УКАЗ

ГЛАВЫ РЕСПУБЛИКИ МОРДОВИЯ

О порядке получения и оперативного доведения решения об установлении уровня опасности проведения целевых компьютерных атак, а также информации о необходимости принятия дополнительных мер по повышению защищенности объектов информационной инфраструктуры

В рамках реализации Указа Президента Российской Федерации от 5 октября 2020 г. № 612 «О дополнительных мерах по обеспечению безопасности информационной инфраструктуры Российской Федерации», распоряжения Секретаря Совета Безопасности Российской Федерации от 14 декабря 2020 г. № А21-68рсб «О кризисном штабе по предупреждению целевых компьютерных атак и порядке установления уровня опасности проведения целевых компьютерных атак», руководствуясь Законом Республики Мордовия от 30 мая 2022 г. № 21-З «О Правительстве Республики Мордовия», **п о с т а н о в л я ю:**

1. Утвердить Порядок получения и оперативного доведения решения об установлении уровня опасности проведения целевых компьютерных атак, а также информации о необходимости принятия дополнительных мер по повышению защищенности объектов информационной инфраструктуры до исполнительных органов государственной власти Республики Мордовия, органов местного самоуправления в Республике Мордовия и подведомственных им организаций, которые являются субъектами критической информационной инфраструктуры.

2. Контроль за исполнением настоящего Указа возложить на Первого Заместителя Председателя Правительства Республики Мордовия И.В. Фрейдина, координирующего вопросы по обеспечению информационной безопасности, в том числе по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты.

3. Настоящий Указ вступает в силу со дня его официального опубликования.

Глава
Республики Мордовия **А. ЗДУНОВ**

г. Саранск
19 октября 2022 года
№ 291–УГ

УТВЕРЖДЕНО
Указом Главы Республики Мордовия
«19» октября 2022 г. № 291-УГ

Порядок получения и оперативного доведения решения об установлении уровня опасности проведения целевых компьютерных атак, а также информации о необходимости принятия дополнительных мер по повышению защищенности объектов информационной инфраструктуры

Глава 1. Общие положения

1. Порядок получения и оперативного доведения решения об установлении уровня опасности проведения целевых компьютерных атак, а также информации о необходимости принятия дополнительных мер по повышению защищенности объектов информационной инфраструктуры (далее – Порядок) до исполнительных органов государственной власти Республики Мордовия, органов местного самоуправления в Республике Мордовия и подведомственных им организаций, которые являются субъектами критической информационной инфраструктуры (далее – органы власти и субъекты КИИ), разработан в соответствии с законодательством Российской Федерации, Стратегией национальной безопасности Российской Федерации, Доктриной информационной безопасности Российской Федерации, а также с иными документами стратегического планирования, регулирующими отношения в области обеспечения информационной безопасности Российской Федерации, в целях исполнения Указа Президента Российской Федерации от 5 октября 2020 г. № 612 «О дополнительных мерах по обеспечению безопасности информационной инфраструктуры Российской Федерации».

2. Уровень опасности проведения целевых компьютерных атак (далее – уровень опасности) устанавливается в целях реализации органами власти и субъектами КИИ мер обеспечения информационной безопасности при угрозе проведения целевых компьютерных атак на объекты критической информационной инфраструктуры (далее – противодействие целевым компьютерным атакам).

Под целевыми понимаются компьютерные атаки на объекты информационной инфраструктуры Российской Федерации, в отношении которых, по данным государственных органов, уполномоченных на осуществление разведывательной и (или) контрразведывательной деятельности, имеются сведения о причастности к их подготовке специальными службами иностранных государств.

Меры противодействия целевым компьютерным атакам в зависимости от уровня опасности определяются нормативными правовыми актами Российской Федерации и методическими рекомендациями федеральных органов исполнительной власти, уполномоченных в сфере обеспечения информационной безопасности критической информационной инфраструктуры.

3. Устанавливаются три уровня опасности:

а) повышенный («желтый») – при получении данных о подготовке целевой

компьютерной атаки без сроков ее проведения;

б) высокий («оранжевый») – при получении данных о возможном проведении целевой компьютерной атаки в краткосрочной перспективе;

в) критический («красный») – при получении данных, что принято решение о проведении целевой компьютерной атаки в краткосрочной перспективе.

Для обеспечения реализации указанных мер Совет по защите информации при Правительстве Республики Мордовия (далее – Совет по ЗИ) (постановление Правительства Республики Мордовия от 1 августа 2005 г. № 306 «О создании Совета по защите информации при Правительстве Республики Мордовия» и Штаб по обеспечению кибербезопасности исполнительных органов государственной власти Республики Мордовия (далее – Штаб) (распоряжение Правительства Республики Мордовия от 18 марта 2022 г. № 127-Р) координирует деятельность органов власти и субъектов КИИ Республики Мордовия.

Глава 2. Порядок доведения информации об установлении (изменении) уровня опасности

4. Решение Секретаря Совета Безопасности Российской Федерации об установлении (изменении) уровня опасности доводится Управлением ФСТЭК России по Приволжскому Федеральному округу до Министерства цифрового развития Республики Мордовия (далее – Министерство), Министерство доводит информацию до Первого Заместителя Председателя Правительства Республики Мордовия, который в свою очередь до Главы Республики Мордовия.

5. Секретари Совета по ЗИ и Штаба организует работу по оперативному доведению Решения Секретаря Совета Безопасности Российской Федерации об установлении уровня опасности до ответственных сотрудников органов власти.

6. Органы власти, в ведении которых находятся субъекты критической информационной инфраструктуры, незамедлительно информируют эти субъекты об установлении в отношении их уровня опасности и о необходимости реализации мер, определенных в решении об установлении уровня опасности.

7. Органы власти и субъекты КИИ обеспечивают реализацию мер в соответствии с нормативными правовыми актами Российской Федерации и методическими документами ФСТЭК.

Для реализации мер по обеспечению информационной безопасности Органы власти и субъекты КИИ:

а) определяют должностное лицо, ответственное за прием информации об установлении соответствующего уровня опасности и её оперативное доведение до сведения руководителя Органа власти и субъекта КИИ;

б) разрабатывают, согласовывают со ФСТЭК и утверждают планы мероприятий при установлении соответствующих уровней опасности, направленные на повышение защищенности объектов информационной инфраструктуры в условиях проведения целевых компьютерных атак и регламентирующие действия соответствующих должностных лиц и

подразделений в зависимости от уровня опасности.

8. Органы власти и субъекты КИИ в соответствии с установленными ФСТЭК формой и Порядком предоставляют отчеты о принятых мерах противодействия целевым компьютерным атакам при установлении определенного уровня опасности и направляют их председателю Совета по ЗИ и во ФСТЭК России.

9. Органы власти, в ведении которых находятся субъекты критической информационной инфраструктуры, обеспечивают выполнение данными субъектами мер противодействия целевым компьютерным атакам.

10. Методическое руководство деятельностью субъектов критической информационной инфраструктуры по обеспечению информационной безопасности их субъектов и ее координацию осуществляет ФСТЭК России.