АДМИНИСТРАЦИЯ ГОРОДА ЮЖНО-САХАЛИНСКА

РАСПОРЯЖЕНИЕ

от 21.11.2023 № 959-р

О внесении изменений в распоряжение администрации города Южно-Сахалинска 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 со статьями 13, 14 и 16 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», ст.37 Устава городского округа «Город Южно-Сахалинск» и распоряжениями администрации города Южно-Сахалинска от 22.08.2023 № 700-р «О внесении изменения в штатное расписание аппарата администрации города Южно-Сахалинска на 2023 год, утвержденное распоряжением администрации города Южно-Сахалинска от 30.12.2022 № 1061-р» и от 07.09.2023 № 730-р «О распределении обязанностей между мэром города, первым вице-мэром, вице-мэрами города Южно-Сахалинска»:

1. Внести в распоряжение администрации города Южно-Сахалинска от 22.07.2019 № 451-р «О назначении ответственных за защиту информации в муниципальной информационной системе «Единая мультисервисная телекоммуникационная сеть администрации города Южно-Сахалинска» (далее — распоряжение) следующие изменения:

1.1. Пункт 1 изложить в следующей редакции:

«1. Назначить МКУ «Муниципальный центр цифровой трансформации администрации города Южно-Сахалинска» ответственным за защиту информации в муниципальной информационной системе «Единая мультисервисная телекоммуникационная сеть администрации города Южно-

Сахалинска» (далее — ЕМТС).».

1.2. Пункт 4 изложить в следующей редакции:

«4. Контроль исполнения распоряжения администрации города возложить на вице-мэра города Южно-Сахалинска (Кожухов В.А.).».

2. Внести в приложение № 1 «Регламент управления конфигурацией Единой мультисервисной телекоммуникационной сети администрации города Южно-Сахалинска», утвержденный распоряжением (далее - регламент), следующие изменения:

2.1. Пункт 1.4 изложить в следующей редакции:

«1.4. В целях настоящего регламента под Оператором понимается 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, предусматривающим её функционирование в составе ЕМТС в качестве прикладного сервиса.».

2.2. Пункт 4.2 изложить в следующей редакции:

«4.2. Согласование с администратором безопасности ЕМТС изменений в конфигурации ЕМТС и/или информационных систем, функционирующих в составе ЕМТС в качестве прикладных сервисов, осуществляется инициатором изменений в письменном (в системе электронного документооборота администрации города Южно-Сахалинска), или электронном (с использованием сервиса «Создать заявку на техподдержку» внутреннего портала ЕМТС (https://portal.ys.local/), или в сервисе https://projects.yuzhno-sakh.ru/) виде.».

2.3. Подпункт 6.1.1.1 пункта 6.1 изложить в следующей редакции:

«6.1.1.1. В течение гарантийного срока технических средств и программного обеспечения защиты информации - поставщики этих средств защиты информации или исполнители по муниципальным контрактам на техническое обслуживание (техническую поддержку) таких средств защиты информации.».

2.4. Пункт 27 приложения 1 «Правила организации идентификации и аутентификации субъектов доступа и объектов доступа в ЕМТС» к регламенту, изложить в следующей редакции:

«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, в т.ч. использование в составе ЕМТС для доступа к объектам доступа служебных мобильных технических средств, в которых реализованы меры защиты информации;

27.2. Ограничение на использование мобильных технических средств в соответствии с условиями эксплуатации сегментов ЕМТС, в которых использование таких средств необходимо, и порядок 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.».

2.5. Пункт 2.4 приложения 2 «Правила управления обновлениями программного обеспечения в ЕМТС» к регламенту, изложить в следующей редакции:

«2.4. Контроль за обеспечением уровня защищенности информации, содержащейся в ЕМТС, должен осуществляться не реже 1 раза в два года».

2.6. Подпункт 8.2.1 пункта 8.2 приложения 2 «Правила управления обновлениями программного обеспечения в ЕМТС» к регламенту исключить.

2.7. Пункт 1.3. приложения 3 «Правила контроля (мониторинга) за обеспечением уровня защищенности информации в ЕМТС» к регламенту, изложить в следующей редакции:

«1.3. Во время анализа и устранения уязвимостей ЕМТС необходимо руководствоваться методическим документом «Руководство по организации процесса управления уязвимостями в органе (организации)» (утв. ФСТЭК России 17.05.2023) и должны проводиться:

1.3.1. На этапе мониторинга уязвимостей и оценки их применимости осуществляется выявление уязвимостей на основании данных, получаемых из внешних и внутренних источников, и принятие решений по их последующей обработке.

1.3.2. На этапе оценки уязвимостей определяется уровень критичности уязвимостей применительно к ЕМТС и информационным системам в составе ЕМТС.

1.3.3. На этапе определения методов и приоритетов устранения уязвимостей определяется приоритетность устранения уязвимостей и выбираются методы их устранения: обновление программного обеспечения и (или) применение компенсирующих мер защиты информации.

1.3.4. На этапе устранения уязвимостей принимаются меры, направленные на устранение или исключение возможности использования (эксплуатации) выявленных уязвимостей.

1.3.5. На этапе контроля устранения уязвимостей осуществляется сбор и обработка данных о процессе управления уязвимостями и его результатах, а также принятие решений по улучшению данного процесса.».

2.8. Раздел 2 «Беспроводный доступ для мобильных устройств» Приложения 4 «Правила использования технологий беспроводного доступа в ЕМТС» к регламенту, изложить в следующей редакции:

«2. Беспроводный доступ для мобильных устройств

2.1. В зданиях и помещениях, в которых размещаются структурные подразделения аппарата, отраслевые (функциональные) органы администрации города Южно-Сахалинска, муниципальные предприятия и учреждения, организованы беспроводные сети в составе ЕМТС, доступ к которым возможен только по условиям эксплуатации сегмента «Предоставление доступа в сеть Интернет».

2.2. Использование беспроводных сетей в составе ЕМТС для доступа к сегментам ЕМТС, не указанным в п.2.1 настоящих правил, допускается при условии использования служебных мобильных технических средств, в которых реализованы меры защиты информации, предусмотренные условиями эксплуатации соответствующего сегмента ЕМТС и с разрешения администратора безопасности ЕМТС.».

3. Внести изменение в утвержденный распоряжением Порядок выявления инцидентов безопасности в ЕМТС и реагирования на них, изложив его в следующей редакции (приложение).

4. Разместить настоящее распоряжение на официальном сайте администрации города Южно-Сахалинска.

5. Контроль исполнения распоряжения администрации города возложить на вице-мэра города Южно-Сахалинска (Кожухов В.А.).

Мэр города С.А.Надсадин

Приложение
Утвержден
распоряжением администрации
города Южно-Сахалинска
от 21.11.2023 № 959-р

ПОРЯДОК ВЫЯВЛЕНИЯ ИНЦИДЕНТОВ БЕЗОПАСНОСТИ В ЕМТС И РЕАГИРОВАНИЯ НА НИХ

1. Общие положения

1.1. Настоящий Порядок определяет процедуры 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 - работник МКУ «Муниципальный центр цифровой трансформации администрации города Южно-Сахалинска», на которого возложены полномочия по организации выявления инцидентов, в т.ч. первичная обработка информации, поступающей из источников, указанных в п. 1.3 настоящего порядка, а так же 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 информационной системы, функционирующей в составе ЕМТС в качестве прикладного сервиса (далее - сотрудник (работник) 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. Администратор безопасности ЕМТС обеспечивает выявление инцидентов, источники информации о которых указаны в п. 1.3 настоящего порядка, организует и осуществляет планирование и проведение мероприятий по реагированию на выявленные инциденты.

2.2. Постановлением администрации города о создании муниципальной информационной системы, предусматривающим её функционирование в составе ЕМТС в качестве прикладного сервиса, могут устанавливаться лица, ответственные за выявление инцидентов и реагирование на них в создаваемых информационных системах.

3. Порядок обнаружения и выявления инцидента

3.1. Способом выявления признаков инцидента является проведение сотрудником (работником) Оператора анализа соответствия текущей ситуации требованиям ИБ ЕМТС.

3.2. Наличие одного из следующих несоответствий дает 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 (работником) Оператора своему непосредственному руководителю, а впоследствии - администратору безопасности ЕМТС, любым доступным способом:

4.1.1. С использованием сервисов «Создать заявку на техподдержку» или «Подача заявки через SMS» раздела «Заявки на IT-поддержку» внутреннего портала ЕМТС (https://portal.ys.local/);

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, 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, планирует и проводит мероприятий по реагированию на выявленный инцидент, а также инициирует формирование регистрационной карточки инцидента с присвоением ему статуса «В процессе разбирательства».

5.4. В срок не более 3 (трех) рабочих дней с момента поступления информации об инциденте администратор безопасности ЕМТС определяет и инициирует 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 администратор безопасности ЕМТС 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 защищенности информации;

6.7.3. Возврат информационной системы в составе ЕМТС в начальное состояние (до возникновения инцидента), обеспечивающее ее 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, функционирующих в составе ЕМТС в качестве прикладных сервисов, 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, обеспечивающий эксплуатацию ЕМТС, применяет технические средства с установленными характеристиками (коэффициентом) готовности и надежности, обеспечивающие требуемые условия непрерывности функционирования ЕМТС, информационной системы, функционирующей в составе ЕМТС в качестве прикладного сервиса, и доступности обрабатываемой

информации.

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

6.12. Оператором 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, функционирующих в составе ЕМТС в качестве прикладных сервисов, 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 также 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, администратора безопасности ЕМТС привлекает к проверке по инциденту системного администратора в соответствии с делегированными ему полномочиями. Также могут привлекаться другие сотрудники (работники) Оператора в зависимости от характера процессов и ресурсов, затронутых инцидентом ИБ.

7.5. При инциденте, затрагивающем более одного объекта учета в составе ЕМТС, администратор безопасности ЕМТС привлекает к проверке по инциденту администратора безопасности ЕМТС, системных администраторов в соответствии с делегированными им полномочиями, также могут привлекаться другие сотрудники (работники) 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. Администратор безопасности ЕМТС вправе запрашивать информацию, необходимую для полноты и объективности проверки по инциденту, у операторов (заказчиков) ЕМТС и информационных систем в составе ЕМТС, а также у исполнителей по муниципальным контрактам на создание (развитие, техническую поддержку) ЕМТС и/или информационных систем в составе ЕМТС. Такие запросы направляются в системе электронного документооборота администрации города в адрес руководителя соответствующего структурного подразделения аппарата, отраслевого (функционального) органа администрации города, подведомственного им муниципального предприятия или учреждения (далее - Подразделение), за подписью директора МКУ «Муниципальный центр цифровой трансформации администрации города Южно-Сахалинска» 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, администратор безопасности ЕМТС инициирует проведение служебной проверки отношении такого сотрудника (работника) Оператора 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, утвержденным

постановлением администрации города.

7.9. 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. Администратор безопасности ЕМТС формирует, согласовывает со всеми участниками проверки и подписывает итоговое заключение по результатам проверки инцидента.

8.3. Итоговое заключение по результатам проверки инцидента направляется для принятия решения вице-мэру города Южно-Сахалинска, на которого возложены полномочия по организации обработки в администрации города Южно-Сахалинска информации ограниченного распространения, не содержащей сведения, составляющие государственную тайну (далее — курирующий вице-мэр).

8.4. Администратор безопасности ЕМТС фиксирует завершение разбирательства в карточке «Инциденты ИБ» и присваивает инциденту статус «Разбирательство завершено».

8.5. При необходимости определения наличия в действиях пользователя ЕМТС, чьи действия привели к возникновению инцидента, признаков преступления или административного правонарушения, администратор безопасности ЕМТС вправе обратиться за правовой оценкой в Правовой департамент аппарата администрации города. Такой запрос направляется с ограничительной пометкой «Для служебного пользования» за подписью курирующего вице-мэра.

8.6. В случае выявления в действиях пользователя ЕМТС приведших к возникновению инцидента, признаков преступления или административного правонарушения, администратор безопасности ЕМТС передает материалы по инциденту курирующему вице-мэру в целях определения целесообразности их направления в правоохранительные 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 администратор безопасности ЕМТС 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 (работников) Оператора и т.п.).

10. Права, обязанности и ответственность участников проверки по инцидентам

10.1. Администратор безопасности ЕМТС, иные сотрудники (работники) Оператора, 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. Администратор безопасности ЕМТС, иные сотрудники (работники) Оператора, 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 «Инциденты ИБ» исходную информацию об инциденте и результаты проверки по нему;

10.2.4. Предоставлять отчеты по проведенным проверкам курирующему вице-мэру;

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 инциденту;

10.3.2. Информировать администратора безопасности ЕМТС о выявленных инцидентах.

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, подключенный к ЕМТС	Рабочий телефон

Статус инцидента	Разбирательство не требуется		В процессе разбирательства		Разбирательство завершено	
Тип инцидента	Действительный		Попытка		Подозрение	
Предполагаемый тип угрозы ИБ	Непреднамеренный	Преднамеренный	Удаленное вмешательство		Ошибка проектирования ИС	Технический сбой
Нарушитель	Отсутствует	Не установлен	Внешний		Внутренний	
			Организация, Ф.И.О., должность		Объект подключенный к ЕМТС, Ф.И.О., должность нарушителя	

		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, подключенный к ЕМТС	Подпись, дата