АДМИНИСТРАЦИЯ ГОРОДА ЮЖНО-САХАЛИНСКА

РАСПОРЯЖЕНИЕ

от 22.07.2019 № 451-р

О назначении ответственных за защиту информации в муниципальной информационной системе «Единая мультисервисная телекоммуникационная сеть администрации города Южно-Сахалинска»

В соответствии с Постановлением Правительства РФ от 06.07.2015 № 676 «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации», Приказом ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», постановлением администрации города Южно-Сахалинска от 04.10.2018 № 2590-па «О возложении обязанностей оператора муниципальной информационной системы «Единая мультисервисная телекоммуникационная сеть администрации города Южно-Сахалинска», в целях распределения функций по организации и обеспечению защиты информации :

1. Назначить ответственными за защиту информации в муниципальной информационной системе «Единая мультисервисная телекоммуникационная сеть администрации города Южно-Сахалинска» (далее — ЕМТС):

1.1. Департамент мобилизационной подготовки и защиты информации в части исполнения функций и обязанностей администрации города Южно-Сахалинска как заказчика МИС ЕМТС и закрепить за ним:

- нормативно-методическое регулирование системы защиты информации в ЕМТС, включая формирование требований к защите информации, содержащейся в ЕМТС;

- разработку предложений по модернизации системы защиты информации ЕМТС;

- аттестацию ЕМТС по требованиям защиты информации;

- периодический контроль за обеспечением уровня защищенности информации в ЕМТС;

- планирование и проведение мероприятий по реагированию на выявленные инциденты безопасности в ЕМТС.

1.2. МКУ «Управление делами администрации города Южно-Сахалинска», как оператора ЕМТС обеспечивающего эксплуатацию аппаратно-технического и программного обеспечения ЕМТС и закрепить за ним:

- обязанность по обеспечению защиты информации в ходе эксплуатации аттестованной ЕМТС в соответствии с проектными решениями системы защиты информации ЕМТС и эксплуатационной документации используемой в составе ЕМТС, средств защиты информации, включая управление (администрирование) системой защиты информации ЕМТС;

- обязанность по выявлению инцидентов безопасности в ЕМТС;

- управление конфигурацией и системой защиты информации аттестованной ЕМТС;

- внутренний контроль за обеспечением уровня защищенности информации в ЕМТС.

2. Утвердить :

2.1. Регламент управления конфигурацией ЕМТС (приложение № 1);

2.2. Порядок выявления инцидентов безопасности в ЕМТС и реагирования на них (приложение № 2).

3. Настоящее распоряжение разместить на официальном сайте администрации города Южно-Сахалинска.

4. Контроль исполнения распоряжения администрации города Южно-Сахалинска возложить на первого вице-мэра, руководителя аппарата.

Исполняющий обязанности мэра города Н.Ю.Куприна

Приложение № 1
УТВЕРЖДЕН
распоряжением администрации
города Южно-Сахалинска
от 22.07.2019 № 451-р

РЕГЛАМЕНТ
управления конфигурацией Единой мультисервисной телекоммуникационной сети администрации города Южно-Сахалинска

1. Общие положения

1.1. Настоящий регламент определяет правила и процедуры следующих процессов обеспечения защиты информации в муниципальной информационной системе «Единая мультисервисная телекоммуникационная сеть администрации города Южно-Сахалинска» (далее – ЕМТС) :

1.1.1. Определения лиц, которым разрешены действия по внесению изменений в конфигурацию ЕМТС и её системы защиты информации;

1.1.2. Управления изменениями конфигурации ЕМТС и её системы защиты информации;

1.1.3. Анализа потенциального воздействия планируемых изменений в конфигурации ЕМТС и её системы защиты информации на обеспечение защиты информации и согласование изменений в конфигурации ЕМТС и её системы защиты информации с должностным лицом (работником), ответственным за обеспечение безопасности ЕМТС;

1.1.4. Документирования информации (данных) об изменениях в конфигурации ЕМТС и её системы защиты информации;

1.1.5. Регламентации и контроля технического обслуживания, в том числе дистанционного (удалённого), технических средств и программного обеспечения ЕМТС.

1.2. Лицами, осуществляющими управление конфигурацией ЕМТС и системой защиты информации в ЕМТС, являются:

1.2.1. Администраторы ЕМТС, в полном объеме архитектуры ЕМТС и центра обработки данных (далее - ЦОД) в ее составе;

1.2.2. Системные администраторы, в пределах делегированных им полномочий :

1.2.2.1. В части управления параметрами учётных записей пользователей ЕМТС – аккаунт-менеджеры;

1.2.2.2. В части управления конфигурацией активных и пассивных сетевых устройств – администраторы сетевых устройств;

1.2.2.3. В части управления конфигурацией информационных систем в составе ЕМТС – администраторы информационных систем.

1.3. Изменения в конфигурацию ЕМТС и систему защиты информации

вносятся в соответствии с Правилами, прилагаемыми к настоящему регламенту.

1.4. В целях настоящего регламента под Оператором понимается МКУ «Управление делами администрации города Южно-Сахалинска» и/или структурное подразделение аппарата, отраслевой (функциональный) орган администрации города Южно-Сахалинска, муниципальное предприятие или учреждение в пределах полномочий, установленных постановлением администрации города о возложении обязанностей оператора ЕМТС или постановлением администрации города о создании муниципальной информационной системы в составе ЕМТС.

2. Определение лиц, которым разрешены действия по внесению изменений в конфигурацию

2.1. Лица, которым разрешены действия по внесению изменений в конфигурацию ЕМТС и её системы защиты информации, приведены в п.1.2 настоящего Регламента.

2.2. Полномочия системных администраторов закрепляются в должностных инструкциях, разработанных в соответствии с распоряжением администрации города Южно-Сахалинска об утверждении Порядка разработки и утверждения должностных инструкций сотрудников администрации города Южно-Сахалинска.

3. Управление изменениями конфигурации

3.1. Поиск и получение предложений по изменению конфигурации

3.1.1. Поиск и получение предложений по изменению конфигурации ЕМТС и её системы защиты информации от их разработчиков или уполномоченными ими лиц должны охватывать:

- средства защиты информации;
- системное и прикладное программное обеспечение;
- сетевое оборудование.

3.1.2. Изменения конфигурации средств защиты информации, сертифицированных по требованиям безопасности информации, должны соответствовать требованиям безопасности информации и не снижать общий уровень защищённости ЕМТС.

3.1.3. Каждое изменение конфигурации должно пройти проверку на наличие уязвимости в соответствии с Правилами выявления инцидентов и реагирования на них в ЕМТС.

3.2. Подготовка среды тестирования изменений конфигурации

3.2.1. Методы управления изменениями конфигурации определяются комбинацией подхода к тестированию изменений конфигурации и подхода к развёртыванию релизов с изменениями конфигурации.

3.2.2. Тестирование изменений конфигурации ЕМТС может проводиться:

3.2.2.1. На виртуальных машинах («метод тестирования на макете»);

3.2.2.2. В тестовой среде, идентичной реальной («метод тестирования в тестовой зоне»).

3.2.3. Тестирование изменений конфигурации ЕМТС на виртуальных машинах используется, как правило, для последующего разворачивания изменений конфигурации на рабочих местах пользователей.

3.2.4. Тестирование изменений конфигурации ЕМТС в тестовой среде, идентичной реальной применяется для последующего изменения конфигурации одной или нескольких информационных систем в составе ЕМТС.

3.3. Тестирование изменений конфигурации программного обеспечения

3.3.1. Тестирование изменений конфигурации включает:

3.3.1.1. Попытку войти в систему под тестовой учётной записью после установки изменения конфигурации и перезагрузки системы, анализ сообщений об ошибках/предупреждений системы;

3.3.1.2. Проверку изменений системных переменных (например, PATH);

3.3.1.3. Проверку наличия в журнале системных событий записи об успешности установки всех изменений конфигурации и отсутствии ошибок;

3.3.1.4. Проверку работоспособности прикладного ПО типового автоматизированного рабочего места пользователя ЕМТС (далее - ТАРМ) или ПО соответствующей информационной системы типовой/специальной деятельности.

3.4. Принятие решения о применении протестированного изменения конфигурации

3.4.1. Принятие решения о применении протестированного изменения конфигурации ЕМТС возлагается на соответствующего администратора в зоне его ответственности, определённой в п.1.2 настоящего регламента.

3.4.2. При принятии решения о применении протестированного изменения конфигурации ЕМТС администратору следует принять во внимание:

3.4.2.1. Результаты тестирования изменения конфигурации ЕМТС;

3.4.2.2. Приоритетность изменения конфигурации (критичность изменения конфигурации, уровень опасности уязвимости, которую оно нейтрализует);

3.4.2.3. Возможность нарушения технологических процессов обработки информации в ЕМТС в ходе или в результате установки изменения конфигурации, их важность для функционирования ЕМТС;

3.4.2.4. Возможность отменить («откатить») применение изменений конфигурации.

3.4.3. Применение изменений конфигурации операционной системы и микропрограммного обеспечения серверов, с которых не сделано резервное копирование, не допускается.

3.4.4. Перечни изменений конфигурации для применения должны быть задокументированы.

3.5. Централизованное применение изменений конфигурации

3.5.1. Централизованное применение изменений конфигурации ЕМТС включает:

3.5.1.1. Составление перечней подлежащих к установке изменений

конфигурации (конфиг-листов) отдельно для каждого сервера и ТАРМ;

3.5.1.2. Выбор времени начала изменения конфигурации ЕМТС на каждом сервере и ТАРМ для распределения нагрузки на вычислительные возможности и учёта необходимости перезапуска ЕМТС;

3.5.1.3. Составление задания на применение изменений конфигурации в соответствии с конфиг-листами и временем начала;

3.5.1.4. Запуск изменения конфигурации ЕМТС;

3.5.1.5. Выборочную проверку работоспособности элементов ЕМТС, на которые были применены изменения конфигурации;

3.5.1.6. Выборочную (или полную) проверку устранения выявленных уязвимостей конфигурации ЕМТС;

3.5.1.7. Актуализацию документации ЕМТС в части параметров настройки, версий программных средств в соответствии с применёнными изменениями конфигурации (при необходимости);

3.5.1.8. Пересчёт контрольных сумм файлов с параметрами настройки системного ПО и средств защиты информации, критичных с точки зрения безопасности (при необходимости).

3.5.2. Изменение конфигурации серверов ЕМТС :

3.5.2.1. Изменение конфигурации серверов ЕМТС осуществляется администратором ЕМТС или авторизованным системным администратором.

3.5.2.2. Все изменения конфигурации серверов ЕМТС должны проходить тестирование в тестовой среде не менее двух недель.

3.5.2.3. Для каждого сервера ЕМТС должна регистрироваться история изменений конфигурации, включая список приложений, запущенных на нём при установке изменения конфигурации.

3.5.3. Изменение конфигурации ТАРМ :

3.5.3.1. Изменение конфигурации ТАРМ может быть сделано с помощью штатных средств сертифицированной операционной системы.

3.5.3.2. Все изменения конфигурации ТАРМ должны проходить тестирование не менее двух дней.

3.5.3.3. Результаты изменения конфигурации, включая пересчёт контрольных сумм файлов с параметрами настройки сертифицированной операционной системы и средств защиты информации, критичных с точки зрения безопасности, вносятся в формуляр сертифицированной операционной системы (при необходимости).

4. Анализ потенциального воздействия планируемых изменений в конфигурации на обеспечение защиты информации

4.1. Анализ потенциального воздействия планируемых изменений в конфигурации ЕМТС и её системы защиты информации на обеспечение защиты информации, проводится в ходе тестирования планируемых изменений в конфигурации, проводимого в соответствии с пунктом 3.3. настоящего регламента.

4.2. Согласование изменений в конфигурации ЕМТС и/или входящих в ее

состав информационных систем и компонентов, системы защиты информации, с администратором безопасности ЕМТС, проводится в письменном (с использованием СЭД) или электронном (с использованием OTRS) виде.

4.3. Изменения в конфигурации ЕМТС, и/или входящих в ее состав информационных систем и компонентов, системы защиты информации вносятся только при условии их согласования лицом, указанном в пункте 4.2. настоящего регламента.

5. Документирование информации (данных) об изменениях в конфигурации

5.1. Документированию подлежит следующая информация (данные) об изменениях в конфигурации ЕМТС и системы защиты информации:

5.1.1. Перечни конфигураций для внедрения отдельно для каждого технического средства и программного обеспечения;

5.1.2. Перечни конфигураций ранее внедрённых отдельно по каждому техническому средству и программному обеспечению.

6. Регламентация и контроль технического обслуживания, в том числе дистанционного (удалённого), технических средств и программного обеспечения

6.1. Регламентация технического обслуживания, в том числе дистанционного (удалённого), технических средств и программного обеспечения ЕМТС

6.1.1. Техническое обслуживание, в том числе дистанционное (удалённое), технических средств и программного обеспечения ЕМТС осуществляет:

6.1.1.1. В течение гарантийного срока технических средств и программного обеспечения защиты информации – разработчики этих средств защиты информации или разработчик системы защиты информации ЕМТС

6.1.1.2. В постгарантийный период - Оператор ЕМТС и иное лицо, в соответствии с муниципальным контрактом.

6.1.2. Дистанционное (удалённое) техническое обслуживание технических средств и программного обеспечения допускается при одновременно выполнении следующих условий:

6.1.2.1. Использование средств криптографической защиты каналов дистанционного (удалённого) технического обслуживания, совместимых с криптографическим оборудованием ЕМТС;

6.1.2.2. Осуществление дистанционного (удалённого) технического обслуживания только с рабочего места и/или из информационной системы, аттестованных по требованиям безопасности информации по классу защищённости, не ниже класса сегмента ЕМТС «разработка и сопровождение информационных систем»;

6.1.2.3. Наличие действующего муниципального контракта между Оператором ЕМТС и лицом, осуществляющим дистанционное (удалённое)

техническое обслуживание технических средств и программного обеспечения ЕМТС, с оговоркой соблюдения Исполнителем порядка оборота служебной информации ограниченного распространения, установленного в администрации г.Южно-Сахалинска.

6.2. Контроль технического обслуживания, в том числе дистанционного (удалённого), технических средств и программного обеспечения ЕМТС проводится администратором безопасности ЕМТС по окончанию выполнения текущих работ по техническому обслуживанию в соответствии с Правилами контроля (мониторинга) за обеспечением уровня защищённости информации в ЕМТС.

Приложения :

1. Правила организации идентификации и аутентификации субьектов доступа и объектов доступа в ЕМТС;

2. Правила управления обновлениями программного обеспечения в ЕМТС;

3. Правила контроля (мониторинга) за обеспечением уровня защищённости информации в ЕМТС;

4. Правила использования технологий беспроводного доступа в ЕМТС;

5. Правила информирования и обучения пользователей ЕМТС;

Приложение 1
к Регламенту управления
конфигурацией ЕМТС

Правила организации идентификации и аутентификации субъектов доступа и объектов доступа в ЕМТС

1. Действие настоящих Правил обеспечивается администраторами ЕМТС и системными администраторами, осуществляющими эксплуатацию ЕМТС в пределах делегированных им полномочий.

2. Доступ в ЕМТС должен осуществляться при помощи идентификации и аутентификации пользователей, идентификации процессов, запускаемых от имени этих пользователей, а также процессов, запускаемых от имени системных учетных записей.

2.1. Категории пользователей ЕМТС определены в Положении о ЕМТС, утвержденном постановлением администрации города Южно-Сахалинска о возложении обязанностей оператора ЕМТС.

3. Пользователи ЕМТС должны однозначно идентифицироваться и аутентифицироваться для всех видов доступа, кроме тех видов доступа, которые определяются как действия, разрешенные до идентификации и аутентификации.

4. Оператором ЕМТС устанавливается перечень действий пользователей, разрешенных до прохождения ими процедур идентификации и аутентификации, и запрет действий пользователей, не включенных в перечень разрешенных действий, до прохождения ими процедур идентификации и аутентификации.

4.1. Разрешение действий пользователей до прохождения ими процедур идентификации и аутентификации осуществляется, в том числе, при предоставлении пользователям доступа к публичным ресурсам ЕМТС (веб-сайтам, порталам, иным общедоступным ресурсам).

4.2. Администратору ЕМТС разрешаются действия в обход установленных процедур идентификации и аутентификации, необходимые только для восстановления функционирования ЕМТС в случае сбоев в работе или выходе из строя отдельных технических средств (устройств).

4.3. Системному администратору разрешаются действия в обход установленных процедур идентификации и аутентификации, необходимые для восстановления функционирования отдельных компонентов ЕМТС в случае сбоев в работе или выходе из строя отдельных технических средств (устройств), только в пределах делегированных ему полномочий и с разрешения администратора ЕМТС.

5. Аутентификация пользователя ЕМТС может осуществляться с использованием паролей, аппаратных средств, биометрических характеристик, иных средств или в случае многофакторной (двухфакторной) аутентификации –

определенной комбинации указанных средств. В ЕМТС должна быть обеспечена возможность однозначного сопоставления идентификатора пользователя с запускаемыми от его имени процессами.

6. Оператор ЕМТС устанавливает и обеспечивает реализацию следующих функций управления идентификаторами пользователей и устройств в ЕМТС:

6.1. Определение должностного лица (администратора), ответственного за создание, присвоение и уничтожение идентификаторов пользователей и устройств;

6.2. Формирование идентификатора, который однозначно идентифицирует пользователя и (или) устройство;

6.3. Присвоение идентификатора пользователю и (или) устройству; предотвращение повторного использования идентификатора пользователя и (или) устройства в течение установленного оператором периода времени;

6.4. Блокирование идентификатора пользователя после установленного оператором времени неиспользования.

7. Оператором установлены и реализованы следующие функции управления средствами аутентификации (аутентификационной информацией) пользователей и устройств в ЕМТС :

7.1. Определение должностного лица (администратора), ответственного за хранение, выдачу, инициализацию, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации;

7.2. Изменение аутентификационной информации (средств аутентификации), заданных их производителями и (или) используемых при внедрении системы защиты информации ЕМТС;

7.3. Выдача средств аутентификации пользователям ЕМТС;

7.4. Генерация и выдача начальной аутентификационной информации (начальных значений средств аутентификации);

7.5. Установление характеристик пароля (при использовании в информационной системе механизмов аутентификации на основе пароля):

7.5.1. Задание минимальной сложности пароля с определяемыми требованиями к регистру, количеству символов, сочетанию букв верхнего и нижнего регистра, цифр и специальных символов;

7.5.2. Задание минимального количества измененных символов при создании новых паролей;

7.5.3. Задание максимального времени действия пароля;

7.5.4. Задание минимального времени действия пароля;

7.5.5. Запрет на использование пользователями определенного Оператором числа последних использованных паролей при создании новых паролей;

7.6. Блокирование (прекращение действия) и замена утерянных, скомпрометированных или поврежденных средств аутентификации;

7.7. Назначение необходимых характеристик средств аутентификации (в том числе механизма пароля);

7.8. Обновление аутентификационной информации (замена средств

аутентификации) с периодичностью, установленной оператором;

7.9. Защита аутентификационной информации от неправомерных доступа к ней и модифицирования.

8. В ЕМТС должна осуществляться защита аутентификационной информации в процессе ее ввода для аутентификации от возможного использования лицами, не имеющими на это полномочий. Защита обратной связи «система - субъект доступа» в процессе аутентификации обеспечивается исключением отображения для пользователя действительного значения аутентификационной информации и (или) количества вводимых пользователем символов аутентификационной информации.

9. В ЕМТС должна осуществляться однозначная идентификация и аутентификация внешних пользователей или процессов, запускаемых от имени этих пользователей.

10. В установленных законодательством случаях идентификация и аутентификация пользователей ЕМТС в целях предоставления государственных и муниципальных услуг в электронной форме должна осуществляется с использованием единой системы идентификации и аутентификации, созданной в соответствии с постановлением Правительства РФ от 28 ноября 2011 г. № 977.

11. Оператором ЕМТС установлены и реализованы следующие функции управления учетными записями пользователей :

11.1. Определение типа учетной записи (внутреннего пользователя, внешнего пользователя, системная, приложения, гостевая (анонимная), временная и (или) иные типы записей);

11.2. Объединение учетных записей в группы (при необходимости);

11.3. Верификацию пользователя (проверка личности пользователя, его должностных (функциональных) обязанностей) при заведении учетной записи пользователя;

11.4. Заведение, активация, блокирование и уничтожение учетных записей пользователей;

11.5. Пересмотр и, при необходимости, корректировка учетных записей пользователей с периодичностью, определяемой оператором;

11.6. Порядок заведения и контроля использования гостевых (анонимных) и временных учетных записей пользователей, а также привилегированных учетных записей администраторов;

11.7. Оповещение администратора, осуществляющего управление учетными записями пользователей, об изменении сведений о пользователях, их ролях, обязанностях, полномочиях, ограничениях;

11.8. Уничтожение временных учетных записей пользователей, предоставленных для однократного (ограниченного по времени) выполнения задач в информационной системе;

11.9. Предоставление пользователям прав доступа к объектам доступа ЕМТС, основываясь на задачах, решаемых пользователями в ЕМТС и взаимодействующими с ней информационными системами;

12. Временная учетная запись может быть заведена для пользователя

ЕМТС на ограниченный срок для выполнения задач, требующих расширенных полномочий, или для проведения настройки, тестирования информационной системы в составе ЕМТС, для организации гостевого доступа (посетителям, сотрудникам сторонних организаций, стажерам и иным пользователям с временным доступом к информационной системе в составе ЕМТС).

13. В ЕМТС для управления доступом субъектов доступа к объектам доступа должны быть реализованы установленные оператором методы управления доступом, назначены типы доступа субъектов к объектам доступа и реализованы правила разграничения доступа субъектов доступа к объектам доступа.

14. Методы управления доступом реализуются в зависимости от особенностей функционирования сегмента ЕМТС с учетом угроз безопасности информации и должны включать один или комбинацию следующих методов:

14.1. Дискреционный метод управления доступом, предусматривающий управление доступом субъектов доступа к объектам доступа на основе идентификационной информации субъекта и для каждого объекта доступа – списка, содержащего набор субъектов доступа (групп субъектов) и ассоциированных с ними типов доступа;

14.2. Ролевой метод управления доступом, предусматривающий управление доступом субъектов доступа к объектам доступа на основе ролей субъектов доступа (совокупность действий и обязанностей, связанных с определенным видом деятельности);

14.3. Мандатный метод управления доступом, предусматривающий управление доступом субъектов доступа к объектам доступа на основе сопоставления классификационных меток каждого субъекта доступа и каждого объекта доступа, отражающих классификационные уровни субъектов доступа и объектов доступа, являющиеся комбинациями иерархических и неиерархических категорий.

15. Типы доступа к объектам доступа должны включать операции по чтению, записи, удалению, выполнению и иные операции, разрешенные к выполнению пользователем (группе пользователей) или запускаемому от его имени процессу при доступе к объектам доступа.

16. Правила разграничения доступа реализуются на основе установленных оператором списков доступа или матриц доступа и должны обеспечивать управление доступом пользователей (групп пользователей) и запускаемых от их имени процессов при входе в систему, доступе к техническим средствам, устройствам, объектам файловой системы, запускаемым и исполняемым модулям, объектам систем управления базами данных, объектам, создаваемым прикладным и специальным программным обеспечением, параметрам настройки средств защиты информации, информации о конфигурации системы защиты информации и иной информации о функционировании системы защиты информации, а также иным объектам доступа.

17. Оператором ЕМТС должно быть обеспечено разделение полномочий

(ролей) пользователей и администраторов, обеспечивающих функционирование ЕМТС и/или информационных систем в ее составе, в соответствии с их должностными обязанностями (функциями), фиксирование в организационно-распорядительных документах по защите информации (документирование) полномочий (ролей) пользователей и администраторов, обеспечивающих функционирование ЕМТС и/или информационных систем в ее составе, а также санкционирование доступа к объектам доступа в соответствии с разделением полномочий (ролей).

18. Оператором должно быть обеспечено назначение прав и привилегий пользователям и запускаемым от их имени процессам, администраторам, обеспечивающим функционирование ЕМТС и/или информационных систем в ее составе, минимально необходимых для выполнения ими своих должностных обязанностей (функций), и санкционирование доступа к объектам доступа в соответствии с минимально необходимыми правами и привилегиями.

19. Оператором ЕМТС должны быть однозначно определены и зафиксированы в организационно-распорядительных документах по защите информации (задокументированы) роли и (или) должностные обязанности (функции), также объекты доступа, в отношении которых установлен наименьший уровень привилегий.

20. В ЕМТС должно быть установлено и зафиксировано в организационно-распорядительных документах по защите информации (задокументировано) ограничение количества неуспешных попыток входа в ЕМТС (доступа к ЕМТС) за период времени, установленный оператором, а также обеспечено блокирование устройства, с которого предпринимаются попытки доступа, и (или) учетной записи пользователя при превышении пользователем ограничения количества неуспешных попыток входа в ЕМТС (доступа к ЕМТС).

21. В ЕМТС должно обеспечиваться блокирование сеанса доступа пользователя после установленного оператором времени его бездействия (неактивности) в ЕМТС или по запросу пользователя.

21.1. Блокирование сеанса доступа пользователя в информационную систему обеспечивает временное приостановление работы пользователя со средством вычислительной техники, с которого осуществляется доступ к ЕМТС (без выхода из ЕМТС). Для заблокированного сеанса должно осуществляться блокирование любых действий по доступу к информации и устройствам отображения, кроме необходимых для разблокирования сеанса.

22. Оператором должна обеспечиваться защита информации при доступе пользователей (процессов запускаемых от имени пользователей) и (или) иных субъектов доступа к объектам доступа ЕМТС через информационно-телекоммуникационные сети, в том числе сети связи общего пользования, с использованием стационарных и (или) мобильных технических средств (защита удаленного доступа).

23. Защита удаленного доступа должна обеспечиваться при всех видах доступа (беспроводной, проводной (коммутируемый), широкополосный и иные

виды доступа) и включает:

23.1. Установление (в том числе документальное) видов доступа, разрешенных для удаленного доступа к объектам доступа ЕМТС;

23.2. Ограничение на использование удаленного доступа в соответствии с задачами (функциями) ЕМТС, для решения которых такой доступ необходим, и предоставление удаленного доступа для каждого разрешенного вида удаленного доступа;

23.3. Предоставление удаленного доступа только тем пользователям, которым он необходим для выполнения установленных должностных обязанностей (функций);

23.4. Мониторинг и контроль удаленного доступа на предмет выявления несанкционированного удаленного доступа к объектам доступа ЕМТС;

23.5. Контроль удаленного доступа пользователей (процессов запускаемых от имени пользователей) к объектам доступа ЕМТС до начала информационного взаимодействия с ЕМТС (передачи защищаемой информации).

24. Оператором должны обеспечиваться регламентация и контроль использования в ЕМТС технологий беспроводного доступа пользователей к объектам доступа (стандарты коротковолновой радиосвязи, спутниковой и пакетной радиосвязи), направленные на защиту информации в ЕМТС.

25. Регламентация и контроль использования технологий беспроводного доступа должны включать:

25.1. Ограничение на использование технологий беспроводного доступа (беспроводной передачи данных, беспроводного подключения оборудования к сети, беспроводного подключения устройств к средству вычислительной техники) в соответствии с задачами (функциями) ЕМТС, для решения которых такой доступ необходим, и предоставление беспроводного доступа;

25.2. Предоставление технологий беспроводного доступа только тем пользователям, которым он необходим для выполнения установленных должностных обязанностей (функций);

25.3. Мониторинг и контроль применения технологий беспроводного доступа на предмет выявления несанкционированного использования технологий беспроводного доступа к объектам доступа ЕМТС;

25.4. Контроль беспроводного доступа пользователей (процессов запускаемых от имени пользователей) к объектам доступа ЕМТС до начала информационного взаимодействия с ЕМТС.

26. Оператором должны обеспечиваться регламентация и контроль использования в ЕМТС мобильных технических средств, направленные на защиту информации в ЕМТС.

В качестве мобильных технических средств рассматриваются съемные машинные носители информации (флэш-накопители, внешние накопители на жестких дисках и иные устройства), портативные вычислительные устройства и устройства связи с возможностью обработки информации (ноутбуки, нетбуки, планшеты, сотовые телефоны, цифровые камеры, звукозаписывающие

устройства и иные устройства).

27. Регламентация и контроль использования мобильных технических средств должны включать:

27.1. Установление (в том числе документальное) видов доступа (беспроводной, проводной (коммутируемый), широкополосный и иные виды доступа), разрешенных для доступа к объектам доступа ЕМТС с использованием мобильных технических средств, входящих в состав ЕМТС;

27.1. Использование в составе ЕМТС для доступа к объектам доступа мобильных технических средств (служебных мобильных технических средств), в которых реализованы меры защиты информации;

27.2. Ограничение на использование мобильных технических средств в соответствии с задачами (функциями) ЕМТС, для решения которых использование таких средств необходимо, и предоставление доступа с использованием мобильных технических средств;

27.3. Мониторинг и контроль применения мобильных технических средств на предмет выявления несанкционированного использования мобильных технических средств для доступа к объектам доступа ЕМТС;

27.4. Запрет возможности запуска без команды пользователя в ЕМТС программного обеспечения (программного кода), используемого для взаимодействия с мобильным техническим средством.

28. Оператором должно быть обеспечено управление взаимодействием с внешними информационными системами, включающими информационные системы и вычислительные ресурсы (мощности) уполномоченных лиц, информационные системы, с которыми установлено информационное взаимодействие на основании заключенного договора (соглашения), а также с иными информационными системами, информационное взаимодействие с которыми необходимо для функционирования ЕМТС.

29. Управление взаимодействием с внешними информационными системами должно включать:

29.1. Предоставление доступа к внешней информационной системе только авторизованным (уполномоченным) пользователям ЕМТС;

29.2. Определение типов прикладного программного обеспечения ЕМТС, к которым разрешен доступ авторизованным (уполномоченным) пользователям из внешних информационных систем;

29.3. Определение системных учетных записей, используемых в рамках данного взаимодействия;

29.4. Определение порядка предоставления доступа к ЕМТС авторизованными (уполномоченным) пользователями из внешних информационных систем;

29.5. Определение порядка обработки, хранения и передачи информации с использованием внешних информационных систем.

Приложение 2
к Регламенту управления
конфигурацией ЕМТС

ПРАВИЛА
управления обновлениями программного обеспечения в ЕМТС

1. Общие положения

1.1. Настоящие Правила определяют порядок осуществления следующих процессов обеспечения защиты информации в ЕМТС :

1.1.1. Определение необходимости установки обновлений программного обеспечения (далее – ПО);

1.1.2. Поиск и получение обновлений ПО от разработчика или уполномоченного им лица;

1.1.3. Подготовка среды тестирования обновлений ПО;

1.1.4. Установка обновлений ПО в среде тестирования;

1.1.5. Тестирование обновлений ПО;

1.1.6. Принятие решения о развёртывании протестированного обновления;

1.1.7. Централизованная установка обновлений ПО.

1.2. Целью управления обновления ПО является минимизация риска эксплуатации известных уязвимостей безопасности информации.

1.3. Лицами, ответственными за управление обновлениями ПО ЕМТС, являются:

1.3.1. В части управления обновлениями ПО активных и пассивных сетевых устройств – администраторы ЕМТС и/или системные администраторы, в пределах делегированных им полномочий;

1.3.2. В части управления обновлениями ПО информационных систем в составе ЕМТС – системные администраторы, в пределах делегированных им полномочий;

1.3.3. В остальном (в части управления обновлениями операционных систем и прикладного ПО рабочих мест пользователей, микропрограммного обеспечения BIOS/UEFI, прошивок периферийных устройств и др.) – системные администраторы, в пределах делегированных им полномочий.

2. Определение необходимости установки обновлений программного обеспечения

2.1. Необходимость установки обновлений ПО определяется по результатам:

2.1.1. Анализа общедоступных источников на предмет наличия опубликованных уязвимостей и патчей (эксплойтов, релизов) для каждого ПО, используемого в ЕМТС;

2.1.2. Автоматического сканирования с помощью программных утилит поставщика или использования веб-сайта поставщика ПО для сканирования системы, на предмет наличия доступных обновлений, которые ещё не были установлены в ЕМТС;

2.1.3. Контроля (анализа) защищённости ЕМТС, в процессе которого детектируются уязвимости в ПО ЕМТС.

2.2. Для обеспечения анализа общедоступных источников на предмет наличия опубликованных уязвимостей и патчей для каждого ПО, используемого в ЕМТС, администраторам в зоне их ответственности, указанной в п.1.3 настоящих Правил, необходимо вести перечни ПО, установленного на всех серверах, рабочих местах пользователей, мобильных устройствах, сетевом оборудовании и других компонентах ЕМТС.

2.3. Автоматическое сканирование сети Интернет на предмет наличия доступных обновлений допускается для следующего ПО ЕМТС:

2.3.1. Офисного ПО;

2.3.2. Браузеров.

2.4. Контроль (анализ) защищённости ЕМТС должен осуществляться не реже 4 раз в год.

2.5. ПО вводимых в эксплуатацию новых серверов и нетиповых автоматизаированных рабочих мест пользователей ЕМТС в форматах настольных компьютеров, ноутбуков, нетбуков, планшетов и аналогичных, должно быть полностью обновлено до первого выхода в Интернет из ЕМТС, чтобы ограничить входящие угрозы.

2.6. Новое ПО, предназначенное для установки (инсталляции) в информационные системы в составе ЕМТС должно быть полностью обновлено до установки (инсталляции) в ЕМТС, чтобы ограничить входящие угрозы.

3. Поиск и получение обновлений программного обеспечения

3.1. Поиск и получение обновлений ПО от разработчика или уполномоченного им лица должны охватывать:

3.1.1. Сервис-паки (релизы);

3.1.2. Периодические (ежеквартальные, ежемесячные, еженедельные и др.) обновления;

3.1.3. Критические обновления, устраняющие известные уязвимости критического или высокого уровней опасности.

3.2. Обновления средств защиты информации, сертифицированных по требованиям безопасности информации, должны загружаться только из соответствующего надёжного источника. Каждое такое обновление должно пройти проверку в порядке, установленном формуляром на средство защиты информации.

3.3. Каждое обновление должно пройти проверку на целостность и отсутствие вредоносного кода.

4. Подготовка среды тестирования обновлений программного обеспечения

4.1. Методы управления обновлениями определяются комбинацией подхода к тестированию обновлений и подхода к развёртыванию релизов с обновлениями.

4.2. Тестирование обновлений ПО может проводиться:

4.2.1. На виртуальных машинах («метод тестирования на макете»);

4.2.2. В тестовой среде, идентичной реальной («метод тестирования в тестовой зоне»).

4.3. Тестирование обновлений ПО на виртуальных машинах используется, как правило, для последующего разворачивания обновлений в ТАРМ.

4.4. Тестирование обновлений ПО в тестовой среде, идентичной реальной, для последующего применения обновлений ПО в одной или нескольких информационных системах в составе ЕМТС.

5. Тестирование обновлений программного обеспечения

5.1. Тестирование обновлений включает:

5.1.1. Попытку войти в ЕМТС под тестовой учётной записью после установки обновления и перезагрузки ПО, анализ сообщений об ошибках/предупреждений системы;

5.1.2. Проверку изменений системных переменных (например, PATH);

5.1.3. Проверку наличия в журнале системных событий записи об успешности установки всех обновлений и отсутствии ошибок;

5.1.4. Проверку работоспособности обновленного ПО с прикладным ПО (офисные приложения, браузеры, и т.п.).

6. Принятие решения о развёртывании протестированного обновления

6.1. Принятие решения о развёртывании протестированного обновления ПО возлагается на соответствующего администратора в зоне его ответственности, определённой в п.1.3 настоящих Правил.

6.2. При принятии решения о развёртывании протестированного обновления ПО администратору следует принять во внимание:

6.2.1. Результаты тестирования обновления ПО;

6.2.2. Приоритетность обновления (критичность обновления, уровень опасности уязвимости, которую оно устраняет);

6.2.3. Необходимость установки предыдущих, связанных с протестированным обновлением, патчей;

6.2.4. Зависимости других программ от ПО, для которого протестировано обновление;

6.2.5. Возможность нарушения технологических процессов в ходе или в результате установки обновления, их важность для функционирования ЕМТС;

6.2.6. Наличие предупреждений разработчика обновления о совместимости с актуальными версиями иного ПО, установленного в ЕМТС;

6.2.7. Возможность отменить («откатить») установку обновлений.

6.3. Установка обновления на операционную систему и микропрограммное обеспечения сервера, с которых не сделано резервное копирование, не допускается.

6.4. Перечни обновлений для развёртывания должны быть задокументированы.

7. Централизованная установка обновлений программного обеспечения

7.1. Централизованная установка обновлений ПО включает :

7.1.1. Составление перечней подлежащих к установке обновлений (патч-листов) отдельно для каждого сервера и ТАРМ;

7.1.2. Выбор времени начала обновления ПО на каждом сервере и ТАРМ для распределения нагрузки на вычислительные ресурсы ЕМТС и учёта необходимости перезапуска ПО;

7.1.3. Составление задания на разворачивание обновлений в соответствии с патч-листами и временем начала;

7.1.4. Запуск обновления ПО;

7.1.5. Выборочную проверку работоспособности элементов ЕМТС, на которые была проведена установка обновлений;

7.1.6. Выборочную (или полную) проверку устранения выявленных уязвимостей безопасности информации;

7.1.7. Актуализацию документации ЕМТС в части параметров настройки, версий программных средств в соответствии с применёнными обновлениями (при необходимости);

7.1.8. Пересчёт контрольных сумм файлов, критичных с точки зрения безопасности (при необходимости).

7.2. Обновление ПО серверов

7.2.1. Обновление ПО серверов осуществляется администратором ЕМТС или системным администратором, в пределах делегированных им полномочий.

7.2.2. Проверка наличия обновлений ПО серверов должна осуществляться не реже одного раза в месяц.

7.2.3. Все обновления ПО серверов должны проходить тестирование в тестовой среде не менее двух недель.

7.2.4. Для каждого сервера должна регистрироваться история обновлений, включая список приложений, запущенных на нём при установке обновления.

7.3. Обновление ПО ТАРМ

7.3.1. Обновление ПО ТАРМ может быть сделано с помощью штатных средств сертифицированной операционной системы.

7.3.2. Проверка наличия обновлений ПО ТАРМ должна осуществляться не реже одного раза в неделю.

7.3.4. Все обновления ПО ТАРМ должны проходить тестирование не менее двух дней.

7.3.5. Обновление операционной системы ТАРМ отображается в формуляре сертифицированной версии операционной системы.

8. Обязанности администраторов и пользователей

8.1. Обязанности системных администраторов

8.1.1. Системные администраторы должны осуществлять управление обновлением ПО в зоне своей ответственности, определённой в п.1.3 настоящих Правил.

8.2. Обязанности пользователей ЕМТС

8.2.1. Все пользователи ЕМТС должны быть осведомлены о важности обновления ПО своих рабочих мест пользователя ЕМТС и возможных последствиях их отсутствия.

8.2.2. Пользователи ЕМТС не должны препятствовать процедуре обновления ПО, в том числе отключать функции автоматического обновления.

8.2.3. Пользователи ЕМТС обязаны уведомлять администратора безопасности ЕМТС о своих подозрениях, что их рабочее место пользователя ЕМТС не получает обновлений.

Приложение 3
к Регламенту управления
конфигурацией ЕМТС

Правила контроля (мониторинга) за обеспечением уровня защищённости информации в ЕМТС

1. Выявление, анализ и устранение уязвимостей информационной безопасности ЕМТС

1.1. Администратор безопасности ЕМТС должен осуществлять выявление, анализ и устранение уязвимостей безопасности информации в ЕМТС (далее — уязвимости ЕМТС) с использованием средств анализа защищенности.

1.2. Обязанность выявления, анализа и устранения уязвимостей информационных систем в составе ЕМТС возлагается на соответствующих системных администраторов.

1.3. Во время анализа и устранения уязвимостей ЕМТС должны проводиться:

1.3.1. Выявление (поиск) уязвимостей, связанных с ошибками кода в программном (микропрограммном) обеспечении (общесистемном, прикладном, специальном), а также программном обеспечении средств защиты информации, правильностью установки и настройки средств защиты информации, технических средств и программного обеспечения, а также корректностью работы средств защиты информации при их взаимодействии с техническими средствами и программным обеспечением;

1.3.2. Устранение выявленных уязвимостей, в том числе путем установки обновлений программного обеспечения средств защиты информации, общесистемного программного обеспечения, прикладного программного обеспечения или микропрограммного обеспечения технических средств;

1.3.3. Информирование должностных лиц оператора ЕМТС о результатах выявленных уязвимостей и оценки достаточности реализованных мер защиты информации (при необходимости).

1.4. Выявление (поиск), анализ и устранение уязвимостей должны проводиться на этапах создания и эксплуатации информационной системы в составе ЕМТС. На этапе эксплуатации информационной системы в составе ЕМТС поиск и анализ уязвимостей проводится с периодичностью не реже 1 раз в год.

1.5. В случае невозможности устранения выявленных уязвимостей путем установки обновлений программного обеспечения средств защиты информации, общесистемного программного обеспечения, прикладного программного обеспечения или микропрограммного обеспечения технических средств необходимо предпринять действия (настройки средств защиты

информации, изменение режима и порядка использования информационной системы), направленные на устранение возможности использования выявленных уязвимостей.

2. Контроль установки обновлений программного обеспечения, включая программное обеспечение средств защиты информации

2.1. Администратор безопасности ЕМТС, а так же системный администратор по согласованию с администратором безопасности ЕМТС, должны осуществлять контроль установки обновлений программного обеспечения, включая программное обеспечение средств защиты информации и программное обеспечение базовой системы ввода-вывода.

2.2. Получение обновлений должно осуществляться из доверенных источников, включая программное обеспечение средств защиты информации и программное обеспечение базовой системы ввода-вывода.

2.3. Во время контроля установки обновлений необходимо производить проверку соответствия версий общесистемного, прикладного и специального программного (микропрограммного) обеспечения, включая программное обеспечение средств защиты информации, установленного в ЕМТС и выпущенного разработчиком, а также наличие отметок в эксплуатационной документации (формуляре или паспорте) об установке (применении) обновлений.

2.4. Контроль установки обновлений осуществляется в соответствии с эксплуатационной документацией на соответствующее программное обеспечение.

3. Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации

3.1. Администратор безопасности ЕМТС должен проводить контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации.

3.2. Во время контроля работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации осуществляется:

3.2.1. Контроль работоспособности программного обеспечения и средств защиты информации;

3.2.2. Проверка правильности функционирования (тестирование на тестовых данных, приводящих к известному результату) программного обеспечения и средств защиты информации;

3.2.3. Контроль соответствия настроек программного обеспечения и средств защиты информации параметрам настройки, приведенным в эксплуатационной документации на систему защиты информации и средства защиты информации;

3.2.4. Восстановление работоспособности (правильности

функционирования) и параметров настройки программного обеспечения и средств защиты информации (при необходимости), в том числе с использованием резервных копий и (или) дистрибутивов.

3.3. Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации проводится с периодичностью, установленной эксплуатационной документацией на соответствующие средства защиты информации.

4. Контроль состава технических средств, программного обеспечения и средств защиты информации

4.1. Администратор безопасности ЕМТС должен проводить контроль состава технических средств, программного обеспечения и средств защиты информации, применяемых в ЕМТС (инвентаризация).

4.2. Во время контроля состава технических средств, программного обеспечения и средств защиты информации осуществляется:

4.2.1. Контроль соответствия состава технических средств, программного обеспечения и средств защиты информации приведенному;

4.2.2. Контроль состава технических средств, программного обеспечения и средств защиты информации на соответствие сведениям действующей (актуализированной) эксплуатационной документации и принятие мер, направленных на устранение выявленных недостатков;

4.2.3. Контроль выполнения условий и сроков действия сертификатов соответствия на средства защиты информации и принятие мер, направленных на устранение выявленных недостатков;

4.2.4. Исключение (восстановление) из состава информационной системы несанкционированно установленных (удаленных) технических средств, программного обеспечения и средств защиты информации.

4.3. Контроль состава технических средств, программного обеспечения и средств защиты информации проводится с периодичностью не реже 1 раза в месяц.

5. Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей ЕМТС

5.1. Администратор безопасности ЕМТС должен проводить контроль правил генерации и смены паролей пользователей ЕМТС, а также заведения и удаления учетных записей пользователей ЕМТС, реализации правил разграничения доступом, полномочий пользователей ЕМТС.

5.2. Во время контроля правил генерации и смены паролей пользователей ЕМТС, заведения и удаления учетных записей пользователей ЕМТС, реализации правил разграничения доступом, полномочий пользователей ЕМТС осуществляется:

5.2.1. Контроль правил генерации и смены паролей пользователей;

5.2.2. Контроль заведения и удаления учетных записей пользователей;

5.2.3. Контроль реализации правил разграничения доступом;

5.2.4. Контроль реализации полномочий пользователей;

5.2.5. Контроль наличия документов, подтверждающих разрешение изменений учетных записей пользователей, их параметров, правил разграничения доступом и полномочий пользователей, предусмотренных организационно-распорядительными документами по защите информации оператора;

5.2.6. Устранение нарушений, связанных с генерацией и сменой паролей пользователей, заведением и удалением учетных записей пользователей, реализацией правил разграничения доступом, установлением полномочий пользователей.

5.2.7. Контроль правил генерации и смены паролей пользователей ЕМТС, заведения и удаления учетных записей пользователей ЕМТС, реализации правил разграничения доступом, полномочий пользователей ЕМТС проводится с периодичностью не реже 1 раза в квартал.

Приложение 4
к Регламенту управления
конфигурацией ЕМТС

Правила
использования технологий беспроводного доступа в ЕМТС

1. Общие положения

1.1. Регламент использования ресурсов ЕМТС, включая порядок предоставления пользователям ЕМТС доступа к сети Интернет и общие ограничения доступа пользователей ЕМТС к отдельным ресурсам (категориям ресурсов) сети Интернет, утвержден постановлением администрации города Южно-Сахалинска о возложении обязанностей оператора ЕМТС.

1.2. Настройку ограничений доступа пользователей ЕМТС к ресурсам ЕМТС, включая доступ к сети Интернет, осуществляют администратор ЕМТС или системный администратор, в соответствии с делегированными им полномочиями.

2. Беспроводной доступ для мобильных устройств

2.1. В зданиях и помещениях структурных подразделений аппарата, отраслевых (функциональных) органов администрации города Южно-Сахалинска, муниципальных предприятий и учреждений, организованы беспроводные сети в составе ЕМТС, доступ к которым возможен только для пользователей ЕМТС, использующих мобильные устройства, зарегистрированные в Управлении информатизации МКУ «Управление делами администрации города Южно-Сахалинска».

2.2. Регистрация мобильного устройства для доступа в беспроводную сеть в составе ЕМТС осуществляется в порядке, установленном п.4.3. Нормативов и порядка формирования типового рабочего места пользователя ЕМТС, утвержденного постановлением администрации города о возложении обязанностей оператора ЕМТС.

2.3. Мобильные устройства, подключенные к беспроводной сети в составе ЕМТС, подключаются к ресурсам ЕМТС в соответствии с требованиями информационной безопасности соответствующих типовых сегментов ЕМТС и условий их эксплуатации.

2.4. Самостоятельное подключение пользователем ЕМТС не зарегистрированного мобильного устройства к беспроводной сети в составе ЕМТС, а равно попытка такого подключения или попытка доступа с зарегистрированного мобильного устройства к ресурсам ЕМТС, доступ к которым пользователя ЕМТС и/или зарегистрированного мобильного устройства ограничен или запрещен, квалифицируется как инцидент информационной безопасности и влечет принятие мер, предусмотренных Порядком выявления инцидентов в ЕМТС и реагирования на них, утвержденных настоящим распоряжением.

Приложение 5
к Регламенту управления
конфигурацией ЕМТС

ПРАВИЛА
информирования и обучения пользователей ЕМТС

1. Общие положения

1.1. Настоящие Правила определяют содержание и процедуры следующих процессов обеспечения защиты информации в ЕМТС :

1.1.1. Информирование пользователей ЕМТС об угрозах безопасности информации, о правилах эксплуатации системы защиты информации ЕМТС и отдельных средств защиты информации;

1.1.2. Обучение пользователей ЕМТС правилам эксплуатации системы защиты информации ЕМТС и отдельных средств защиты информации;

1.1.3. Проведение практических занятий с пользователями ЕМТС по правилам эксплуатации системы защиты информации ЕМТС и отдельных средств защиты информации.

1.2. Целью информирования и обучения пользователей ЕМТС является повышение уровня знаний пользователей и администраторов ЕМТС в сфере защиты информации.

1.3. Лицом, ответственным организацию информирования и обучения пользователей ЕМТС, является администратор безопасности ЕМТС.

2. Информирование пользователей ЕМТС об угрозах безопасности информации, о правилах эксплуатации системы защиты информации и отдельных средств защиты информации

2.1. Пользователи ЕМТС, до начала самостоятельной обработки в ЕМТС информации, должны пройти инструктаж по обеспечению безопасности информации, на котором до пользователей ЕМТС должны быть доведены:

2.1.1. Перечень угроз безопасности информации ЕМТС;

2.1.2. Правила эксплуатации системы защиты информации ЕМТС;

2.1.3. Правила эксплуатации отдельных средств защиты информации;

2.1.4. Ответственность за нарушение требований защиты информации.

2.2. Пользователи ЕМТС, не прошедшие инструктаж, к работе в ЕМТС не допускаются.

3. Обучение пользователей ЕМТС правилам эксплуатации системы и средств защиты информации

3.1. Обучение пользователей ЕМТС правилам эксплуатации системы защиты информации ЕМТС и отдельных средств защиты информации должно охватывать требования законодательства, нормативных правовых актов и методических документов федеральных органов исполнительной власти,

уполномоченных в области обеспечения безопасности и технической защиты информации, в сфере:

3.1.1. Защиты информации;

3.1.2. Обработки информации в муниципальных информационных системах;

3.1.3. Обработки служебной информации ограниченного распространения;

3.1.4. Межведомственного взаимодействия.

3.2. Обучение пользователей ЕМТС может проводиться в форме самоподготовки должно охватывать:

3.2.1. Руководящие и нормативно-методические документы в области защиты информации и обеспечения безопасности служебной информации ограниченного распространения;

3.2.2. Правила эксплуатации системы защиты информации ЕМТС;

3.2.3. Правила эксплуатации отдельных средств защиты информации;

3.2.4. Муниципальные правовые акты и/или локальные нормативные акты) администрации города Южно-Сахалинска, отраслевых (функциональных) органов, муниципальных предприятий или учреждений, устанавливающие порядок обращения со служебной информацией ограниченного распространения и ее защиты.

3.2.5. Время для самостоятельного изучения определяется непосредственным руководителем пользователя ЕМТС.

3.2.6. При необходимости возможно направление пользователя ЕМТС на профильные курсы повышения квалификации.

4. Проведение практических занятий с пользователями ЕМТС по правилам эксплуатации ЕМТС и средств защиты информации

4.1. Практические занятия с пользователями ЕМТС по правилам эксплуатации системы защиты информации ЕМТС и отдельных средств защиты информации проводятся по мере необходимости под руководством администратора безопасности ЕМТС или системного администратора.

4.2. В ходе практических занятий:

4.2.1. Проверяются знания пользователями ЕМТС положений нормативной документации по вопросам обеспечения безопасности служебной информации ограниченного распространения, обрабатываемой в ЕМТС;

4.2.2. Прививаются (или повышаются) навыки пользователей ЕМТС в части защиты информации.

4.3. Практические занятия с пользователями ЕМТС могут проводиться:

4.3.1. На виртуальных машинах («на макете»);

4.3.2. В тестовой среде, идентичной реальной («в тестовой зоне»).

Приложение № 2
УТВЕРЖДЕН
распоряжением администрации
города Южно-Сахалинска
от 22.07.2019 № 451-р

ПОРЯДОК
выявления инцидентов безопасности в ЕМТС и реагирования на них

1. Общие положения

1.1. Настоящий Порядок определяет процедуры обнаружения и выявления инцидентов безопасности информации, обрабатываемой в ЕМТС (далее — инцидент), информирования о произошедших инцидентах, анализа и идентификации инцидентов и мер по их устранению, планирования и принятия мер по предотвращению инцидентов, определяет лиц, ответственных за выявление инцидентов, права и обязанности лиц, ответственных за организацию выявления инцидентов, управления инцидентами и реагирования на них.

1.2. В целях регулирования настоящим Порядком применяются следующие определения :

1.2.1. Инцидент — одно или несколько нежелательных или неожиданных событий информационной безопасности (далее - ИБ), имеющих значительную вероятность создания и/или реализации угрозы ИБ ЕМТС.

1.2.2. Администратор безопасности ЕМТС — сотрудник МКУ «Управление делами администрации города Южно-Сахалинска», на которого возложена организация выявления инцидентов, в т.ч. первичная обработка информации, поступающей из источников, указанных в п.1.3. настоящего порядка.

1.2.3. Уполномоченное лицо — сотрудник Департамента мобилизационной подготовки и защиты информации, на которого возложены планирование и проведение мероприятий по реагированию на выявленные инциденты.

1.3. Основными источниками информации об инцидентах являются:

1.3.1. Факты нарушения ИБ или предпосылок к нарушению ИБ, выявленные пользователем ЕМТС, администратором безопасности ЕМТС, администратором ЕМТС или системным администратором, а так же обладателем информации, обрабатываемой в ЕМТС (далее — сотрудник Оператора);

1.3.2. Результаты работы технических средств защиты информации, обрабатываемой в ЕМТС;

1.3.3. Запросы и предписания органов, осуществляющих контрольно-надзорные функции в установленной сфере деятельности;

1.3.4. Другие источники информации.

2. Порядок определения лиц, ответственных за выявление инцидентов и реагирования на них

2.1. МКУ «Управление делами администрации города Южно-Сахалинска» обеспечивает выявление инцидентов, источники информации о которых указаны в п.1.3. настоящего порядка.

2.2. Департамент мобилизационной подготовки и защиты информации обеспечивает планирование и проведение мероприятий по реагированию на выявленные инциденты.

2.3. Постановлением администрации города о создании муниципальной информационной системы в составе ЕМТС могут устанавливаться иные лица, ответственные за выявление инцидентов и реагирование на них в создаваемых информационных системах в составе ЕМТС.

3. Порядок обнаружения и выявления инцидента

3.1. Сотрудник Оператора может выявить признаки наличия инцидента путем анализа соответствия текущей ситуации требованиям ИБ ЕМТС.

3.2. Наличие одного из следующих несоответствий, даёт основание предполагать факт возникновения инцидента :

3.2.1. Нарушение Инструкции пользователя ЕМТС, установленных в ЕМТС правил и регламентов ИБ;

3.2.2. Нарушения в работе технических средств ЕМТС;

3.2.3. Выявленные ошибки в работе программных средств ЕМТС;

3.2.4. Неисправность технических и программных средств защиты информации в ЕМТС;

3.2.5. Другие ситуации и факты, критические для ИБ по мнению пользователя ЕМТС.

4. Порядок информирования об инцидентах

4.1. Любые сведения о происшествии или инциденте должны быть незамедлительно переданы выявившим их сотрудником своему непосредственному руководителю, а впоследствии – администратору безопасности ЕМТС, любым доступным способом:

4.1.1. По контактам, указанным на внутреннем портале (http://start.ys.local/), в т.ч. с использованием сервисов «Новая заявка» или «Подача заявки через SMS»;

4.1.2. Через непосредственного руководителя.

5. Анализ и идентификация инцидентов

5.1. Администратор безопасности ЕМТС после получения информации о предполагаемом инциденте незамедлительно проводит первоначальный анализ полученных данных в целях выявления и документирования (закрепления объективных данных) факта нарушения ИБ.

5.2. При незначительности инцидента, не приведшего к негативным

последствиям ИБ и совершенного пользователем ЕМТС впервые, Администратор безопасности ЕМТС по согласованию с сотрудником Департамента мобилизационной подготовки и защиты информации, на которого возложены планирование и проведение мероприятий по реагированию на выявленные инциденты сведения об инциденте фиксирует в карточке «Инциденты ИБ» (Приложение к настоящему Порядку) с присвоением статуса «Разбирательство не требуется».

5.3. В иных случаях администратор безопасности ЕМТС определяет предварительную степень важности инцидента для ИБ ЕМТС и информирует уполномоченное лицо о необходимости планирования и проведения мероприятий по реагированию на выявленный инцидент, а так же инициирует формирование регистрационной карточки инцидента с присвоением ему статуса «В процессе разбирательства».

5.4. Сотрудник Департамента мобилизационной подготовки и защиты информации незамедлительно уведомляет об инциденте директора Департамента мобилизационной подготовки и защиты информации аппарата администрации города Южно-Сахалинска

5.5. В срок не более 3 (трех) рабочих дней с момента поступления информации об инциденте, уполномоченное лицо совместно с администратором безопасности ЕМТС определяют и инициируют первоочередные меры, направленные на локализацию инцидента и на минимизацию его последствий.

6. Меры по реагированию на выявленный инцидент

6.1. Для реагирования на выявленный инцидент применяются следующие меры:

6.1.1. Получение (сбор) доказательств возникновения инцидента, обеспечение их сохранности и целостности;

6.1.2. Минимизация последствий инцидента;

6.1.3. Информирование и консультирование пользователей ЕМТС о порядке действий при обнаружении, устранении последствий и предотвращении инцидентов;

6.1.4. Разработка и осуществление комплекса периодических мероприятий по обнаружению и/или предупреждению инцидентов.

6.2. С целью минимизации последствий инцидента возможно временное отключение или ограничение прав доступа пользователя ЕМТС к информационным ресурсам ЕМТС (ИР) на время проведения проверки по инциденту. Такое отключение или ограничение согласовывается с непосредственным руководителем пользователя ЕМТС.

6.3. В случае если у пользователя ЕМТС были отключены или ограничены права доступа к ИР на время проведения проверки по инциденту, то по ее результатам уполномоченное лицо инициирует :

6.3.1. Восстановление пользователю ЕМТС прав доступа к ИР в полном или ограниченном объеме;

6.3.2. Отмену (изменение) прав доступа пользователя ЕМТС к ИР в соответствии с порядком, установленным в ЕМТС.

6.4. Если в ходе проверки будет установлено, что причиной инцидента является незнание пользователем ЕМТС установленных правил (технологии) работы с ИР, то основанием для восстановления прав доступа является успешное прохождение пользователем ЕМТС повторного инструктажа по порядку и правилам обработки информации в ЕМТС.

6.5. Восстановление пользователю ЕМТС прав доступа, ограничивавшихся на период проверки по инциденту (разблокировка пользователя ЕМТС), осуществляется по заявке его непосредственного руководителя, согласованной с администратором безопасности ЕМТС.

6.6. Администратором ЕМТС, системным администратором должна быть обеспечена возможность восстановления программного обеспечения ЕМТС, включая программное обеспечение средств защиты информации ЕМТС, при возникновении инцидента.

6.7. Возможность восстановления программного обеспечения ЕМТС, включая программное обеспечение средств защиты информации ЕМТС, при возникновении инцидента должна предусматривать:

6.7.1. Восстановление программного обеспечения, включая программное обеспечение средств защиты информации, из резервных копий (дистрибутивов) программного обеспечения;

6.7.2. Восстановление и проверку работоспособности системы защиты информации, обеспечивающие необходимый уровень защищённости информации;

6.7.3. Возврат информационной системы в составе ЕМТС в начальное состояние (до возникновения инцидента), обеспечивающее её штатное функционирование, или восстановление отдельных функциональных возможностей такой информационной системы, позволяющих решать задачи по обработке информации.

6.8. Администратором ЕМТС, системным администратором применяются компенсирующие меры защиты информации в случаях, когда восстановление работоспособности системы защиты информации невозможно.

6.9. Администратором ЕМТС, системным администратором обеспечивается использование отказоустойчивых технических средств, предусматривающее:

6.9.1. Определение типовых сегментов ЕМТС или информационных систем в составе ЕМТС, в которых должны применяться отказоустойчивые технические средства, обладающие свойствами сохранять свою работоспособность после отказа одного или нескольких их составных частей;

6.9.2. Установление минимального перечня отказоустойчивых средств, исходя из требуемых условий обеспечения непрерывности функционирования ЕМТС, информационной системы в составе ЕМТС и доступности обрабатываемой информации.

6.10. Оператор ЕМТС, ответственный за эксплуатацию ЕМТС применяет

технические средства с установленными характеристиками (коэффициентом) готовности и надёжности, обеспечивающие требуемые условия непрерывности функционирования ЕМТС, информационной системы в составе ЕМТС и доступности обрабатываемой информации;

6.11. Замена технических средств, характеристики (коэффициенты) готовности и надёжности которых достигли предельного значения, производится в соответствии с порядком, установленным собственником технических средств ЕМТС.

6.12. Оператором ЕМТС, ответственным за эксплуатацию ЕМТС обеспечивается резервирование технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования информационной системы, предусматривающее:

6.12.1. Определение типовых сегментов ЕМТС, информационных систем в составе ЕМТС, в которых должно осуществляться резервирование технических средств, программного обеспечения, каналов передачи информации и средств обеспечения функционирования, а также перечня резервируемых средств исходя из требуемых условий обеспечения непрерывности функционирования ЕМТС, информационной системы в составе ЕМТС и доступности обрабатываемой информации;

6.12.2. Применение резервных (дублирующих) технических средств, программного обеспечения, каналов передачи информации и (или) средств обеспечения функционирования;

6.12.3. Ввод в действие резервного технического средства, программного обеспечения, канала передачи информации или средства обеспечения функционирования при нарушении требуемых условий непрерывности функционирования ЕМТС, информационной системы в составе ЕМТС и доступности обрабатываемой информации.

6.13. При резервировании программного обеспечения осуществляется создание резервных копий общесистемного, специального и прикладного программного обеспечения, а также программного обеспечения средств защиты информации, необходимых для обеспечения требуемых условий непрерывности функционирования ЕМТС, информационной системы в составе ЕМТС и доступности информации.

6.14. Резервирование средств обеспечения функционирования включает:

6.14.1. Использование кратковременных резервных источников питания для обеспечения правильного (корректного) завершения работы типового сегмента ЕМТС, информационной системы в составе ЕМТС (технического средства, устройства) в случае отключения основного источника питания;

6.14.2. Использование долговременных резервных источников питания в случае длительного отключения основного источника питания и необходимости продолжения выполнения типовым сегментом ЕМТС, информационной системой в составе ЕМТС (техническим средством, устройством) установленных функциональных задач;

6.14.3. Определение перечня энергозависимых технических средств,

которым необходимо обеспечить наличие резервных источников питания (кратковременных и долговременных). В качестве таких средств выступают серверы, активные сетевые устройства промышленного и среднего уровня, а также хранилища информации.

7. Проверка по инциденту ИБ

7.1. Целями проверки по инциденту ИБ являются:

7.1.1. Выработка организационных и технических решений, направленных на снижение рисков нарушения ИБ ЕМТС, предотвращение и минимизацию подобных нарушений в будущем;

7.1.2. Защита прав оператора ЕМТС;

7.1.3. Защита репутации оператора ЕМТС;

7.1.4. Обеспечение безопасности защищаемой информации, обрабатываемой в ЕМТС;

7.1.5. Обеспечение прав обладателя информации на обеспечение безопасности и конфиденциальности информации, обрабатываемой в ЕМТС;

7.1.6. Предотвращение несанкционированного доступа к информации ограниченного доступа и (или) передачи ее лицам, не имеющим права доступа к такой информации.

7.2. Проверка инцидента состоит из следующих этапов:

7.2.1. Подтверждение/опровержение факта возникновения инцидента;

7.2.2. Подтверждение/корректировка уровня значимости инцидента;

7.2.3. Уточнение обстоятельств (деталей) инцидента;

7.2.4. получение (сбор) доказательств возникновения инцидента, обеспечение их сохранности и целостности;

7.2.5. Минимизация последствий инцидента;

7.2.6. Информирование и консультирование пользователей ЕМТС по действиям, направленным на обнаружение, устранение последствий и предотвращение инцидентов;

7.2.7. Разработка мероприятий по обнаружению и/или предупреждению инцидентов.

7.3. Порядок проведения проверки по инциденту:

7.3.1. В процессе проведения проверки по инциденту обязательными для установления являются:

7.3.2. Дата и время возникновения (обнаружения) инцидента;

7.3.3. ФИО, должность, подразделение/учреждение/предприятие, пользователя ЕМТС, выявившего инцидент, а так же пользователя ЕМТС, нарушившего требования ИБ ЕМТС, действия которого привели к инциденту (нарушителя);

7.3.4. Уровень критичности инцидента;

7.3.5. Обстоятельства и мотивы совершения пользователем ЕМТС действий, которые привели к инциденту;

7.3.6. Информационные системы в составе ЕМТС и/или информационные ресурсы ЕМТС, затронутые инцидентом;

7.3.7. Характер и размер реального и потенциального ущерба, причиненного обладателю информации в ЕМТС и/или собственнику технических средств ЕМТС;

7.3.8. Обстоятельства, способствовавшие совершению инцидента.

7.4. При инциденте, затрагивающем не более одного объекта учета в составе ЕМТС, уполномоченное лицо привлекает к проверке по инциденту администратора безопасности ЕМТС, системного администратора в соответствии с делегированными им полномочиями, также могут привлекаться другие сотрудники оператора в зависимости от характера процессов и ресурсов, затронутых инцидентом ИБ.

7.5. При инциденте, затрагивающим более одного объекта учета в составе ЕМТС, уполномоченное лицо привлекает к проверке по инциденту администратора безопасности ЕМТС, системных администраторов в соответствии с делегированными им полномочиями, также могут привлекаться другие сотрудники оператора в зависимости от характера процессов и ресурсов, в отношении затронутых инцидентом объектов учета в составе ЕМТС.

7.6. В случае временного отключения или ограничения на период проверки прав доступа в ЕМТС пользователя ЕМТС, выявившего инцидент, и/или нарушителя, информация об отключении или ограничении прав доступа направляется его (их) непосредственному руководителю.

7.7. Уполномоченное лицо в праве запрашивать информацию, необходимую для полноты и объективности проверки по инциденту, у операторов ЕМТС и информационных систем в составе ЕМТС. Такие запросы направляются на имя руководителя соответствующего структурного подразделения аппарата, отраслевого (функционального) органа администрации города, подведомственного муниципального предприятия или учреждения, за подписью директора Департамента мобилизационной подготовки и защиты информации с обязательным указанием сроков предоставления информации (с учетом необходимости ее анализа, сбора и подготовки).

7.8. В случае выявления в ходе проверки пользователя ЕМТС, чьи действия привели к возникновению инцидента, уполномоченное лицо инициирует проведение служебной проверки в соответствии с Положением о порядке организации и проведения служебных проверок по фактам неисполнения и (или) ненадлежащего исполнения должностных обязанностей муниципальными служащими и лицами, замещающими должности, не относящиеся к должностям муниципальной службы, администрации города Южно-Сахалинска, руководителями и сотрудниками муниципальных предприятий и учреждений города Южно-Сахалинска, утвержденном постановлением администрации города.

7.9. Уполномоченное лицо совместно с администратор безопасности ЕМТС проводит оценку негативных последствий инцидента. В ходе данной оценки учитываются:

7.9.1. Прямой финансовый ущерб;

7.9.2. Репутационный ущерб;

7.9.3. Потенциальный ущерб;

7.9.4. Прямые и косвенные потери от инцидента, например, связанные с недоступностью сервисов ЕМТС, утратой информации и т.п.;

7.9.5. Иной вред или негативные последствия инцидента для ЕМТС.

8. Оформление результатов проверки по инциденту

8.1. Накопленная в ходе проверки по инциденту информация фиксируется уполномоченным лицом в карточке «Инциденты ИБ» и учитывается при подготовке итогового заключения по инциденту.

8.2. Уполномоченное лицо формирует, согласовывает со всеми участниками проверки и подписывает итоговое заключение по результатам проверки инцидента.

8.3. Итоговое заключение по результатам проверки инцидента направляется директору Департамента мобилизационной подготовки и защиты информации.

8.4. О результатах проверки инцидентов, причинивших существенный ущерб, информируется председатель ПДТК — первый вице-мэр, руководитель аппарата.

8.5. Уполномоченное лицо фиксирует завершение разбирательства в карточке «Инциденты ИБ» и присваивает инциденту статус «Разбирательство завершено».

8.6. При необходимости определения наличия в действиях пользователя ЕМТС, чьи действия привели к возникновению инцидента, признаков преступления или административного правонарушения, уполномоченное лицо вправе обратиться за правовой оценкой в Правовой департамент администрации города. Такой запрос направляется с ограничительной пометкой «Для служебного пользования» за подписью председателя ПДТК — первого вице-мэра, руководителя аппарата.

8.7. В случае выявления в действиях пользователя ЕМТС, чьи действия привели к возникновению инцидента, признаков преступления или административного правонарушения, уполномоченное лицо передает все материалы по инциденту председателю ПДТК — первому вице-мэру, руководителю аппарата в целях определения целесообразности их направления в компетентные органы для принятия процессуального решения.

9. Планирование и принятие мер по предотвращению повторного возникновения инцидентов

9.1. В рамках планирования и принятия мер по предотвращению повторного возникновения инцидентов, уполномоченное лицо в срок не более 3 (трех) рабочих дней после оформления итогового заключения по результатам проверки по инциденту, организует проведение одного или нескольких мероприятий, направленных на снижение рисков ИБ в форме :

9.1.1. Проведения внеплановых инструктажей с лицами, причастными к возникновению инцидента;

9.1.2. Планового обучения пользователей ЕМТС, в т.ч. на курсах повышения квалификации;

9.1.3. Периодического доведения пользователям ЕМТС основных норм и требований ИБ;

9.1.4. Корректировки параметров настроек системы защиты информации ЕМТС и/или пользовательских интерфейсов информационных систем и сервисов в составе ЕМТС (при необходимости по результатам проверки по инциденту);

9.1.5. Применения других организационных мер (издание и актуализация муниципальных правовых актов, распоряжений вице-мэров, приказов учреждений или предприятий, внесение изменений в должностные инструкции сотрудников и т. п.).

10. Права, обязанности и ответственность участников проверки по инцидентам

10.1. Уполномоченное лицо, администратор безопасности ЕМТС, иные сотрудники, участвующие в проверке по инциденту, имеют право :

10.1.1. Запрашивать и получать от пользователей ЕМТС и их непосредственных руководителей в рамках их компетенции, устные и письменные разъяснения и иную информацию, необходимую для проведения проверки по инциденту;

10.1.2. Инициировать отключение или ограничение доступа к ИР пользователя ЕМТС, нарушившего правила или требования ИБ, на период проведения проверки по инциденту, в случае если имеется риск увеличения размера ущерба от выявленного инцидента или его повторение;

10.1.3. По результатам проверки по инциденту инициировать изменения в технологических процессах обработки информации в ЕМТС и/или в информационной системе в составе ЕМТС, с целью повышения защищенности ИР и снижения рисков возникновения инцидентов.

10.2. Уполномоченное лицо, администратор безопасности ЕМТС, иные сотрудники, участвующие в проверке по инциденту, обязаны :

10.2.1. Объективно и основательно проводить проверку по каждому инциденту;

10.2.2. Определять первоочередные меры, направленные на локализацию инцидента и минимизацию его негативных последствий;

10.2.3. Фиксировать в карточке данных «Инциденты ИБ» всю исходную информацию об инциденте и результаты проверки по нему;

10.2.4. Предоставлять отчеты и рекомендации по проведенным проверкам директору Департамента мобилизационной подготовки и защиты информации, МКУ «Управление делами администрации города Южно-Сахалинска» и, по результатам проверки инцидентов, повлекших значительный ущерб, председателю ПДТК — первому вице-мэру, руководителю аппарата;

10.2.5. Проводить анализ обстоятельств, способствовавших возникновению каждого инцидента, и, на его основе, разрабатывать рекомендации и предложения по оптимизации процессов обработки информации в ЕМТС, снижения вероятности причинения ущерба от подобных инцидентов и минимизации возможности их повторения в будущем;

10.2.6. Фиксировать факты несоблюдения условий хранения носителей информации, использования средств защиты информации, приводящие к снижению уровня защищенности информации в ЕМТС, требовать принятия мер по предотвращению возможных негативных последствий подобных нарушений.

10.3. Пользователи ЕМТС и их непосредственные руководители обязаны:

10.3.1. Предоставлять по запросу уполномоченного лица, администратора безопасности ЕМТС, иных сотрудников, участвующих в проверке по инциденту, устные и письменные разъяснения и иную информацию в рамках своей компетенции, необходимую для проведения проверки по инцидента;

10.3.2. Информировать администратора безопасности ЕМТС о выявленных инцидентах.

Приложения :

1. Карточка инцидента информационной безопасности.

Приложение
к Порядку выявления инцидентов
безопасности в ЕМТС и реагирования на них

Карточка инцидента информационной безопасности

Дата инцидента ИБ _____ Номер инцидента ИБ _____

Информация о сообщившем:

Ф.И.О.	Должность	Объект, подключённый к ЕМТС	Рабочий телефон

Статус инцидента	Разбирательство не требуется		В процессе разбирательства		Разбирательство завершено
Тип инцидента	Действительный		Попытка		Подозрение
Предполагаемый тип угрозы ИБ	Непредна-меренный	Преднамеренный	Удаленное вмешательство	Ошибка проектирования ИС	Технический сбой
Нарушитель	Отсутствует	Не установлен	Внешний	Внутренний	
			Организация, Ф.И.О., должность нарушителя	Объект подключенный к ЕМТС, Ф.И.О., должность нарушителя	
Последствия инцидента	Без последствий	Нарушение работоспособности компонентов ИС	Нарушение целостности ИР, фальсификация документов	Нарушение режима конфиденциальности информации	
Объект, которому нанесен ущерб	Информация	Средства вычислительной техники	Программное обеспечение	Средства связи	

Действия, предпринятые для разрешения инцидента	Описание действий	Никаких действий не требуется	Без привлечения внешнего исполнителя	С привлечением внешнего исполнителя
Дополнительная информация				

Разбирательство проводил:

Ф.И.О.	Должность	Объект, подключённый к ЕМТС	Подпись, дата