АДМИНИСТРАЦИЯ ГОРОДА МАГНИТОГОРСКА ЧЕЛЯБИНСКОЙ ОБЛАСТИ

РАСПОРЯЖЕНИЕ

31.08.2026 № 273 - Р

Об утверждении Политики защиты информации в администрации города Магнитогорска

В соответствии с федеральными законами от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», от 27.07.2006 № 152-ФЗ «О персональных данных», руководствуясь Уставом города Магнитогорска,

СЧИТАЮ НЕОБХОДИМЫМ:

1. Утвердить Политику защиты информации в администрации города Магнитогорска (приложение).
2. Руководителям органов администрации города Магнитогорска ознакомить сотрудников с настоящим распоряжением.
3. Настоящее распоряжение вступает в силу со дня его подписания.
4. Контроль исполнения настоящего распоряжения оставляю за собой.

Глава города Магнитогорска С.Н. Бердников

Разослано: заместителям Главы города, руководителям органов администрации города
нк

Вр-2455631

Приложение
к распоряжению администрации
города Магнитогорска
от 31.03.2026 № 273-р

ПОЛИТИКА
ЗАЩИТЫ ИНФОРМАЦИИ
НА ОБЪЕКТЕ ИНФОРМАТИЗАЦИИ
АДМИНИСТРАЦИИ ГОРОДА МАГНИТОГОРСКА

Вр-2455631

I. Основные понятия

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

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

Информационная система персональных данных – информационная система, в которой осуществляется обработка персональных данных.

Информационно-телекоммуникационная сеть – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

Конфиденциальность – состояние информации, при котором доступ к ней осуществляют только те субъекты, которые имеют на это право.

Целостность– состояние информации, при котором изменять информацию могут только те субъекты, которые имеют на это право.

Доступность – состояние информации, при котором субъекты, имеющие право доступа к информации, могут осуществлять его беспрепятственно.

Информационная безопасность – состояние защищённости информации и информационных систем от угроз безопасности информации.

Защита информации – деятельность, направленная на предотвращение утечки информации, несанкционированного и (или) непреднамеренного воздействия на информацию.

Угроза информационной безопасности – совокупность условий и факторов, создающих опасность нарушения безопасности информации.

Риск информационной безопасности – возможность реализации угрозы безопасности информации и величина возможного ущерба.

Уязвимость – недостаток или слабое место в информационной системе, которое может быть использовано для реализации угрозы.

Инцидент информационной безопасности – событие или совокупность событий, нарушающих или создающих угрозу нарушения безопасности информации.

Доступ к информации – возможность получения информации и её использования.

Несанкционированный доступ – доступ к информации, нарушающий установленные правила разграничения доступа.

Субъект доступа – пользователь или процесс, осуществляющий доступ к информации.

Объект доступа – информация или ресурс, к которому осуществляется доступ.

Идентификация – присвоение субъекту доступа уникального идентификатора.

Аутентификация – проверка подлинности субъекта доступа.

Разграничение доступа – установление и реализация правил доступа субъектов к объектам.

Удалённый доступ – доступ к информационной системе с использованием сетей связи вне контролируемой зоны.

Мобильное устройство – переносное средство вычислительной техники, используемое для доступа к информационным системам.

Меры защиты информации – организационные и (или) технические меры, направленные на обеспечение безопасности информации.

Средства защиты информации – технические, программные или программно-аппаратные средства защиты информации.

Криптографическая защита информации – защита информации с применением криптографических методов.

Регистрация событий безопасности – фиксация действий пользователей и процессов, влияющих на безопасность информации.

Резервное копирование – создание копий для восстановления в случае утраты или повреждения.

Непрерывность функционирования – способность информационной системы выполнять заданные функции без недопустимых перерывов.

Локальный нормативный акт – внутренний документ, обязательный для исполнения.

II. Общие положения

1. Настоящая Политика определяет цели, принципы, основные требования и организационные меры по обеспечению защиты информации в администрации города Магнитогорска (далее – Администрация).

2. Политика разработана в соответствии с законодательством Российской Федерации, государственными стандартами и нормативными документами уполномоченных органов в области защиты информации, в том числе с требованиями Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Приказа ФСТЭК России от 11.04.2025 № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений», иных нормативных правовых актов.

3. Действие настоящей Политики распространяется на все виды конфиденциальной информации, обрабатываемой в Администрации, независимо от формы её представления, способов обработки и средств хранения, за исключением информации, составляющей государственную тайну.

4. Настоящая Политика применяется в отношении информационных систем, находящихся в собственности Администрации, в

которых осуществляется обработка конфиденциальной информации, указанной в подпункте 14.

5. Политика обязательна для исполнения всеми работниками Администрации, а также лицами, привлекаемыми к обработке информации на договорной основе, в части, их касающейся.

6. Настоящая Политика подлежит пересмотру и актуализации при изменении законодательства Российской Федерации, требований регуляторов, структуры Администрации, состава информационных систем или условий обработки информации.

III. Область действия политики

7. Настоящая Политика защиты информации определяет цели, принципы и основные требования по обеспечению информационной безопасности в Администрации и распространяется на все процессы, связанные с созданием, обработкой, хранением, передачей и уничтожением информации в деятельности Администрации.

8. Действие Политики распространяется на все органы Администрации, включая органы Администрации в форме муниципального казенного учреждения.

9. Требования настоящей Политики являются обязательными для исполнения всеми категориями пользователей информационных ресурсов Администрации, в том числе:

1) муниципальными служащими;

2) работниками, занимающих должности, не отнесенные к должностям муниципальной службы;

3) работники, занятые обслуживанием деятельности органов Администрации;

4) работниками подведомственных учреждений, имеющими доступ к информационным системам Администрации;

5) иными лицами, получившими доступ к информационным ресурсам и системам Администрации на законных основаниях.

10. Политика защиты информации распространяется на все виды информации, перечисленные в подпункте 14 настоящего раздела, независимо от формы её представления, включая электронную, бумажную, графическую, аудио-, видео- и иные формы, а также все этапы жизненного цикла информации: сбор, обработку, хранение, передачу, архивирование и уничтожение.

11. Настоящая Политика распространяется на все используемые в Администрации информационные системы, перечисленные в подпункте 16 настоящего раздела, а также на информационные ресурсы Администрации.

12. Настоящая Политика применяется ко всем техническим средствам обработки информации Администрации, включая серверы, рабочие станции, мобильные устройства, многофункциональные устройства и съёмные

носители информации независимо от их принадлежности, если они используются при работе с конфиденциальной информацией.

Требования настоящей Политики обязательны к соблюдению при использовании работниками Администрации как корпоративных, так и личных устройств в случаях, когда такие устройства применяются для доступа к информационным системам или ресурсам Администрации.

13. Политика защиты информации распространяется на деятельность сторонних организаций и подрядчиков, привлекаемых Администрацией, в части, касающейся их доступа к информационным ресурсам и системам Администрации. Соответствующие требования должны быть закреплены в договорах, соглашениях о конфиденциальности, обязательствах о неразглашении конфиденциальной информации и иных документах.

Настоящая Политика действует совместно с иными локальными нормативными актами Администрации в области информационной безопасности и не отменяет требований законодательства Российской Федерации, государственных стандартов и нормативных документов в области защиты информации.

14. Перечень конфиденциальной информации, подлежащей защите в Администрации:

1) персональные данные (Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»);

2) служебная информация ограниченного распространения;

3) сведения, составляющие коммерческую тайну (Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне»);

4) сведения о доходах, об имуществе и обязательствах имущественного характера муниципальных служащих (Федеральный закон от 25.12.2008 № 273-ФЗ «О противодействии коррупции»);

5) информация, содержащаяся в муниципальных информационных системах, доступ к которой ограничен в соответствии с федеральными законами;

6) сведения о результатах градостроительной, земельной и имущественной деятельности, составляющие служебную тайну;

7) иная информация конфиденциального характера, признанная Администрацией подлежащей защите.

15. Политика применяется к информационным системам независимо от функционального назначения, уровня автоматизации и архитектуры, места размещения, принадлежности технических средств, режима эксплуатации.

Выделяются следующие категории информационных систем, на которые распространяется действие настоящей Политики:

1) муниципальные информационные системы (далее - МИС), созданные на основании решений органов местного самоуправления;

2) информационные системы персональных данных (далее - ИСПДн);

3) системы электронного документооборота;

4) информационные системы, обрабатывающие служебную информацию ограниченного доступа;

5) информационные системы, предназначенные для ведения кадрового и табельного учёта, расчёта заработной платы;

6) информационные системы, используемые для предоставления муниципальных услуг в электронной форме;

7) информационные системы автоматизации административно-хозяйственной деятельности;

8) системы контроля управления доступом и видеонаблюдения;

9) информационные системы, предназначенные для ведения бухгалтерской отчетности.

16. В рамках настоящей Политики защиты информации под компонентами информационно-телекоммуникационной инфраструктуры понимаются программные, программно-аппаратные средства, а также телекоммуникационные сети и каналы связи, обеспечивающие функционирование информационных систем Администрации, передачу, обработку, хранение и доступ к информации.

К компонентам информационно-телекоммуникационной инфраструктуры Администрации относятся:

1) сетевые компоненты и средства передачи данных (локальные вычислительные сети, сетевое оборудование, беспроводные сети и т.д.);

2) серверная и вычислительная инфраструктура (физические серверы, виртуализированные серверные среды);

3) программная инфраструктура и системное программное обеспечение (операционные системы серверов и рабочих станций, средства виртуализации, системы управления базами данных);

4) пользовательские и периферийные компоненты (автоматизированные рабочие места пользователей, мобильные устройства, средства печати и сканирования, многофункциональные устройства, съёмные носители информации).

IV. Цели и задачи защиты информации

17. Цели защиты информации:

1) обеспечение конфиденциальности, целостности и доступности информации;

2) предотвращение несанкционированного доступа к информационным системам и содержащейся в них информации, обнаружение фактов несанкционированного доступа и реагирование на них;

3) защита от утечки информации ограниченного доступа и иной конфиденциальной информации;

4) предотвращение несанкционированной модификации информации, обнаружение фактов несанкционированной модификации и реагирование на них;

5) обеспечение устойчивости информационных систем к различного рода угрозам;

6) обеспечение непрерывности основных процессов деятельности Администрации, в том числе предоставления муниципальных услуг;

7) минимизация ущерба от инцидентов информационной безопасности;

8) соблюдение законодательных и нормативных требований в области обеспечения информационной безопасности;

9) предотвращение несанкционированной подмены информации, обнаружение фактов несанкционированной подмены и реагирование на них;

10) предотвращение несанкционированного удаления информации и программного обеспечения, обнаружение фактов несанкционированного удаления и реагирование на них;

11) недопущение использования информационных систем и содержащейся в них информации не по назначению;

12) недопущение распространения с использованием информационных систем противоправной информации;

13) обеспечение защиты информации при удалённом доступе пользователей к информационным системам.

18. Задачи защиты информации:

1) разработка и актуализация положений, регламентов, инструкций и иных локальных нормативных актов, касающихся обеспечения информационной безопасности Администрации;

2) контроль за выполнением требований по обеспечению информационной безопасности работниками Администрации;

3) обучение работников Администрации основам информационной безопасности, а также информирование их об актуальных угрозах, схемах мошенничества и рекомендациях уполномоченных органов;

4) реализация организационных и технических мероприятий по защите конфиденциальной информации, в том числе: контроль физического доступа в помещения, где обрабатывается конфиденциальная информация, а также к носителям конфиденциальной информации; идентификация и аутентификация пользователей; разграничение прав доступа; регистрация и аудит событий безопасности; защита от вредоносного программного обеспечения посредством использования антивирусного программного обеспечения;

5) снижение рисков информационной безопасности на основе анализа угроз и уязвимостей;

6) поддержание заданного уровня защищённости информации за счёт использования современных средств и методов защиты информации.

V. Принципы защиты информации

19. Принципы защиты информации:

1) соблюдение конфиденциальности информации, доступ к которой ограничен федеральными законами, а также целостности и доступности информации;

2) соблюдение конфиденциальности сведений, признанных Администрацией подлежащими защите, а также целостности и доступности данных сведений;

3) дифференцированный подход к обеспечению безопасности информации;

4) принцип ответственности и отчётности Администрации перед гражданином (в том числе перед работником Администрации) за обработку сведений, содержащих его персональные данные;

5) учёт и контроль всех этапов автоматизированной и неавтоматизированной обработки конфиденциальной информации;

6) осведомлённость работников Администрации, осуществляющих обработку конфиденциальной информации, в вопросах информационной безопасности;

7) персональная ответственность работников Администрации за выполнение норм информационной безопасности;

8) использование принципа минимальных привилегий: доступ к конфиденциальной информации предоставляется только лицам, которым он необходим для выполнения должностных или контрактных обязательств в минимально возможном объёме.

VI. Перечень разрешённого и запрещённого для использования программного обеспечения

20. В целях обеспечения защиты информации, устойчивого и безопасного функционирования информационных систем и информационно-телекоммуникационной инфраструктуры Администрации, а также во исполнение требований законодательства Российской Федерации и нормативных документов уполномоченных органов, в Администрации установлены требования к использованию программного обеспечения.

Допускается использование исключительно программного обеспечения, которое:

1) используется в рамках выполнения функций и полномочий Администрации;

2) соответствует требованиям информационной безопасности;

3) официально приобретено, лицензировано или распространяется на законных основаниях;

4) при необходимости соответствует требованиям по сертификации или оценке соответствия.

К разрешённому программному обеспечению могут относиться:

1) операционные системы и системное программное обеспечение;

2) офисные и прикладные программы;

3) специализированное программное обеспечение для бюджетного учёта и иных направлений деятельности;

4) программное обеспечение для администрирования и мониторинга;

5) средства защиты информации, в том числе средства криптографической защиты информации;

6) программное обеспечение для организации электронного документооборота и взаимодействия с гражданами;

7) программное обеспечение для автоматизации муниципальных услуг и функций.

Запрещённое к использованию программное обеспечение:

1) не имеет законных оснований для использования (нелицензионное);

2) «пиратское» программное обеспечение, которое может содержать вредоносный код либо представляет иную угрозу информационной безопасности;

3) предназначено для обхода средств защиты информации;

4) нарушает требования законодательства Российской Федерации и локальных нормативных актов Администрации;

5) программное обеспечение, предназначенное для несанкционированного доступа, перехвата или модификации информации;

6) программное обеспечение, предназначенное для несанкционированного удалённого управления средствами вычислительной техники.

VII. Ограничения и запреты действий для пользователей при использовании и обеспечении эксплуатации информационных систем

21. В целях обеспечения защиты информации, устойчивого функционирования информационных систем и предотвращения различного рода угроз информационной безопасности в Администрации устанавливаются следующие ограничения и запреты действий пользователей при использовании и обеспечении эксплуатации информационных систем:

1) использовать информационные системы в целях, не связанных с исполнением должностных обязанностей;

2) предоставлять доступ к информационным системам третьим лицам, не имеющим соответствующих полномочий;

3) использовать чужие учётные записи для работы в информационных системах либо передавать свои данные учётной записи другим лицам;

4) осуществлять доступ к информации, которая не является необходимой для исполнения служебных обязанностей;

5) обходить или пытаться обходить установленные меры и средства защиты (в том числе средства криптографической защиты информации);

6) отключать, изменять или препятствовать функционированию средств защиты информации (в том числе средств криптографической защиты информации);

7) вносить изменения в конфигурацию операционной системы, касающуюся информационной безопасности.

VIII. Требования к защите служебных мобильных устройств, служебных планшетных компьютеров, применяемых пользователями для доступа к информационным системам (далее – мобильные устройства)

22. В целях предотвращения несанкционированного доступа к информации и обеспечения безопасности информационных систем Администрации устанавливаются требования к защите мобильных устройств, планшетных компьютеров, и иных переносных средств вычислительной техники, используемых пользователями для доступа к информационным системам и информационным ресурсам Администрации. Требования данного пункта являются обязательными для всех работников Администрации, использующих для исполнения должностных обязанностей служебные мобильные устройства.

Доступ с мобильных устройств к информационным системам и информационным ресурсам Администрации допускается только при выполнении следующих требований:

1) идентификация и аутентификация пользователя перед доступом к информационным системам;

2) использование сложных паролей, PIN-кодов либо иных средств аутентификации;

3) автоматическая блокировка устройства при отсутствии активности пользователя в течение заданного временного промежутка;

4) запрет использования общих учётных записей на одном и том же мобильном устройстве.

Требования к защите информации на мобильных устройствах:

1) защита информации, хранимой на устройстве, от несанкционированного доступа;

2) использование встроенных или специализированных средств защиты;

3) запрет хранения на мобильных устройствах информации ограниченного доступа без служебной необходимости;

4) при необходимости применение средств криптографической защиты информации для передачи данных;

5) обеспечение возможности удалённой блокировки или удаления данных при утрате устройства.

Пользователи мобильных устройств обязаны:

1) обеспечивать физическую сохранность устройств;

2) не передавать устройства и средства аутентификации третьим

лицам;

3) незамедлительно информировать своего непосредственного руководителя, а также сектор информационной безопасности управления информационных технологий и телекоммуникаций администрации города Магнитогорска о фактах кражи, утраты или компрометации мобильного устройства.

IX. Использование личных мобильных устройств, планшетных компьютеров, ноутбуков и иных переносных средств вычислительной техники (далее – личные мобильные устройства) для доступа к информационным системам Администрации, а также для обработки, хранения и передачи служебной информации и информации ограниченного доступа категорически запрещается

23. Запрет распространяется на все виды деятельности, связанные с исполнением служебных обязанностей, в том числе:

1) доступ к системам электронного документооборота, муниципальным информационным системам, базам данных, корпоративным ресурсам;

2) создание, редактирование, согласование, подписание и отправка служебных документов;

3) обмен служебной информацией с использованием любых каналов связи (мессенджеры, электронная почта, облачные сервисы, социальные сети и т.д.);

4) хранение на личных устройствах служебной информации, в том числе персональных данных, сведений, составляющих служебную и коммерческую тайну.

Запрещается передача персональных данных, служебной информации ограниченного доступа и иной конфиденциальной информации с использованием личных устройств, а также через незащищённые каналы связи, не предназначенные для таких целей.

24. Исключения из указанного запрета допускаются только в следующих случаях:

1) по письменному разрешению заместителя Главы города - начальника управления информационных технологий и телекоммуникаций администрации города Магнитогорска при наличии служебной необходимости;

2) с использованием корпоративных средств защиты информации, предоставленных Администрацией, и при условии установки на личное устройство сертифицированных средств криптографической защиты и антивирусного программного обеспечения, одобренных специалистами по защите информации;

3) при условии заключения с работником соглашения о неразглашении и обязательства по соблюдению всех требований настоящей

Политики.

В указанных исключительных случаях работник обязан соблюдать все требования к защите мобильных устройств, установленные внутренними регламентами Администрации (сложная аутентификация, шифрование данных, блокировка при бездействии, запрет на установку стороннего ПО и т.д.).

X. Требования к защите физических и виртуальных устройств информационных систем, имеющих постоянный доступ к сети «Интернет»

25. К физическим и виртуальным устройствам, имеющим постоянный доступ к сети Интернет, относятся: серверы, виртуальные машины, сетевые устройства и иные средства вычислительной техники, обеспечивающие функционирование информационных систем и сервисов Администрации.

В целях предотвращения несанкционированного доступа, утечки информации и нарушения функционирования информационных систем устанавливаются следующие требования к защите физических и виртуальных устройств:

1) физические устройства должны размещаться в специально выделенных и оборудованных помещениях, в которых обеспечивается ограничение физического доступа;

2) виртуальные устройства должны размещаться в изолированных сегментах виртуальной инфраструктуры с разграничением доступа к средам управления виртуализацией;

3) на физических и виртуальных устройствах должны быть реализованы следующие требования к программной защите:

a) установлены актуальные версии операционных систем, совместимые с прикладным и системным программным обеспечением;

b) применены все обновления безопасности;

c) отключены неиспользуемые сервисы и службы;

d) отключены небезопасные протоколы;

e) используются средства защиты информации (при необходимости – средства криптографической защиты информации);

f) администрирование устройств осуществляют только уполномоченные лица с использованием обязательной идентификации и аутентификации, а также с регистрацией и учётом всех административных действий.

XI. Категории лиц, участвующих в защите информации, их обязанности (функции) и полномочия

26. Заместитель Главы города - начальник управления информационных технологий и телекоммуникаций администрации города Магнитогорска:

1) осуществляет общий контроль и координацию работ по обеспечению информационной безопасности, в том числе кибербезопасности Администрации;

2) организовывает и координирует деятельности по защите информации в Администрации;

3) представляет на утверждение Главе города Магнитогорска внутренние стандарты и регламенты по защите информации;

4) осуществляет руководство разработкой планов работы по обеспечению информационными ресурсами структурных подразделений Администрации и осуществляет контроль за их выполнением;

5) организует развитие единой компьютерной сети Администрации, подключение её к информационно-телекоммуникационной сети Интернет и обеспечивает её функционирование.

27. Сектор информационной безопасности управления информационных технологий и телекоммуникаций администрации города Магнитогорска:

1) разрабатывает необходимую нормативную, регламентирующую и организационную документацию по информатизации, соответствующую требованиям Администрации, а также законодательству Российской Федерации;

2) принимает участие в разработке стратегических документов в области информационной безопасности;

3) ведёт техническую документацию, связанную с эксплуатацией систем защиты автоматизированных систем;

4) обеспечивает защиту информации при выводе из эксплуатации автоматизированных систем;

5) обеспечивает защиту информации в автоматизированных системах в процессе их эксплуатации;

6) проводит диагностику систем защиты информации автоматизированных систем;

7) обнаруживает инциденты в процессе эксплуатации автоматизированной системы;

8) администрирует системы защиты информации автоматизированных систем;

9) управляет защитой информации в автоматизированных системах;

10) осуществляет мониторинг защищённости информации в автоматизированных системах;

11) проводит аудит защищённости информации в автоматизированных системах;

12) устанавливает и настраивает средства защиты информации в автоматизированных системах;

13) разрабатывает организационно-распорядительные документы по информационной безопасности в автоматизированных системах;

14) внедряет организационные меры по информационной

безопасности в автоматизированных системах;

15) разрабатывает проектные решения по информационной безопасности в автоматизированных системах.

16) разрабатывает необходимую нормативную, регламентирующую и организационную документацию по информатизации, соответствующую требованиям Администрации, а также законодательству Российской Федерации;

XII. Состав организационной системы управления деятельностью по защите информации и схема взаимодействия её элементов

28. Организационная система управления защитой информации в Администрации построена по иерархическому принципу с разделением функций стратегического управления, реализации и контроля.

Схема взаимодействия элементов организационной системы управления деятельностью по защите информации приведена в Приложении к настоящей Политике.

XIII. Ответственность работников за нарушение требований о защите информации

29. Руководители структурных подразделений несут персональную ответственность за обеспечение информационной безопасности в возглавляемых ими подразделениях, обязаны незамедлительно сообщать в сектор информационной безопасности Управления информационных технологий обо всех инцидентах, связанных с нарушениями требований информационной безопасности.

30. За нарушение требований настоящей Политики, а также иной внутренней локально-нормативной документации в сфере информационной безопасности (в том числе инструкции пользования информационными системами) работники несут персональную ответственность.

За разглашение персональных данных, нарушение порядка работы с документами и (или) машинными носителями, содержащими такую информацию, и иные нарушения безопасности информации, обрабатываемой в информационных системах персональных данных Администрации, работники могут быть привлечены к ответственности в соответствии с действующим законодательством Российской Федерации.

31. Работники несут персональную ответственность за использование идентификаторов и паролей, не соответствующих требованиям, установленным в соответствующей внутренней локально-нормативной документации, а также за разглашение парольной информации.

Работники несут персональную ответственность за несвоевременное информирование о произошедших инцидентах информационной безопасности своего непосредственного руководителя или сектор

информационной безопасности Управления информационных технологий.

Работники несут персональную ответственность в соответствии с действующим законодательством Российской Федерации за использование запрещённого или несанкционированного программного обеспечения.

32. Пользователи несут персональную ответственность в соответствии с действующим законодательством Российской Федерации за несоблюдение требований защиты информации при использовании мобильных устройств.

33. Нарушение пунктов обязательства о неразглашении конфиденциальной информации влечёт наложение дисциплинарной, уголовной, административной, гражданско-правовой ответственности в соответствии с законодательством Российской Федерации.

34. Сектор информационной безопасности управления информационных технологий и телекоммуникаций администрации города Магнитогорска несёт ответственность за контроль исполнения настоящей Политики, обеспечение выполнения требований регуляторов и реагирование на инциденты информационной безопасности.

Приложение
к политике защиты информации
на объекте информатизации
администрации города
Магнитогорска

Схема взаимодействя элементов организационной системы равления деятельностью по защите информации

