МИНИСТЕРСТВО ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И СВЯЗИ АСТРАХАНСКОЙ ОБЛАСТИ

ПОСТАНОВЛЕНИЕ

20.04.2021 № 4-П

О работе в единой мультисервисной телекоммуникационной сети Правительства Астраханской области

В соответствии с распоряжением Правительства Астраханской области от 18.09.2013 № 424-Пр «О единой мультисервисной телекоммуникационной сети Правительства Астраханской области», а также в целях установления единых требований к работе в единой мультисервисной телекоммуникационной сети Правительства Астраханской области министерство государственного управления, информационных технологий и связи Астраханской области ПОСТАНОВЛЯЕТ:

1. Утвердить прилагаемые:

- инструкцию пользователя единой мультисервисной телекоммуникационной сети Правительства Астраханской области;
- инструкцию администратора сегмента единой мультисервисной телекоммуникационной сети Правительства Астраханской области;
- инструкцию по организации парольной защиты пользователей единой мультисервисной телекоммуникационной сети Правительства Астраханской области;
- порядок подключения к единой мультисервисной телекоммуникационной сети Правительства Астраханской области;
- перечень мер по защите информации при подключении к единой мультисервисной телекоммуникационной сети Правительства Астраханской области;
- регламент контроля доступа к техническим ресурсам и информации в информационных системах единой мультисервисной телекоммуникационной сети Правительства Астраханской области;
- требования по обеспечению безопасности информации внешними пользователями при работе в единой мультисервисной телекоммуникационной сети Правительства Астраханской области;
- требования по обеспечению безопасности информации внешними

пользователями при работе с информационными системами персональных данных;

- порядок реагирования на компьютерные инциденты в единой мультисервисной телекоммуникационной сети Правительства Астраханской области.

2. Отделу информационной безопасности министерства обеспечить размещение текста настоящего постановления на официальном сайте министерства в информационно-телекоммуникационной сети «Интернет» по адресу http://mingos.astrobl.ru/.

3. Отделу правового сопровождения реализации проектов министерства в семидневный срок со дня подписания настоящего постановления направить его копию:

- в прокуратуру Астраханской области и Управление Министерства юстиции Российской Федерации по Астраханской области;

- поставщикам справочно-правовых систем «КонсультантПлюс», ЗАО «ТЕЛЕКОМ-СКИФ» и «ГАРАНТ» ЗАО НПП «Астрахань-Гарант-Сервис».

4. Постановление вступает в силу со дня его опубликования.

Министр А.В. Сашин

Приложение № 1

к постановлению министерства
государственного управления,
информационных технологий и
связи Астраханской области
от 20.04.2021 № 4-П

Инструкция пользователя единой мультисервисной телекоммуникационной сети Правительства Астраханской области

1. Общие положения

1.1. Инструкция пользователя единой мультисервисной телекоммуникационной сети Правительства Астраханской области (далее – Инструкция) определяет права, обязанности, запреты и ответственность пользователей при работе в единой мультисервисной телекоммуникационной сети Правительства Астраханской области (далее – ЕМТС) и разработана в соответствии с законодательством Российской Федерации в области обеспечения информационной безопасности.

1.2. Настоящая Инструкция разработана в целях повышения эффективности работы ЕМТС и всех ее составляющих, координации действий пользователей ЕМТС.

1.3. Для целей настоящей Инструкции используются понятия, определенные в Положении о единой мультисервисной телекоммуникационной сети Правительства Астраханской области, утвержденном распоряжением Правительства Астраханской области от 18.09.2013 № 424-Пр «О единой мультисервисной телекоммуникационной сети Правительства Астраханской области».

1.4. Автоматизированное рабочее место (далее – АРМ) – рабочая станция, представляющая собой комплекс технических и программных средств, предназначенных для выполнения пользователем ЕМТС его функциональных обязанностей.

1.5. Пароль – комбинация символов (буквы, цифры, знаки препинания, специальные символы), используемая для подтверждения подлинности владельца учетной записи.

1.6. Компрометация пароля – нарушение конфиденциальности пароля.

1.7. Средство защиты информации – техническое, программное, программно-техническое средство, предназначенное или используемое для защиты информации.

1.8. Несанкционированный доступ – доступ, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.

1.9. Требования настоящей Инструкции распространяются на всех пользователей ЕМТС.

1.10. Пользователи ЕМТС должны быть под роспись ознакомлены с настоящей Инструкцией до начала работы на АРМ. Доступ пользователей ЕМТС к работе на АРМ до ознакомления с настоящей Инструкцией запрещен.

1.11. Пользователи ЕМТС несут персональную ответственность за свои действия при работе в ЕМТС.

2. Права пользователя ЕМТС

2.1. Пользователь ЕМТС имеет право:

2.1.1. Получать доступ к ресурсам ЕМТС в пределах своих должностных полномочий, если этот доступ не противоречит настоящей Инструкции.

2.1.2. Обращаться к администратору ЕМТС, администратору сегмента ЕМТС за справочной информацией, консультацией по работе в ЕМТС.

2.1.3. Оформлять заявки в адрес администратора ЕМТС, администратора сегмента ЕМТС на проведение работ по установке и настройке программного обеспечения (далее – ПО) и аппаратного обеспечения на его АРМ.

3. Обязанности пользователя ЕМТС

3.1.Пользователь ЕМТС обязан:

3.1.1. Соблюдать требования по обеспечению информационной безопасности, установленные Федеральными законами от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», от 27.07.2006 № 152-ФЗ «О персональных данных», от 06.04.2011 № 63-ФЗ «Об электронной подписи».

3.1.2. Использовать средства защиты информации в соответствии с технической и эксплуатационной документацией на эти средства.

3.1.3. Выполнять требования администратора сегмента ЕМТС, не противоречащие настоящей Инструкции.

3.1.4. Обеспечивать конфиденциальность атрибутов доступа (паролей, кодов авторизации, сертификатов ключей проверки электронной подписи и т. д.), используемых в процессе получения доступа к ресурсам ЕМТС.

3.1.5. Незамедлительно оповещать администратора сегмента ЕМТС о возникновении инцидента информационной безопасности (заражение АРМ вредоносным ПО, обнаружение ошибок в ПО, подозрение на компрометацию личных ключей и паролей, отклонения в работе системного и прикладного ПО, в том числе и средств защиты информации).

3.1.6. Содержать в чистоте и исправном состоянии свое АРМ.

4. Запреты при работе в ЕМТС

4.1. Пользователю ЕМТС запрещается:

4.1.1. Осуществлять несанкционированные попытки доступа к ЕМТС и использование ее ресурсов. В том числе:

- использовать для подключения к ЕМТС личные технические средства обработки информации;

- использовать программное обеспечение, предназначенное для анализа и/или эксплуатации уязвимостей информационно-телекоммуникационных сетей и компьютерных систем;

- использовать чужие учетные записи для подключения к ресурсам ЕМТС без разрешения администратора сегмента ЕМТС, а также предпринимать несанкционированные попытки к завладению чужими учетными записями и атрибутами доступа;

- получать несанкционированный доступ к ресурсам ЕМТС (АРМ, сетевому и другому оборудованию или информационным ресурсам), а также уничтожать или модифицировать ПО;

- осуществлять попытки обхода или обход систем контроля доступа, учетных систем получаемого трафика, их повреждения или дезинформирования;

- осуществлять несанкционированное копирование информационных ресурсов ЕМТС на съемные электронные носители информации (магнитные диски, оптические диски, flash-носители, внешние жесткие диски и иные портативные запоминающие устройства).

4.1.2. Осуществлять действия по анализу сети с целью определения ее внутренней структуры, списков открытых портов, наличия сервисов и использования полученной информации для решения задач, не входящих в должностные обязанности.

4.1.3. Вносить изменения в АРМ, в том числе установку, изменение конфигурации, удаление системного и прикладного программного обеспечения, а также изменение состава технического обеспечения, без согласования с администратором сегмента ЕМТС.

4.1.4. Обрабатывать конфиденциальную информацию на АРМ, не прошедших процедуру проверки соответствия требованиям по безопасности информации в соответствии с законодательством Российской Федерации.

4.1.5. Передавать конфиденциальную информацию посредством информационно-телекоммуникационных сетей общего пользования без использования средств защиты информации.

4.1.6. Распространять информацию, полученную в ходе выполнение должностных обязанностей, лицам, не имеющим права на доступ к такой информации.

4.1.7. Хранить на АРМ, предоставлять общий доступ и передавать информацию личного характера, в том числе аудио-, фото-, видеофайлы личного характера, информацию развлекательного характера, компьютерные игры.

4.1.8. Использовать учтенные съемные электронные носители информации для задач, не связанных с исполнением должностных обязанностей.

4.1.9. Использовать неучтенные съемные электронные носители информации на АРМ, прошедших процедуру определения соответствия требованиям по безопасности информации.

4.1.10. При работе с почтовыми сервисами ЕМТС:

- использовать личную электронную почту в служебных целях (слу-

жебная переписка должна осуществляться с использованием почтовых сервисов ЕМТС. Полученные или отправленные с использованием почтовых сервисов ЕМТС сообщения являются неотъемлемой частью внутреннего документооборота и не являются частной собственностью);

- использовать служебную электронную почту в личных целях;

- предоставлять кому-либо идентификаторы и атрибуты доступа к служебной электронной почте;

- использовать адрес служебной электронной почты для оформления подписок без предварительного согласования с непосредственным руководителем и/или администратором сегмента ЕМТС;

- осуществлять массовую рассылку почтовых сообщений (более 10) внешним адресатам без их согласия, а также почтовых сообщений рекламного характера или поздравлений, если рассылка не связана с выполнением служебных обязанностей;

- открывать вложенные файлы во входящих сообщениях без их предварительной проверки средствами антивирусной защиты информации.

4.1.11. Отключать антивирусное ПО, а также отказываться от обновления баз антивирусного ПО.

4.1.12. Оставлять на рабочем месте без личного присмотра включенное АРМ с не активированными средствами защиты информации.

4.1.13. Создавать, использовать и распространять вредоносное ПО.

4.1.14. Распространять информацию (установочные файлы лицензионного программного обеспечения, регистрационные ключи лицензионного программного и т.п.), являющуюся собственностью учреждения и защищенную законодательством Российской Федерации.

4.1.15. Распространять и использовать нелицензионное ПО, в том числе серийные номера к коммерческим программным продуктам или программы для их генерации;

4.1.16. Использовать результаты интеллектуальной деятельности способами, не предусмотренными действующими лицензионными договорами и влекущими нарушение исключительного права на данные результаты интеллектуальной деятельности.

4.1.17. Распространять информацию, запрещенную к распространению на территории Российской Федерации.

Приложение № 2

к постановлению министерства государственного управления, информационных технологий и связи Астраханской области
от 20.04.2021 № 4-П

Инструкция
администратора сегмента единой мультисервисной телекоммуникационной сети Правительства Астраханской области

1. Общие положения

1.1. Инструкция администратора сегмента единой мультисервисной телекоммуникационной сети Правительства Астраханской области (далее – Инструкция) определяет права, обязанности, ответственность и порядок работы администратора сегмента единой мультисервисной телекоммуникационной сети Правительства Астраханской области (далее – ЕМТС) и разработана в соответствии с законодательством Российской Федерации в области обеспечения информационной безопасности.

1.2. Настоящая Инструкция разработана в целях регламентации действий администратора сегмента ЕМТС.

1.3. Для целей настоящей Инструкции используются понятия, определенные в Положении о единой мультисервисной телекоммуникационной сети Правительства Астраханской области, утвержденном распоряжением Правительства Астраханской области от 18.09.2013 № 424-Пр «О единой мультисервисной телекоммуникационной сети Правительства Астраханской области».

1.4. Запрещается доступ администратора сегмента ЕМТС к работе до ознакомления с настоящей Инструкцией.

1.5. Администратор сегмента ЕМТС несет ответственность за свои действия при администрировании обслуживаемого сегмента ЕМТС.

2. Права администратора сегмента ЕМТС

2.1. Администратор сегмента ЕМТС имеет право:

2.1.1 Получать доступ к ресурсам ЕМТС в пределах своих должностных полномочий, если этот доступ не противоречит настоящей Инструкции.

2.1.2 Обращаться к администратору ЕМТС за справочной информацией, консультацией по администрированию обслуживаемого сегмента и реализации требований настоящей Инструкции.

2.1.3 Оформлять заявки в адрес администратора ЕМТС на проведение работ по установке и настройке программного обеспечения (далее – ПО) в пределах обслуживаемого сегмента ЕМТС.

3. Обязанности администратора сегмента ЕМТС

3.1. Администратор сегмента ЕМТС обязан:

3.1.1 Обеспечивать непрерывность работы всех элементов обслуживаемого сегмента ЕМТС.

3.1.2 Оперативно сообщать о любых инцидентах, угрожающих непрерывности работы средств защиты и/или сохранности информации, руководителю исполнительного органа государственной власти Астраханской области (далее – ИОГВ АО) или органа местного самоуправления муниципального образования Астраханской области (далее – ОМСУ АО).

3.1.3 Осуществлять резервирование информации с серверов сегмента ЕМТС:

- обеспечивать создание, хранение и использование резервных и архивных копий массивов данных;

- обеспечивать хранение резервных копий информации отдельно от оригиналов.

3.1.4 В случае обнаружения неисправности технических средств и ПО элементов ЕМТС, в том числе средств защиты информации, в кратчайшие сроки (не превышающие одного рабочего дня) принимать меры по восстановлению работоспособности и выявлению причин, приведших к неисправности.

3.1.5 В случае утраты доступа к информации в кратчайшие сроки (не превышающие одного рабочего дня) принимать меры по их восстановлению из актуальной копии и выявлению причин, которые привели к удалению или недоступности информации.

3.1.6 Осуществлять мониторинг обслуживаемого сегмента ЕМТС на наличие несанкционированного подключения к ЕМТС личных персональных компьютеров и портативных средств вычислительной и телекоммуникационной техники пользователей.

4. Порядок работы с учетными записями пользователей

4.1.Учетные записи пользователей в домене astrobl.ru и информационных системах ЕМТС создаются администратором ЕМТС или администраторами сегментов ЕМТС в пределах обслуживаемого сегмента на основании заявок (приложения к Регламенту контроля доступа к техническим ресурсам и информации в информационных системах единой мультисервисной телекоммуникационной сети Правительства Астраханской области).

4.2. Учетные записи пользователей в информационных системах ИОГВ АО и ОМСУ АО, не входящие в домен astrobl.ru, создаются администратором сегмента ЕМТС самостоятельно.

4.3. Пароли для учетных записей создаются в соответствии с инструкцией по организации парольной защиты пользователей единой мультисервисной телекоммуникационной сети Правительства Астраханской области.

4.4. Порядок работы с учетными записями пользователей определен Регламентом контроля доступа к техническим ресурсам и информации в ин-

формационных системах единой мультисервисной телекоммуникационной сети Правительства Астраханской области.

5. Порядок установки, замены и модернизации программных и аппаратных средств

5.1. Все изменения конфигурации программных средств и аппаратных устройств производятся администратором сегмента ЕМТС только после согласования с руководителем структурного подразделения, в котором производятся данные работы.

5.2. Используемое программное и техническое обеспечение сегмента ЕМТС должно принадлежать ИОГВ АО и ОМСУ АО на законном основании.

5.3. Программное и техническое обеспечение сегмента ЕМТС, которое относится к категории средств защиты информации, также должно иметь соответствующие сертификаты соответствия требованиям по информационной безопасности, установленным законодательством Российской Федерации.

5.4.После установки(обновления) или монтажа (наладки) программного или технического обеспечения администратор сегмента ЕМТС проводит проверку работоспособности данного программного или технического средства в соответствии с технической и эксплуатационной документацией на него.

5.5. После проведения модификации ПО на автоматизированных рабочих местах (далее – АРМ) администратор сегмента ЕМТС производит антивирусную проверку.

5.6. Изменение конфигурации серверов кем-либо, кроме администратора ЕМТС и администратора сегмента ЕМТС, запрещено.

6. Порядок передачи, изъятия носителей информации с серверов, АРМ ЕМТС

6.1. При передаче носителей информации с серверов и АРМ ЕМТС на сервисное обслуживание администратор сегмента ЕМТС предпринимает необходимые меры для обеспечения безопасности передаваемых данных.

6.2. Изъятие сервера, АРМ и/или их компонентов из состава ЕМТС для передачи оборудования на склад/со склада, в другое подразделение, списания с баланса организации и т.п. осуществляется по согласованию с администратором сегмента ЕМТС при информировании материально-ответственного лица организации только после оформления соответствующих документов (например, акта приема-передачи техники).

6.3. Изъятие сервера, АРМ и/или их компонентов из состава ЕМТС для передачи оборудования на сервисное обслуживание осуществляется по согласованию с администратором сегмента ЕМТС только после оформления соответствующих документов (например, акта приема-передачи техники) при условии обеспечения безопасности передаваемых данных.

7. Применение средств антивирусного контроля

7.1. Администратор сегмента ЕМТС принимает меры по настройке ан-

тивирусного ПО, которая должна соответствовать следующим требованиям:

- обновление антивирусных баз выполнятся по мере выпуска их у разработчика антивирусного ПО;

- проведение антивирусного контроля системной области жесткого диска выполнятся ежедневно;

- полная антивирусная проверка проводится не реже одного раза в неделю.

7.2. Обязательному антивирусному контролю подлежит любая информация, получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях (магнитных дисках, оптических дисках, flash-дисках внешних жестких дисках и иных портативных запоминающих устройствах).

7.3. Разархивирование и антивирусный контроль входящей информации необходимо проводить непосредственно после ее приема.

7.4. Антивирусный контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

7.5. Антивирусный контроль информации на съемных носителях производится непосредственно перед ее использованием.

7.6. Устанавливаемое (обновляемое) ПО должно быть предварительно проверено на отсутствие вирусов.

7.7. При возникновении подозрения на наличие вредоносного ПО на АРМ пользователь ЕМТС или администратор сегмента ЕМТС должны провести внеочередной антивирусный контроль.

8. Блокирование рабочих станций пользователей

Администратор сегмента ЕМТС принимает меры по настройке рабочих станций пользователей путем автоматической блокировки рабочих станций пользователей, которая должна производиться при бездействии пользователя на протяжении более 10 минут.

Приложение № 3

к постановлению министерства
государственного управления, информационных технологий и связи
Астраханской области
от 20.04.2021 № 4-П

Инструкция по организации парольной защиты пользователей
единой мультисервисной телекоммуникационной сети
Правительства Астраханской области

1. Общие положения

1.1. Инструкция по организации парольной защиты пользователей единой мультисервисной телекоммуникационной сети Правительства Астраханской области (далее – Инструкция) регламентирует процессы создания, смены и прекращения действия паролей пользователей единой мультисервисной телекоммуникационной сети Правительства Астраханской области (далее – ЕМТС).

1.2. Порядок создания, использования, смены и прекращения действия паролей входа на автоматизированное рабочее место (далее — АРМ) и в информационные системы сегмента ЕМТС, а также контроль за действиями пользователей сегментов ЕМТС при работе с паролями осуществляется в соответствии с Регламентом контроля доступа к техническим ресурсам и информации в информационных системах единой мультисервисной телекоммуникационной сети Правительства Астраханской области.

1.3. Для целей настоящей Инструкции используются понятия, определенные в Положении о единой мультисервисной телекоммуникационной сети Правительства Астраханской области, утвержденном распоряжением Правительства Астраханской области от 18.09.2013 № 424-Пр «О единой мультисервисной телекоммуникационной сети Правительства Астраханской области».

1.4. Требования настоящей Инструкции распространяются на всех пользователей ЕМТС.

1.5.Пользователи ЕМТС должны быть ознакомлены с настоящей Инструкцией до начала работы на автоматизированном АРМ. Доступ пользователей ЕМТС к работе на АРМ до ознакомления с настоящей Инструкцией запрещен.

1.6.Пользователи ЕМТС несут персональную ответственность за несоблюдение требований настоящей Инструкции.

2. Правила формирования паролей

2.1. Генерация и выдача начальной аутентификационной информации (пароль для первого входа) осуществляется централизованно.

2.2.После использования пароля для первого входа пользователь осу-

ществляет самостоятельное создание пароля с учетом следующих требований:

2.2.1. При наличии технической возможности пароль должен состоять не менее чем из восьми символов.

2.2.2. В пароле обязательно должны присутствовать следующие группы символов:

- буквы латинского алфавита из верхнего регистра;
- буквы латинского алфавита из нижнего регистра;
- цифры;
- специальные символы (! @ # $ % /\ & * () _ - + = { } [ ] |:; " ' <>,. ?).

2.2.3. Пароль не должен включать в себя:

- имя учетной записи пользователя или часть полного имени пользователя длиной более двух рядом стоящих знаков;
- легко вычисляемые сочетания символов (имена, фамилии, известные названия, словарные и жаргонные слова и т.п.);
- последовательности символов и знаков (111, qwerty, abcd и т.п.);
- общепринятые сокращения и аббревиатуры (ЭВМ, ЛВС, USER и т.п.);
- клички домашних животных, номера автомобилей, телефонов и другие значимые сочетания букв и знаков, которые можно угадать, основываясь на информации о пользователе.

2.2.4. При смене пароля новый пароль должен отличаться от старого не менее чем в шести позициях.

2.3. Срок действия пароля должен быть ограничен. Смена паролей проводится регулярно, не реже одного раза в два месяца.

3. Ограничения при использовании и хранении паролей

Пользователю запрещается:

– хранить пароли вместе с иной идентифицирующей информацией (имя пользователя, телефонные номера, адреса электронной почты и иные персональные данные);

– хранить пароли на электронных носителях, подключаемых к сети общего пользования, а также в облачных или иных сетевых сервисах;

– передавать пароли по электронной почте, а также с использованием систем быстрого обмена сообщениями, включая средства мобильной связи;

– сообщать другим пользователям личный пароль и авторизовать их в системе под своей учетной записью.

4. Действия в случае утери и компрометации паролей

В случае утери, компрометации или подозрения на компрометацию пароля пользователя ЕМТС необходимо немедленно сообщить администратору ЕМТС о необходимости временного блокирования учетной записи.

Приложение № 4

к постановлению министерства государственного управления, информационных технологий и связи Астраханской области
от 20.04.2021 № 4-П

Порядок подключения к единой мультисервисной телекоммуникационной сети Правительства Астраханской области

1. Общие положения

1.1. Порядок подключения к единой мультисервисной телекоммуникационной сети Правительства Астраханской области (далее – Порядок) регламентирует порядок подключения к единой мультисервисной телекоммуникационной сети Правительства Астраханской области (далее – ЕМТС) новых сегментов ЕМТС, новых пользователей ЕМТС, а также порядок актуализации сведений и разработан в соответствии с законодательством Российской Федерации в области обеспечения информационной безопасности.

1.2. Настоящий Порядок разработан в целях повышения уровня информационной безопасности ЕМТС.

1.3.Требования настоящего Порядка распространяются на всех пользователей ЕМТС.

1.4. Оператор ЕМТС – исполнительный орган государственной власти Астраханской области, определяющий архитектуру ЕМТС.

1.5. Технический оператор ЕМТС – исполнительный орган государственной власти Астраханской области или подведомственное учреждение, отвечающие за бесперебойную работу ядра и границы сети до пограничного маршрутизирующего оборудования ЕМТС, а также осуществляющие техническую и программную поддержку.

1.6. Оператор безопасности ЕМТС – исполнительный орган государственной власти Астраханской области, осуществляющий мониторинг и анализ событий в ЕМТС в сфере информационной безопасности.

1.7. Операторы ЕМТС – оператор ЕМТС, технический оператор ЕМТС, оператор безопасности ЕМТС.

1.8. Владелец информационной системы или сервиса – исполнительный орган государственной власти или организация, являющиеся собственником или осуществляющие полномочия собственника информационной системы или сервиса.

1.9. Ресурсы ЕМТС – совокупность аппаратных, программных и информационных систем и сервисов, доступ к которым предоставляется через ЕМТС.

1.10. Защищенное криптографическое соединение с ЕМТС (далее –

ЗКС) – организация удаленного защищенного доступа по открытым каналам связи к ресурсам ЕМТС с использованием средств криптографии;

1.11. Организация-участник ЕМТС – исполнительный орган государственной власти Астраханской области, орган местного самоуправления муниципального образования Астраханской области, подведомственное учреждение, иная организации, имеющие собственные сегменты ЕМТС и отвечающие за их бесперебойную работу.

1.12. Топология сети – способ описания конфигурации сети, схема расположения и соединения сетевых устройств.

2. Порядок подключения к ЕМТС новых сегментов

2.1. При подключении к ЕМТС организация-заявитель из числа исполнительных органов государственной власти Астраханской области либо органов местного самоуправления Астраханской области уровня района обязуется соблюдать процедуру создания учетных записей пользователей сегмента ЕМТС и производить подключение рабочих станций подключаемого сегмента ЕМТС к единым средствам идентификации, аутентификации и авторизации, используемым в ЕМТС, в соответствии с Регламентом контроля доступа к техническим ресурсам и информации в информационных системах единой мультисервисной телекоммуникационной сети Правительства Астраханской области. Подключение к ЕМТС новых сегментов осуществляется в соответствии с Перечнем мер по защите информации при подключении к единой мультисервисной телекоммуникационной сети Правительства Астраханской области.

2.2. В целях подключения нового сегмента к ЕМТС организация-заявитель представляет операторам ЕМТС заявку, содержащую:

- полное наименование, фирменное наименование (последнее – при наличии) юридического лица с указанием организационно-правовой формы или фамилию, имя, отчество (последнее – при наличии) индивидуального предпринимателя, а также фамилию, имя, отчество (последнее – при наличии) и наименование должности руководителя (для юридического лица);
- юридический адрес, почтовый адрес, адрес электронной почты, телефонный номер контактного лица для осуществления связи с ним;
- перечень необходимых ресурсов ЕМТС.

2.3. Заявка должна быть подписана руководителем юридического лица, либо индивидуальным предпринимателем, иным уполномоченным в установленном порядке лицом.

2.4. К заявке прилагаются следующие документы:

- топология сети;
- планы помещений.

2.5. Технический оператор ЕМТС в течение 10 рабочих дней рассматривает возможность подключения нового сегмента к ЕМТС в соответствии с настоящим Порядком.

2.6. Подключение к ЕМТС осуществляется посредством программно-

технических средств передачи данных, обеспечивающих защиту передаваемой информации криптографическими методами и соответствующих следующим требованиям:

- наличие сертификата соответствия требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, не ниже класса КС2, выданного ФСБ России;

- наличие сертификата соответствия требованиям к устройствам типа межсетевые экраны не ниже 4 класса защищенности, выданного ФСБ России;

- наличие сертификата соответствия требованиям к межсетевым экранам, типа «А», не ниже 5 класса защиты, выданного ФСТЭК России

2.7. Генерация ключевых дистрибутивов, ключей обновления и справочной информации производится техническим оператором ЕМТС.

2.8. При выявлении несоответствия представленного организацией оборудования требованиям подключения к ЕМТС, технический оператор ЕМТС направляет организации-заявителю мотивированное уведомление об отказе в подключении.

2.9. После устранения обстоятельств, послуживших основанием для отказа в подключении, организация-заявитель вправе повторно предоставить техническому оператору ЕМТС заявку на подключение в соответствии с настоящим Порядком.

2.10. Для возможности работы с ресурсами ЕМТС после согласования операторами ЕМТС подключения к ЕМТС организация-заявитель заключает Соглашение о предоставлении соответствующих услуг (далее – Соглашение) с оператором ЕМТС. Соглашение должно содержать:

- описание сегмента ЕМТС организации-заявителя;

- технические характеристики;

- перечень ответственных лиц и их контактные данные;

- перечень информационных сервисов и/или систем с указанием рабочих станций.

2.11. В ходе подключения нового сегмента ЕМТС настройка защищенного криптографического соединения производится организацией-заявителем совместно с техническим оператором ЕМТС.

3. Порядок подключения к ЕМТС новых пользователей

3.1. Доступ к ресурсам ЕМТС пользователю организации-участника предоставляется в целях обеспечения надлежащих организационно-технических условий, необходимых для исполнения его должностных обязанностей.

3.2. Доступ к информационным и программным ресурсам ЕМТС осуществляется при соблюдении всех следующих условий:

3.2.1. Наличие доступа пользователя ЕМТС к программно-техническому комплексу (АРМ).

3.2.2. Использования на АРМ системного и прикладного программного

обеспечения, включая средства защиты информации, совместимых со средствами управления, установленными на серверном оборудовании технического оператора ЕМТС, на законном основании.

4. Порядок актуализации сведений

4.1. ЕМТС может использоваться только для предоставления тех ресурсов ЕМТС, которые указаны в Соглашении. В случае необходимости расширения перечня используемых ресурсов ЕМТС необходимо внести соответствующие изменения в Соглашение.

4.2. Организация-участник обязана уведомлять оператора ЕМТС в течение трех рабочих дней обо всех изменениях условий, зафиксированных в Соглашении.

4.3. Требования Порядка касаются только подключения к ЕМТС и защиты каналов связи таких подключений.

4.4. Операторы ЕМТС, владелец информационной системы или сервиса вправе отказать организации-заявителю в предоставлении соответствующих услуг при несоблюдении установленных требований информационной безопасности.

Приложение № 5

к постановлению министерства
государственного управления, информационных технологий и связи
Астраханской области
от 20.04.2021 № 4-П

Перечень мер по защите информации при подключении к единой мультисервисной телекоммуникационной сети Правительства Астраханской области

1. Общие положения

1.1. Перечень мер по защите информации при подключении к единой мультисервисной телекоммуникационной сети Правительства Астраханской области (далее – Перечень) регламентирует организационные и технические меры по защите информации и порядок их проведения при подключении к единой мультисервисной телекоммуникационной сети Правительства Астраханской области (далее – ЕМТС).

1.2.Настоящий Перечень разработан в целях повышения уровня информационной безопасности ЕМТС.

1.3. Для целей настоящего Перечня используются понятия, определенные в Положении о единой мультисервисной телекоммуникационной сети Правительства Астраханской области, утвержденном распоряжением Правительства Астраханской области от 18.09.2013 № 424-Пр «О единой мультисервисной телекоммуникационной сети Правительства Астраханской области».

1.4. Перечень разработан на основании следующих документов:

- Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- приказа ФСТЭК России от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;
- приказа ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- методического документа «Меры защиты информации в государственных информационных системах», утвержденного ФСТЭК России

11.02.2014;

- «Методических рекомендаций по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации», утвержденные руководством 8 центра ФСБ России 21.02.2008 № 149/5-144;

- «Типовых требований по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденные руководством 8 центра ФСБ России 21.02.2008 № 149/6/6-622.

1.5. При подключении и работе в ЕМТС и информационных системах персональных данных внешних пользователей необходимо руководствоваться следующими документами:

- требования по обеспечению безопасности информации внешними пользователями при работе в единой мультисервисной телекоммуникационной сети Правительства Астраханской области;

- требования по обеспечению безопасности информации внешними пользователями при работе с информационными системами персональных данных.

2. Мероприятия по защите информации в ЕМТС

2.1. Общие требования

При подключении к ЕМТС должны быть реализованы следующие меры защиты информации:

- идентификация и аутентификация субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- ограничение программной среды;
- защита машинных носителей информации;
- регистрация событий безопасности;
- антивирусная защита;
- обнаружение (предотвращение) вторжений;
- контроль (анализ) защищенности информации;
- обеспечение целостности информационной системы и информации;
- обеспечение доступности информации;
- защита среды виртуализации;
- защита технических средств;
- защита информационной системы, ее средств и систем связи и передачи данных.

2.2. Организационные мероприятия по обеспечению безопасности

информации при подключении к ЕМТС

Комплекс организационных мероприятий по защите информации при подключении к ЕМТС обязан включать в себя следующие меры:

- определение и назначение круга лиц, допущенных к обработке информации в информационных системах;

- оснащение помещений с оборудованием, обеспечивающим технологический процесс обработки информации, средствами охранно-пожарной сигнализации;

- физическую охрану технических средств информационных систем и доступа к ним, которая должна предусматривать контроль доступа в помещения;

- допуск и нахождение в помещениях, задействованных в процессе обработки информации с использованием ЕМТС, посторонних лиц, включая вспомогательный и обслуживающий персонал (уборщиц, электромонтеров, сантехников и т.д.), разрешаются только в случаях, исключающих их бесконтрольные несанкционированные действия на автоматизированных рабочих местах пользователей ЕМТС;

- назначение лиц, ответственных за обеспечение безопасности информации в исполнительных органах государственной власти Астраханской области (далее – ИОГВ АО) или органах местного самоуправления муниципальных образований Астраханской области (далее – ОМСУ АО) или подведомственных им учреждениях;

- учет машинных носителей информации, средств защиты информации в соответствующих журналах учета.

2.3. Технические мероприятия

2.3.1. Реализация технических мероприятий по обеспечению безопасности информации

Применяемые технические средства защиты информации должны соответствовать требованиям к средствам защиты информации, определенным в пункте 26 приказа ФСТЭК России от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» для информационных систем 3 класса защищенности.

Выбранные для использования сертифицированные по требованиям безопасности информации средства защиты должны соответствовать:

- средства вычислительной техники – не ниже 5 класса в соответствии с руководящим документом ФСТЭК России «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации»;

- системы обнаружения вторжений и средства антивирусной защиты – не ниже 4 класса защиты в случае взаимодействия информационной системы с информационно-телекоммуникационными сетями международного информационного обмена и не ниже 5 класса в случае отсутствия взаимодействия

информационной системы с информационно-телекоммуникационными сетями международного информационного обмена;

- межсетевые экраны – не ниже 3 класса защиты в случае взаимодействия информационной системы с информационно-телекоммуникационными сетями международного информационного обмена.

2.3.2. Обеспечение безопасности информации при передаче по телекоммуникационным каналам связи

При передаче информации по телекоммуникационным каналам связи необходимо обеспечить защиту передаваемой информации от несанкционированного доступа к ней криптографическими средствами защиты информации.

Применяемые криптографические средства защиты информации должны быть полностью совместимы с уже использующимися средствами защиты каналов передачи данных ЕМТС.

2.3.3. Обеспечение безопасности информации при передаче по беспроводным телекоммуникационным каналам связи

При передаче информации по беспроводным телекоммуникационным каналам связи необходимо выполнить следующие требования:

- отключить технологию WPS;
- настроить шифрование канала;
- установить пароль на доступ к беспроводному соединению (пароль должен соответствовать требованиям инструкции по организации парольной защиты пользователей ЕМТС);
- отключить транслирование имени SSID;
- включить и настроить фильтрацию MAC-адресов.

Использование беспроводных технологий для подключения к ресурсам ЕМТС иными организациями-участниками, кроме ИОГВ АО, ОМСУ АО и подведомственных им учреждений запрещено.

3. Порядок проведения мероприятий по защите информации при подключении к информационным системам ЕМТС

Для проведения работ по защите информации при подключении к информационным системам ЕМТС необходимо руководствоваться нормативными документами, перечисленными в разделе 1 настоящего Перечня.

Для проведения указанных мероприятий допускается привлечение организаций, имеющих лицензию на деятельность по технической защите конфиденциальной информации в соответствии с Федеральным законом от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности».

4. Рекомендации к средствам защиты информации

Применяемые технические средства защиты информации должны быть сертифицированы ФСТЭК России (ФСБ России – в части средств криптографической защиты информации) и соответствовать требованиям к средствам

защиты информации, определенным:

- приказом ФСТЭК России от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» для информационных систем 3 класса защищенности;

- приказом ФСТЭК России от 06.12.2011 № 638 «Об утверждении требований к системам обнаружения вторжений»;

- приказом ФСТЭК России от 20.03.2012 № 28 «Требования к средствам антивирусной защиты».

Меры по защите автоматизированных рабочих мест пользователей ЕМТС определяются ИОГВ АО или ОМСУ АО самостоятельно (или с привлечением организаций-лицензиатов ФСТЭК России и ФСБ России по направлениям технической и криптографической защиты информации) в зависимости от уже реализованных организационных и технических мер по обеспечению безопасности информации в соответствии с требованиями федеральных законов и нормативных документов ФСТЭК России и ФСБ России, а также в соответствии с требованиями настоящего Перечня.

Приложение № 6

к постановлению министерства государственного управления, информационных технологий и связи Астраханской области
от 20.04.2021 № 4-П

Регламент контроля доступа к техническим ресурсам и информации в информационных системах единой мультисервисной телекоммуникационной сети Правительства Астраханской области

1. Общие положения

1.1. Регламент контроля доступа к техническим ресурсам и информации в информационных системах единой мультисервисной телекоммуникационной сети правительства Астраханской области (далее – Регламент) разработан в соответствии с законодательством Российской Федерации в целях повышения эффективности контроля и упорядочивания доступа к информационным системам (далее – ИС) и техническим ресурсам (далее – ТР) единой мультисервисной телекоммуникационной сети Правительства Астраханской области (далее – ЕМТС), порядка их использования, повышения уровня информационной безопасности.

1.2. Регламент определяет требования для выполнения процедур по предоставлению и прекращению доступа к ИС и ТР ЕМТС.

1.3. В Регламенте под доступом к информации, содержащейся в ИС, и под доступом к ТР ЕМТС понимается возможность получения и использования информации, содержащейся в ИС и ресурсах ЕМТС, в порядке, установленном Регламентом и в соответствии с законодательством Российской Федерации, а также положениями об этих ИС или ТР.

1.4. Регламент предназначен для использования в исполнительных органах государственной власти Астраханской области (далее – ИОГВ АО) и подведомственных им государственных учреждениях, органах местного самоуправления муниципальных образований Астраханской области (далее – ОМСУ АО) и подведомственных им муниципальных учреждениях.

1.5. Для целей Регламента используются понятия, определенные в Положении о единой мультисервисной телекоммуникационной сети Правительства Астраханской области, утвержденном распоряжением Правительства Астраханской области от 18.09.2013 № 424-Пр «О единой мультисервисной телекоммуникационной сети Правительства Астраханской области».

2. Основные определения и сокращения

авторизация – предоставление определенному лицу прав на выполнение определенных действий, а также процесс проверки (подтверждения) данных прав при попытке выполнения этих действий;

администрирование (административные механизмы) – процедуры управления информационными ресурсами, регламентирующие некоторые процессы или их часть;

администратор ИС – специалист (организация), обеспечивающий надлежащую работоспособность ИС и выполняющий следующие функции:

- управление учетными записями пользователей (включает в себя регистрацию пользователей в ИС (создание учетных записей), контроль использования учетных записей, задание ограничений на использование учетных записей, блокирование временно не использующихся учетных записей, удаление учетных записей);

- управление доступом к ресурсам ИС (включает в себя создание логических и регистрацию физических ресурсов ИС, обеспечение управляемого доступа к ресурсам с помощью списков управления доступом, контроль использования ресурсов);

- обеспечение сохранности, конфиденциальности и актуальности данных (включает в себя создание и поддержание нужного количества резервных копий, восстановление при необходимости данных, защиту данных от несанкционированного доступа путем установки соответствующих прав доступа, своевременное обновление данных);

- установка и сопровождение программного и аппаратного обеспечения (включая, в том числе, установку операционных систем на серверах и рабочих станциях ИС, установку серверного и клиентского программного обеспечения (далее – ПО), установку дополнительного аппаратного обеспечения; настройку и контроль работоспособности программного и аппаратного обеспечения);

административный пароль – комбинация символов (буквы, цифры, знаки препинания, специальные символы), известная администратору ЕМТС и/или администратору сегмента ЕМТС, используемая при настройке служебных учетных записей, учетных записей служб и сервисов, а также специальных учетных записей;

актуализация данных – приведение данных в соответствие с состоянием отображаемых объектов предметной области. Актуализация данных реализуется посредством операций добавления, исключения и редактирования записей;

временное прекращение полномочий – временное прекращение пользователем исполнения должностных обязанностей при длительном отсутствии пользователя на рабочем месте;

доступ к информационной системе – возможность ознакомления, поиска и обработки информации, находящейся в ИС, а также возможность использования информационных технологий и технических средств, необходимых для функционирования ИС;

компрометация пароля – нарушение конфиденциальности пароля;

контроль доступа – функция системы, обеспечивающая технологию безопасности, которая разрешает или запрещает доступ к определенным ти-

пам данных, основанную на идентификации субъекта, которому нужен доступ, и объекта данных, являющегося целью доступа;

локальная вычислительная сеть (далее – ЛВС) - это совокупность аппаратного и программного обеспечения, позволяющего объединить компьютеры в единую распределенную систему обработки и хранения информации;

несанкционированный доступ – доступ, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами;

одноразовый пароль – пароль, действительный только для одного сеанса аутентификации и в течение определенного промежутка времени;

пароль – комбинация символов (буквы, цифры, знаки препинания, специальные символы), используемая для подтверждения подлинности владельца учетной записи;

первичный пароль – средство аутентификации пользователя при первом входе, представляющее собой последовательность символов (буквы латинского алфавита и/или цифры);

прекращение полномочий пользователя – отстранение пользователя от исполнения должностных обязанностей;

рабочая станция – комплекс технических и программных средств, предназначенных для выполнения пользователем его функциональных обязанностей. Рабочая станция как автоматизированное рабочее место (далее – АРМ) пользователя представляет собой компьютер с соответствующим программным обеспечением;

система электронного документооборота ИОГВ АО (далее – СЭД) – организационно-техническая система, обеспечивающая автоматизированный процесс документооборота и делопроизводства в ИОГВ АО;

технический ресурс (ТР) – аппаратный или программно-аппаратный комплекс, предназначенный для обеспечения функционирования информационной инфраструктуры ЕМТС или обеспечения связанности сегмента ЕМТС с центральным коммутационным узлом ЕМТС;

центральный коммутационный узел ЕМТС – комплекс программных и технических средств, расположенных в серверном помещении и необходимых для функционирования ЕМТС и ее сервисов.

3. Порядок организации доступа к ТР и информации в ИС ЕМТС

3.1. Ответственный исполнитель.

3.1.1. В ИОГВ АО и ОМСУ АО назначается лицо, ответственное за представление актуальной информации о сотрудниках ИОГВ АО и ОМСУ АО в рамках реализации Регламента (далее – ответственный исполнитель). Ответственный исполнитель назначается из числа сотрудников ИОГВ АО или ОМСУ АО, обладающих необходимыми полномочиями контроля личного состава (руководитель кадрового подразделения организации).

3.1.2. Приказом или иным правовым актом организации назначается ответственный исполнитель, а также лицо, на которое возлагается временное исполнение обязанностей по актуализации данных во исполнение Регламента

при отсутствии на рабочем месте ответственного исполнителя на срок более 1 рабочего дня (отпуск, командировка, временная нетрудоспособность и т.д.). Копия данного приказа или иного правового акта направляется администратору ИС посредством СЭД.

3.1.3. Ответственный исполнитель направляет актуальную информацию о сотрудниках ИОГВ АО или ОМСУ АО путем оформления заявки по форме в соответствии с Приложением 1 Регламента в адрес администратора ИС посредством СЭД ежеквартально в период с 10 по 20 число последнего месяца квартала.

3.1.4. Ответственный исполнитель в срок не более 2 рабочих дней с момента вступления в силу кадровых изменений предоставляет информацию об увольнении, приеме и ином кадровом перемещении в рамках своей организации администратору ИС в виде заявки (Приложение 2), направленной в адрес администратора ИС посредством СЭД.

3.1.5. В целях обеспечения эффективности предоставления информации ОМСУ АО рекомендуется назначить исполнителя, ответственного за сбор сведений с ОМСУ АО, находящихся на территории района, городского округа (при наличии) и дальнейшую передачу сводной информации в адрес администратора ИС.

3.1.6. Во исполнение пунктом 3.1.2. настоящего Регламента в приказе о назначении ответственного исполнителя районной администрации, необходимо перечислить ОМСУ АО, находящихся на территории района, городского округа (при наличии).

3.1.7. Ответственный исполнитель передает учетные данные, полученные от администратора ЕМТС/ИС соответствующему владельцу, соблюдая целостность и конфиденциальность данной информации во избежание несанкционированного доступа к информации или компрометации пароля.

3.1.8. Ответственный исполнитель несет ответственность за достоверность и актуальность информации, направляемой администратору ЕМТС/ИС в рамках реализации настоящего Регламента.

3.1.9. Ответственный исполнитель обязан знать и выполнять требования настоящего Регламента.

3.2. Администратор сегмента ЕМТС.

3.2.1. Администратор сегмента ЕМТС назначается приказом или иным правовым актом организации. Копия данного приказа или иного правового акта в течение 3 рабочих дней направляется администратору ЕМТС.

3.2.2. Администратор сегмента ЕМТС может производить администрирование учетных записей пользователей в пределах сегмента в соответствии с инструкцией администратора сегмента ЕМТС и документацией ИС при наличии технической возможности по согласованию с администратором ЕМТС и администратором ИС.

3.2.3. Администратор сегмента ЕМТС обеспечивает смену паролей пользователей в ИС и ресурсах ЕМТС в соответствии с требованиями инструкции по организации парольной защиты пользователей ЕМТС или иной документацией ИС в пределах обслуживаемого сегмента.

3.2.4. Учетные записи пользователей, не входящие в единую службу каталогов, создаются администратором сегмента ЕМТС самостоятельно.

3.2.5. При прекращении полномочий пользователя его учетная запись блокируется администратором сегмента ЕМТС в соответствии с инструкцией администратора сегмента ЕМТС и документацией ИС в пределах обслуживаемого сегмента при наличии технической возможности по согласованию с администратором ИС.

3.2.6. Администратор сегмента ЕМТС обязан знать и выполнять требования настоящего Регламента.

3.2.7. Администратор сегмента ЕМТС несет ответственность за контроль доступа к ТР ЕМТС в соответствии с требованиями Регламента в пределах обслуживаемого сегмента ЕМТС.

3.3. Организация доступа.

3.3.1. Предоставление, прекращение, ограничение доступа к информации в ИС при наделении или прекращении полномочий пользователя, осуществляется на основании заявки (Приложение 2), направленной ответственным исполнителем в адрес администратора ИС.

3.3.2. Предоставление, прекращение, ограничение доступа пользователей к ТР ЕМТС при наделении или прекращении полномочий пользователя осуществляется на основании заявки (Приложение 2), направленной ответственным исполнителем в адрес администратора сегмента ЕМТС или администратора ЕМТС (по сфере обслуживания).

3.3.3. При длительном отсутствии пользователя на рабочем месте на срок более 1 месяца (отпуск, временная нетрудоспособность и т.д.), доступ к информации в ИС и ТР ЕМТС временно приостанавливается.

3.3.4. Восстановление доступа к ИС и ТР ЕМТС по истечении срока временного прекращения полномочий осуществляется в соответствии с требованиями пункта 4 настоящего Регламента.

3.3.5. В случае, если вход в ИС не производился пользователем, и/или подключение к ТР ЕМТС отсутствует более трех месяцев, администратор ИС/ЕМТС имеет право ограничить доступ к информации в ИС и ТР ЕМТС (временно заблокировать учетную запись пользователя).

3.3.6. В случае, если вход в ИС не производился пользователем и/или подключение к ТР ЕМТС отсутствует более шести месяцев, администратор ИС/ЕМТС имеет право удалить учетную запись пользователя без возможности восстановления.

4. Порядок предоставления доступа к ТР и информации в ИС ЕМТС

4.1. Предоставление доступа пользователям к информации в ИС и ТР ЕМТС осуществляется на основании заявки (Приложение 2) в срок не более двух рабочих дней.

4.2. Передача реквизитов доступа пользователя осуществляется способами, гарантирующими конфиденциальность и целостность информации.

4.3. В случае утраты пользователем реквизитов доступа к информации в ИС и ТР ЕМТС, реквизиты доступа предоставляется только на основании

заявки (Приложение 2), направленного посредством СЭД от ответственного исполнителя.

4.4. При поступлении информации об утрате реквизитов доступа пользователя администратор ИС/ЕМТС в кратчайшие сроки (не превышающие одного рабочего дня) принимает меры по восстановлению реквизитов доступа пользователя, путем изменения (сброса) основного пароля пользователя на первичный или одноразовый пароль.

4.5. При выявлении факта несанкционированного доступа к информации или компрометации реквизитов доступа пользователя, администратор ИС/ЕМТС должен незамедлительно принять меры (временно заблокировать учетную запись пользователя) в зависимости от полномочий владельца скомпрометированного пароля.

4.6. Устная заявка пользователя на изменение пароля не является основанием для проведения таких изменений.

5. Правила присвоения имен АРМ пользователей и формирования паролей

5.1. Присвоение имен АРМ.

5.1.1. АРМ пользователей ЕМТС присваиваются уникальные имена, состоящие из следующих компонентов:

- префикс органа власти (Приложение 3);
- инициалы и фамилия пользователя, использующего в данный момент АРМ для служебных целей.

Пример: Образец правильного имени компьютера, используемого пользователем Сергеевым Александром Ивановичем и установленного в министерстве здравоохранения Астраханской области: **MZ-AISergeev**.

5.1.2. Присвоение имен АРМ осуществляется администраторами сегмента ЕМТС либо администратором ЕМТС в соответствии с требованиями настоящего Регламента.

5.1.3. Присвоение имени АРМ необходимо производить при каждой смене пользователя ЕМТС, осуществляющего служебную деятельность с использованием данного АРМ.

5.2. Правила формирования и хранения паролей.

5.2.1. Пароли доступа к ТР ЕМТС формируются и распространяются централизованно администратором ЕМТС и/или администратором сегмента ЕМТС, либо формируются пользователями ЕМТС самостоятельно с учетом требований правил формирования паролей инструкции по организации парольной защиты пользователей ЕМТС.

5.2.2. Хранение паролей осуществляется в соответствии с ограничениями, указанными в пункте 3 инструкции по организации парольной защиты пользователей единой мультисервисной телекоммуникационной сети Правительства Астраханской области.

5.3. Требования к смене паролей.

5.3.1. Восстановление доступа к информации в ИС и ТР ЕМТС при утрате пользователем реквизитов доступа осуществляется в соответствии с пунктом 4.3. настоящего Регламента.

5.3.2. В случае прекращения полномочий пользователя, блокирование его учетной записи производится администратором ИС/ЕМТС в срок не более 2 рабочих дней после получения соответствующей заявки от ответственного исполнителя.

5.3.3. Срочная (внеплановая) смена паролей производится в случае прекращения полномочий (увольнение, переход на другую должность в ИОГВ АО или ОМСУ АО и т.п.) администратора сегмента ЕМТС и других работников, которым по роду деятельности были предоставлены полномочия по управлению системой парольной защиты.

5.3.4. Первичный пароль, заданный администратором ИС при регистрации нового пользователя, подлежит замене пользователем при первом входе в систему. При первом входе в систему с одноразовым паролем система автоматически требует ввести новый пароль.

5.4. Действия пользователя в случае утери и компрометации пароля.

5.4.1. В случае утери, компрометации или подозрения на компрометацию пароля в ИС, необходимо немедленно сообщить администратору ИС о необходимости временного блокирования учетной записи.

5.4.2. В случае утери, компрометации или подозрения на компрометацию пароля, предназначенного для доступа к ТР ЕМТС, необходимо немедленно сообщить администратору ЕМТС или администратору сегмента ЕМТС, о необходимости временного блокирования учетной записи.

Приложение № 1
к регламенту контроля доступа к техническим ресурсам и информации в информационных системах единой мультисервисной телекоммуникационной сети Правительства Астраханской области

Форма предоставления информации о сотрудниках

№ п/п	Ф.И.О. (полностью)	Должность	Рабочий телефон	Фактический адрес рабочего места
Наименование структурного подразделения (департамент, отдел, сектор)				

Приложение № 2
к регламенту контроля доступа к техническим ресурсам и информации в информационных системах единой мультисервисной телекоммуникационной сети Правительства Астраханской области

Заявка на выполнение работ по администрированию пользователей

_____
(наименование ведомства/организации)

Дата заявки «___» _____ 20__год дата кадровых изменений «___»_____20__год

☐ домен astrobl.ru
☐ электронная почта
☐ сервис обмена сообщениями
☐ ЕСЭД

☐ добавить
☐ заблокировать
☐ изменить

☐ ТВИС*

☐ заблокировать

Сведения о сотруднике	
Фамилия Имя Отчество	
Структурное подразделение	
Должность	
Фактический адрес рабочего места	
Рабочий телефон	
Замещающий сотрудник:	
Права пользователя (например, помощник, делопроизводитель):	
Доп. информация (изменяемая информация в случае изменения учетной записи):	

*При необходимости добавления учетной записи пользователя в ТВИС требуется утвержденный приказ о назначении ответственных лиц (образец размещен на сайте egov.astrobl.ru).

Даю свое согласие на обработку, хранение и передачу третьим лицам моих персональных данных.
С правилами работы в ЕМТС ознакомлен.

_____/_____
(подпись пользователя) (расшифровка)

«___»_____20__год

_____/_____
(подпись ответственного исполнителя) (расшифровка)

Заявка на выполнение работ по администрированию пользователей

_____
(наименование ведомства/организации)

Дата заявки «___» _____ 20__ год дата кадровых изменений «___»_____20__год

Содержание заявки:

☐ добавить
☐ заблокировать
☐ изменить

в _____
(наименование информационной системы)

Даю свое согласие на обработку, хранение и передачу третьим лицам моих персональных данных.
С правилами работы в ЕМТС ознакомлен.

_____/_____
(подпись пользователя) (расшифровка)

«___»_____20__год

Сведения о сотруднике	
Фамилия Имя Отчество	
Структурное подразделение	
Должность	
Рабочий телефон	
Замещающий сотрудник:	
Права пользователя:	
Доп. информация (изменяемая информация в случае изменения учетной записи):	

_____/_____
(подпись ответственного исполнителя) (расшифровка)

Приложение № 3
к регламенту контроля доступа к техническим ресурсам и информации в информационных системах единой мультисервисной телекоммуникационной сети Правительства Астраханской области

Префиксы исполнительных органов государственной власти Астраханской области и подведомственных им учреждений

В таблице приведены префиксы NetBIOS имен АРМ для организаций-участников ЕМТС. В случае, если нецелесообразно использование рекомендованного префикса NetBIOS имени АРМ из-за превышения максимальной длины допускается использование резервного префикса.

Рекомендуемый префикс	Резервный префикс	Наименование участника ЕМТС
AG-		Администрация Губернатора Астраханской области
GDRF-		Государственная Дума Астраханской области
MGUITS-		Министерство государственного управления, информационных технологий и связи Астраханской области
MZ-		Министерство здравоохранения Астраханской области
MKIT-	MK-	Министерство культуры и туризма Астраханской области
MOBR-	MO-	Министерство образования и науки Астраханской области
MPPR-	MP-	Министерство промышленности и природных ресурсов Астраханской области
MSH-		Министерство сельского хозяйства и рыбной промышленности Астраханской области
MSRT-	MSR-	Министерство социального развития и труда Астраханской области
MSJKH-	MS-	Министерство строительства и жилищно-коммунального хозяйства Астраханской области
MTDI-		Министерство транспорта и дорожной инфраструктуры Астраханской области
MFKS-	MFS-	Министерство физической культуры и спорта Астраханской области
MF-		Министерство финансов Астраханской области
MER-		Министерство экономического развития Астраханской области
AID-		Агентство международных связей Астраханской области
ARH-		Агентство по делам архивов Астраханской области
AML-		Агентство по делам молодежи Астраханской области

AZN-		Агентство по занятости населения Астраханской области
AMS-		Агентство по организации деятельности мировых судей Астраханской области
AUGI-	AGI-	Агентство по управлению государственным имуществом Астраханской области
UDG-	UD-	Управление делами Губернатора Астраханской области
SV-		Служба ветеринарии Астраханской области
SGTN-	ST-	Служба государственного технического надзора Астраханской области
SGOOKN-		Служба государственной охраны и объектов культурного наследия Астраханской области
SZHN-		Служба жилищного надзора Астраханской области
SZAGS-	SZ-	Служба записи актов гражданского состояния Астраханской области
SPK-		Служба по противодействию коррупции Астраханской области
STR-		Служба по тарифам Астраханской области Астраханской области
SPP-		Служба природопользования и охраны окружающей среды Астраханской области
SSN-		Служба строительного надзора Астраханской области
CIK-		АУ АО «Центр информационной компетенции»
CSAUP-	CSA-	ГБУ АО «Центр стратегического анализа и управления проектами»
ICEP-		ГБУ АО «Инфраструктурный центр электронного правительства»
RCOZ-		ГКУ АО "Региональный центр организации закупок"
CSEMA-	CSM-	ГУ АО «Центр социально-экономического мониторинга и аналитики»
MIAC-		ОГУ «Медицинский информационно-аналитический центр»
CISDR-	CS-	ГКУ АО «Центр по исполнению смет доходов и расходов ИОГВ АО»
MFC-	MC-	АУ АО «Многофункциональный центр»
ARRC-		ГКУ АО «Астраханский региональный ресурсный центр»

Приложение № 7

к постановлению министерства государственного управления, информационных технологий и связи Астраханской области
от 20.04.2021 № 4-П

Требования по обеспечению безопасности информации внешними пользователями при работе в единой мультисервисной телекоммуникационной сети Правительства Астраханской области

1. Общие положения

1.1. Требования по обеспечению безопасности информации внешними пользователями при работе в единой мультисервисной телекоммуникационной сети Правительства Астраханской области (далее – Требования) разработаны в соответствии с законодательством Российской Федерации в целях повышения уровня информационной безопасности единой мультисервисной телекоммуникационной сети Правительства Астраханской области (далее – ЕМТС).

1.2. Внешними пользователями являются пользователи, подключенные к центральному коммутационному узлу ЕМТС посредством внешних каналов передачи данных (VPN, Internet и т.д.).

1.3. Для целей настоящих Требований используются понятия, определенные в Положении о единой мультисервисной телекоммуникационной сети Правительства Астраханской области, утвержденном распоряжением Правительства Астраханской области от 18.09.2013 № 424-Пр «О единой мультисервисной телекоммуникационной сети Правительства Астраханской области».

2. Технические меры защиты информации

2.1. Внешние пользователи при подключении к ЕМТС должны применять следующие технические средства защиты информации:

- средство антивирусной защиты;
- криптошлюзы для организации защищенного канала связи;
- межсетевой экран.

2.2. Используемые технические средства защиты информации должны иметь сертификаты ФСТЭК России и ФСБ России, соответствующие следующим классам:

- межсетевые экраны не ниже 4 класса;
- устройства типа межсетевые экраны не ниже 3 уровня и 3 класса контроля отсутствия недекларированных возможностей ФСТЭК России;
- средства криптографической защиты информации (далее – СКЗИ) должны обеспечивать защиту информации при передаче по

внешним каналам связи по классу КСЗ;

- средства антивирусной защиты типа В не ниже класса 4 (автоматизированные рабочие места);

- средства антивирусной защиты типа Б не ниже класса 4 (сервера).

3. Организационные меры защиты информации

3.1. Для подключения к ЕМТС в организации-участнике ЕМТС должна иметься организационно-распорядительная документация, регламентирующая следующее:

- перечень лиц, допущенных к обработке информации в ЕМТС;
- контроль и управление физическим доступом к техническим средствам защиты информации, а также в помещения и сооружения, в которых они установлены;
- учет средств криптографической защиты информации;
- хранение и учет съемных носителей информации с персональными данными;
- форму журнала учета съемных носителей информации;
- форму акта затирания информации;
- форму журнала учета ключей и атрибутов доступа;
- форму журнала приема и сдачи помещений под охрану;
- форму журнала учета применяемых СКЗИ, эксплуатационной и технической документации к ним;
- порядок резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации;
- обязанности в должностных инструкциях пользователей/сотрудников выполнять требования законодательства Российской Федерации и локальных нормативных актов организации-участника ЕМТС, регламентирующих вопросы защиты информации, а также меру ответственности, которую несут пользователи за неисполнение данных требований.

3.2. Дополнительной организационной мерой, необходимой к исполнению организацией-участником ЕМТС, является проведение работ по устранению выявленных ФСТЭК России уязвимостей в используемых сертифицированных средствах защиты информации.

Приложение № 8

к постановлению министерства государственного управления, информационных технологий и связи Астраханской области
от 20.04.2022 № 49-п

Требования по обеспечению безопасности информации внешними пользователями при работе с информационными системами персональных данных

1. Технические меры защиты

1.1. Требования по обеспечению безопасности информации внешними пользователями при работе с информационными системами персональных данных (далее – Требования) разработаны в соответствии с законодательством Российской Федерации в целях повышения уровня информационной безопасности информационных систем персональных данных единой мультисервисной телекоммуникационной сети Правительства Астраханской области (далее – ЕМТС).

1.2. Внешними пользователями являются пользователи, подключенные к центральному коммутационному узлу ЕМТС посредством внешних каналов передачи данных (VPN, Internet и т.д.).

1.3. Информационная система персональных данных (далее – ИСПДн) — совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

1.4. Для целей настоящих Требований используются понятия, определенные в Положении о единой мультисервисной телекоммуникационной сети Правительства Астраханской области, утвержденном распоряжением Правительства Астраханской области от 18.09.2013 № 424-Пр «О единой мультисервисной телекоммуникационной сети Правительства Астраханской области».

1.5. При работе с ИСПДн внешние пользователи должны руководствоваться настоящими Требованиями.

2. Технические меры защиты информации

2.1. Внешние пользователи при подключении к ИСПДн должны применять следующие средства защиты информации:

- средства защиты от несанкционированного доступа;
- средства антивирусной защиты;
- криптошлюзы для организации защищенного канала связи;
- межсетевой экран.

2.2. Используемые технические средства защиты информации должны иметь сертификаты ФСТЭК России и ФСБ России, соответствующие следу-

ющим классам:

- средства вычислительной техники не ниже 5 класса;
- межсетевые экраны не ниже 4 класса;
- устройства типа межсетевые экраны не ниже 3 уровня и 3 класса контроля отсутствия недекларированных возможностей ФСТЭК России;
- средства криптографической защиты информации должны обеспечивать защиту информации при передаче по внешним каналам связи по классу КСЗ;
- средства антивирусной защиты типа В не ниже класса 4 (автоматизированные рабочие места);
- средства антивирусной защиты типа Б не ниже класса 4 (сервера).

3. Организационные меры защиты информации

3.1. Для подключения к ИСПДн в организации должна иметься организационно-распорядительная документация, регламентирующая следующее:

- перечень сведений конфиденциального характера;
- перечень информационных систем персональных данных и лиц, допущенных к обработке персональных данных;
- перечень лиц, допущенных к неавтоматизированной обработке персональных данных;
- обязательство о соблюдении режима конфиденциальности персональных данных гражданина (при работе с персональными данными граждан);
- контроль и управление физическим доступом к техническим средствам защиты информации, а также в помещения и сооружения, в которых они установлены;
- учет средств криптографической защиты информации;
- хранение и учет съемных носителей информации с персональными данными;
- резервирование и восстановление работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации;
- форму журнала приема и сдачи помещений под охрану;
- форму журнала учета применяемых СКЗИ, эксплуатационной и технической документации к ним;
- форму акта затирания информации;
- форму журнала учета ключей и атрибутов доступа;
- форму журнала учета съемных носителей информации;
- обязанности в должностных инструкциях пользователей/сотрудников выполнять требования законодательства Российской Федерации и локальных нормативных актов организации, регламентирующих вопросы защиты информации, а также меру ответственности, которую несут пользователи, за неисполнение данных требований;
- порядок оценки уязвимостей используемых средств защиты инфор-

мации.

3.2. Дополнительной организационной мерой, необходимой к исполнению организацией-участником ЕМТС, является проведение работ по устранению выявленных ФСТЭК России уязвимостей в используемых сертифицированных средствах защиты информации.

3.3. Рекомендуемые организационные меры защиты информации в рамках Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»:

- политика обработки и обеспечения защиты персональных данных;
- приказ о назначении ответственного за организацию обработки персональных данных;
- перечень сведений, содержащих персональные данные и обрабатываемых в информационных системах персональных данных;
- регламент реагирования на запросы субъектов персональных данных по выполнению их законных прав;
- регламент мониторинга и контроля обработки персональных данных;
- регламент проведения технического обслуживания;
- регламент передачи персональных данных;
- форма журнала по учету мероприятий по контролю защищенности персональных данных;
- форма запроса на предоставление сведений о наличии персональных данных;
- форма журнала регистрации запросов на предоставление сведений о наличии персональных данных.

Приложение № 9

к постановлению министерства государственного управления, информационных технологий и связи Астраханской области
от 20.04.2021 № 4-П

Порядок реагирования на компьютерные инциденты
в единой мультисервисной телекоммуникационной
сети Правительства Астраханской области

1. Порядок реагирования на компьютерные инциденты в единой мультисервисной телекоммуникационной сети Правительства Астраханской области (далее – Порядок) разработан в целях повышения эффективности работы единой мультисервисной телекоммуникационной сети Правительства Астраханской области (далее – ЕМТС) и всех ее составляющих, координации действий пользователей ЕМТС и повышения уровня информационной безопасности ЕМТС.

2. Для целей настоящего Порядка используются понятия, определенные в Положении о единой мультисервисной телекоммуникационной сети Правительства Астраханской области, утвержденном распоряжением Правительства Астраханской области от 18.09.2013 № 424-Пр «О единой мультисервисной телекоммуникационной сети Правительства Астраханской области».

3. При выявлении пользователем ЕМТС или администратором сегмента ЕМТС признаков функционирования вредоносного программного обеспечения необходимо:

3.1.Сообщить о данном факте с указанием внутреннего ip-адреса зараженного автоматизированного рабочего места (далее – АРМ) администратору ЕМТС (ГБУ АО «Инфраструктурный центр электронного правительства»).

3.2.Отключить зараженное АРМ ото всех средств коммуникации и сети электропитания.

3.3.Зафиксировать точную дату и время отключения зараженного АРМ.

3.4.Проинформировать администратора ЕМТС о проведенных мероприятиях и ждать дальнейших инструкций.

4. При поступлении сведений о проведении компьютерной атаки, а также наличии признаков проведения компьютерной атаки необходимо:

4.1.Отключить зараженное АРМ ото всех средств коммуникации и сети электропитания.

4.2.Сообщить администратору ЕМТС о данном факте и проведенных мероприятиях с указанием ip-адреса зараженного АРМ, ждать дальнейших инструкций.

5. При выявлении указанных фактов и невозможности отключения зараженного АРМ от сети необходимо:

5.1.Снять побитный образ операционной системы.

5.2.Зафиксировать на съемном носителе все записи журналов, log-файлы интернет-соединений за последние трое суток.

5.3.При необходимости осуществить резервное копирование файловой системы.

5.4.Сообщить администратору сети ЕМТС о проведенных мероприятиях с указанием внутреннего ip-адреса зараженного АРМ и ждать дальнейших инструкций.

6. Администратору ЕМТС при получении соответствующей информации в течение 24 часов необходимо проинформировать федеральный орган исполнительной власти, уполномоченный в области обеспечения функционирования ГосСОПКА (УФСБ России по Астраханской области, телефон: 44-36-88, факс: 44-39-76). В сообщении уведомить о факте возникновения компьютерного инцидента и месте его возникновения, предоставить контактный номер телефона для организации последующего взаимодействия.