ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

ПОСТАНОВЛЕНИЕ

от 12 февраля 2020 г. № 127

МОСКВА

Об утверждении Правил централизованного управления сетью связи общего пользования

В соответствии с пунктом 5 статьи 65[1] Федерального закона "О связи" Правительство Российской Федерации **п о с т а н о в л я е т :**

Утвердить прилагаемые Правила централизованного управления сетью связи общего пользования.

Председатель Правительства
Российской Федерации М.Мишустин

4385137

УТВЕРЖДЕНЫ
постановлением Правительства
Российской Федерации
от 12 февраля 2020 г. № 127

П Р А В И Л А
централизованного управления сетью связи общего пользования

I. Общие положения

1. Настоящие Правила определяют:

а) виды угроз устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети "Интернет" (далее - сеть "Интернет") и сети связи общего пользования;

б) регламент определения угроз, указанных в подпункте "а" настоящего пункта, и меры по их устранению, в том числе случаи управления техническими средствами противодействия таким угрозам (далее - технические средства противодействия угрозам) и передачи обязательных к выполнению указаний Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций лицам, участвующим в централизованном управлении сетью связи общего пользования (далее соответственно - указания, централизованное управление);

в) требования к организационно-техническому взаимодействию в рамках централизованного управления, 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;

г) способы определения Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций технической возможности исполнения указаний, передаваемых в рамках централизованного управления;

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

2. Централизованное управление осуществляется Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций.

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, организаторы распространения информации в сети "Интернет", имеющие уникальный идентификатор совокупности средств связи и иных технических средств в сети "Интернет" (далее - номер автономной системы), иные лица, если такие лица имеют номер автономной системы.

II. Виды угроз устойчивости, безопасности и целостности функционирования на территории Российской Федерации сети "Интернет" и сети связи общего пользования

4. Под угрозой устойчивости функционирования на территории Российской Федерации сети "Интернет" и сети связи общего пользования понимается угроза, при которой нарушается работоспособность сети связи при неисправности фрагмента сети связи, а также в условиях внешних дестабилизирующих воздействий природного и техногенного характера. Угрозами устойчивости функционирования на территории Российской Федерации сети "Интернет" и сети связи общего пользования являются:

а) угрозы невозможности доступа к услугам связи из-за аварий или перегрузки узла связи, вследствие которых услуги связи становятся недоступными для физических и юридических лиц, в том числе не может быть осуществлен вызов экстренных оперативных служб;

б) угрозы невозможности оказания услуг связи владельцам критически важных объектов, если такая невозможность оказания услуг связи может привести к нарушению или прекращению функционирования критически важных объектов.

5. Под угрозой безопасности функционирования на территории Российской Федерации сети "Интернет" и сети связи общего пользования понимается нарушение способности сети связи противостоять попыткам несанкционированного доступа к техническим и программным средствам

сети связи общего пользования, преднамеренным дестабилизирующим внутренним или внешним информационным воздействиям, при которых нарушается функционирование сети связи общего пользования, а также воздействиям, связанным с распространением в сети "Интернет" информации, доступ к которой подлежит ограничению в соответствии с законодательством Российской Федерации. Угрозами безопасности функционирования на территории Российской Федерации сети "Интернет" и сети связи общего пользования являются:

а) угрозы нарушения информационной безопасности (конфиденциальности, целостности, доступности) автоматизированных систем управления сетями связи операторов связи, автоматизированных систем управления технологических сетей связи, систем управления точками обмена трафиком, технических средств и программного обеспечения центра мониторинга и управления сетью связи общего пользования в составе радиочастотной службы (далее - центр мониторинга и управления), технических средств противодействия угрозам, национальной системы доменных имен, а также критической информационной инфраструктуры Российской Федерации;

б) угрозы предоставления доступа к информации или информационным ресурсам в сети "Интернет", доступ к которым подлежит ограничению в соответствии с законодательством Российской Федерации;

в) угрозы противодействия (затруднения) ограничению доступа к информации или информационным ресурсам в сети "Интернет", доступ к которым подлежит ограничению в соответствии с законодательством Российской Федерации;

г) угрозы осуществления компьютерных атак и иных информационных воздействий (как преднамеренных, так и непреднамеренных) на средства связи и сети связи, в результате которых может быть нарушено функционирование на территории Российской Федерации сети "Интернет" и сети связи общего пользования;

д) угрозы нарушения доступности для граждан информационных ресурсов органов государственной власти и органов местного самоуправления в сети "Интернет".

6. Под угрозой целостности функционирования на территории Российской Федерации сети "Интернет" и сети связи общего пользования понимается угроза нарушения способности взаимодействия сетей связи, при котором становятся невозможными соединение и передача информации между пользователями взаимодействующих сетей и доступ

пользователей к информационным ресурсам в сети "Интернет". Угрозами целостности функционирования на территории Российской Федерации сети "Интернет" и сети связи общего пользования являются:

а) угрозы нарушения взаимодействия сети связи общего пользования Российской Федерации с сетями связи общего пользования иностранных государств, вследствие которого становятся невозможными соединение и передача информации между пользователями взаимодействующих сетей связи или доступ пользователей к информационным ресурсам в сети "Интернет", расположенным на территории одного или нескольких иностранных государств;

б) угрозы нарушения функционирования сети "Интернет", вследствие которого становятся невозможными соединение и передача информации между пользователями сети "Интернет" или информационными ресурсами в сети "Интернет", находящимися на территории Российской Федерации, и пользователями сети "Интернет" или информационными ресурсами в сети "Интернет", расположенными на территории Российской Федерации либо одного или нескольких иностранных государств;

в) угрозы нарушения взаимодействия сетей связи, вследствие которого становятся невозможными соединение и передача информации между пользователями взаимодействующих сетей связи или доступ к информационным ресурсам в сети "Интернет", расположенным на территории одного или нескольких субъектов Российской Федерации;

г) угрозы нарушения взаимодействия технологических сетей связи лиц, имеющих номер автономной системы, расположенных на территории одного или нескольких субъектов Российской Федерации, вследствие которого становятся невозможными соединение и передача информации между пользователями взаимодействующих технологических сетей или доступ к информационным ресурсам в сети "Интернет".

III. Регламент определения угроз устойчивости, безопасности и целостности функционирования на территории Российской Федерации сети "Интернет" и сети связи общего пользования, меры по их устранению, в том числе случаи управления техническими средствами противодействия угрозам и передачи указаний

7. Угрозы устойчивости, безопасности и целостности функционирования на территории Российской Федерации сети "Интернет" и сети связи общего пользования определяются Министерством цифрового

развития, связи и массовых коммуникаций Российской Федерации, Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций и Федеральной службой безопасности Российской Федерации в рамках своей компетенции по результатам учений, проведенных в соответствии с пунктом 3 статьи 56^1 Федерального закона "О связи", мониторинга функционирования указанных сетей, проводимого в соответствии с пунктом 1 статьи 65^1 Федерального закона "О связи", а также по результатам исследований по вопросам устойчивости, безопасности и целостности функционирования на территории Российской Федерации сети "Интернет" и сети связи общего пользования.

8. Угрозы устойчивости, безопасности и целостности функционирования на территории Российской Федерации сети "Интернет" и сети связи общего пользования определяются в соответствии с видами угроз, указанными в пунктах 4 - 6 настоящих Правил.

9. Информация об угрозах устойчивости, безопасности и целостности функционирования на территории Российской Федерации сети "Интернет" и сети связи общего пользования направляется Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации и Федеральной службой безопасности Российской Федерации в Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций.

10. Информацию, указанную в пункте 9 настоящих Правил, а также описание угрозы, данные об уязвимости средств и технологий связи, количественные и качественные показатели влияния угрозы на функционирование сети "Интернет" и сети связи общего пользования Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций вносит в перечень угроз устойчивости, безопасности и целостности функционирования на территории Российской Федерации сети "Интернет" и сети связи общего пользования (далее - перечень угроз).

Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций вносит в перечень угроз информацию в отношении угроз устойчивости, безопасности и целостности функционирования на территории Российской Федерации сети "Интернет" и сети связи общего пользования, определенных Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций самостоятельно.

Вопросы внесения в перечень угроз информации, указанной в пункте 9 настоящих Правил, данных об уязвимости средств и технологий связи, количественных и качественных показателей влияния угрозы на функционирование сети "Интернет" и сети связи общего пользования, а также вопросы формирования модели угроз и нарушителей могут быть вынесены на заседание экспертной комиссии, состав и порядок деятельности которой утверждается Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций по согласованию с Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации и Федеральной службой безопасности Российской Федерации, в том числе в случае разногласий по представленной информации с указанными федеральными органами исполнительной власти.

11. Внесение информации, указанной в пунктах 9 и 10 настоящих Правил, в перечень угроз является основанием для осуществления Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций централизованного управления.

12. Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций по согласованию с Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации и Федеральной службой безопасности Российской Федерации утверждает регламент реагирования в отношении каждой угрозы, содержащейся в перечне угроз (далее - регламент реагирования), который должен содержать конкретные мероприятия по устранению угроз устойчивости, безопасности и целостности функционирования на территории Российской Федерации сети "Интернет" и сети связи общего пользования в соответствии с мерами, указанными в пункте 13 настоящих Правил.

13. Мерами по устранению угроз устойчивости, безопасности и целостности функционирования на территории Российской Федерации сети "Интернет" и сети связи общего пользования являются:

а) организационно-технические мероприятия по восстановлению работоспособности сети связи общего пользования;

б) изменение маршрутов сообщений электросвязи;

в) обеспечение резервирования линий связи и каналов связи в сети связи общего пользования;

г) изменение конфигурации средств связи в сети связи общего пользования;

д) применение средств защиты информации в сети связи общего пользования;

е) оповещение лиц, участвующих в централизованном управлении, и пользователей сети связи общего пользования о наличии угрозы и принимаемых мерах противодействия;

ж) мероприятия по предупреждению возникновения угроз, в том числе в соответствии с разработанными моделями угроз и нарушителей.

14. Доступ лиц, участвующих в централизованном управлении, к информации, содержащейся в регламенте реагирования, осуществляется с использованием личного кабинета на сайте Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций в сети "Интернет" (далее - личный кабинет). Информация ограниченного доступа, содержащаяся в регламенте реагирования, предоставляется лицам, участвующим в централизованном управлении, по запросу. Ответ на запрос о предоставлении информации, содержащейся в регламенте реагирования, Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций направляет на электронную почту или иным способом в течение 2 рабочих дней со дня получения запроса.

15. Управление техническими средствами противодействия угрозам осуществляется в случае необходимости реагирования на угрозу безопасности функционирования на территории Российской Федерации сети "Интернет" и сети связи общего пользования и угрозу целостности функционирования на территории Российской Федерации сети "Интернет" и сети связи общего пользования, предусмотренные пунктами 5 и 6 настоящих Правил, а также для решения задач мониторинга выявления возникновения угроз устойчивости, безопасности и целостности функционирования на территории Российской Федерации сети "Интернет" и сети связи общего пользования.

Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций может вынести вопрос об осуществлении управления техническими средствами противодействия угрозам на заседание экспертной комиссии, указанной в пункте 10 настоящих Правил, в случае, если осуществление управления техническими средствами противодействия угрозам может привести к нарушению или прекращению функционирования сети "Интернет" и сети связи общего пользования.

16. Передача указаний осуществляется в случае необходимости реагирования на угрозы устойчивости, безопасности и целостности функционирования на территории Российской Федерации сети "Интернет" и сети связи общего пользования в рамках централизованного управления.

IV. Требования к организационно-техническому взаимодействию в рамках централизованного управления, 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

17. Лица, участвующие в централизованном управлении, определяют должностное лицо (лиц) из числа сотрудников, ответственное за организационно-техническое взаимодействие в рамках централизованного управления (далее - лицо, ответственное за взаимодействие).

18. Взаимодействие лиц, участвующих в централизованном управлении, с Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций в рамках централизованного управления осуществляется с использованием личного кабинета на сайте Службы и автоматического взаимодействия систем управления или средств связи лиц, участвующих в централизованном управлении, с информационной системой мониторинга и управления сетью связи общего пользования.

19. При осуществлении централизованного управления указания могут быть переданы лицу, ответственному за взаимодействие, любым способом, позволяющим установить факт их получения, в том числе посредством телефонной связи.

Указания подлежат исполнению в срок, определенный в указании. В случае невозможности исполнения указаний лицо, участвующее в централизованном управлении, уведомляет об этом Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций способом, позволяющим подтвердить факт уведомления.

20. Лицо, участвующее в централизованном управлении, обязано предпринять все необходимые меры для исполнения указаний при осуществлении централизованного управления.

21. Оператор связи вправе направить в Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций запрос о предоставлении сведений о функционировании технических средств противодействия угрозам (далее - запрос) способом, позволяющим подтвердить факт направления запроса, в том числе посредством его размещения в личном кабинете.

Запрос подлежит рассмотрению в течение 5 рабочих дней со дня его регистрации.

22. По результатам рассмотрения запроса Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций в течение 2 рабочих дней направляет оператору связи ответ на запрос, содержащий также вывод о влиянии функционирования технических средств противодействия угрозам на работу сети связи оператора связи, способом, позволяющим подтвердить факт его направления, в том числе посредством его размещения в личном кабинете.

23. В случаях, требующих проведения дополнительных исследований, Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций принимает решение о продлении срока рассмотрения запроса не более чем на 20 рабочих дней, а запрос передается на рассмотрение в комиссию, положение о которой и состав которой утверждаются Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций (далее - комиссия).

24. Оператор связи, направивший запрос, уведомляется о продлении срока рассмотрения запроса и его передачи в комиссию в течение 2 рабочих дней со дня принятия решения о продлении срока рассмотрения запроса способом, позволяющим подтвердить факт направления уведомления, в том числе посредством его размещения в личном кабинете.

25. Комиссия рассматривает запрос в срок, не превышающий 15 рабочих дней со дня передачи запроса в комиссию.

26. По результатам рассмотрения запроса комиссия готовит мотивированное заключение, содержащее сведения о функционировании технических средств противодействия угрозам и влиянии функционирования технических средств противодействия угрозам на работу сети связи оператора связи, используемой для оказания услуг связи пользователям услуг связи, и передает его в Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций в течение 3 рабочих дней.

27. Мотивированное заключение, указанное в пункте 26 настоящих Правил, направляется в течение 2 рабочих дней Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций оператору связи любым доступным способом, позволяющим подтвердить факт его получения, в том числе посредством его размещения в личном кабинете.

28. Операторы связи вправе направить в Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций претензию к функционированию технических средств противодействия угрозам (далее - претензия) способом, позволяющим подтвердить факт направления претензии, в том числе посредством ее размещения в личном кабинете.

29. В претензии оператор связи указывает обстоятельства, свидетельствующие о негативном влиянии технических средств противодействия угрозам на работу сети связи оператора связи.

30. Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций в течение 2 рабочих дней со дня поступления претензии передает ее в комиссию, которая рассматривает претензию в течение 20 рабочих дней со дня получения.

31. Комиссия по результатам рассмотрения претензии принимает одно из следующих решений:

а) решение о наличии основания (оснований) для признания претензии обоснованной и ее удовлетворения;

б) решение о наличии основания (оснований) для отказа в удовлетворении претензии.

32. Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций на основании решения комиссии принимает одно из следующих решений:

а) решение о признании претензии обоснованной и ее удовлетворении;

б) решение об отказе в удовлетворении претензии.

33. Принятое решение Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций направляет оператору связи в течение 2 рабочих дней со дня принятия решения способом, позволяющим подтвердить факт направления решения, в том числе посредством его размещения в личном кабинете.

34. В случае принятия решения, указанного в подпункте "а" пункта 32 настоящих Правил, Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций обеспечивает проведение работ, направленных на оптимизацию функционирования технических средств противодействия угрозам, а также работ по устранению недостатков их функционирования, выявленных по итогам рассмотрения претензии.

V. Способы определения технической возможности исполнения указаний

35. Техническую возможность исполнения указаний определяет Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций.

36. Техническая возможность исполнения указаний в отношении угрозы устойчивости, безопасности и целостности функционирования на территории Российской Федерации сети "Интернет" и сети связи общего пользования определяется следующими способами:

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

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

в) анализ информации, полученной от технических средств противодействия угрозам и технических средств контроля за соблюдением операторами связи, собственниками или иными владельцами технологических сетей связи требований Федерального закона "О связи" и Федерального закона "Об информации, информационных технологиях и о защите информации", предусматривающих ограничение доступа к информации;

г) анализ информации, полученной в соответствии с пунктами 1, 7 и подпунктом 4 пункта 8 статьи 56^2 Федерального закона "О связи".

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

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

а) нарушение функционирования технического средства противодействия угрозам, при котором прекращается пропуск трафика через данное техническое средство, при условии соблюдения требований к эксплуатации технических средств противодействия угрозам;

б) нарушение функционирования технического средства противодействия угрозам, при котором параметры пропуска трафика не соответствуют параметрам, указанным в проектной документации

на установку и функционирование технических средств противодействия угрозам, при условии соблюдения требований к эксплуатации технических средств противодействия угрозам;

в) выявление информации или информационных ресурсов, доступ к которым не подлежит ограничению в соответствии с законодательством Российской Федерации, но доступ к которым ограничивается.

38. Оператор связи вправе не направлять трафик через техническое средство противодействия угрозам в случае, предусмотренном подпунктом "а" пункта 37 настоящих Правил, после размещения информации о нем в личном кабинете.

39. Оператор связи вправе не направлять трафик через техническое средство противодействия угрозам в случаях, предусмотренных подпунктами "б" и "в" пункта 37 настоящих Правил, после размещения информации о них в личном кабинете и получения указания.

40. Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций обеспечивает рассмотрение информации, размещенной оператором связи в личном кабинете, в срок, не превышающий 24 часов с момента ее размещения.

41. Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций при подтверждении информации о случаях, предусмотренных подпунктами "а" и "б" пункта 37 настоящих Правил, незамедлительно обеспечивает проведение работ по восстановлению функционирования технических средств противодействия угрозам.

42. При неподтверждении информации о случае, предусмотренном подпунктом "а" пункта 37 настоящих Правил, или после восстановления функционирования технических средств противодействия угрозам Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций незамедлительно доводит до оператора связи указание, содержащее информацию о направлении трафика через техническое средство противодействия угрозам, любым доступным способом, позволяющим подтвердить факт получения указания, в том числе через личный кабинет.

43. Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций при подтверждении информации о случае, предусмотренном подпунктом "в" пункта 37 настоящих Правил, незамедлительно обеспечивает доступ к информации или информационным ресурсам, доступ к которым не подлежит ограничению

в соответствии с законодательством Российской Федерации, но доступ к которым ограничивается, и доводит до оператора связи указание, содержащее информацию о направлении трафика через техническое средство противодействия угрозам, любым доступным способом, позволяющим подтвердить факт получения указания, в том числе через личный кабинет.
