РОССИЙСКАЯ ФЕДЕРАЦИЯ
РОСТОВСКАЯ ОБЛАСТЬ
МУНИЦИПАЛЬНОЕ ОБРАЗОВАНИЕ «ГОРОД ТАГАНРОГ»

АДМИНИСТРАЦИЯ ГОРОДА ТАГАНРОГА

РАСПОРЯЖЕНИЕ

30.10.2025 № 678 г. Таганрог

Об утверждении документов в области защиты информации

В соответствии с Федеральным законом от 26.07.2017 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», приказом ФСТЭК России от 11.04.2025 № 117 «Об утверждении Требований к защите информации в информационных системах, информационно-телекоммуникационных сетях, сетях связи, предназначенных для обработки информации, содержащейся в государственных информационных системах, а также информации, принадлежащей государственным органам, органам местного самоуправления и организациям», в целях обеспечения информационной безопасности в Администрации города Таганрога:

1. Утвердить:

1.1. Политику защиты информации в Администрации города Таганрога согласно приложению № 1.

1.2. Внутренние стандарты по защите информации в Администрации города Таганрога согласно приложению № 2.

1.3. Внутренние регламенты по защите информации в Администрации города Таганрога согласно приложению № 3.

2. Заместителям главы Администрации города Таганрога, руководителям структурных подразделений Администрации города Таганрога довести документы, указанные в пункте 1 настоящего распоряжения, до сведения всех работников Администрации города Таганрога, допущенных к обработке информации.

3. Настоящее распоряжение вступает в силу с 01.03.2026.

4. Контроль за исполнением настоящего распоряжения оставляю за собой.

Глава города Таганрога С.А. Камбулова

Приложение № 1
к распоряжению
Администрации
города Таганрога
от 30.10.2025 № 678

ПОЛИТИКА
защиты информации в Администрации города Таганрога

1. Область действия политики

1.1. Настоящая Политика защиты информации в Администрации города Таганрога (далее – Политика) разработана в соответствии с Федеральным законом от 26.07.2017 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», приказом ФСТЭК России от 11.04.2025 № 117 «Об утверждении Требований к защите информации в информационных системах, информационно-телекоммуникационных сетях, сетях связи, предназначенных для обработки информации, содержащейся в государственных информационных системах, а также информации, принадлежащей государственным органам, органам местного самоуправления и организациям» (далее – Требования) и иными нормативными правовыми актами Российской Федерации в области защиты информации.

1.2. Действие настоящей Политики распространяется на следующие объекты защиты:

1.2.1. Информация:

1.2.1.1. Ограниченного доступа (конфиденциальная информация), не содержащая сведений, составляющих государственную тайну.

1.2.1.2. Персональные данные, обрабатываемые в Администрации города Таганрога.

1.2.1.3. Служебная информация, доступ к которой ограничен в соответствии с федеральными законами.

1.2.1.4. Иная информация, защита которой предусмотрена законодательством Российской Федерации.

1.2.2. Информационные системы:

1.2.2.1. Информационная система персональных данных Администрации города Таганрога (далее – ИСПДн).

1.2.2.2. Официальный сайт Администрации города Таганрога (далее – сайт Администрации).

1.2.2.3. Иные информационные системы.

1.2.3. Компоненты информационно-телекоммуникационной инфраструктуры (технические средства информационных систем):

1.2.3.1. Серверное и телекоммуникационное оборудование (в том числе, маршрутизаторы, коммутаторы, межсетевые экраны).

1.2.3.2. Локальные вычислительные сети (далее – ЛВС).

1.2.3.3. Рабочие станции пользователей (персональные компьютеры, ноутбуки, моноблоки).

1.2.3.4. Планшетные компьютеры.

1.3. Политика обязательна для исполнения всеми работниками Администрации города Таганрога, а также сторонними лицами (подрядные организации), допущенными к обработке информации и эксплуатации указанных выше объектов защиты.

1.4. Администрация города Таганрога является оператором информационных систем и компонентов информационно-телекоммуникационной инфраструктуры (технических средств информационных систем), принадлежащих ей на праве собственности или переданных в оперативное управление.

2. Цели и задачи защиты информации

2.1. Цель защиты информации: обеспечение безопасности информации, обрабатываемой в Администрации города Таганрога, от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий, направленных на нарушение информационной безопасности.

2.2. Задачи защиты информации:

2.2.1. Предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации.

2.2.2. Своевременное обнаружение и предотвращение компьютерных атак на объекты защиты.

2.2.3. Непрерывность обработки информации и устойчивость функционирования объектов защиты.

2.2.4. Предотвращение воздействия вредоносного компьютерного кода.

2.2.5. Контроль уровня защищенности информации.

2.2.6. Обеспечение аутентификации и разграничения доступа пользователей к информационным ресурсам.

2.2.7. Регистрация и учет событий безопасности информации.

2.2.8. Управление конфигурацией программно-аппаратных средств защиты информации и объектов защиты.

3. Принципы защиты информации

Защита информации в Администрации города Таганрога основывается на следующих принципах:

Законности: соблюдение требований законодательства Российской Федерации в области защиты информации.

Системности: реализация согласованных и взаимосвязанных мер защиты на всех этапах жизненного цикла объектов защиты.

Комплексности: применение всех необходимых и достаточных методов и средств защиты информации (правовых, организационных, технических).

Непрерывности: осуществление защиты информации на постоянной основе.

Своевременности: проактивное внедрение мер защиты и оперативное реагирование на новые угрозы.

Персональной ответственности: возложение ответственности на каждого работника за соблюдение требований по защите информации в рамках его должностных обязанностей.

Разумной достаточности: соотношение затрат на защиту информации с возможным ущербом от ее нарушения.

4. Перечни объектов защиты

4.1. Программные средства:

4.1.1. Операционные системы серверов и рабочих станций (системное программное обеспечение).

4.1.2. Системы управления базами данных (далее – СУБД).

4.1.3. Прикладное программное обеспечение (офисные пакеты, почтовые клиенты, браузеры и иное).

4.1.4. Антивирусное программное обеспечение рабочих станций и серверов.

4.1.5. Средства защиты информации от несанкционированного доступа.

4.1.6. Средства криптографической защиты информации (далее – СКЗИ).

4.2. Программно-аппаратные средства:

4.2.1. Аппаратные межсетевые экраны.

4.2.2. Системы обнаружения вторжений.

4.2.3. Аппаратные СКЗИ.

4.3. Информационные системы:

4.3.1. ИСПДн.

4.3.2. Сайт Администрации.

4.3.3. Система защиты информации (сервер централизованного управления СЗИ от НСД и системы антивирусной защиты).

4.3.4. Сервис электронной почты.

4.4. Сети и подсети, образующие информационно-телекоммуникационную инфраструктуру:

4.4.1. Сегмент ЛВС для подключения рабочих станций и печатающей техники, имеющей сетевые интерфейсы.

4.4.2. Сегмент ЛВС для размещения публично доступных серверов – демилитаризованная зона.

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

5.1. Лицом, принимающим решение об обработке информации, является Глава города Таганрога (далее – Оператор).

Оператор:

утверждает Политику и смежные документы;

выделяет необходимые бюджетные ассигнования;

несет персональную ответственность за организацию защиты информации.

издает распорядительные документы по вопросам защиты информации.

5.2. Ответственным за обеспечение защиты информации в Администрации города Таганрога является заместитель главы Администрации города Таганрога, определенный Оператором в соответствии с распоряжением Администрации города Таганрога.

Лицо, ответственное за обеспечение защиты информации в Администрации города Таганрога:

организует выполнение Политики;

координирует работу по защите информации;

контролирует эффективность применяемых мер.

5.3. Администраторами информационных систем и администраторами безопасности являются работники Администрации города Таганрога, определенные в соответствии с распоряжением Администрации города Таганрога.

Администраторы информационных систем и администраторы безопасности:

реализуют технические меры защиты;

настраивают системы защиты;

обеспечивают эксплуатацию и мониторинг информационных систем и сетей;

производят выдачу реквизитов доступа (учетных записей);

проводят расследования инцидентов безопасности.

имеют доступ уровня «администратор» или «суперпользователь» к соответствующим информационными системам и объектам защиты в рамках своих должностных инструкций.

5.4. Пользователями информационных систем являются работники Администрации города Таганрога, допущенные к работе с информацией.

Пользователями информационных систем:

работают с информацией в рамках установленных прав доступа и должностной инструкцией;

соблюдают требования Политики и инструкций;

используют предоставленные им средства защиты;

сообщают о любых возникших подозрительных событиях или инцидентах.

6. Состав организационной системы управления деятельностью по защите информации и схема взаимодействия ее элементов

6.1. Организационная система управления представляет собой трехуровневую структуру:

6.1.1. Уровень 1 (стратегический): Лицо, принимающее решение об обработке информации (Оператор), – Глава города Таганрога. Определяет стратегию и политику в области защиты информации.

6.1.2. Уровень 2 (тактический): Ответственный за обеспечение защиты информации, – заместитель главы Администрации города Таганрога, назначаемый распоряжением Администрации города Таганрога. Планирует, организует и контролирует работы по защите информации. Взаимодействует с администраторами информационных систем, администраторами безопасности, руководителями структурных подразделений Администрации города Таганрога и Главой города Таганрога.

6.1.3. Уровень 3 (операционный): Администраторы информационных систем, администраторы безопасности, пользователи. Непосредственно реализуют и соблюдают меры защиты.

6.2. Схема взаимодействия:

6.2.1. Ответственный за защиту информации получает задания от Оператора и доводит их до сведения сотрудников на оперативном уровне (поручениями по системе электронного документооборота и делопроизводства «Дело»).

6.2.2. Администраторы информационных систем и администраторы безопасности направляют ответственному за защиту информации о состоянии защищенности, возникающих инцидентах и проблемах (при наличии соответствующих сведений).

6.2.3. Пользователи информируют своего непосредственного руководителя и администраторов безопасности обо всех нарушениях режима защиты и инцидентах безопасности.

6.2.4. В случае, когда инцидент безопасности может иметь резонансный характер, администраторы безопасности принимают незамедлительные меры к минимизации последствий такого инцидента.

7. Ответственность работников за нарушение требований о защите информации

7.1. Работники Администрации города Таганрога несут дисциплинарную, административную, гражданско-правовую и уголовную ответственность за нарушение требований законодательства Российской Федерации в области защиты информации, настоящей Политики, а также установленных правил обработки информации.

7.2. Дисциплинарная ответственность за неисполнение должностных обязанностей в области защиты информации наступает по основаниям и в порядке, предусмотренном Трудовым кодексом Российской Федерации.

7.3. Административная ответственность наступает за совершение административных правонарушений, предусмотренных статьями 13.11, 13.12, 13.14 Кодекса об административных правонарушениях Российской Федерации.

7.4. Уголовная ответственность наступает за совершение преступлений, предусмотренных статьями 272, 273, 274 Уголовного кодекса Российской Федерации.

7.5. О каждом случае нарушения требований защиты информации должно быть немедленно доложено непосредственному руководителю и ответственному за обеспечение защиты информации для принятия решения о проведении служебной проверки и применения иных мер воздействия.

Начальник общего отдела
Администрации города Таганрога О.С. Каренко

Приложение № 2
к распоряжению
Администрации
города Таганрога
от 30.10.2025 № 678

ВНУТРЕННИЕ СТАНДАРТЫ
по защите информации в Администрации города Таганрога

1. Требования к первичной идентификации пользователей

1.1. Доступ к информационным системам (далее – ИС) и информации предоставляется только идентифицированным и аутентифицированным пользователям.

Пользователями информационных систем являются работники Администрации города Таганрога, допущенные к работе с информацией.

1.2. Первичная идентификация пользователя осуществляется уполномоченными работниками отдела информационно-коммуникационных технологий Администрации города Таганрога на основании служебной записки, подписанной руководителем структурного подразделения Администрации города Таганрога или курирующим заместителем главы Администрации города Таганрога, при предъявлении документа, удостоверяющего личность.

1.3. Для каждого пользователя заводится уникальная учетная запись (идентификатор). Использование общих (групповых) учетных записей запрещено, за исключением случаев, технически не предусматривающих индивидуальную идентификацию.

1.4. Идентификатор пользователя должен быть уникальным и не раскрывать личные данные пользователя.

1.5. Первичная выдача учетных данных (логина и временного пароля) осуществляется отделом информационно-коммуникационных технологий Администрации города Таганрога (далее – отдел ИКТ) при предъявлении документа, удостоверяющего личность.

2. Требования к применяемым моделям доступа пользователей

2.1. В информационных системах применяется модель дискреционного (избирательного) управления доступом, при которой права доступа определяются на основе установленных правил, списков доступа, в соответствии с функциональными и должностными обязанностями пользователей.

2.2. Реализуется принцип минимальных привилегий: пользователю предоставляются только те права доступа, которые необходимы для выполнения им своих должностных обязанностей, зафиксированных в должностной инструкции.

2.3. Запрещается предоставление пользователям прав, избыточных по отношению к их функциональным обязанностям (например, рядовому пользователю – прав администратора).

2.4. Отделом ИКТ не реже 1 раза в год проводится аудит актуальности предоставленных прав доступа.

2.5. На основании сведений об увольнении (долгосрочном отсутствии), поступающих из отдела муниципальной службы и кадров Администрации города Таганрога (далее – ОМСиК), отдел ИКТ блокирует соответствующие учетные записи.

3. Перечень разрешенного и (или) запрещенного для использования программного обеспечения

3.1. Перечень разрешенного к использованию лицензионного и свободно распространяемого программного обеспечения устанавливается в соответствии с Единым реестром российских программ для электронных вычислительных машин и баз данных (далее – Реестр).

3.2. Использование программного обеспечения (далее – ПО) неизвестного происхождения и полученного из непроверенных источников, нелицензионного, устаревшего ПО, а также иного ПО, не входящего в Реестр, запрещено.

3.3. Установка любого ПО осуществляется отделом ИКТ.

4. Требования к типовым конфигурациям и настройкам программных, программно-аппаратных средств

4.1. Все средства защиты информации от несанкционированного доступа (далее – СЗИ от НСД), операционные системы и приложения должны быть установлены и настроены в соответствии с руководствами по эксплуатации соответствующего ПО.

4.2. Обязательные настройки включают:

4.2.1. Отключение неиспользуемых сетевых служб и портов.

4.2.2. Применение общих правил настройки СЗИ от НСД.

4.2.3. Подключение к централизованным консолям управления СЗИ от НСД и системе антивирусной защиты.

4.2.4. Ограничение прав пользователей на изменение критических настроек системы (создание для пользователей учетных записей с минимальными привилегиями).

4.3. Настройки системы антивирусной защиты и СЗИ от НСД распространяются на все рабочие станции централизовано.

5. Требования к конфигурациям и настройкам средств для доступа в Интернет, а также для удаленного доступа

5.1. Доступ пользователей в информационно-телекоммуникационную сеть «Интернет» осуществляется централизовано через единый шлюз.

5.2. Контентная фильтрация осуществляется средствами системы антивирусной защиты.

5.3. Запрещается доступ в сеть «Интернет» с рабочих станций, минуя установленные средства защиты и средства контентной фильтрации, в том числе, запрещено использование сайтов-анонимайзеров и сторонних прокси-серверов.

5.4. Удаленный доступ к ИС для пользователей не предусмотрен.

6. Ограничения и запреты действий для пользователей

6.1. Пользователи должны использовать сеть «Интернет» исключительно в служебных целях.

6.2. Пользователям запрещается:

6.2.1. Передавать свои учетные данные (логин/пароль) другим лицам.

6.2.2. Устанавливать ПО.

6.2.3. Отключать средства защиты информации (антивирусное ПО, брандмауэры, СЗИ от НСД).

6.2.4. Осуществлять несанкционированную передачу конфиденциальной информации за пределы защищаемого периметра.

6.2.5. Использовать простые пароли, записывать пароли на носители (бумажные и электронные) информации в открытом виде.

6.2.6. Подключать к локальной вычислительной сети Администрации города Таганрога, автоматизированным рабочим местам, копировально-множительной технике любые персональные устройства.

6.2.7. Использовать в служебных целях почтовые ящики, созданные вне домена tagancity.ru.

6.3. Пользователь обязан немедленно сообщить любому работнику отдела ИКТ о всех подозрительных событиях (например, утеря устройства, подозрение на компрометацию пароля, утеря персонального аппаратного ключа).

7. Требования к защите конечных устройств (с постоянным доступом в сеть «Интернет»)

7.1. Все конечные устройства должны быть оснащены:

7.1.1. Антивирусным программным обеспечением с актуальными базами сигнатур.

7.1.2. СЗИ от НСД.

7.2. Должна быть исключена возможность несанкционированного изменения конфигурации защитных механизмов пользователем.

8. Требования к защите мобильных устройств

8.1. Регламент работы с планшетными компьютерами утверждается распоряжением Администрации города Таганрога.

8.2. В указанном документе определяются методы и средства по защите мобильных устройств.

9. Требования к непрерывности функционирования информационных систем

9.1. Технические средства информационных систем функционируют круглосуточно.

9.2. Отделом ИКТ проводятся следующие мероприятия:

9.2.1. Плановые профилактические работы (когда оборудование функционирует штатно, работы нацелены на поддержание корректного режима работы).

9.2.2. Неотложные работы (когда оборудование по совокупности событий безопасности может перейти в аварийный режим работы, работы нацелены на предотвращение перехода оборудование в аварийный режим).

9.2.3. Экстренные работы (когда оборудование функционирует в аварийном режиме, работы нацелены на стабилизацию работы оборудования).

10. Требования к резервному копированию

10.1. Для обеспечения надежности информационных систем предусмотрено создание резервных копий.

10.2. Резервные копии могу создаваться автоматически или в ручном режиме.

10.3. Отделом ИКТ не реже 1 раза в квартал проводится проверка целостности и возможности восстановления данных из резервных копий.

11. Требования к сбору, регистрации и анализу событий безопасности

Регламент работы с инцидентами безопасности утверждается распоряжением Администрации города Таганрога.

12. Требования к защите информации при межсистемном взаимодействии

12.1. Локальная вычислительная сеть Администрации города Таганрога имеет подключение к корпоративной сети телекоммуникационной связи Ростовской области.

12.2. Передача данных между сетями осуществляется по защищенным каналам связи с использованием средств криптографической защиты информации, сертифицированных ФСБ России.

12.3. Регламент подключения к корпоративной сети телекоммуникационной связи Ростовской области определяется министерством цифрового развития, информационных технологий и связи Ростовской области.

Начальник общего отдела
Администрации города Таганрога О.С. Каренко

Приложение № 3
к распоряжению
Администрации
города Таганрога
от 30.10.2025 № 678

ВНУТРЕННИЕ РЕГЛАМЕНТЫ
по защите информации в Администрации города Таганрога

1. Регламент управления учетными записями пользователей

1.1. Основанием для создания учетной записи является служебная записка, подписанная руководителем структурного подразделения Администрации города Таганрога или курирующим заместителем главы Администрации города Таганрога.

1.2. Служебная записка направляется посредством межведомственной системы электронного документооборота и делопроизводства «Дело» (далее – система «Дело») в адрес начальника отдела информационно-коммуникационных технологий Администрации города Таганрога (далее – отдел ИКТ).

1.3. В отношении работников структурных подразделений служебные записки направляются за подписью руководителя структурного подразделения. Заместители главы Администрации города Таганрога направляют служебные записки в отношении работников соответствующей приемной и руководителей структурных подразделений, оперативно подчиненных соответствующему заместителю главы Администрации города Таганрога.

1.4. Обязательным приложением к такой служебной записке является сканированный образ выписки из распоряжения Администрации города Таганрога о приеме на работу нового работника. Форма служебной записки утверждается приказом начальника отдела ИКТ и доводится до сведения всех руководителей структурных подразделений Администрации города Таганрога и заместителей главы Администрации города Таганрога.

1.5. Сканированные образы выписок из распоряжений Администрации города Таганрога о приеме на работу заместителей главы Администрации города Таганрога и руководителей структурных подразделений, оперативно подчиненных Главе города Таганрога, отдел муниципальной службы и кадров Администрации города Таганрога (далее – ОМСиК) направляет в отдел ИКТ.

Права доступа указанным работникам назначает отдел ИКТ в соответствии с функциональными обязанностями работников.

1.6. Уполномоченные работники отдела ИКТ создают уникальные учетные записи для доступа к информационным системам, указанным в служебной записке, присваивают временный пароль. Такие действия отражаются в электронных журналах соответствующих информационных систем. Временные учетные данные передаются пользователю лично.

1.7. Изменение прав доступа осуществляется на основании служебной записки, составленной в порядке, определенном в настоящем разделе. В тексте указываются только те права, которые необходимо добавить, изменить или отозвать.

1.8. Учетная запись блокируется автоматически после достижения допустимого количества неверных попыток ввода пароля (в соответствии с документацией на информационную систему) или вручную уполномоченным работником отдела ИКТ в связи с увольнением, переводом в другое структурное подразделение (до поступления служебной записки от нового руководителя), отпуском по беременности и родам или иными случаями длительного отсутствия (в том числе, на основании кадровых документов, информации, поступившей из ОМСиК), обнаружением подозрительной активности учетной записи (реакция администратора безопасности на возможный инцидент). Изменение должности, фамилии осуществляется в порядке, определенном настоящим разделом.

1.9. Не реже 1 раза в квартал работники отдела ИКТ проводят сверку учетных записей с кадровыми данными.

1.10. Доступ к информационным системам может предоставляться посредством авторизации через Единую систему идентификации и аутентификации (далее – ЕСИА). Для реализации такого метода уполномоченный работник отдела ИКТ направляет работнику на электронную почту приглашение, а работник его принимает. После присоединения работника к профилю Администрации города Таганрога в ЕСИА назначаются необходимые права доступа.

2. Регламент управления привилегированными учетными записями

2.1. Привилегированные учетные записи (далее – ПУЗ) или учетные записи администраторов информационной системы создаются работниками отдела ИКТ только для новых работников отдела ИКТ.

2.2. Работники отдела ИКТ обладают одинаковыми правами в отношении всех эксплуатируемых информационных систем.

2.3. Операции изменения, блокирования, удаления ПУЗ осуществляются по основаниям, предусмотренным для учетных записей пользователей.

3. Регламент управления аутентификационной информацией и средствами аутентификации

3.1. Аутентификационная информация (пароли) создается уполномоченным работником отдела ИКТ (первичная аутентификационная информация), устанавливается пользователем в соответствии с действующей политикой паролей. Аппаратные средства аутентификации (токены, USB-ключи) выдаются пользователям и администраторам под подпись

в журнале поэкземплярного учета средств криптографической защиты информации.

3.2. Пароль изменяется при первой авторизации по истечении срока действия при подозрении на компрометацию. Смена средств аутентификации (например, перевыпуск ключа) осуществляется при их утере или смене сотрудника.

3.3. При увольнении, переводе на другую работу или плановом долгосрочном отсутствии аппаратные средства аутентификации подлежат возврату в отдел ИКТ.

3.4. В случае утери аппаратного средства аутентификации отделом ИКТ инициируется служебная проверка в отношении пользователя, которому было выдано аппаратное средство аутентификации.

3.5. Для аутентификации (а также совершения иных юридически значимых действий в информационных системах) может использоваться электронная подпись. Заявку на выпуск квалифицированной электронной подписи работники формируют самостоятельно в соответствии с регламентом работы удостоверяющего центра Федерального казначейства. Работники отдела ИКТ оказывают методическую помощь в составлении заявки.

3.6. Делегирование полномочий на выполнение юридически значимых действий в информационных системах может осуществляться путем выпуска машиночитаемой доверенности (далее – МЧД). Выпуск МЧД осуществляется в следующем порядке:

3.6.1. Инициатор выпуска МЧД (руководитель структурного подразделения Администрации города Таганрога или заместитель главы Администрации города Таганрога) подготавливает ходатайство о выпуске МЧД в адрес Главы города Таганрога, в котором указываются Ф.И.О. работника, для которого необходимо выпустить МЧД, ИНН, СНИЛС, дата рождения, гражданство, паспортные данные, а также наименование информационной системы и перечень полномочий в указанной системе.

3.6.2. Ходатайство (регистрационную карту проекта документа в системе «Дело», далее – РКПД) обязательно визируют: руководитель инициатора, начальник правового управления Администрации города Таганрога.

3.6.3. РКПД подписывает руководитель инициатора.

3.6.4. Регистрационная карта с ходатайством направляется в адрес Главы города Таганрога.

3.6.5. Глава города Таганрога поручает подготовку МЧД отделу ИКТ.

3.6.6. Отдел ИКТ готовит МЧД в соответствующей системе.

3.6.7. Глава города Таганрога подписывает МЧД в соответствующей системе.

3.6.8. Отдел ИКТ загружает МЧД в распределенный реестр ФНС России (или иную систему, предназначенную для хранения МЧД).

4. Регламент доступа для подрядных организаций

4.1. Основанием для предоставления доступа к информационным системам и техническим средствам информационных систем является договор (муниципальный контракт), содержащий раздел об ответственности за нарушение требований защиты информации, и список сотрудников подрядчика, допускаемых к работе.

4.2. При необходимости сотрудникам подрядчика создаются временные учетные записи с ограниченным сроком действия и минимально необходимыми правами.

4.3. Уполномоченными работниками отдела ИКТ проводится вводный инструктаж по правилам работы.

4.4. Доступ предоставляется только к тем ресурсам, которые необходимы для выполнения работ по договору (муниципальному контракту).

4.5. Действия учетных записей подрядчиков контролируются уполномоченным работником отдела ИКТ. После завершения работ учетные записи немедленно блокируются.

5. Регламент доступа для иных государственных органов

5.1. Основанием для рассмотрения вопроса предоставления доступа государственных органов к информационным системам, содержащейся в них информации и (или) передачи им информации, является наличие соответствующего правового основания и заключенного соглашения о межведомственном информационном взаимодействии, регламентирующее порядок, объем и цели обмена информацией.

5.2. Решение о предоставлении доступа государственным органам принимается Главой города Таганрога.

6. Регламент предоставления доступа в сеть «Интернет» и удаленного доступа

6.1. Доступ предоставляется по умолчанию всем пользователям, с использованием системы фильтрации контента (URL – фильтрация, категории), функции которой выполняет система антивирусной защиты.

6.2. Блокируется доступ к ресурсам, не связанным со служебной деятельностью (социальные сети, развлекательные порталы, ресурсы с запрещенным контентом, ресурсы, рекомендованные к блокировке уполномоченными органами). Особые доступы к ресурсам сети «Интернет» рассматриваются отделом ИКТ индивидуально на основании служебной записки с обоснованием необходимости в соответствующем доступе.

6.3. Удаленный доступ для пользователей не предусмотрен.

7. Регламент повышения уровня знаний и информированности пользователей по вопросам защиты информации

7.1. Все вновь принимаемые работники проходят вводный инструктаж по информационной безопасности. Для всех пользователей не реже 1 раза в год проводится обязательное обучение (очно или в форме онлайн-курсов) с последующей проверкой знаний.

7.2. Актуальная информация об угрозах и мерах безопасности доводится через рассылку по системе «Дело», в чате в корпоративном мессенджере «Среда».

8. Регламент управления уязвимостями

8.1. Отделом ИКТ производится регулярное автоматизированное сканирование узлов информационной системы с помощью средств анализа защищенности. Мониторинг источников информации об обнаруженных уязвимостях.

8.2. Обнаруженные уязвимости классифицируются по степени риска (критическая, высокая, средняя, низкая) с учетом критичности системы и возможности эксплуатации. Принимаются решения о возможности устранения выявленных уязвимостей.

8.3. Критические и высокоуровневые уязвимости устраняются в максимально короткие сроки или принимаются компенсирующие меры.

9. Регламент управления обновлениями

9.1. Обновления загружаются только с официальных сайтов производителей.

9.2. Перед массовым развертыванием обновления проходят проверку в тестовой среде на предмет совместимости и отсутствия сбоев.

9.3. Установка обновлений критических и важных систем проводится централизовано по утвержденному графику.

9.4. Антивирусные базы обновляются ежедневно, обновления средств защиты информации от несанкционированного доступа (далее – СЗИ от НСД) устанавливаются по мере их выпуска производителем ПО.

10. Регламент обработки информации ограниченного доступа

10.1. Конфиденциальная информация с пометкой «Для служебного пользования» обрабатывается на рабочих местах, аттестованных для таких целей. Запрещается передача такой информации по незащищенным каналам связи (например, по электронной почте) и ее хранение на непредназначенных для этого носителях.

10.2. Хранение бумажных носителей осуществляется в закрывающихся на ключ шкафах.

10.3. Порядок работы с конфиденциальной информацией в Администрации города Таганрога установлен распоряжением Администрации города Таганрога от 21.07.2016 № 2 дсп «Об утверждении Положения

о порядке обращения со служебной информацией ограниченного распространения в Администрации города Таганрога».

11. Регламент обеспечения физической защиты

11.1. Помещения, в которых размещены технические средства информационных систем (серверное, телекоммуникационное и маршрутизирующее оборудование), оборудуются охранной и пожарной сигнализацией, здание Администрации города Таганрога оборудовано системой контроля и управления доступом, видеонаблюдением. Вестибюли оборудуются металлодетекторами. Доступ в помещения разрешен только уполномоченным работникам.

11.2. Окна помещений, в которых расположены технические средства информационных систем, оборудуются решетками. Если решетки являются открываемыми, на них должен быть установлен замок, а также пломба.

11.3. Доступ в здание Администрации города Таганрога осуществляется в соответствии с распоряжением Администрации города Таганрога.

11.4. В целях обеспечения защиты и контроля за доступом к аппаратной конфигурации автоматизированных рабочих станций системные блоки (моноблоки и ноутбуки) опечатываются уполномоченными работниками отдела ИКТ номерными наклейками. Учет опломбировки ведется отделом ИКТ в электронном журнале.

12. Регламент разработки безопасного программного обеспечения (при наличии)

В случае самостоятельной разработки программного обеспечения применяется национальный стандарт Российской Федерации ГОСТ Р 56939-2024 «Защита информации. Разработка безопасного программного обеспечения. Общие требования», утвержденный и введенный в действие приказом Росстандарта от 24.10.2024 № 1504-ст.

13. Регламент вывода в контур промышленной эксплуатации сервисов, доступ к которым осуществляется с использованием сети «Интернет»

13.1. Перед выводом сервиса, доступного из сети «Интернет», проводится:

13.1.1. Проверка на наличие уязвимостей.

13.1.2. Проверка установки актуальных обновлений, полученных из официальных репозиториев.

13.1.3. Проверка конфигурации защитных механизмов.

13.1.4. Нагрузочное тестирование.

14. Регламент мониторинга информационной безопасности

14.1. Мониторинг осуществляется в соответствии с ГОСТ Р 59547-2021 «Защита информации. Мониторинг информационной безопасности. Общие положения», утвержденным и введенным в действие приказом Росстандарта от 27.07.2021 № 656-ст, и включает:

14.1.1. Сбор и корреляцию событий от всех источников (СЗИ от НСД, операционных систем, систем управления базами банных, сетевого оборудования, антивирусного программного обеспечения, сетевых сканеров безопасности, систем обнаружения вторжений, отчетов о DDOS-атаках).

14.1.2. Ежедневный анализ событий информационной безопасности.

14.1.3. Реагирование на инциденты по утвержденному регламенту.

15. Регламент восстановления функционирования информационных систем и тестирования

15.1. Действия по восстановлению осуществляются в целях обеспечения непрерывности работы информационных систем и восстановления работоспособности после сбоев. Приоритет отдается восстановлению из актуальных резервных копий.

15.2. Тестирование: не реже 1 раза в год проводятся учения по восстановлению информационных систем после сбоев. Результаты учений обсуждаются на совещании с работниками отдела ИКТ, формулируются предложения по повышению эффективности процесса.

15.3. Тестированию подлежат также вспомогательные технические средства (например, источники бесперебойного питания, KVM-переключатели и консоли).

16. Регламент контроля уровня защищенности информации

Контроль осуществляется отделом ИКТ путем:

проведения внутренних периодических проверок (аудит политик, настроек, журналов);

анализа отчетов, формируемых информационными системами, средствам антивирусной безопасности, СЗИ от НСД, сетевыми сканерами безопасности, системами обнаружения вторжений, отчетами о DDOS-атаках;

проведения ежегодной оценки выполнения требований приказа Федеральной службы по техническому и экспортному контролю 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»;

исправления выявленных недостатков в установленные сроки.

Начальник общего отдела
Администрации города Таганрога О.С. Каренко