АДМИНИСТРАЦИЯ ГОРНОЗАВОДСКОГО ГОРОДСКОГО ОКРУГА

П О С Т А Н О В Л Е Н И Е

13.01.2020 № 12

Об утверждении Положения по обеспечению безопасности информации в администрации Горнозаводского городского округа

Руководствуясь Федеральными законами от 27 июля 2006 г. № 152-ФЗ «О персональных данных», от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», приказом Федерального агентства Правительственной связи и информации при Президенте Российской Федерации от 13 июня 2001 г. № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну», приказами Федеральной службы безопасности Российской Федерации от 09 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации», от 10 июля 2014 г. № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в 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», приказом Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», постановлением администрации Горнозаводского городского округа от 09 января 2020 г. № 9 «Об обработке персональных данных

в администрации Горнозаводского городского округа», статьями 23, 29 Устава Горнозаводского городского округа Пермского края, администрация Горнозаводского городского округа

ПОСТАНОВЛЯЕТ:

1. Утвердить прилагаемое Положение по обеспечению безопасности информации в администрации Горнозаводского городского округа.

2. Признать утратившим силу постановление администрации Горнозаводского муниципального района от 28 сентября 2017 г. № 1058 «Об утверждении Положения по обеспечению безопасности информации в администрации Горнозаводского муниципального района».

3. Обнародовать настоящее постановление в зданиях, расположенных по адресам: г. Горнозаводск, ул. Кирова, 65, г. Горнозаводск, ул. Свердлова, 59, р.п. Теплая Гора, ул. 1 Мая, 11, р.п. Промысла, ул. Комсомольская, 1, р.п. Кусье – Александровский, ул. Ленина,13, р.п. Пашия, ул. Ленина, 7, п. Вильва, ул. Пионерская, 6, р.п. Медведка, ул. Октябрьская, 15, п. Средняя Усьва, ул. Советская, 3, р.п. Бисер, ул. Советская, 23, р.п. Старый Бисер, ул. Ермакова, 1, р.п. Сараны, ул. Кирова, 19, а также разместить на официальном сайте администрации Горнозаводского городского округа (www.gornozavodskii.ru).

4. Контроль за исполнением настоящего постановления возложить на управляющего делами администрации Горнозаводского городского округа Шилову М.Г.

Глава городского округа - глава
администрации Горнозаводского
городского округа А.Н. Афанасьев

Подлинный экземпляр находится в администрации Горнозаводского городского округа Пермского края в деле № 01-07 за 2020 год

Шилова

D:\картотека\TXT\60783.doc 11

УТВЕРЖДЕНО
постановлением администрации
Горнозаводского городского округа
от 13.01.2020 № 12

ПОЛОЖЕНИЕ
по обеспечению безопасности информации в администрации Горнозаводского городского округа

I. Общие положения

1.1. Настоящее Положение устанавливает комплекс организационных, технических и правовых мер защиты информации.

1.2. Положение является обязательным для всех сотрудников администрации Горнозаводского городского округа (далее – администрация округа), осуществляющих обработку персональных данных и иной конфиденциальной информации.

1.3. Управляющий делами администрации округа, руководители структурных подразделений администрации округа организуют работу по обеспечению информационной безопасности и осуществляют контроль за соблюдением требований безопасности информации.

1.4. Термины и формулировки, использующиеся в настоящем Положении:

1.4.1. конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;

1.4.2. предоставление информации - действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц;

1.4.3. распространение информации - действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц;

1.4.4. электронное сообщение - информация, переданная или полученная пользователем информационно-телекоммуникационной сети;

1.4.5. документированная информация - зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель;

1.4.6. электронный документ - документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах;

1.4.7. оператор информационной системы - гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных;

1.4.8. система защиты информации – это совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты, организованная и функционирующая по правилам и нормам, устанавливаемыми соответствующими документами в области защиты информации;

1.4.9. техника защиты информации – это средства защиты информации, средства контроля эффективности защиты информации, средства и системы управления, предназначенные для обеспечения защиты информации;

1.4.10. средство криптографической защиты информации (далее - СКЗИ) – программа (служба), которая обеспечивает шифрование и расшифровку документов, отвечает за работу с электронной подписью. СКЗИ может быть встроена в носитель или представлена как отдельный программный продукт;

1.4.11. автоматизированное рабочее место (далее - АРМ) – рабочее место специалиста, оснащенное персональным компьютером, программным обеспечением и совокупностью информационных ресурсов индивидуального или коллективного пользования, которые позволяют ему вести обработку данных с целью получения информации, обеспечивающей поддержку принимаемых им решений при выполнении профессиональных функций;

1.4.12. информационная система (далее - ИС) – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

1.4.13. доступ к информации - возможность получения информации и ее использования;

1.4.14. несанкционированный доступ к информации – действия, нарушающие установленный порядок доступа или правила разграничения, установленные в администрации округа;

1.4.15. информационная безопасность – защищенность информации от ее перехвата, утечки по техническим и иным каналам, модификации, блокирования, уничтожения, несанкционированного доступа к ней, а также защищенность технических и программных средств сбора, обработки, накопления, хранения, поиска и передачи информации, информационных и телекоммуникационных систем от нарушения их функционирования или от вывода их из строя;

1.4.16. системный администратор – специалист администрации округа, обеспечивающий эксплуатацию АРМ;

1.4.17. средства защиты информации – программные, технические, программно-технические средства, предназначенные для защиты информации;

1.4.18. матрица доступа - таблица, отображающая правила разграничения доступа.

1.5. Допуск пользователей ИС для работы с конфиденциальными данными, находящимися в ИС, осуществляется в соответствии со списком лиц, допущенных к работе, утвержденным актом администрации округа.

1.6. Вход пользователя ИС в ИС осуществляется на основе ввода (по запросу системы) личных пароля и электронного идентификатора конкретного пользователя ИС.

1.7. Правами администратора в операционной системе АРМ может обладать только системный администратор администрации округа.

II. Цели и основные меры по защите информации

Целями по защите информации являются:

2.1. информирование сотрудников администрации о мерах и требованиях по защите информации;

2.2. соблюдение конфиденциальности информации ограниченного доступа;

2.3. обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

2.4. обеспечение реализации права граждан о не разглашении их персональных данных;

2.5. информационная безопасность в администрации обеспечивается средствами защиты информации и комплексом организационных и технических мер.

2.6. К организационным мерам относятся:

2.6.1. организация охранного режима на территории администрации;

2.6.2. контроль за соблюдением сотрудниками должностных инструкций и иной документации в сфере обеспечения информационной безопасности;

2.6.3. своевременное информирование сотрудников об изменениях законодательства в сфере обеспечения информационной безопасности;

2.6.4. назначение должностных лиц, ответственных за организацию работы по обеспечению информационной безопасности;

2.6.5. применение утвержденной в установленном порядке эксплуатационной документации;

2.6.6. соблюдение установленных правил обеспечения безопасности информации при работе с программными и техническими средствами, в том числе со средствами защиты информации и антивирусной защиты в администрации округа;

2.6.7. разграничение доступа к файлам, каталогам и дискам;

2.6.8. разграничение доступа к комплексам программ;

2.6.9. идентификация пользователей.

2.7. К техническим мерам относятся:

Применение сертифицированных специальных и лицензионных программных средств общего назначения, а также сертифицированных технических средств и средств связи.

III. Соблюдение мер защиты информации при использовании средств автоматизации

3.1. Защита информации, содержащейся в информационной системе:

3.1.1. Для обеспечения защиты информации, содержащейся в ИС, проводятся следующие мероприятия:

3.1.1.1. формирование требований к защите информации, содержащейся в ИС;

3.1.1.2. разработка системы защиты информации ИС;

3.1.1.3. внедрение системы защиты информации ИС;

3.1.1.4. аттестация информационной системы по требованиям защиты информации (далее - аттестация информационной системы) и ввод ее в действие;

3.1.1.5. обеспечение защиты информации, в ходе эксплуатации аттестованной ИС;

3.1.1.6. обеспечение защиты информации при выводе из эксплуатации аттестованной ИС или после принятия решения об окончании обработки информации.

3.1.2. При принятии решения о необходимости защиты информации, содержащейся в ИС, осуществляется:

3.1.2.1. анализ целей создания ИС и задач, решаемых этой ИС;

3.1.2.2. определение информации, подлежащей обработке в ИС;

3.1.2.3. анализ нормативных правовых актов, методических документов и национальных стандартов, которым должна соответствовать ИС;

3.1.2.4. принятие решения о необходимости создания системы защиты информации ИС, а также определение целей и задач защиты информации в ИС, основных этапов создания системы защиты информации ИС и функций по обеспечению защиты информации, содержащейся в ИС, обладателя информации (заказчика), оператора и уполномоченных лиц.

3.1.3. Разработка и внедрение системы защиты информации ИС.

Требования к системе защиты информации ИС включаются в техническое задание на создание ИС и (или) техническое задание (частное техническое задание) на создание системы защиты информации ИС, разрабатываемые с учетом ГОСТ 34.602, ГОСТ Р 51583 и ГОСТ Р 51624, и должны в том числе содержать:

цель и задачи обеспечения защиты информации в ИС;

класс защищенности ИС;

перечень нормативных правовых актов, методических документов и национальных стандартов, которым должна соответствовать ИС;

перечень объектов защиты ИС;

требования к мерам и средствам защиты информации, применяемым в ИС;

стадии (этапы работ) создания системы защиты ИС;

требования к поставляемым техническим средствам, программному обеспечению, средствам защиты информации;

функции заказчика и оператора по обеспечению защиты информации в ИС;

требования к защите средств и систем, обеспечивающих функционирование ИС (обеспечивающей инфраструктуре);

требования к защите информации при информационном взаимодействии с иными ИС и информационно-телекоммуникационными сетями, в том числе с ИС уполномоченного лица, а также при применении вычислительных ресурсов (мощностей), предоставляемых уполномоченным лицом для обработки информации.

3.1.4. Угрозы безопасности информации определяются по результатам оценки возможностей (потенциала) внешних и внутренних нарушителей, анализа возможных уязвимостей ИС, возможных способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации (конфиденциальности, целостности, доступности).

3.1.5. Требования к системе защиты информации ИС определяются в зависимости от класса защищенности ИС и угроз безопасности информации, включенных в модель угроз безопасности информации.

3.2. Основные функциональные обязанности пользователя ИС:

3.2.1. Пользователь ИС обязан:

3.2.1.1. знать и выполнять требования действующих нормативных правовых актов и руководящих документов, а также Положение по обеспечению безопасности информации в администрации округа, регламентирующих порядок действий по обеспечению безопасности информации;

3.2.1.2. выполнять на АРМ только те процедуры, которые определены для него его обязанностями;

3.2.1.3. соблюдать правила при работе в сетях общего доступа и (или) международного обмена – сети «Интернет» и других;

3.2.1.4. экран монитора в помещении располагать во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на нем информацией посторонними лицами;

3.2.1.5. обо всех выявленных нарушениях, связанных с информационной безопасностью, а также для получения консультаций по вопросам информационной безопасности, необходимо обратиться к лицу, ответственному за обеспечение информационной безопасности, в отношении которой установлено требование об обеспечении ее конфиденциальности (далее – администратор безопасности информации).

3.2.2. Для получения консультаций по вопросам работы и настройки элементов ИС, связанных с обеспечением безопасности, необходимо обращаться к администратору безопасности информации.

3.2.3. При отсутствии визуального контроля за рабочей станцией доступ к компьютеру должен быть немедленно заблокирован. Для этого необходимо нажать комбинацию клавиш «Win»+«L», либо комбинацию клавиш «Ctrl»+«Alt»+«Del» и выбрать опцию «Блокировка», либо заблокировать доступ иным способом, предусмотренным в операционной системе.

3.2.4. При использовании планировщика заданий состав запускаемого программного обеспечения на рабочем месте согласовывается с администратором безопасности информации.

3.2.5. В пределах, возложенных на него функций, принимать меры по реагированию в случае возникновения внештатных ситуаций и аварийных ситуаций с целью ликвидации их последствий.

3.2.6. По окончании работы в ИС выйти из системы и выключить компьютер.

3.2.7. Пользователям ИС запрещается:

3.2.7.1. разглашать информацию, в отношении которой установлено требование об обеспечении ее конфиденциальности, третьим лицам;

3.2.7.2. копировать информацию, в отношении которой установлено требование об обеспечении ее конфиденциальности, на внешние носители без разрешения своего руководителя;

3.2.7.3. самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств;

3.2.7.4. несанкционированно открывать общий доступ к каталогам на своем АРМ;

3.2.7.5. подключать к АРМ и корпоративной информационной сети личные отчуждаемые машинные носители и мобильные устройства;

3.2.7.6. отключать (блокировать) средства защиты информации;

3.2.7.7. обрабатывать на АРМ информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя ИС по доступу к ИС;

3.2.7.8. сообщать (или передавать) посторонним лицам личные ключи и атрибуты доступа к ресурсам ИС;

3.2.7.9. привлекать посторонних лиц для осуществления ремонта или настройки АРМ без согласования с администратором безопасности информации;

3.2.7.10. сообщать, передавать, распространять кому-либо личный пароль;

3.2.7.11. производить запись паролей на бумажные и иные неучтенные носители информации.

3.3. Организация парольной защиты:

3.3.1. В соответствии с Матрицей доступа системный администратор:

3.3.1.1. осуществляет ведение журнала выдачи паролей доступа к АРМ администрации округа (приложение 1 к настоящему Положению) и назначает для каждого пользователя администрации округа уникальные имя пользователя

(логин) и пароль для авторизации в операционной системе АРМ. Хранение журнала должно осуществляться в запираемом металлическом сейфе;

3.3.1.2. в операционной системе АРМ создает учетную запись ответственного специалиста и, в соответствии с Матрицей доступа, задает параметры доступа к информационным ресурсам;

3.3.1.3. проверяет на АРМ заданные возможности доступа для каждого ответственного специалиста.

3.3.2. Полная плановая смена паролей в ИС проводится не реже одного раза в 3 месяца.

3.3.3. Во время ввода пароля необходимо исключить возможность его просматривания посторонними лицами или техническими средствами (видеокамеры и др.).

3.3.4. Правила хранение пароля:

3.3.4.1. запрещается записывать пароль на бумаге, в файле, электронной записной книжке и других носителях информации, в том числе на предметах;

3.3.4.2. запрещается сообщать другим пользователям ИС личный пароль и регистрировать их в системе под своим паролем;

3.3.4.3. лица, использующие паролирование, обязаны знать и выполнять требования настоящего Положения;

3.3.4.4. своевременно сообщать администратору безопасности информации об утере, компрометации, несанкционированном изменении паролей и несанкционированном изменении сроков действия паролей.

3.4. Требования по обеспечению безопасности с использованием СКЗИ:

3.4.1. СКЗИ, находящиеся в эксплуатации, должны подвергаться контрольным тематическим исследованиям, конкретные сроки, проведения которых определяются заказчиком СКЗИ по согласованию с разработчиком СКЗИ, специализированной организацией и Федеральной службой безопасности России.

3.4.2. СКЗИ и их опытные образцы подлежат поэкземплярному учету с использованием индексов или условных наименований и регистрационных номеров.

3.4.3. Контроль за соблюдением правил пользования СКЗИ и условий их использования, указанных в правилах пользования на них, осуществляется:

обладателем, пользователем (потребителем) защищаемой информации, установившим режим защиты информации с применением СКЗИ;

собственником (владельцем) информационных ресурсов (информационных систем), в составе которых применяются СКЗИ.

3.4.4. Эксплуатация СКЗИ должна осуществляться в соответствии с документацией на СКЗИ и требованиями, установленными в настоящем Положении, а также в соответствии с иными нормативными правовыми актами, регулирующими отношения в соответствующей области.

3.4.5. Хранение криптографических ключей должно осуществляться в запираемых сейфах (металлических шкафах).

3.4.6. Размещение, специальное оборудование, охрана и организация режима на рабочих местах сотрудников использующих СКЗИ должны исключить возможность неконтролируемого проникновения или пребывания в них посторонних лиц, а также просмотра посторонними лицами ведущихся там работ.

3.5. Обязанности пользователя ИС по обеспечению антивирусной защиты:

3.5.1. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажение данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) пользователь ИС самостоятельно или вместе с администратором безопасности информации должен провести внеочередной антивирусный контроль своего АРМ.

3.5.2. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователи ИС обязаны:

3.5.2.1. приостановить работу;

3.5.2.2. немедленно поставить в известность о факте обнаружения зараженных вирусом файлов администратора безопасности информации, владельца зараженных файлов, а также смежные подразделения, использующие эти файлы в работе;

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

3.5.2.4. провести лечение или уничтожение зараженных файлов (для выполнения требований данного пункта при необходимости привлечь администратора безопасности информации).

3.5.3. В случае обнаружения нового вируса, не поддающегося лечению применяемыми антивирусными средствами, передать зараженный вирусом файл в организацию, с которой заключен договор на антивирусную поддержку.

3.5.4. По факту обнаружения зараженных вирусом файлов составить служебную записку, в которой необходимо указать предположительный источник (отправителя, владельца и т.д.) зараженного файла, тип зараженного файла, характер содержащейся в файле информации, тип вируса и выполненные антивирусные мероприятия.

3.5.5. При необходимости пополнения базы ИС данными, полученными со стороны с помощью съемных носителей, контролировать отсутствие вирусного заражения информации на съемном носителе.

3.5.6. Периодически, не реже одного раза в неделю, проводить проверку антивирусом на наличие вирусного заражения.

3.5.7. Следить за тем, чтобы антивирус был все время включен, а также следить за своевременным обновлением антивирусных баз.

IV. Соблюдение мер защиты информации без использования средств автоматизации

4.1. Основные требования по обеспечению информационной безопасности.

4.1.1. Шторы на оконных проемах должны быть завешаны (жалюзи закрыты).

4.1.2. При отсутствии сотрудника на рабочем месте должны соблюдаться следующие условия:

4.1.2.1. помещение, в котором находится рабочее место, следует плотно запирать на ключ;

4.1.2.2. на рабочих местах не должно оставаться материальных носителей, содержащих информацию, в отношении которой установлено требование об обеспечении ее конфиденциальности.

4.1.3. Сотрудники ответственные за помещения, в которых размещается оборудование, предназначенное для обработки сведений конфиденциального характера, должны исключать возможность бесконтрольного проникновения в них посторонних лиц, а также обеспечивать сохранность оборудования, машиночитаемых носителей информации и документов.

4.1.4. Лица для проведения регламентных (наладочных), ремонтных и других работ в эти помещения во время обработки конфиденциальной сведений конфиденциального характера могут быть допущены только в экстренных случаях по согласованию с управляющим делами администрации округа, руководителями структурных подразделений администрации округа и в присутствии ответственного специалиста при условии исключения несанкционированного доступа к персональным данным и иной информации конфиденциального характера и контроля за порядком осуществления проводимых работ.

4.2. Организация обработки персональных данных и иной конфиденциальной информации, осуществляемой без использования средств автоматизации.

При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее - типовая форма), должны соблюдаться следующие условия:

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

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

4.2.2. Типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации, - при необходимости получения письменного согласия на обработку персональных данных.

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

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

V. Порядок работы с носителями конфиденциальной информации

5.1. Перед началом использования служебного носителя информации ответственный специалист заносит информацию о носителе в журнал учета съемных носителей информации (приложение 2 к настоящему Положению).

5.2. Учет носителей конфиденциальной информации осуществляется ответственными специалистами в журнале регистрации носителей информации, содержащих персональные данные и иную конфиденциальную информацию (приложение 3 к настоящему Положению).

5.3. Документы на бумажных носителях информации, содержащие персональные данные или иную конфиденциальную информацию, подлежат обязательному поэкземплярному учету. Учет осуществляется ответственными специалистами в журнале учета документов, имеющих конфиденциальный характер (приложение 4 к настоящему Положению).

5.4. Хранение персональных данных и иной конфиденциальной информации работников администрации осуществляется на съемном жестком диске, хранимом в сейфе, металлическом шкафу.

5.5. Передача носителей конфиденциальной информации должна сопровождаться соответствующими актами приема-передачи, в которых в обязательном порядке указывается регистрационный номер передаваемого носителя конфиденциальной информации.

5.6. Акты передачи носителей конфиденциальной информации составляются в двух экземплярах.

5.7. Для уничтожения конфиденциальной информации (носителей конфиденциальной информации) распоряжением администрации округа должна

быть создана постоянно действующая комиссия по уничтожению персональных данных и иной конфиденциальной информации.

5.8. По факту уничтожения комиссией по уничтожению персональных данных и иной конфиденциальной информации составляется акт уничтожения персональных данных и иной конфиденциальной информации, находящейся на АРМ (приложение 5 к настоящему Положению).

5.9. По факту уничтожения комиссией по уничтожению персональных данных и иной конфиденциальной информации составляется акт уничтожения персональных данных и иной конфиденциальной информации, находящейся на бумажном носителе (приложение 6 к настоящему Положению).

VI. Правила работы в сетях общего доступа и (или) международного обмена

6.1. Работа в сетях общего доступа и (или) международного обмена (сети «Интернет» и других) (далее – Сеть) на элементах ИС должна проводиться при служебной необходимости.

6.2. При работе в Сети запрещается:

6.2.1. осуществлять работу при отключенных средствах защиты (антивирус и другие);

6.2.2. передавать по Сети информацию, в отношении которой установлено требование об обеспечении ее конфиденциальности, без использования средств шифрования;

6.2.3. скачивать из Сети программное обеспечение и другие файлы;

6.2.4. посещать сайты сомнительной репутации (сайты, содержащие нелегально распространяемое программное обеспечение, и другие);

6.2.5. Нецелевое использование подключения к Сети.

VII. Порядок учета и хранения резервных копий баз данных программ, в которых осуществляется обработка персональных данных

7.1. Работы по формированию резервных копий баз данных программ осуществляются системным администратором или ответственными специалистами.

7.2. Резервное копирование баз данных должно осуществляться только на предварительно учтенные в установленном порядке носители конфиденциальной информации.

7.3. Все факты резервного копирования баз данных на соответствующих АРМ должны фиксироваться системным администратором и/или ответственным специалистом в журнале учета резервных копий баз данных (приложение 7 к настоящему Положению).

XIII. Порядок действий в случае выявления нарушений информационной безопасности

8.1. выявление факта нарушения;

8.2. прекращение всех операций, связанных с участком, на котором произошло нарушение;

8.3. принятие экстренных мер для прекращения несанкционированного доступа или использования информации;

8.4. оповещение управляющего делами администрации округа, руководителей структурных подразделений и системного администратора о нарушении;

8.5. восстановление работоспособности информационной системы;

8.6. расследование причин нарушения информационной безопасности;

8.7. проверка состояния информационной безопасности по факту нарушения.

IX. Ответственность

Лица, виновные в нарушении положений законодательства Российской Федерации в области персональных данных при обработке персональных данных, привлекаются к ответственности в соответствии с действующим законодательством.

Приложение 1
к Положению по обеспечению безопасности информации в администрации Горнозаводского городского округа

Журнал выдачи паролей доступа к АРМ администрации Горнозаводского городского округа

№ п/п	АРМ №	Имя пользователя в операционной системе АРМ (логин)	Ф.И.О. ответственного специалиста	Должность/ подразделение	Дата выдачи пароля	Пароль в операционной системе АРМ	Роспись ответственного специалиста в получении пароля	Роспись лица, производившего выдачу пароля
1	2	3	4	5	6	7	8	9

Приложение 2
к Положению по обеспечению безопасности информации в администрации Горнозаводского городского округа

Журнал учета съемных носителей информации

№ п/п	Дата начала использования носителя информации	Ф.И.О. ответственного специалиста	Тип носителя информации	Номер носителя информации	Дата окончания использования носителя информации
1	2	3	4	5	6

Приложение 3
к Положению по обеспечению безопасности информации в администрации Горнозаводского городского округа

Журнал регистрации носителей информации, содержащих персональные данные и иную конфиденциальную информацию

№ п/п	Дата поступления носителя	Регистрационный номер носителя	Содержание	Прием (поступление) носителя				Учетный номер носителя	Передача носителя		Дата и номер акта уничтожения	ФИО	
				Откуда поступил	Вид носителя	Количество листов	Дата и номер сопроводительного документа		Кому передан носитель	Дата и номер сопроводительного документа		передавшего	получившего
1	2	3	4	5	6	7	8	9	10	11	12	13	14

Примечания:
1. Данный журнал должен быть учтен;
2. Страницы пронумерованы, прошиты и опечатаны (опломбированы).

Приложение 4
к Положению по обеспечению безопасности
информации в администрации
Горнозаводского городского округа

Журнал учета документов, имеющих конфиденциальный характер

№ п/п	Наименование документа	Регистрационный номер	Дата регистрации	Количество листов
1	2	3	4	5

Приложение 5
к Положению по обеспечению безопасности
информации в администрации
Горнозаводского городского округа

АКТ
уничтожения персональных данных и иной конфиденциальной информации, находящейся на АРМ

«_____»_____ 20___ г.

Председатель комиссии _____
(Ф.И.О.)

Члены комиссии _____
(Ф.И.О.)

_____
(Ф.И.О.)

_____
(Ф.И.О.)

составили настоящий акт в том, что «_____»_____ 20___ г. произведено уничтожение персональных данных или иной конфиденциальной информации,

находящейся на:

_____
(указывается тип носителя информации)

регистрационный номер носителя информации:

_____
(указывается регистрационный номер носителя информации)

способ уничтожения информации:

_____
(указывается способ уничтожения информации)

Председатель комиссии _____
(Ф.И.О.)

Члены комиссии _____
(Ф.И.О.)

_____
(Ф.И.О.)

_____
(Ф.И.О.)

Приложение 6
к Положению по обеспечению безопасности
информации в администрации
Горнозаводского городского округа

АКТ
уничтожения персональных данных и иной конфиденциальной информации, находящейся на бумажном носителе

«_____»_____ 20___ г.

Председатель комиссии _____
(Ф.И.О.)

Члены комиссии _____
(Ф.И.О.)

_____
(Ф.И.О.)

_____
(Ф.И.О.)

составили настоящий акт в том, что «_____»_____ 20___ г. произведено уничтожение персональных данных или иной конфиденциальной информации.

способ уничтожения информации:

_____
(указывается способ уничтожения информации)

Председатель комиссии _____
(подпись)

Члены комиссии _____
(подпись)

_____
(подпись)

_____
(подпись)

Приложение 7
к Положению по обеспечению безопасности информации в администрации Горнозаводского городского округа

Журнал учета резервных копий баз данных

№ п/п	Дата создания резервной копии	Название АРМ, путь к файлам	Тип резервной копии	Регистрационный номер носителя конфиденциальной информации	Путь к файлам резервной копии	Ф.И.О. ответственного лица	Подпись ответственного лица	Примечание
1	2	3	4	5	6	7	8	9