок;

№ 4: Ф.И.О. исполнителей и их подписи – с указанием юридического лица (если такое лицо привлекается к работам);

№ 5: Ф.И.О. ответственного за эксплуатацию АРМ, подпись сотрудника, осуществляющего обработку за АРМ;

№ 6: подпись специалиста по защите информации – администратора безопасности информации в муниципальных информационных системах персональных данных;

№ 7: примечание (ссылка на заявку) – в случае наличия заявки либо иного документа, побудившего к проведению работ.

Периодичность заполнения: журнал заполняется по мере возникновения указанных ситуаций.

Срок хранения: 5 лет (п. 217 приказа Министерства культуры Российской Федерации от 25.09.2010 № 558   
«Об утверждении Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения»).

Журнал

учета нештатных ситуаций в муниципальных информационных системах персональных данных, выполнения профилактических работ, установки и модификации программных средств на автоматизированных рабочих местах

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| № п/п | Дата | Краткое описание выполненной работы (нештатной ситуации) | Ф.И.О. исполнителей и их подписи | Ф.И.О. ответственного за эксплуатацию АРМ, подпись | Подпись специалиста по защите информации | Примечание (ссылка  на заявку) |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

Приложение 12

к распоряжению администрации

Ханты-Мансийского района

от 11.01.2019 № 8-р

СПИСОК СОТРУДНИКОВ  
администрации Ханты-Мансийского района,

допущенных к работе со средствами криптографической защиты

информации (далее – СКЗИ)

| № п/п | Фамилия, имя, отчество | Наименование должности | Наименование СКЗИ | Тип доступа |
| --- | --- | --- | --- | --- |
| 1. | Новицкий В.О. | начальник управления по информационным технологиям | ViPNet Client 4.3 | дискреционный |
| 2. | Попков А.А. | заместитель начальника управления по информационным технологиям | ViPNet Client 4.3 | дискреционный |
| 3. | Хмелев Р.В. | специалист по защите информации  II категории управления по информационным технологиям | ViPNet Client 4.3 | дискреционный |
| 4. | Боричко Н.В. | эксперт I категории управления по учету  и отчетности | ViPNet Client 4.3 | дискреционный |
| 5. | Дьяченко С.Г. | начальник отдела опеки и попечительства | ViPNet Client 4.3 | дискреционный |
| 6. | Ефремова А.Г. | консультант отдела опеки и попечительства | ViPNet Client 4.3 | дискреционный |
| 7. | Ломова Т.В. | консультант отдела опеки и попечительства | ViPNet Client 4.3 | дискреционный |
| 8. | Акимова Э.Н. | консультант отдела опеки и попечительства | ViPNet Client 4.3 | дискреционный |
| 9. | Екимова А.Н. | консультант отдела опеки и попечительства | ViPNet Client 4.3 | дискреционный |
| 10. | Гилева М.Ю. | консультант отдела опеки и попечительства | ViPNet Client 4.3 | дискреционный |
| 11. | Новицкая И.М. | начальник отдела ЗАГС | ViPNet Client 4.3 | дискреционный |
| 12. | Осокина А.А. | специалист-эксперт отдела ЗАГС | ViPNet Client 4.3 | дискреционный |
| 13. | Сагирова О.А. | консультант отдела организационной и контрольной работы | ViPNet Client 4.3 | дискреционный |
| 14. | Буракова М.Н. | начальник отдела по организации работы комиссии по делам несовершеннолетних и защите их прав | ViPNet Client 4.3 | дискреционный |
| 15. | Рассохина С.О. | заместитель начальника отдела по организации работы комиссии по делам несовершеннолетних и защите их прав | ViPNet Client 4.3 | дискреционный |
| 16. | Ангел Т.С. | консультант отдела по организации работы комиссии по делам несовершеннолетних и защите их прав | ViPNet Client 4.3 | дискреционный |
| 17. | Захарова А.Р. | консультант отдела по организации работы комиссии по делам несовершеннолетних и защите их прав | ViPNet Client 4.3 | дискреционный |
| 18. | Безукладников В.В. | секретарь административной комиссии | ViPNet Client 4.3 | дискреционный |

Приложение 13

к распоряжению администрации

Ханты-Мансийского района

от 11.01.2019 № 8-р

СПИСОК СОТРУДНИКОВ  
администрации Ханты-Мансийского района, доступ которых

к персональным данным, обрабатываемым в МИСПДн, необходим

для выполнения служебных обязанностей

| № п/п | ФИО | Наименование должности | Наименование МИСПДн |
| --- | --- | --- | --- |
| 1. | Боричко Н.В. | эксперт I категории управления по учету и отчетности | «АМБА Зарплата» |
| 2. | Дьяченко С.Г. | начальник отдела опеки и попечительства | «Опека, Аист» |
| 3. | Ефремова А.Г. | консультант отдела опеки и попечительства | «Опека, Аист» |
| 4. | Ломова Т.В. | консультант отдела опеки и попечительства | «Опека» |
| 5. | Екимова А.Н. | консультант отдела опеки и попечительства | «Опека» |
| 6. | Акимова Э.Н. | консультант отдела опеки и попечительства | «Опека» |
| 7. | Гилева М.Ю. | консультант отдела опеки и попечительства | «Опека» |
| 8. | Новицкая И.М. | начальник отдела ЗАГС | «МАИС ЗАГС» |
| 9. | Осокина А.А. | специалист-эксперт отдела ЗАГС | «МАИС ЗАГС» |
| 10. | Сагирова О.А. | консультант отдела организационной и контрольной работы | «Учет обращений граждан» |
| 11. | Буракова М.Н. | начальник отдела по организации работы комиссии по делам несовершеннолетних и защите их прав | «Комиссия по делам несовершеннолетних» |
| 12. | Рассохина С.О. | заместитель начальника отдела по организации работы комиссии по делам несовершеннолетних и защите их прав | «Комиссия по делам несовершеннолетних» |
| 13. | Ангел Т.С. | консультант отдела по организации работы комиссии по делам несовершеннолетних и защите их прав | «Комиссия по делам несовершеннолетних» |
| 14. | Захарова А.Р. | консультант отдела по организации работы комиссии по делам несовершеннолетних и защите их прав | «Комиссия по делам несовершеннолетних» |
| 15. | Безукладников В.В. | секретарь административной комиссии | «Административная комиссия» |