Проект

ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

ПОСТАНОВЛЕНИЕ

от «___» _____ 2019 г. № _____

МОСКВА

Об утверждении Порядка централизованного управления сетью связи общего пользования

В соответствии со статьей 65^1 Федерального закона от 7 июля 2003 г. № 126-ФЗ «О связи» (Собрание законодательства Российской Федерации, 2003, № 28, ст. 2895; № 52, ст. 5038; 2004, № 35, ст. 3607; № 45, ст. 4377; 2005, № 19, ст. 1752; 2006, № 6, ст. 636; № 10, ст. 1069; № 31, ст. 3431, ст. 3452; 2007, № 1, ст. 8; № 7, ст. 835; 2008, № 18, ст. 1941; 2009, № 29, ст. 3625; 2010, № 7, ст. 705; № 15, ст. 1737; № 27, ст. 3408; № 31, ст. 4190; 2011, № 7, ст. 901; № 9, ст. 1205; № 25, ст. 3535; № 27, ст. 3873, ст. 3880; № 29, ст. 4284, ст. 4291; № 30, ст. 4590; № 45, ст. 6333; № 49, ст. 7061; № 50, ст. 7351, ст. 7366; 2012, № 31, ст. 4322, ст. 4328; № 53, ст. 7578; 2013, № 19, ст. 2326; № 27, ст. 3450; № 30, ст. 4062; № 43, ст. 5451; № 44, ст. 5643; № 48, ст. 6162; № 49, ст. 6339, ст. 6347; № 52, ст. 6961; 2014, № 6, ст. 560; № 14, ст. 1552; № 19, ст. 2302; № 26, ст. 3366, ст. 3377; № 30, ст. 4229, ст. 4273; № 49, ст. 6928; 2015, № 29, ст. 4342, ст. 4383, ст. 4389; 2016, № 10, ст. 1316, ст. 1318; № 15, ст. 2066; № 18, ст. 2498; № 26, ст. 3873; № 27, ст. 4213, ст. 4221; № 28, ст. 4558; 2017, № 17, ст. 2457; № 24, ст. 3479; № 31, ст. 4742, ст. 4794; № 50, ст. 7557; 2018, № 17, ст. 2419; № 32, ст. 5135; № 51, ст. 7862; № 53, ст. 8455) Правительство Российской Федерации **п о с т а н о в л я е т :**

1. Утвердить прилагаемый Порядок централизованного управления сетью связи общего пользования.

2. Настоящее постановление вступает в силу с 1 ноября 2019 года.

Председатель Правительства
Российской Федерации Д. Медведев

УТВЕРЖДЕН
постановлением Правительства
Российской Федерации
от _____ 2019 г. № ____

Порядок
централизованного управления сетью связи общего пользования

I. Общие положения

1. Настоящий Порядок централизованного управления сетью связи общего пользования (далее – Порядок) включает в себя:

1) виды угроз устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети «Интернет» и сети связи общего пользования (далее соответственно – угрозы, сеть связи общего пользования);

2) регламент определения угроз, указанных в подпункте 1 настоящего пункта, и меры по их устранению, в том числе случаи управления техническими средствами противодействия угрозам и передачи обязательных к выполнению указаний;

3) требования к организационно-техническому взаимодействию в рамках централизованного управления сетью связи общего пользования, в том числе порядок и сроки рассмотрения претензий операторов связи к функционированию технических средств противодействия угрозам и запросов операторов связи о предоставлении сведений о функционировании технических средств противодействия угрозам в сети связи оператора связи;

4) способы определения федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, технической возможности исполнения указаний, передаваемых в рамках централизованного управления сетью связи общего пользования;

5) условия и случаи, при которых оператор связи имеет право не направлять трафик через технические средства противодействия угрозам.

2. Настоящий Порядок не применяются в целях управления сетью связи общего пользования в чрезвычайных ситуациях и в условиях чрезвычайного положения в случаях, предусмотренных статьями 65, 66 Федерального закона от 7 июля 2003 г. № 126-ФЗ «О связи».

3. К лицам, участвующим в централизованном управлении, относятся операторы связи, собственники или иные владельцы технологических сетей связи, собственники или иные владельцы точек обмена трафиком,

собственники или иные владельцы линий связи, пересекающих Государственную границу Российской Федерации, иные лица, имеющие номер автономной системы (далее – лица, участвующие в централизованном управлении).

4. Централизованное управление сетью связи общего пользования осуществляется Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций в случаях возникновения угроз безопасности сетей связи общего пользования.

II. Виды угроз сети связи общего пользования

5. Под угрозой целостности сетей связи общего пользования понимается угроза нарушения способности взаимодействия сетей связи, при котором становится не возможным установление соединения и (или) передача информации между пользователями услугами связи.

6. Под угрозой устойчивости сетей связи общего пользователя понимается угроза при которой нарушается способность сети связи сохранять свою целостность в условиях эксплуатации технических средств связи, соответствующих установленным в документации производителей, при отказе части элементов сети связи и возвращаться в исходное состояние (надежность сети связи), а также в условиях внешних дестабилизирующих воздействий природного и техногенного характера (живучесть сети связи).

7. Под угрозой безопасности функционирования сетей связи общего пользования понимается угроза нарушения способности оператора связи противостоять попыткам несанкционированного доступа к техническим и программным средствам сети связи общего пользования и преднамеренным дестабилизирующим внутренним или внешним информационным воздействиям, следствием которых может быть нарушение функционирования сети связи.

III. Регламент определения угроз и меры по их устранению

8. Министерство цифрового развития связи и массовых коммуникаций Российской Федерации по согласованию с Федеральной службой безопасности определяет перечень актуальных угроз целостности, устойчивости и безопасности функционирования на территории Российской Федерации сети связи общего пользования.

9. Актуальность угроз определяется на основании анализа вероятности реализации угрозы и уровня опасности угрозы, определяемой в соответствии с пунктом 8 настоящего Порядка в порядке, установленном Министерством цифрового развития связи и массовых коммуникаций Российской Федерации по согласованию с Федеральной службой безопасности. Вероятности

реализации угрозы может быть присвоены уровни: низкий, средний, высокий. Уровень опасности угрозы может устанавливаться: низким, средним, высоким.

10. Вероятность реализации и уровень опасности угрозы определяется Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций на основании данных мониторинга функционирования сети связи общего пользования, который проводится в соответствии с частью 1 статьи 65^1 Федерального закона от 7 июля 2003 г. № 126-ФЗ «О связи» и в порядке, определяемом в соответствии с абзацем первым пункта 4 постановления Правительства Российской Федерации от 13 февраля 2019 г. № 136 «О Центре мониторинга и управления сетью связи общего пользования» (Собрание законодательства Российской Федерации, 2019, № 8, ст. 776).

11. Перечень актуальных угроз публикуется на официальном сайте Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций.

12. К мерам по противодействию угрозам относятся:

1) самостоятельное управление трафиком в сети связи общего пользования оператором связи, собственником или иным владельцем технологических сетей связи, собственником или иным владельцем точки обмена трафиком, собственником или иным владельцем линий связи, пересекающих Государственную границу Российской Федерации, иным лицом, имеющим номер автономной системы, в целях снижения вероятности реализации угрозы при низких и средних вероятностях реализации угрозы и уровнях опасности угрозы;

2) централизованное управление сетью связи общего пользования, осуществляемое Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций.

13. Централизованное управление сетью связи общего пользования осуществляется в случае актуальности угрозы, вероятность реализации которой высокая и (или) уровень опасности которой определен высоким.

14. Централизованное управление сетью связи общего пользования осуществляется следующими способами:

а) в случае неотложного реагирования на угрозу целостности, устойчивости и безопасности функционирования на территории Российской Федерации (реализация которой имеет высокую вероятность), по указанию Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций центром мониторинга и управления сетью связи общего пользования в составе радиочастотной службы, путем управления техническими средствами противодействия угрозам;

б) в иных случаях путем передачи обязательных к выполнению указаний Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций операторам связи, собственникам или владельцам технологических сетей связи, а также иным лицам, имеющим номер автономной системы.

VI. Требования к организационно-техническому взаимодействию в рамках централизованного управления сетью связи общего пользования

15. Органы власти и организации, участвующие в централизованном управлении, определяют подразделение или лицо (лица) из числа своих работников, ответственное за взаимодействие в рамках централизованного управления сетью связи общего пользования (далее – ответственный за взаимодействие).

16. Взаимодействие органов власти и организаций, участвующих в централизованном управлении, с Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций осуществляется посредством средств телекоммуникационной связи, в том числе путем обмена электронными документами.

В документооборот включаются:

а) указание Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по централизованному управлению сетью связи общего пользования (далее – указание);

б) отчет лица, участвующего в централизованном управлении о выполнении (невозможности выполнения) указания (далее – отчет);

в) претензия оператора связи к функционированию технических средств противодействия угрозам (далее – претензия оператора);

г) ответ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций на претензию оператора;

д) запрос оператора связи о предоставлении сведений о функционировании технических средств противодействия угрозам в сети связи оператора связи (далее – запрос оператора);

е) ответ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций на запрос оператора.

17. Структура, формат, правила формирования и передачи (в том числе с использованием средств криптографической защиты информации) электронных документов определяются Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций.

18. Электронные документы:

1) указанные в подпунктах «а», «г», «е», пункта 16 настоящего Порядка, подписываются усиленной квалифицированной электронной подписью уполномоченного работника Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций;

2) указанные в подпунктах «б», «в», «д», пункта 16 настоящего Порядка, подписываются усиленной квалифицированной электронной подписью ответственного за взаимодействие.

19. В случае, указанном в подпункте «а» пункта 14 настоящего Порядка, указание может быть передано посредством телефонной связи, с дальнейшим направлением соответствующего электронного документа не позднее, чем через 12 часов.

20. Указание подлежит исполнению в срок, определенный в таком указании, за исключением случаев невозможности исполнения указания.

21. Отчет направляется в срок до 3 часов с момента исполнения указания или немедленно при невозможности исполнения указания с мотивированным обоснованием причин.

22. Претензия оператора рассматривается комиссией, в которую включаются представители Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации, Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций, а также центра мониторинга и управления сетью связи общего пользования в течении суток с момента получения. При наличии необходимости срок рассмотрения может быть продлен, но не более чем на 2 суток, о чем информируется оператор связи.

По результатам рассмотрения претензия оператора связи признается обоснованной или необоснованной сбоями в сетях связи в результате функционирования технических средств противодействия угрозам, что указывается в отчете комиссии, включенном в ответ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций на претензию оператора с указанием обоснованных причин такого решения.

23. Запрос оператора рассматривается комиссией, в которую включаются представители Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций и центра мониторинга и управления сетью связи общего пользования в течении 3 суток с момента получения. При наличии необходимости срок рассмотрения может быть продлен, но не более чем на 5 суток, о чем информируется оператор.

По результатам рассмотрения запроса оператора Федеральная служба по надзору в сфере связи, информационных технологий и массовых

коммуникаций направляет оператору связи сведения о функционировании технических средств противодействия угрозам в сети связи оператора связи или мотивированный возврат запроса оператора.

Возврат запроса оператора осуществляется в следующих случаях:

1) наличие в представленном запросе оператора и (или) прилагаемых к нему документах недостоверной или искаженной информации;

2) невозможности идентификации сведений, содержащихся в запросе, и (или) направившего его оператора связи.

После получения возврата запроса оператора от Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций такой оператор связи имеет право повторно направить запрос.

VII. Способы определения технической возможности исполнения указаний, передаваемых в рамках централизованного управления сетью связи общего пользования

24. Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций определяет техническую возможность исполнения указаний в следующих случаях:

а) в случаях централизованного управления в соответствии с подпунктом «а» пункта 14 настоящего Порядка;

б) в случае получения от лица, участвующего в централизованном управлении, информации о невозможности исполнения указания.

25. Определение технической возможности исполнения указаний производится следующими способами:

а) моделирование исполнения указания в сети связи оператора связи и сети связи общего пользования на основании данных центра мониторинга и управления сетью связи общего пользования;

б) запрос дополнительной информации (в том числе посредством телефонной связи и иных средств телекоммуникационной связи) у лица, ответственного за взаимодействие;

в) анализ информации, получаемой от технических средств противодействия угрозам и технических средств контроля за соблюдением операторами связи, собственниками или иными владельцами технологических сетей связи требований Федерального закона от 7 июля 2003 г. № 126-ФЗ «О связи» и Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (Собрание законодательства Российской Федерации, 2006, № 31, ст. 3448; 2010, № 31, ст. 4196; 2011, № 15, ст. 2038; № 30, ст. 4600; 2012, № 31, ст. 4328; 2013, № 14, ст. 1658; № 23, ст. 2870; № 27, ст. 3479; № 52, ст. 6961, ст. 6963; 2014, № 19, ст. 2302; № 30, ст. 4223, ст. 4243; № 48, ст. 6645; 2015, № 1, ст. 84; № 27, ст. 3979; № 29, ст. 4389, ст. 4390; 2016,

№ 26, ст. 3877; № 28, ст. 4558; № 52, ст. 7491; 2017, № 18, ст. 2664; № 24, ст. 3478; № 25, ст. 3596; № 27, ст. 3953; № 31, ст. 4790, ст. 4825, ст. 4827; № 48, ст. 7051; 2018, № 1, ст. 66; № 18, ст. 2572; № 27, ст. 3956; № 30, ст. 4546; № 52, ст. 8101; 2019, № 12, ст. 1220, ст. 1221), предусматривающих ограничение доступа к информации.

VIII. Условия и случаи, при которых оператор связи имеет право не направлять трафик через технические средства противодействия угрозам

26. Оператор связи имеет право не направлять трафик через технические средства противодействия угрозам в следующих случаях:

а) нарушения функционирования технического средства (технических средств) противодействия угрозам, подтвержденные Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций ответом на запрос оператора;

б) нарушения функционирования технического средства (технических средств) противодействия угрозам, выявленные техническими средствами сети связи оператора связи.

27. Если оператором связи установлены случаи, при которых оператор связи вправе не направлять трафик через технические средства противодействия угрозам, такой оператор вправе не направлять трафик через технические средства противодействия угрозам при условии уведомления об этом в электронной форме Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций до момента реализации такого решения. Формат и структура уведомления определяется Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций.

28. При устранении причин, по которым оператор связи имеет право не направлять трафик через технические средства противодействия угрозам, оператор связи незамедлительно осуществляет направление трафика через указанные технические средства, о чем информирует Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций.

29. Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций вправе проинформировать оператора связи об устранении причин, по которым оператор связи имеет право не направлять трафик через технические средства противодействия угрозам, в форме указания.