МИНИСТЕРСТВО ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И СВЯЗИ АСТРАХАНСКОЙ ОБЛАСТИ

ПОСТАНОВЛЕНИЕ

27.09.2022 № 4-П

О внесении изменений в постановление министерства государственного управления, информационных технологий и связи Астраханской области от 20.04.2021 № 4-П

В соответствии с Приказом ФСБ России от 19.06.2019 № 282 «Об утверждении Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации», 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. Внести в постановление министерства государственного управления, информационных технологий и связи Астраханской области от 20.04.2021 № 4-П «О работе в единой мультисервисной телекоммуникационной сети Правительства Астраханской области» следующие изменения:

1.1. В приложениях, утвержденных постановлением, по всему тексту слова «исполнительные органы государственной власти Астраханской области» заменить словами «исполнительные органы Астраханской области», слова «ИОГВ АО» заменить словами «ИО АО» в соответствующем числе и падеже.

1.2. Порядок реагирования на компьютерные инциденты в единой мультисервисной телекоммуникационной сети Правительства Астраханской области изложить в новой редакции согласно приложению к настоящему постановлению.

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 нормативно-правового обеспечения 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 ООО « АИЦ «Консультант Плюс» и ООО «Астрахань-Гарант-Сервис».

4. Постановление вступает в силу со дня его официального опубликования.

Министр А.В. Набутовский

Приложение
к постановлению министерства государственного управления, информационных технологий и связи Астраханской области
от 27.09.2022 № 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).

2. Настоящий Порядок определяет процедуру информирования ФСБ России в рамках работы ЕМТС о компьютерных инцидентах, а также реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении объектов информационной инфраструктуры ЕМТС.

3. Для целей настоящего Порядка используются понятия, определённые 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».

4. При поступлении сведений о компьютерной атаке, а также о наличии признаков компьютерного инцидента администратору сегмента ЕМТС необходимо:

снять образ операционной системы;

зафиксировать на съемном носителе все записи журналов, log файлы интернет соединений за последние трое суток;

осуществить копирование файловой системы (при необходимости);

незамедлительно направить информацию о компьютерном инциденте администратору ЕМТС по форме, утвержденной настоящим Порядком.

5. Информирование администратором ЕМТС Национального координационного центра по компьютерным инцидентам (далее – НКЦКИ) осуществляется в соответствии с определенными НКЦКИ форматами представления информации о компьютерных инцидентах в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (далее – ГосСОПКА) с использованием технической инфраструктуры НКЦКИ.

6. В случае отсутствия подключения к данной технической инфраструктуре информация передается администратором ЕМТС по форме, утвержденной настоящим Порядком, посредством личного кабинета организации в НКЦКИ, почтовой, факсимильной или электронной связью на адреса (телефонные номера) НКЦКИ, указанные на официальном сайте в информационно-телекоммуникационной сети «Интернет» по адресу: «http://cert.gov.ru».

7. Информация о компьютерном инциденте направляется администратором ЕМТС в НКЦКИ в срок не позднее 24 часов с момента его обнаружения.

8. В ходе реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак администратор ЕМТС совместно с администратором сегмента ЕМТС проводят анализ компьютерных инцидентов (включая определение очередности реагирования на них), установление их связи с компьютерными атаками, а также определяют:

состав подразделений и должностных лиц информационной инфраструктуры, ответственных за проведение мероприятий по реагированию на компьютерные инциденты и принятие мер по ликвидации последствий компьютерных атак, и их задачи в рамках принимаемых мер;

перечень средств, необходимых для принятия мер по ликвидации последствий компьютерных атак;

очередность объектов информационной инфраструктуры (их структурных элементов) сегмента ЕМТС, в отношении которых будут приниматься меры по ликвидации последствий компьютерных атак;

перечень мер по восстановлению функционирования объекта информационной инфраструктуры ЕМТС.

9. О результатах мероприятий по реагированию на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак, администратор ЕМТС информирует НКЦКИ в срок не позднее 48 часов после завершения таких мероприятий в соответствии с пунктом 4 настоящего Порядка.

Приложение
к Порядку реагирования на компьютерные инциденты в единой мультисервисной телекоммуникационной сети Правительства Астраханской области

Форма регистрации инцидента

Наименование объекта:	Сведения об объекте (местонахождение объекта):
Взаимодействие с сетями электросвязи:	Дата и время заполнения:
Должность и ФИО лица, ответственного за регистрацию компьютерного инцидента:	
Основные сведения о компьютерном инциденте	
Дата и время возникновения инцидента:	Нарушение конфиденциальности, целостности, доступности: полное/частичное/ отсутствует
Описание инцидента (о функционировании объекта):	Класс инцидента (выбрать один):
Характеристика инцидента (кратко, тип инцидента, использованная уязвимость):	НСД/блокирование доступности элементов непреднамеренное нарушение:
Контактные данные работника, выявившего инцидент:	
ФИО: Организация: Контактные данные:	Адрес: Подразделение: e-mail:
Контактные данные работника, обрабатывающего инцидент:	
ФИО: Организация: Контактные данные:	Адрес: Подразделение: e-mail:
Дополнительные сведения:	
Выявленные уязвимости: Сведения о средстве/способе выявления: Хронология принятых мер:	Результат принятых мер: Последствия инцидента (выбрать один вариант):
Технические сведения:	Дополнительная информация: