ГЛАВА
УДМУРТСКОЙ РЕСПУБЛИКИ

УДМУРТ ЭЛЬКУНЛЭН
ТӦРОЕЗ

У К А З

О внесении изменений в Указ Главы Удмуртской Республики от 16 октября 2019 года № 133 «О мерах по защите информации ограниченного доступа в Удмуртской Республике»

1. Внести в Указ Главы Удмуртской Республики от 16 октября 2019 года № 133 «О мерах по защите информации ограниченного доступа в Удмуртской Республике» следующие изменения:

1) наименование изложить в следующей редакции:

«О мерах по защите информации ограниченного доступа в Удмуртской Республике и противодействию целевым компьютерным атакам на информационную инфраструктуру Удмуртской Республики»;

2) преамбулу изложить в следующей редакции:

«В целях обеспечения эффективного функционирования в Удмуртской Республике системы защиты информации ограниченного доступа и обеспечения безопасности информационной инфраструктуры Удмуртской Республики постановляю:»;

3) дополнить пунктом 1.1 следующего содержания:

«1.1. Утвердить прилагаемый Порядок противодействия целевым компьютерным атакам на информационную инфраструктуру Удмуртской Республики.»;

4) в пункте 2 слово «районов» исключить;

5) пункт 3 изложить в следующей редакции:

«3. Установить, что:

1) Руководитель Администрации Главы и Правительства Удмуртской Республики является уполномоченным должностным лицом, ответственным за реализацию мер по противодействию целевым компьютерным атакам на информационную инфраструктуру Удмуртской Республики;

2) министр цифрового развития Удмуртской Республики является должностным лицом, ответственным за приём информации об установлении соответствующего уровня опасности проведения целевых компьютерных атак и за оперативное доведение её до сведения Главы Удмуртской Республики и Руководителя Администрации Главы и Правительства Удмуртской Республики;

3) Отдел защиты государственной тайны Администрации Главы и Правительства Удмуртской Республики является головным подразделением, осуществляющим координацию и контроль деятельности государственных

органов Удмуртской Республики, методическое обеспечение деятельности органов местного самоуправления в Удмуртской Республике по защите информации, составляющей государственную тайну;

4) Управление развития инфраструктуры связи и информационной безопасности Министерства цифрового развития Удмуртской Республики является головным подразделением, осуществляющим координацию и контроль деятельности государственных органов Удмуртской Республики, методическое обеспечение деятельности органов местного самоуправления в Удмуртской Республике по обеспечению безопасности персональных данных в информационных системах персональных данных, объектов критической информационной инфраструктуры и защите информации, содержащейся в государственных и муниципальных информационных системах, в том числе по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты.»;

6) дополнить Порядком противодействия целевым компьютерным атакам на информационную инфраструктуру Удмуртской Республики согласно приложению.

2. Настоящий Указ вступает в силу со дня его подписания.

Глава
Удмуртской Республики **А.В. Бречалов**

г. Ижевск
2 ноября 2022 года
№ 294

Приложение
к Указу Главы
Удмуртской Республики
от 2 ноября 2022 года № 294

«УТВЕРЖДЁН
Указом Главы
Удмуртской Республики
от 16 октября 2019 года № 133

ПОРЯДОК
противодействия целевым компьютерным атакам на информационную инфраструктуру Удмуртской Республики

1. Порядок противодействия целевым компьютерным атакам на информационную инфраструктуру Удмуртской Республики (далее – Порядок) разработан в рамках реализации Указа Президента Российской Федерации от 5 октября 2020 года № 612 «О дополнительных мерах по обеспечению безопасности критической информационной инфраструктуры Российской Федерации», распоряжения Секретаря Совета Безопасности Российской Федерации от 14 декабря 2020 года № А21-68рсб «О кризисном штабе по предупреждению целевых компьютерных атак и порядке установления уровня опасности проведения целевых компьютерных атак».

2. Порядок действует в отношении информационной инфраструктуры исполнительных органов государственной власти Удмуртской Республики и Администрации Главы и Правительства Удмуртской Республики. В отношении информационной инфраструктуры органов местного самоуправления в Удмуртской Республике Порядок является рекомендательным.

3. Целями утверждения Порядка являются:

1) организация процедуры получения и оперативного информирования о принятии решения об установлении (изменении) уровня опасности проведения целевых компьютерных атак Главы Удмуртской Республики, Руководителя Администрации Главы и Правительства Удмуртской Республики, исполнительных органов государственной власти Удмуртской Республики, органов местного самоуправления в Удмуртской Республике, подведомственных им организаций;

2) реализация мер противодействия целевым компьютерным атакам на информационную инфраструктуру Удмуртской Республики и контроля за их выполнением;

3) координация деятельности исполнительных органов государственной власти Удмуртской Республики, Администрации Главы и Правительства Удмуртской Республики и органов местного самоуправления в Удмуртской

Республике по предупреждению целевых компьютерных атак на информационную инфраструктуру Удмуртской Республики.

4. Уровень опасности проведения целевых компьютерных атак устанавливается в целях реализации государственными органами и организациями мер обеспечения информационной безопасности при угрозе проведения целевых компьютерных атак на объекты информационной инфраструктуры.

5. Решение об установлении (изменении) уровня опасности принимается Секретарём Совета Безопасности Российской Федерации на основании решения Кризисного штаба по предупреждению целевых компьютерных атак, созданного Указом Президента Российской Федерации от 5 октября 2020 года № 612 «О дополнительных мерах по обеспечению безопасности критической информационной инфраструктуры Российской Федерации».

6. Установлены три уровня опасности:

1) повышенный («жёлтый») – при получении данных о подготовке целевой компьютерной атаки без сроков её проведения;

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

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

7. Координация, методическое руководство и контроль при установлении уровней опасности проведения целевых компьютерных атак в отношении исполнительных органов государственной власти Удмуртской Республики, Администрации Главы и Правительства Удмуртской Республики осуществляется Управлением Федеральной службы по техническому и экспортному контролю по Приволжскому федеральному округу (далее – Управление ФСТЭК по ПФО).

8. Руководитель Администрации Главы и Правительства Удмуртской Республики в рамках противодействия целевым компьютерным атакам на информационную инфраструктуру Удмуртской Республики:

1) организует проведение заседания Межведомственной комиссии по защите информации при Правительстве Удмуртской Республики для формирования перечня мер противодействия целевым компьютерным атакам и повышения защищённости объектов информационной инфраструктуры Удмуртской Республики;

2) организует информирование исполнительных органов государственной власти Удмуртской Республики и органов местного самоуправления в Удмуртской Республике об установлении соответствующего уровня опасности проведения целевых компьютерных атак;

3) организует направление в исполнительные органы государственной власти Удмуртской Республики и органы местного самоуправления в Удмуртской Республике перечень мер противодействия целевым

компьютерным атакам и повышения защищённости объектов информационной инфраструктуры Удмуртской Республики;

4) организует принятие мер противодействия целевым компьютерным атакам и повышения защищённости объектов информационной инфраструктуры в Администрации Главы и Правительства Удмуртской Республики.

9. Министр цифрового развития Удмуртской Республики в рамках противодействия целевым компьютерным атакам на информационную инфраструктуру Удмуртской Республики:

1) получает от Управления ФСТЭК по ПФО информацию об установлении соответствующего уровня опасности проведения целевых компьютерных атак;

2) информирует об установлении соответствующего уровня опасности проведения целевых компьютерных атак Главу Удмуртской Республики и Руководителя Администрации Главы и Правительства Удмуртской Республики;

3) организует методическое обеспечение работы Межведомственной комиссии по защите информации при Правительстве Удмуртской Республики.

10. Исполнительные органы государственной власти Удмуртской Республики при получении информации об установлении соответствующего уровня опасности проведения целевых компьютерных атак:

1) приступают к выполнению согласованных Управлением ФСТЭК по ПФО и утверждённых руководителем исполнительного органа государственной власти Удмуртской Республики планов мероприятий, реализуемых при установлении уровней опасности проведения целевых компьютерных атак;

2) информируют об установлении соответствующего уровня опасности проведения целевых компьютерных атак подведомственные учреждения и направляют им перечень мер противодействия целевым компьютерным атакам и повышения защищённости объектов информационной инфраструктуры.

11. Органам местного самоуправления в Удмуртской Республике при получении информации об установлении соответствующего уровня опасности проведения целевых компьютерных атак рекомендуется:

1) приступить к выполнению перечня мер противодействия целевым компьютерным атакам и повышения защищённости объектов информационной инфраструктуры Удмуртской Республики;

2) информировать об установлении соответствующего уровня опасности проведения целевых компьютерных атак подведомственные учреждения и направлять им перечень мер противодействия целевым компьютерным атакам и повышения защищённости объектов информационной инфраструктуры.

12. Ответственность за организацию работы по реализации мер противодействия целевым компьютерным атакам и повышению защищённости объектов информационной инфраструктуры Удмуртской Республики в исполнительных органах государственной власти Удмуртской Республики, Администрации Главы и Правительства Удмуртской Республики и органах местного самоуправления в Удмуртской Республике несут заместители

руководителей этих органов, ответственные за обеспечение мероприятий по защите информации.

13. Министерство цифрового развития Удмуртской Республики в рамках противодействия целевым компьютерным атакам на информационную инфраструктуру Удмуртской Республики:

1) организует мероприятия по разработке исполнительными органами государственной власти Удмуртской Республики, согласованию с Управлением ФСТЭК по ПФО и утверждению планов мероприятий, реализуемых при установлении уровней опасности проведения целевых компьютерных атак;

2) вырабатывает и реализует решения по предупреждению целевых компьютерных атак;

3) планирует и организует проведение контроля выполнения исполнительными органами государственной власти Удмуртской Республики, Администрацией Главы и Правительства Удмуртской Республики и органами местного самоуправления в Удмуртской Республике мер противодействия целевым компьютерным атакам и повышения защищённости объектов информационной инфраструктуры при установлении соответствующего уровня опасности проведения целевых компьютерных атак;

4) осуществляет координацию и методическое руководство по противодействию целевым компьютерным атакам, повышению защищённости объектов информационной инфраструктуры и предупреждению целевых компьютерных атак;

5) разрабатывает предложения для формирования перечня мер противодействия целевым компьютерным атакам и повышения защищённости объектов информационной инфраструктуры Удмуртской Республики.».