Приложение 1
к распоряжению администрации города
от 22.11.2019 №337

# ПОЛИТИКА
## в области обеспечения безопасности персональных данных в администрации города Мегиона

1.Общие положения.

1.1.В целях обеспечения безопасности персональных данных (далее - ПДн) при их обработке в информационных системах персональных данных (далее - ИСПДн) администрации города Мегиона (далее - администрация города), в соответствии с требованиями Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных», определяется политика в области обеспечения безопасности ПДн, содержащая основные правила и порядок обработки ПДн граждан и сотрудников администрации города.

1.2.Политика заключается в выполнении требований и норм обработки ПДн, установленных в Постановлении Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

2.Лица, ответственные за обеспечение безопасности ПДн.

2.1.В администрации города назначаются следующие ответственные лица:

2.1.1.Ответственный за организацию работ по обеспечению безопасности ПДн, на которого Распоряжением главы города возлагается:

утверждение списка лиц, доступ которых к ПДн необходим для выполнения служебных (трудовых) обязанностей, а также изменений к нему;

принятие решения о распространении (передаче) ПДн;

проведение разбирательств по фактам несоблюдения условий хранения носителей ПДн, использования средств защиты информации (далее - СЗИ), которые могут привести к нарушению конфиденциальности ПДн или другим нарушениям, приводящим к снижению уровня защищенности ПДн;

приостановка предоставления ПДн пользователям информационной системы при обнаружении нарушений порядка предоставления ПДн;

руководство работами по обеспечению безопасности ПДн при их обработке в ИСПДн.

2.1.2.Администратор информационной безопасности (далее – администратор ИБ), ответственный за выполнение работ по обеспечению безопасности ПДн, на которого Распоряжением главы города возлагается:

организация парольной защиты;

организация криптографической защиты ПДн;

организация учета средств защиты информации, эксплуатационной и технической документации к ним;

администрирование средств и систем защиты ПДн в ИСПДн, включая средства антивирусной защиты (за исключением средств криптографической защиты информации);

учет лиц, допущенных к работе с ПДн в информационных системах;

учет носителей ПДн, используемых в ИСПДн (как с использованием средств автоматизации, так и без их использования);

периодическая (не реже одного раза в квартал) проверка электронного журнала обращений пользователей информационных систем к ПДн;

инструктаж пользователей ИСПДн о порядке и правилах использования СЗИ, включая средства антивирусной защиты;

контроль за соблюдением условий использования СЗИ (за исключением средств криптографической защиты информации).

3.Организация резервирования и восстановления программного обеспечения (далее - ПО), баз ПДн ИСПДн.

3.1.В ИСПДн резервированию подлежат:

базы ПДн;

специальное ПО;

СЗИ;

общее ПО;

средства вычислительной техники;

средства обеспечения функционирования информационных систем.

3.2.Резервные носители ПДн хранятся в подразделении, эксплуатирующем ИСПДн.

3.3.Резервные носители ПДн не могут быть переданы за пределы подразделения, эксплуатирующего ИСПДн.

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

3.5.Резервирование общего и прикладного ПО, а также ПО СЗИ обеспечивается путем хранения машинных носителей дистрибутивов данных программ и машинных носителей обновлений к ним в подразделениях, отвечающих за их установку, настройку и сопровождение.

3.6.В случаях сбоев, отказов и аварий технических средств и систем ИСПДн, а также ее ПО осуществляется обязательное восстановление работоспособности ИСПДн.

4.Учет лиц, допущенных к работе с ПДн в ИСПДн.

4.1.Лица, допущенные к работе с ПДн в ИСПДн утверждаются соответствующим Актом, подписанным главой города.

4.2.Основанием для допуска сотрудника к ПДн, обрабатываемым в ИСПДн, является необходимость обработки ПДн в связи с выполнением должностных обязанностей, а также соответствующее Распоряжение, утвержденное главой города.

4.3.Основанием для прекращения допуска сотрудника к ПДн, обрабатываемым в ИСПДн, может служить приказ об его увольнении (переводе на другую должность, не требующую работы с ПДн) и при исчезновении необходимости работы сотрудника с ПДн.

5.Организация парольной защиты в ИСПДн.

5.1. Защите паролем подлежит доступ к:

базовым системам ввода вывода компьютеров;

настройкам сетевого оборудования;

настройкам операционных систем;

настройкам СЗИ (в том числе средств антивирусной защиты);

запуску специализированного ПО, предназначенного для обработки ПДн;

ресурсам автоматизированного рабочего места (далее - АРМ) и баз данных ИСПДн.

5.2.Базовые системы ввода вывода, сетевое оборудование, операционные системы, СЗИ и файловые массивы (далее – объекты парольной защиты) должны быть настроены таким образом, чтобы:

исключить возможность просмотра ранее вводимых паролей;

блокировать доступ пользователей после пятикратной ошибки при вводе пароля и сигнализировать о наступлении данного события.

5.3.Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах ИСПДн и контроль за действиями пользователей при работе с паролями возлагается на сотрудников Муниципального бюджетного учреждения Мегионского центра информационно-коммуникационных технологий «Вектор».

5.4.Пользователь обязан запомнить личные пароли и никому их не передавать, и не записывать их на местах, где их могут увидеть другие лица.

5.5.Информация о паролях пользователей является информацией ограниченного доступа, предназначенной для идентификации и доступа каждого конкретного пользователя к ресурсам ИСПДн согласно разрешительной системы доступа.

5.6.Запрещено:

умышленное и неумышленное ознакомление с парольной информацией сотрудников и посторонних лиц независимо от их должности;

передача личного пароля другим работникам или посторонним лицам;

запись личного пароля на бумагу и хранение его в потенциально доступном для ознакомления посторонними лицами и другими сотрудниками месте;

вход в систему с использованием чужих идентификаторов или паролей;

оставление без присмотра рабочего места при работе в ИСПДн.

5.7.Владельцы паролей должны быть ознакомлены под роспись с Инструкцией по организации парольной защиты и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

5.8. Контроль за действиями пользователей системы при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на администратора ИБ.

6.Антивирусная защита в ИСПДн.

6.1.К использованию в ИСПДн допускаются только лицензионные и сертифицированные по требованиям безопасности информации антивирусные средства.

6.2.Установка и настройка средств антивирусного контроля на компьютерах осуществляется в соответствии с руководствами по применению конкретных антивирусных средств.

6.3.Обязательному антивирусному контролю подлежит любая информация на съемных носителях. Разархивирование и контроль входящей информации необходимо проводить непосредственно после ее приема. Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

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

6.5.Устанавливаемое (изменяемое) ПО должно быть предварительно проверено на отсутствие вирусов. Непосредственно после установки (изменения) ПО, должна быть выполнена антивирусная проверка на всех компьютерах ИСПДн.

6.6.При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) сотрудник подразделения самостоятельно должен провести внеочередной антивирусный контроль своего компьютера.

6.7.Ответственность за организацию антивирусного контроля в соответствии с требованиями настоящей Инструкции возлагается на сотрудников отдела развития информационного общества и муниципальных услуг.

6.8.Ответственность за проведение мероприятий антивирусного контроля и соблюдение требований настоящей Инструкции возлагается на сотрудников отдела развития информационного общества и муниципальных услуг, и всех сотрудников, являющихся пользователями ИСПДн.

6.9.Периодический контроль за состоянием антивирусной защиты в ИСПДн, а также за соблюдением установленного порядка антивирусного контроля и выполнением требований по антивирусной защите осуществляется ответственным за организацию работ по обеспечению безопасности ПДн при их обработке в ИСПДн.

7. Перечень ПДн, обрабатываемых в ИСПДн и подлежащих защите:

любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе:

фамилия;

имя;

отчество;

год рождения;

месяц рождения;

дата рождения;

место рождения;

адрес;

образование;

профессия;

семейное положение;

свидетельство о заключении (расторжении) брака;

свидетельство о рождении ребенка (детей);

социальное положение;

гражданство;

трудовая книжка;

период работы в организации;

должность;

доходы;

расходы;

фотография;

контактный номер телефона;

электронная почта;

сведения о документе, удостоверяющем личность;

реквизиты ИНН, СНИЛС, пенсионного удостоверения, расчетных счетов;

военный билет;

диплом, в том числе документы о дополнительном образовании;

периоды временной нетрудоспособности;

информация о негосударственном пенсионном обеспечении;

состояние здоровья;

национальность;

причина смерти (медицинский диагноз);

пол, дата и место рождения ребенка (мертворожденный, живорожденный);

количество рожденных детей;

место жительства родителей;

сведения о документе, подтверждающем факт рождения ребенка;

сведения о документе, являющемся основанием для внесения сведений об отце - место работы, род занятий;

год проживания по месту жительства;

наименование органа записи актов гражданского состояния;

серия и номер свидетельства о заключении, расторжении брака и признании его недействительным;

решения суда о признании брака недействительным;

сведения об общих детях (добрачных);

дата прекращения брака;

занятие (специальность, должность, ремесло);

количество заключенных браков;

количество детей на иждивении;

имена и возраст детей;

соглашения родителей о содержании детей друг у друга;

реквизиты решения суда об усыновлении ребенка;
серия и номер свидетельства об усыновлении ребенка;
серия и номер выданного свидетельства о перемени имени;
последнее место жительства;
дата и место смерти умершего;
причина смерти;
реквизиты документа, подтверждающего факт смерти;
серия и номер свидетельства о смерти.

8.Порядок предоставления ПДн.

8.1.Распространение ПДн - действия, направленные на передачу ПДн определенному кругу лиц.

8.2.До передачи любых ПДн за пределы организации от каждого субъекта ПДн должно быть получено письменное согласие на распространение его ПДн, оформленное в соответствии с требованиями статьи 9 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных», в каждом конкретном случае.

8.3.В случае смерти субъекта ПДн согласие на обработку его ПДн дают в письменной форме наследники субъекта ПДн, если такое согласие не было дано субъектом ПДн при его жизни.

8.4.Решение на предоставление ПДн принимается ответственным за организацию обработки персональных данных.

8.5.ПДн, обрабатываемые в ИСПДн, могут быть предоставлены органам власти и органам местного самоуправления без согласия субъекта ПДн, если данные действия осуществляются в соответствии с федеральными законами Российской Федерации в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства. При этом решение на распространение ПДн должно содержать ссылку на соответствующую статью федерального закона Российской Федерации.

9.Порядок приостановки предоставления ПДн, в случае обнаружения нарушений порядка их предоставления, и порядок разбирательств по фактам, которые могут привести к нарушению конфиденциальности ПДн или другим нарушениям.

9.1.При обнаружении нарушений порядка предоставления ПДн предоставление ПДн пользователям информационной системы незамедлительно приостанавливается до выявления причин нарушений и устранения этих причин.

9.2.Принятие решения на приостановку обработки ПДн принимается ответственным за организацию обработки ПДн.

9.3.Основаниями для приостановки обработки ПДн в ИСПДн и проведения разбирательства являются:

выявление недостоверных ПДн в ИСПДн;
предоставление ПДн в нарушение установленных правил;
допуск к ИСПДн лица, не имеющего на то разрешения;
утрата носителя ПДн;
нарушение правил хранения носителей ПДн;
нарушение правил эксплуатации СЗИ;
нарушение правил парольной защиты;
нарушение правил антивирусной защиты;
нарушение правил резервирования и восстановления общего и специального ПО, а также баз ПДн;
выявление в ИСПДн вредоносных программ (вирусов);
выявление в электронных журналах СЗИ несанкционированных действий пользователей, нарушающих безопасность ПДн или целостность (неизменность) ПО ИСПДн;
выявление несанкционированного внесения изменений в состав технических средств и (или) ПО ИСПДн.

9.4.Разбирательство проводится комиссией или должностным лицом (работником), ответственным за обеспечение безопасности ПДн с обязательным привлечением руководителя структурного подразделения, осуществляющего эксплуатацию ИСПДн.

9.5.В ходе разбирательства составляется заключение, в котором отражается:

состав комиссии, проводившей разбирательство;

период времени, в который проводилось разбирательство;

основание для проведения разбирательства;

факты, выявленные в ходе разбирательства и имеющие значение в определении наличия нарушений конфиденциальности ПДн или нарушений правил использования СЗИ, а также иные факты, которые могут привести к нарушению конфиденциальности ПДн или к снижению уровня защищенности ПДн;

вывод о значимости нарушений, их причинах и виновных, допустивших данные нарушения;

рекомендации по совершенствованию обеспечения безопасности ПДн, исключающие в дальнейшем подобные нарушения.

9.6.Заключение представляется ответственному за организацию обработки ПДн, который принимает решение на возобновление обработки ПДн и принятие дополнительных мер защиты.

10.Порядок взаимодействия по вопросам обеспечения безопасности ПДн.

10.1.Взаимодействие по вопросам обеспечения безопасности ПДн может осуществляться с:

администрацией города Мегион;

организациями, оказывающими услуги по обеспечению безопасности ПДн, с действительными лицензиями на данный вид работ;

подведомственными учреждениями администрации города.

10.2.Взаимодействие по вопросам обеспечения безопасности ПДн с администрацией города осуществляется в части методического обеспечения и контроля, а также в целях определения единой стратегии и технической политики в области обеспечения безопасности ПДн. Методическое обеспечение в части методов и способов защиты информации в информационных системах осуществляется Федеральной службой по техническому и экспортному контролю и Федеральной службой безопасности Российской Федерации в пределах их полномочий.

10.3.Взаимодействие с организациями, оказывающими услуги по обеспечению безопасности ПДн, осуществляется на договорной основе. Такие организации в обязательном порядке должны иметь лицензию Федеральной службы по техническому и экспортному контролю на деятельность по технической защите конфиденциальной информации, а в случае оказания ими услуг в области криптографической защиты информации – лицензии Федеральной службы безопасности Российской Федерации.

10.4.Существенным условием договора с организацией, оказывающей услуги по обеспечению безопасности ПДн, является требование соблюдения конфиденциальности сведений о степени защищенности ИСПДн (внедренных методах и способах защиты и их эффективности).

10.5.Взаимодействие с подведомственными учреждениями администрации города осуществляется в части методического руководства и контроля за полнотой и эффективностью принятых мер обеспечения безопасности ПДн. Контрольные мероприятия в подведомственных учреждениях осуществляются ответственным за организацию работ по обеспечению безопасности ПДн и администратором ИБ, сотрудниками отдела развития информационного общества и муниципальных услуг департамента экономического развития администрации города Мегиона, осуществляющими работы по обеспечению безопасности ПДн.

Приложение 2
к распоряжению администрации города
от «___»_____2019 № ____

ПОЛОЖЕНИЕ
о порядке выявления и реагирования на инциденты информационной безопасности администрации города Мегион

1.Общие положения.

1.1.Настоящее Положение устанавливает порядок управления инцидентами (одним событием или группой событий), способными привести к сбоям или нарушению функционирования информационных систем администрации города Мегион (далее – администрация города) и (или) возникновению угроз безопасности конфиденциальной информации администрации города (далее – инциденты ИБ), а также регулирует порядок проведения служебного расследования нарушений режима служебной тайны (далее – служебное расследование) в администрации города.

1.2.Настоящее Положение разработано в соответствии с требованиями Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных», Федерального закона от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации», Инструкции по порядку обращения с конфиденциальной информацией в администрации города и подведомственных организациях, расположенных на территории городского округа город Мегион, принятой постановлением администрации города Мегиона от 01.11.2017 №2177 «О порядке обращения с конфиденциальной информацией».

1.3.Процесс управления инцидентами ИБ включает:

учет и регистрацию инцидентов ИБ;

оповещение ответственного лица о возникновении инцидентов ИБ;

расследование обнаруженных инцидентов ИБ;

устранение причин и последствий инцидентов ИБ;

определение плана корректирующих и превентивных мероприятий.

1.4.Требования настоящего Положения являются обязательными для выполнения всеми сотрудниками администрации города.

2.Учет и регистрация инцидентов информационной безопасности.

2.1.Для выявления инцидентов ИБ должны использоваться встроенные механизмы регистрации и учета событий безопасности операционных систем, систем управления базами данных, прикладного программного обеспечения и средств защиты информации, а также специализированные средства анализа защищенности информационных систем администрации города.

2.2.В обязательном порядке должны регистрироваться следующие события безопасности:

попытки входа (выхода) пользователей в операционную систему (из операционной системы);

загрузка и инициализация операционной системы и ее программного останова для рабочих станций и серверов;

попытка доступа к средствам виртуализации;

факт изменения конфигурации средств виртуализации;

запуск и остановка служб (системных сервисов) средств виртуализации;

попытки подключения к рабочим станциям и серверам мобильных устройств и внешних носителей информации.

2.2.В параметрах регистрации событий безопасности в обязательном порядке должны указываться следующие параметры:

тип события;

дата и время события;

результат события;

источник события;

идентификатор пользователя информационной системы, предъявленный при попытке доступа.

2.3.Хранение информации об инцидентах ИБ должно осуществляться в течение срока, достаточного для проведения служебного расследования.

2.4.Учет инцидентов ИБ осуществляется администратором информационной безопасности информационных систем администрации города (далее – администратор ИБ), назначенным Распоряжением главы города. Допускается ведение учета инцидентов ИБ в электронном виде.

2.5.При обнаружении инцидента администратор ИБ проводит его классификацию в соответствии с приложением к настоящему Положению. Инциденты ИБ и их последствия классифицируются по значимости на текущие, значимые и имеющие признаки преступления.

3.Порядок оповещения ответственного лица о возникновении инцидентов информационной безопасности.

3.1.Средства защиты информации должны обеспечивать возможность информирования администратора ИБ о критических событиях безопасности в информационной системе по электронной почте или посредством SMS.

3.2.В случае, если зафиксированный инцидент ИБ был классифицирован как «значимый» или «имеющий признаки компьютерного преступления», администратор ИБ обязан незамедлительно сообщить о выявленном инциденте ИБ ответственному за обеспечение безопасности конфиденциальной информации по электронной почте или иному средству связи.

3.3.Ответственный за обеспечение безопасности конфиденциальной информации должен провести внеплановый анализ выявленного инцидента ИБ и, в случае необходимости, инициировать процедуру служебного расследования в соответствии с порядком, установленным данным Положением.

4.Порядок расследования обнаруженных инцидентов информационной безопасности.

4.1.Проведение служебного расследования инициируется Поручением первого заместителя главы города. В этом же Поручении устанавливается состав Комиссии для проведения служебного расследования (далее – Комиссия).

4.2.Служебное расследование может быть возбуждено:

по решению первого заместителя главы города;

по инициативе любого сотрудника администрации города на основании служебной записки в произвольной форме на имя первого заместителя главы города;

по устному докладу.

4.3.В состав Комиссии входят следующие сотрудники администрации города:

председатель Комиссии – ответственный за организацию обработки ПДн;

ответственный за защиту информации;

администратор ИБ.

В случае необходимости Комиссия вправе привлекать к расследованию:

администратора информационных систем администрации города;

руководителя структурного подразделения, в котором произошел инцидент ИБ;

непосредственного руководителя сотрудника, в отношении которого проводится служебное расследование;

экспертов из других структурных подразделений и, при необходимости, представителей сторонних организаций.

4.4.Комиссия для проведения служебного расследования в рабочем порядке в максимально короткие сроки, привлекая все необходимые ресурсы, проводит служебное расследование.

Результаты работы Комиссии оформляются в виде аналитического экспертного заключения на имя главы города Мегион, с предложениями:

по внесению изменений в организационные и (или) технические меры по защите ПДн;

по внесению изменений и улучшений в комплект организационно-распорядительной документации администрации города;

по расширению или дополнению списка инцидентов ИБ, установленного данным Положением, если это необходимо.

4.5.В аналитическом экспертном заключении должен быть приведен перечень ответственных за выполнение запланированных работ и сроки выполнения запланированных работ. Материалы служебного расследования, его выводы и заключения могут быть использованы как основание для реализации уголовной, гражданской, административной или дисциплинарной ответственности, в порядке, определяемом действующим законодательством и локальными правовыми актами администрации города.

5.Устранение причин и последствий инцидентов информационной безопасности.

5.1.Для инициирования работ по устранению причин и последствий инцидентов ИБ ответственный за обеспечение безопасности конфиденциальной информации направляет аналитическое экспертное заключение по электронной почте первому заместителю главы города и ответственным за выполнение запланированных работ.

Если ответственный за выполнение запланированных работ не согласен с установленными сроками, он вправе обратиться к ответственному за обеспечение безопасности конфиденциальной информации с просьбой перенести срок с обоснованием причин переноса.

При изменении сроков реализации действий, ответственный за защиту информации вносит необходимые изменения в экспертное заключение и информирует о них по электронной почте ответственного за выполнение запланированных работ и первого заместителя главы города.

5.2.После реализации запланированных работ ответственное лицо должно направить по электронной почте ответственному за защиту информации подтверждение выполнения работ, не позднее срока реализации, установленного в экспертном заключении.

5.3.Ответственный за обеспечение безопасности конфиденциальной информации вправе запросить у назначенного лица информацию о выполнении в случае, если ему не поступило подтверждение выполнения работ в течение 3 (трех) рабочих дней с даты, установленной в экспертном заключении.

5.4.О результативности предпринятых корректирующих и превентивных мер свидетельствует отсутствие повторных инцидентов ИБ.

6.Ответственность.

6.1.Ответственность за проведение служебного расследования и за контроль своевременного и качественного выполнения работ по проведению корректирующих и превентивных мероприятий несет ответственный за обеспечение безопасности конфиденциальной информации.

6.2.Ответственность за обеспечение своевременной регистрации инцидентов ИБ несет администратор ИБ, назначенный Распоряжением администрации города.

6.3.Ответственность за выделение требуемых ресурсов (в том числе финансовых и трудовых) для реализации положений настоящего документа несет первый заместитель главы города, ответственный за вопросы разработки, принятия и внедрения мер защиты информации (далее – заместитель руководителя).

Приложение 3
к распоряжению администрации города
от «___»_____2019 № ____

ПЕРЕЧЕНЬ
инцидентов информационной безопасности администрации города Мегиона

| № п/п | Описание инцидента информационной безопасности |
|---|---|
| 1 | 2 |
| 1. Текущие нарушения | |
| 1.1. | Ошибка при регистрации в информационной системе: ввод неправильных персональных регистрационных данных (пароля, имени пользователя и т.п.) более трех раз подряд (однократная) |
| 1.2. | Периодические попытки неудачного доступа к объектам: компьютерам, принтерам, файлам, документам |
| 1.3. | Несанкционированный перевод времени на рабочей станции либо на других элементах информационной инфраструктуры администрации города |
| 1.4. | Выполнение производственных обязанностей с использованием компьютерного оборудования в нерабочее время |
| 1.5. | Оставление работающего (включенного) компьютерного оборудования без запущенного хранителя экрана в нерабочее время |
| 1.6. | Перезагрузка рабочей станции при сбоях в работе (однократная), в том числе аварийная перезагрузка путем нажатия кнопки горячей перезагрузки или полного отключения питания |
| 1.7. | Нецелевое использование элементов информационной инфраструктуры администрации города (печать, сервисы сети Интернет, электронная почта, и т.п.) |
| 2. Значимые нарушения | |
| 2.1. | Ошибка при регистрации в информационной системе: ввод неправильных персональных регистрационных данных (пароля, имени пользователя и т.п.) более трех раз подряд (многократная) |
| 2.2. | Неоднократное оставление работающего (включенного) компьютерного оборудования без запущенного хранителя экрана в нерабочее время |
| 2.3. | Утрата учтенного магнитного, оптического или иного носителя конфиденциальной информации |
| 2.4. | Утрата носителя информации с резервной копией |
| 2.5. | Неудачная попытка регистрации в информационной системе под чужими регистрационными данными (именем пользователя, паролем и т.п.) (многократная) |
| 2.6. | Удачная попытка регистрации в информационной системе под чужими регистрационными данными (именем пользователя, паролем и т.п.) |
| 2.7. | Нерегламентированная очистка журналов событий безопасности информационных систем администрации города |
| 2.8. | Нерегламентированное подключение неучтенных внутренних и (или) периферийных устройств и носителей информации |

| 1 | 2 |
|---|---|
| 2.9. | Нерегламентированное изменение аппаратной конфигурации компьютерного оборудования |
| 2.10. | Нерегламентированное копирование информации (файлов) на флеш-накопители или иные внешние носители информации, а также нерегламентированная передача подобной информации с использованием сервисов электронной почты, мгновенных сообщений (ICQ и т.п.) и других сервисов сети Интернет |
| 2.11. | Нерегламентированная установка (удаление) прикладного программного обеспечения, не разрешенного к использованию на рабочих станциях и серверах администрации города |
| 2.12. | Попытка получения привилегированного доступа к рабочей станции или к другим ресурсам информационных систем администрации города (повышение уровня прав доступа, получение прав на отладку программ и т.п.) |
| 2.13. | Заражение программного обеспечения рабочих станций и серверов вредоносным кодом (непреднамеренное) |
| 2.14. | Нерегламентированное использование сканирующего (на различные уязвимости) программного обеспечения |
| 2.15. | Нерегламентированное использование анализаторов протоколов (снифферов) |
| 2.16. | Нерегламентированный просмотр, вывод на печать, передача третьим лицам сведений, содержащих конфиденциальные данные (информацию, подлежащую защите) |
| 2.17. | Несанкционированное проведение обновления версий системного и прикладного программного обеспечения |
| 3. Нарушения, имеющие признаки преступления | |
| 3.1. | Несанкционированное получение привилегированного доступа к любым элементам информационной инфраструктуры администрации города |
| 3.2. | Несанкционированное изменение конфигурации элементов информационной инфраструктуры администрации города |
| 3.3. | Утрата резервных копий |
| 3.4. | Утечка конфиденциальной информации (баз данных информационных систем и др.) |
| 3.5. | Подозрение в умышленном нарушении работоспособности информационной сети администрации города, элементов информационной инфраструктуры администрации города, системного и прикладного программного обеспечения |
| 3.6. | Юридически необоснованная передача (распространение) конфиденциальной информации |
| 3.7. | Несанкционированное внесение изменений в базы данных информационных систем администрации города |
| 3.8. | Несанкционированное уничтожение конфиденциальной информации |
| 3.9. | Проведение обновления версии информационных систем администрации города (равно как и другого программного обеспечения), повлекшее за собой потерю конфиденциальной информации |
| 3.10. | Намеренное заражение информационных систем администрации города вредоносным кодом |

Приложение 4
к распоряжению администрации города
от «___»_____2019 № ____

# ИНСТРУКЦИЯ
## пользователя информационных систем персональных данных

1.Общие положения.

1.1.Настоящий документ разработан в соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», а также другими документами по безопасности информации, и определяет порядок обеспечения информационной безопасности при проведении работ пользователями информационных систем персональных данных (далее – ИСПДн) администрации города Мегиона (далее – администрации города).

1.2.Субъектами доступа к ресурсам ИСПДн являются администратор безопасности (далее – АБ), пользователи и обслуживающий персонал.

1.3.Обрабатываемая в ИСПДн информация относится к сведениям, составляющим персональные данные (далее – ПДн).

1.4.Машинные носители с персональными данными имеют пометку «ПДн».

1.5.Пользователи получают свои права на доступ к ресурсам ИСПДн через администратора ИБ.

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

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

2.Пользователь обязан:

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

2.2.Выполнять на автоматизированном рабочем месте (далее - АРМ) только те процедуры и функции, которые предусмотрены ИСПДн, к которым у пользователя предоставлен доступ согласно Журналу учета допуска к работе пользователей информационной системы персональных данных.

2.3.Знать и соблюдать установленные требования к обработке ПДн, учету и хранению носителей информации, обеспечению безопасности ПДн, а также руководящих и организационно-распорядительных документов.

2.4.Соблюдать требования парольной политики в соответствии с Инструкцией по организации парольной защиты.

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

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

2.7.При возникновении подозрения на наличие вредоносного программного обеспечения (частые ошибки в работе программ, появление посторонних графических и звуковых эффектов, искажения данных, неконтролируемое пропадание файлов, появление сообщений о системных ошибках, замедление работы компьютера и т.п.) самостоятельно или вместе с АБ ИСПДн провести внеочередной антивирусный контроль своего АРМ. При

самостоятельном проведении антивирусного контроля - уведомить о результатах АБ ИСПДн для определения им факта наличия или отсутствия вредоносного программного обеспечения.

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

2.8.1.Приостановить обработку данных;

2.8.2.Немедленно поставить в известность о факте обнаружения вредоносного программного обеспечения АБ ИСПДн, владельца зараженных файлов, а также смежные структурные подразделения, использующие эти файлы в работе;

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

2.8.4.Произвести лечение или уничтожение зараженных файлов (для выполнения требований данного пункта привлечь АБ ИСПДн).

2.9.Немедленно вызывать АБ ИСПДн и поставить в известность руководителя структурного подразделения при обнаружении:

2.9.1.Нарушений целостности пломб (наклеек, нарушении или несоответствии номеров печатей) на аппаратных средствах АРМ или иных фактов совершения в его отсутствие попыток несанкционированного доступа к защищаемой АРМ;

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

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

2.9.4.Некорректного функционирования установленных на АРМ технических средств защиты;

2.9.5.Непредусмотренных отводов кабелей и подключенных к АРМ дополнительных устройств.

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

2.11.Обо всех выявленных нарушениях, связанных с информационной безопасностью администрации города, а также для получения консультаций по вопросам информационной безопасности, необходимо обратиться к АБ.

2.12.При отсутствии визуального контроля за рабочей станцией доступ к компьютеру должен быть немедленно заблокирован. Для этого необходимо нажать одновременно комбинацию клавиш <Ctrl><Alt><Del> и выбрать опцию <Блокировка> , либо использовать комбинацию клавиш <Win>+<L>.

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

2.14.Пользователям запрещается:

разглашать защищаемую информацию посторонним лицам;

копировать защищаемую информацию на неучтенные внешние носители;

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

подключать к рабочей станции и корпоративной информационной сети личные внешние носители и мобильные устройства;

отключать (блокировать) средства защиты информации;

выполнять на АРМ работы, не касающиеся рабочей деятельности;

сообщать (или передавать) посторонним лицам параметры своей учетной записи (имя, персональный идентификатор и пароль) в ИСПДн;

оставлять без присмотра и передавать другим лицам персональный идентификатор;

привлекать посторонних лиц для ремонта или настройки АРМ без согласования с ответственным за обеспечение безопасности ПДн;

оставлять без присмотра свое АРМ, не активизировав блокировку доступа, или оставлять свое АРМ включенным по окончании работы;

умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к нарушению безопасности персональных данных.

3.Алгоритм использования рабочей станции пользователем, позволяющий обеспечивать информационную безопасность в администрации города.

3.1.Создание учетной записи в информационной сети администрации города Мегиона:

3.1.1.Сотрудник в отделе развития информационного общества и муниципальных услуг администрации города Мегиона ознакамливается (под роспись) с Инструкцией по организации парольной защиты и Инструкцией по организации антивирусной защиты.

3.1.2.Сотрудники отдела развития информационного общества и муниципальных услуг департамента экономического развития и инвестиций, ответственные за информационную безопасность в администрации города, согласно приложению 8 - составляют заявку на сайте МБУ МЦИКТ «Вектор» (https://support.mbu-vector.ru/) о создании учетной записи для пользователя в информационной сети администрации города.

3.2.Установка информационной системы персональных данных (далее - ИСПДн) на АРМ пользователя:

3.2.1.Сотрудник в отделе развития информационного общества и муниципальных услуг администрации города Мегиона ознакамливается (под роспись) с Инструкцией пользователя информационных систем персональных данных и заполняет акт о допуске к работе пользователя с персональными данными в информационных системах администрации города Мегиона.

3.2.2.После рассмотрения акта о допуске к работе пользователя с персональными данными в информационных системах администрации города Мегиона администратором информационной безопасности – акт подписывается ответственными лицами, сканируется и отправляется пользователю по электронной почте.

3.2.3.Администратор вправе отказать в доступе к ИСПДн, если указанная в акте информационная система не задействована в рабочей деятельности пользователя.

3.2.4.Пользователь самостоятельно составляет заявку на установку ИСПДн на сайте МБУ МЦИКТ «Вектор» (https://support.mbu-vector.ru/), прикладывая подписанный акт о допуске к работе пользователя с персональными данными в информационных системах администрации города Мегиона.

3.2.5.Без акта о допуске к работе пользователя с персональными данными в информационных системах администрации города Мегиона установка ИСПДн на АРМ пользователя производится не будет.

3.3.Изменения конфигурации АРМ пользователя.

3.3.1.Для установки программного продукта на компьютер пользователя сотрудник должен написать заявление об изменении конфигурации рабочей станции в отделе развития информационного общества и муниципальных услуг с обоснованием необходимости на его компьютере указываемого программного продукта.

3.3.2.Администртор информационной безопасности рассматривает заявление об изменении конфигурации рабочей станции сотрудника и выносит решение о разрешении установки или отказе, указанного программного продукта.

3.3.3.Пользователь самостоятельно составляет заявку на установку информационного ресурса или системы на сайте МБУ МЦИКТ «Вектор» (https://support.mbu-vector.ru/) прикладывая к заявке заявление об изменении конфигурации рабочей станции, подписанное администратором информационной безопасности с положительным решением об установке.

3.3.4.Без заявления об изменении конфигурации рабочей станции установка программного продукта, не входящего в перечень программного обеспечения разрешенного к

установке на ПЭВМ из состава информационной системы администрации города, производится не будет.

4.Порядок работы пользователя с ресурсами ИСПДн.

4.1.Начало работы на АРМ.

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

4.2.Завершение работы на АРМ.

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

4.3.Требования к распечатыванию информации.

Все распечатываемые документы должны быть учтены. Бракованные бумажные носители и черновики документов должны быть уничтожены, согласно Пункту 13 «Инструкции по порядку обращения с конфиденциальной информацией в администрации города и подведомственных организациях, расположенных на территории городского округа город Мегион» от 01.11.2017 №2177.

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

5.Ответственность.

5.1.Пользователь несет персональную ответственность за:

сохранность носителей информации и содержащейся на них информации (в рабочее время);

вне рабочее время носители информации должны быть убраны в сейф или запираемый шкаф;

соблюдение требований данной Инструкции, неправомерное использование ресурсов ИСПДн и за все действия, совершенные от имени его учетной записи в ИСПДн, если с его стороны не было предпринято необходимых действий для предотвращения несанкционированного использования его учетной записи.

5.2.За разглашение ПДн и нарушение порядка работы со средствами ИСПДн, содержащими персональные данные, работники могут быть привлечены к гражданской, уголовной, административной, дисциплинарной и иной ответственности, предусмотренной законодательством Российской Федерации.

Приложение 5
к распоряжению администрации города
от «___»_____2019 № ____

ИНСТРУКЦИЯ
по организации антивирусной защиты

1.Общие положения.

1.1. Настоящий документ разработан в соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», а также другими документами по безопасности информации, и определяет требования к организации защиты информационной системы персональных данных (далее – ИСПДн) администрации города Мегиона (далее – администрации города) от разрушающего воздействия компьютерных вирусов и другого вредоносного программного обеспечения (далее – вредоносное ПО), устанавливает ответственность администратора безопасности (далее – АБ) и других должностных лиц, настраивающих и сопровождающих средства антивирусной защиты в ИСПДн, за выполнение указанных требований.

1.2. К использованию в администрации города допускаются только лицензионные средства антивирусной защиты, централизованно закупленные у разработчиков или поставщиков данных средств.

1.3. Установка средств антивирусного контроля на компьютеры и сервера ИСПДн администрации города осуществляется АБ или под его контролем, настройка параметров средств антивирусного контроля осуществляется в соответствии с руководствами по применению конкретных антивирусных средств и требованиями документов ФСТЭК РФ в области защиты персональных данных.

2.Применение средств антивирусного контроля.

2.1.Антивирусный контроль должен осуществляться в режиме постоянной антивирусной защиты. Еженедельно по понедельникам в 10:30 при загрузке компьютера (для серверов – при перезапуске) в автоматическом режиме должен проводиться антивирусный контроль дисков и файлов автоматизированного рабочего места (далее – АРМ).

2.2.Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), хранящаяся на АРМ, передающаяся по сети, а также информация на съемных носителях. Контроль входящей информации должен осуществляться автоматически, непосредственно после ее приема. При передаче файлов, запакованных в архивы, без их распаковки, должна вручную инициироваться антивирусная проверка этих архивов.

2.3.Процедура обновления баз данных средства антивирусной защиты проводится сразу при появлении последнего обновления в хранилище.

2.4.Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено АБ на предмет отсутствия вредоносного программного обеспечения. Непосредственно после установки (изменения) программного обеспечения должна быть выполнена антивирусная проверка на всех защищаемых серверах и АРМ ИСПДн.

2.5.При возникновении подозрения на наличие вредоносного программного обеспечения (частые ошибки в работе программ, появление посторонних графических и звуковых эффектов, искажения данных, неконтролируемое пропадание файлов, появление сообщений о системных ошибках, замедление работы компьютера и т.п.) самостоятельно или вместе с АБ провести внеочередной антивирусный контроль своего АРМ. При самостоятельном проведении антивирусного контроля - уведомить о результатах АБ для опре-

деления им факта наличия или отсутствия вредоносного программного обеспечения.

3.Ответственность.

3.1.Ответственность за проведение мероприятий антивирусного контроля и настройку средств антивирусного контроля в ИСПДн администрации города в соответствии с требованиями настоящей Инструкции возлагается на АБ и всех должностных лиц, настраивающих и сопровождающих средства антивирусной защиты в ИСПДн администрации города.

3.2.Периодический контроль за состоянием антивирусной защиты (обновление антивирусной программы и антивирусных баз, а так же проверка работоспособности средств антивирусной защиты) в ИСПДн администрации города, осуществляется АБ и всеми должностными лицами, настраивающими и сопровождающими средства антивирусной защиты в ИСПДн администрации города.

Приложение 6
к распоряжению администрации города
от «___»_____2019 № ____

ИНСТРУКЦИЯ
по организации парольной защиты

1.Общие положения.

1.1.Настоящий документ разработан в соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», а также другими правовыми актами по защите информации, и регламентирует процессы генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в информационных системах персональных данных (далее – ИСПДн) администрации города Мегион (далее – администрация города), а также контроль над действиями пользователей и обслуживающего персонала системы при работе с паролями.

1.2.Осуществление процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах ИСПДн и контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями возлагается на администратора ИСПДн.

2.Правила формирования паролей.

2.1.Временный пароль, заданный администратором безопасности ИСПДн при регистрации нового пользователя, должен действовать в течение ограниченного срока времени. Пользователь должен изменить временный пароль при первой авторизации в системе.

Личные пароли доступа выдаются пользователям администратором информационной безопасности. Пароль нового пользователя, как правило, устанавливается следующий «Meg!on календарный год», без пробелов.

Пользователь должен изменить временный пароль при первом входе в систему.

Смена паролей проводится не реже одного раза в 3 месяца.

Правила формирования пароля:

пароль не может содержать имя учетной записи пользователя или какую-либо его часть;

пароль должен состоять не менее чем из 8 символов;

в пароле должны присутствовать символы всех нижеописанных категорий:

прописные буквы английского алфавита от A до Z;

строчные буквы английского алфавита от a до z;

десятичные цифры (от 0 до 9);

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

пароль не должен включать в себя имя пользователя, легко вычисляемые сочетания символов (имена, фамилии, известные названия, словарные и жаргонные слова и т.д.), последовательности символов и знаков (111, qwerty, абвгд и т.д.), общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.), аббревиатуры, клички домашних животных, номера автомобилей, телефонов и другие значимые сочетаний букв и знаков, которые можно угадать, основываясь на информации о пользователе;

запрещено использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов;

при смене пароля новое значение должно отличаться от предыдущего не менее чем в шести позициях.

2.2.Пользователям допускается использовать пароли, составленные из первых букв слов запоминающихся высказываний в разном регистре, смешанные в произвольном порядке со специальными символами (например Кожзгсф7!).

2.3.В случае если формирование личных паролей пользователей осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается на администратора безопасности ИСПДн.

3.Ввод пароля.

3.1 При вводе пароля пользователю необходимо исключить произнесение его вслух, возможность его просмотра посторонними лицами и техническими средствами (стационарными и встроенными в мобильные телефоны видеокамерами и т.п.).

3.2 При неверном вводе пароля более 3 раз, учетная запись пользователя должна блокироваться не менее чем на 3 минуты и не более чем на 15 минут.

4.Порядок смены личных паролей.

4.1.Смена паролей должна проводиться регулярно, не реже одного раза в 3 месяца, самостоятельно каждым пользователем.

4.2.В случае прекращения полномочий пользователя (увольнение, переход на другую работу и т.п.) должно производиться немедленное удаление его учетной записи сразу после окончания последнего сеанса работы данного пользователя с системой.

4.3.Срочная (внеплановая) полная смена паролей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу и т.п.) ответственного за обеспечение безопасности персональных данных, администратора безопасности и других работников, которым по роду работы были предоставлены полномочия по управлению системой парольной защиты.

5.Хранение пароля.

5.1.Запрещается записывать пароли на бумаге, в файле, электронной записной книжке, мобильном телефоне и любых других предметах, и носителях информации.

5.2.Запрещается сообщать свой пароль полностью или частично другим пользователям, запрещается спрашивать или подсматривать пароль других пользователей.

5.3.Запрещается регистрировать других пользователей в ИСПДн со своим личным паролем, запрещается входить в ИСПДн под учетной записью и паролем другого пользователя.

6.Действия в случае утери и компрометации пароля.

В случае утери или компрометации (разглашения, утраты) или подозрения в компрометации пароля пользователя должна быть немедленно проведена внеплановая процедура смены пароля.

7.Ответственность.

7.1.Каждый пользователь ИСПДн несет персональную ответственность за соблюдение требований настоящей Инструкции и за все действия, совершенные от имени его учетной записи в ИСПДн, если с его стороны не было предпринято необходимых действий для предотвращения компрометации пароля его учетной записи.

7.2.Ответственность за контроль проведения мероприятий по организации парольной защиты возлагается на ответственного за обеспечение безопасности персональных данных.

7.3.За разглашение персональных данных и нарушение порядка работы со средствами ИСПДн, обрабатывающими персональные данные, работники могут быть привлечены к гражданской, уголовной, административной, дисциплинарной и иной предусмотренной законодательством Российской Федерации ответственности.

Приложение 7
к распоряжению администрации города
от «___»_____ 2019 № ___

# ЖУРНАЛ
# ПРОВЕДЕНИЯ ИНСТРУКТАЖЕЙ
# ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Начат «___»_____20__ г.

Окончен «___»_____20__ г.

На _____листах

| _____ | _____ | _____ |
|---|---|---|
| (должность руководителя) | (подпись) | (Фамилия И.О.) |

| № п/п | ФИО сотрудника проходящего инструктаж | Дата проведения инструктажа | Инструкция пользователя информационных систем персональных данных (подпись сотрудника об ознакомлении) | Инструкцию по организации парольной защиты (подпись сотрудника об ознакомлении) | Положение об использовании ресурсов сети Интернет в ИСПДн администрации города (подпись сотрудника об ознакомлении) | Подпись инструктирующего |
|---|---|---|---|---|---|---|
| 1 | | | | | | |
| 2 | | | | | | |
| 3 | | | | | | |
| 4 | | | | | | |
| 5 | | | | | | |
| 6 | | | | | | |
| 7 | | | | | | |
| 8 | | | | | | |
| 9 | | | | | | |
| 10 | | | | | | |
| 11 | | | | | | |

Приложение 8
к распоряжению администрации города
от «___»_____ 2019 № ___

ПЕРЕЧЕНЬ
сотрудников департамента экономического развития и инвестиций администрации города, ответственных за проведение инструкций по информационной безопасности в администрации города Мегиона

1.Главный специалист департамента экономического развития и инвестиций администрации города.

2.Специалист МКУ «Служба обеспечения», обеспечивающий деятельность департамента экономического развития и инвестиций администрации города.

Приложение 9
к распоряжению администрации города
от «___»_____ 2019 № ___

# ИНСТРУКЦИЯ
## по порядку учета и хранению отчуждаемых носителей информации в администрации города Мегиона

1.Общие положения

Настоящая Инструкция разработана с целью обеспечения безопасности персональных данных при их хранении на съемных носителях.

Действие настоящей Инструкции распространяется на сотрудников Администрации города Мегиона (далее – администрация города), допущенных к обработке персональных данных.

2.Порядок использования отчуждаемых носителей информации

2.1.Под использованием отчуждаемых носителей информации в информационных системах персональных данных (далее - ИСПДн) понимается их подключение к инфраструктуре ИСПДн с целью обработки, приема/передачи информации между ИСПДн и носителями информации.

2.2.В ИСПДн допускается использование только учтенных отчуждаемых носителей информации, которые являются собственностью администрации города.

2.3.Отчуждаемые носители информации предоставляются сотрудникам администрации города на основании письменного разрешения директора департамента экономического развития и инвестиций:

необходимости выполнения вновь принятым работником своих должностных обязанностей;

возникновения у сотрудника администрации города производственной необходимости.

3.Порядок учета, хранения и обращения с отчуждаемыми носителями информации.

3.1.Все находящиеся на хранении и в обращении отчуждаемые носители с персональными данными в администрации города подлежат учёту.

3.2.Каждый отчуждаемый носитель с записанными на нем персональными данными должен иметь этикетку, на которой указывается его уникальный учетный номер.

3.3.Учет и выдачу отчуждаемых носителей информации осуществляет ответственный за защиту информации. Факт выдачи съемного носителя фиксируется в Журнале учета отчуждаемых носителей информации.

4.Требования для сотрудников, использующих отчуждаемые носители информации.

4.1.Использовать носители информации исключительно для выполнения своих служебных обязанностей.

4.2.Ставить в известность ответственного за защиту информации о любых фактах нарушения требований настоящей Инструкции.

4.3.Бережно относится к носителям информации (персональных данных).

4.4.Обеспечивать физическую безопасность отчуждаемых носителей информации.

4.5.Извещать ответственного за защиту информации о фактах утраты (кражи) носителей конфиденциальной информации.

4.6.Перед работой проверять отчуждаемые носители информации на наличие вредоносного программного обеспечения.

4.7.Осуществлять вынос съемных носителей информации (персональных данных) для непосредственной передачи адресату только с письменного разрешения главы города.

4.8.При отправке или передаче персональных данных адресатам на отчуждаемые носители записываются только предназначенные адресатам данные.

4.9.В случае утраты или уничтожения отчуждаемых носителей информации либо при разглашении содержащихся в них сведений немедленно ставится в известность глава города. На утраченные носители составляется акт. Соответствующие отметки вносятся в Журнал учета отчуждаемых носителей информации персональных данных.

4.10.Отчуждаемые носители информации, пришедшие в негодность, или отслужившие установленный срок, подлежат уничтожению. По результатам уничтожения носителей составляется акт.

4.11.В случае увольнения или перевода работника в другое структурное подразделение, предоставленные носители конфиденциальной информации изымаются.

5.Запрещается:

использовать отчуждаемые носители в личных целях;

передавать отчуждаемые носители другим лицам (за исключением администратора информационной безопасности);

хранить отчуждаемые носители с персональными данными вместе с носителями открытой информации, на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам;

выносить отчуждаемые носители с персональными данными из служебных помещений.

6.Ответственность.

Работники, нарушившие требования данной Инструкции, несут ответственность в соответствии с действующим законодательством.

Приложение 10
к распоряжению администрации города
от «___»_____ 2019 № ___

# ЖУРНАЛ УЧЕТА
# ОТЧУЖДАЕМЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ
# ПЕРСОНАЛЬНЫХ ДАННЫХ

Начат «___» _____20__ г.

Окончен «___» _____20__ г.

На _____листах

| _____ | _____ | _____ |
|---|---|---|
| (должность руководителя) | (подпись) | (Фамилия И.О.) |

М.П.

| № п/п | Регистрационный номер отчуждаемого носителя информации | Дата выдачи отчуждаемого носителя информации | ФИО, должность сотрудника, получившего отчуждаемый носитель информации | Наименование департамента / учреждения | Подпись получившего носитель информации |
|---|---|---|---|---|---|
| 1 | | | | | |
| 2 | | | | | |
| 3 | | | | | |
| 4 | | | | | |
| 5 | | | | | |
| 6 | | | | | |
| 7 | | | | | |
| 8 | | | | | |
| 9 | | | | | |
| 10 | | | | | |
| 11 | | | | | |