# Министерство информатизации и связи Республики Мордовия

## П Р И К А З

г.Саранск

от 13 декабря 2018г. № 201

**Об утверждении регламента реагирования на компьютерные инциденты, связанные с совершением компьютерных атак и внедрением вредоносного программного обеспечения**

В целях совершенствования системы защиты информации в органах исполнительной власти Республики Мордовия, обеспечения информационной безопасности и организации порядка реагирования на события информационной безопасности п р и к а з ы в а ю:

1. Утвердить регламент реагирования на компьютерные инциденты, связанные с совершением компьютерных атак и внедрением вредоносного программного обеспечения (далее - регламент), согласно приложению.

2. Рекомендовать органам местного самоуправления муниципальных образований Республики Мордовия руководствоваться в своей деятельности регламентом.

3. Приказ вступает в силу с даты подписания.

4. Контроль за исполнением настоящего приказа оставляю за собой.

Министр И.А. Вольфсон

**У Т В Е Р Ж Д Е Н О**
приказом Министерства информатизации и связи Республики Мордовия
от « 13 » декабря 2018 г. № 201

# РЕГЛАМЕНТ РЕАГИРОВАНИЯ НА КОМПЬЮТЕРНЫЕ ИНЦИДЕНТЫ, СВЯЗАННЫЕ С СОВЕРШЕНИЕМ КОМПЬЮТЕРНЫХ АТАК И ВНЕДРЕНИЕМ ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

## I. Общие положения

1. Настоящий Регламент устанавливает порядок действий при возникновении угроз информационной безопасности, обусловленных возможностью несанкционированного доступа к государственным информационным ресурсам сторонних лиц (третьих лиц), внедрения и распространения вредоносного программного обеспечения, проведения массированных атак типа "отказ в обслуживании", а также возможными техническими сбоями в работе.

Регламент разработан для исполнительных органов государственной власти Республики Мордовия (далее – ИОГВ РМ) и подведомственных им организаций.

2. В настоящем Регламенте используются следующие понятия:

инцидент информационной безопасности - любое непредвиденное или нежелательное событие, которое может нарушить деятельность информационных систем или информационную безопасность;

информационное взаимодействие - процесс взаимодействия двух и более участников, целью которого является обработка информации в общих информационных системах и сетях;

участники информационного взаимодействия - пользователи информационных систем (далее - пользователи) ИОГВ РМ, системные администраторы, специалисты по информационной безопасности (далее - администраторы безопасности) ИОГВ РМ.

3. Действие положений настоящего Регламента распространяется на деятельность ИОГВ РМ и подведомственных им организаций и обязательны к соблюдению всеми сотрудниками ИОГВ РМ, участвующих в выявлении, разбирательстве и предотвращении инцидентов информационной безопасности.

4. Задачами настоящего Регламента являются:

организация деятельности сотрудников ИОГВ РМ осуществляющих администрирование информационных систем в ИОГВ РМ;

определение порядка работы пользователей, системных администраторов и администраторов безопасности;

обеспечение целостности, конфиденциальности и доступности информации;

соблюдение требований правовых актов в области защиты информации.

## II. Источники и виды инцидентов информационной безопасности

5. Источниками информации об инцидентах информационной безопасности в ИОГВ РМ являются:

факты, выявленные сотрудниками органов ИОГВ РМ;

результаты работы средств мониторинга информационной безопасности, аудита (внутреннего или внешнего);

журналы и оповещения операционных систем серверов и рабочих станций, антивирусной системы, системы резервного копирования и других систем;

обращения субъектов персональных данных с указанием инцидента информационной безопасности;

сообщения Министерства информатизации и связи Республики Мордовия (далее - Мининформсвязи) и ГУП Республики Мордовия «НПЦ информатизации и новых технологий» (далее - ГУП НПЦ);

сообщения Федеральной службы технического и экспортного контроля России;

сообщения Федеральной службы безопасности Российской Федерации;

сообщения Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций;

иные источники информации.

6. Основными видами инцидентов информационной безопасности в ИОГВ РМ являются:

несанкционированный доступ к информационным ресурсам ИОГВ РМ;

превышение полномочий - несанкционированный доступ к каким-либо ресурсам и помещениям сотрудников ИОГВ РМ;

компрометация учетных записей или паролей;

вирусная атака или вирусное заражение;

сетевые атаки (отказ в обслуживании (DoS-атаки), атаки типа Man-in-the-Middle, сниффер пакетов, переадресация портов, IP-спуфинг, атаки на уровне приложений и другое).

## III. Анализ исходной информации

7. При получении информации о несанкционированном воздействии на информационную систему и сеть системный администратор совместно с администратором безопасности обязаны убедиться, что инцидент информационной безопасности не является результатом их собственной ошибки или санкционированных действий.

8. При выявлении инцидента информационной безопасности в ИОГВ РМ системному администратору совместно с администратором безопасности необходимо:

принять меры по пресечению несанкционированного воздействия в случае, если на момент выявления оно не завершено;

принять меры по устранению причин возникновения инцидента информационной безопасности;

сохранить образ или содержание информационной системы, в том числе журналы событий (информационного ресурса) на момент обнаружения события (несанкционированного воздействия);

провести мероприятия по восстановлению работоспособности информационной системы (информационного ресурса);

провести служебную проверку с целью выявления причин, которые могли привести к произошедшему несанкционированному воздействию.

9. Администратору безопасности информационной системы, подвергшейся несанкционированному воздействию, необходимо в течение трех рабочих дней с момента обнаружения несанкционированного воздействия представить в Мининформсвязи (8342-39-14-08, 8342-39-14-12, RKurmakaev@e-mordovia.ru, svs-zi@e-mordovia.ru) и ГУП НПЦ (8342-39-10-00, IT@e-mordovia.ru) результаты служебной проверки и информацию о последствиях несанкционированного воздействия и принятых мерах по устранению причин несанкционированного воздействия.

10. Совместно с результатами служебной проверки администратор безопасности также должен представить в Мининформсвязи и ГУП НПЦ:

наименование информационной системы (информационного ресурса), на которую произведено несанкционированное воздействие;

время несанкционированного воздействия и (или) время обнаружения несанкционированного воздействия;

место несанкционированного воздействия (площадка, на которой размещается информационный ресурс, хостинг);

краткое изложение (описание) произошедшего несанкционированного воздействия и его последствий;

контактные данные (фамилия, имя, отчество, номер телефона, адрес электронной почты) системного администратора или администратора безопасности, ответственного за обеспечение работоспособности информационной системы (информационного ресурса);

правовой акт о создании и (или) вводе в эксплуатацию информационной системы (информационного ресурса);

паспорт информационной системы (при наличии);

договор об обслуживании или о техническом сопровождении (при наличии);

договор об оказании услуг по предоставлению вычислительных мощностей (договор о размещении на ресурсе, облаке) в случае, если информационная система (информационный ресурс) размещена на коммерческом ресурсе;

порядок работы или положение об информационной системе (информационном ресурсе) (при наличии).

11. По результатам рассмотрения полученной информации Мининформсвязи и ГУП НПЦ в течение одного рабочего дня со дня ее получения принимает решение о необходимости совершения конкретных действий и информирования Управления Федеральной службы безопасности Российской Федерации по Республике Мордовия о несанкционированном воздействии.

## IV. Обязанности участников информационного взаимодействия0

12. Обязанностями пользователя являются:

предоставление своего автоматизированного рабочего места администратору безопасности для контроля;

выполнение требований и рекомендаций администратора безопасности и системного администратора;

незамедлительное информирование администратора безопасности и системного администратора обо всех выявленных нарушениях, связанных с информационной безопасностью и обнаружением нештатного режима работы информационных систем и сетей.

13. Обязанностями системного администратора являются:

обеспечение бесперебойной работы системного программного обеспечения, серверного оборудования и автоматизированных рабочих мест пользователей;

обеспечение резервного копирования данных (восстановление данных при необходимости);

незамедлительное информирование администратора безопасности обо всех выявленных нарушениях, связанных с информационной безопасностью;

осуществление мероприятий по предотвращению несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации;

предотвращение незаконного вмешательства в информационные ресурсы и системы в иных формах;

выполнение требований и рекомендаций администратора безопасности;

ведение журнала учета инцидентов информационной безопасности, составленного по форме согласно приложению, к настоящему Регламенту;

принятие в течение 1 рабочего дня мер по восстановлению работоспособности информационных ресурсов и информационных систем, согласуемых с администратором безопасности и вышестоящим руководством (при необходимости);

проведение совместно с администратором безопасности анализа зарегистрированных инцидентов информационной безопасности с целью разработки мероприятий (плана мероприятий) по их предотвращению.

14. Обязанностями администратора безопасности являются:

проведение инструктажа пользователей по вопросам информационной безопасности;

обеспечение функционирования установленных систем защиты информации;

обновление антивирусных баз;

осуществление контроля за резервным копированием информации, сроками действия сертификатов соответствия средств защиты информации, ведением журнала учета инцидентов информационной безопасности;

проведение не реже 1 раза в год внутреннего аудита информационной безопасности;

осуществление совместно с системным администратором при получении информации об инцидентах информационной безопасности мероприятий по предотвращению несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации, предотвращение других форм незаконного вмешательства в информационные ресурсы и системы;

информирование непосредственного руководителя обо всех инцидентах, повлекших выход из строя либо временную приостановку работоспособности автоматизированных рабочих мест, автоматизированных систем и государственных информационных систем (информационных ресурсов, серверного оборудования), а также о фактах несанкционированного воздействия, заражения вредоносными программами;

проведение совместно с системным администратором анализа зарегистрированных инцидентов информационной безопасности с целью разработки плана мероприятий по их предотвращению.

## V. Ответственность участников информационного взаимодействия

15. Каждый участник информационного взаимодействия несет персональную ответственность за:

свои действия во время информационного взаимодействия в рамках своих служебных обязанностей;

соблюдение требований, установленных настоящим Регламентом.

Системный администратор, администратор безопасности и пользователи несут персональную ответственность за неисполнение или исполнение не в полном объеме своих обязанностей, указанных в разделе IV настоящего Регламента.

## Приложение. Журнал учета инцидентов информационной безопасности

Приложение
к регламенту
реагирования на компьютерные
инциденты, связанные
с совершением компьютерных атак
и внедрением вредоносного
программного обеспечения

**Журнал учета инцидентов информационной безопасности**

| № п/п | Краткое описание инцидента ИБ | Кем обнаружен (ФИО, должность) | Дата и время обнаружения | Дата и время решения проблемы | Подпись системного администратора /АИБ |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |