ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

П О С Т А Н О В Л Е Н И Е

от 27 октября 2025 г. № 1667

МОСКВА

Об утверждении Правил централизованного управления сетью связи общего пользования

В соответствии со статьей 65^1 Федерального закона "О связи" Правительство Российской Федерации **п о с т а н о в л я е т :**

1. Утвердить прилагаемые Правила централизованного управления сетью связи общего пользования.

2. Признать утратившими силу:

постановление Правительства Российской Федерации от 12 февраля 2020 г. № 127 "Об утверждении Правил централизованного управления сетью связи общего пользования" (Собрание законодательства Российской Федерации, 2020, № 8, ст. 1002);

постановление Правительства Российской Федерации от 17 декабря 2021 г. № 2343 "О внесении изменений в постановление Правительства Российской Федерации от 12 февраля 2020 г. № 127" (Собрание законодательства Российской Федерации, 2021, № 52, ст. 9177);

постановление Правительства Российской Федерации от 15 сентября 2023 г. № 1505 "О внесении изменения в Правила централизованного управления сетью связи общего пользования" (Собрание законодательства Российской Федерации, 2023, № 39, ст. 7023);

пункт 2 изменений, которые вносятся в акты Правительства Российской Федерации, утвержденных постановлением Правительства Российской Федерации от 27 октября 2023 г. № 1790 "О внесении изменений в некоторые акты Правительства Российской Федерации" (Собрание законодательства Российской Федерации, 2023, № 44, ст. 7900).

3. Настоящее постановление вступает в силу с 1 марта 2026 г. и действует до 1 марта 2032 г.

Председатель Правительства
Российской Федерации

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ
51AFAB8781ED9E42DC41EE5D43E303E3
Действителен с 26.06.2025 по 19.09.2026
Владелец: Правительство Российской Федерации

М.Мишустин

УТВЕРЖДЕНЫ
постановлением Правительства
Российской Федерации
от 27 октября 2025 г. № 1667

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" пункта 1 настоящих Правил, 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 (далее - указания) лицам, участвующим в централизованном управлении сетью связи общего пользования (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, а также лица, указанные в статье 10^{2-1} Федерального закона "Об информации, информационных технологиях и о защите информации") (далее - 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 (далее - запрос о предоставлении сведений);

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.

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

3. 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 и к которой относятся следующие виды угроз:

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.

4. Под угрозой безопасности функционирования на территории Российской Федерации сети "Интернет" и сети связи общего пользования понимается угроза, при которой нарушается способность сети связи противостоять попыткам несанкционированного доступа к техническим и программным средствам сети связи общего пользования,

преднамеренным дестабилизирующим внутренним или внешним информационным воздействиям, нарушающим функционирование сети связи общего пользования, а также к воздействиям, связанным с распространением в сети "Интернет" информации, доступ к которой подлежит ограничению в соответствии с законодательством Российской Федерации и к которой относятся следующие виды угроз:

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";

е) угрозы подмены абонентского номера или уникального кода идентификации абонента при осуществлении соединения, поступающего из-за пределов Российской Федерации, по сети передачи данных (сеанс связи) для передачи голосовой информации в целях распространения заведомо ложных сообщений об актах терроризма и иной информации, создающей угрозу причинения вреда жизни и (или) здоровью граждан, имуществу, угрозу массового нарушения общественного порядка и (или) общественной безопасности либо угрозу создания помех функционированию или прекращения функционирования объектов жизнеобеспечения, транспортной или социальной инфраструктуры, кредитных организаций, объектов энергетики, промышленности или связи;

ж) угрозы предоставления доступа к информации или информационным ресурсам в сети "Интернет", посредством которых создается возможность получения услуг связи и (или) их заказа, использования услуг связи в нарушение законодательства Российской Федерации, а также передачи организатором сервиса обмена мгновенными сообщениями электронных сообщений пользователей такого сервиса обмена мгновенными сообщениями без их идентификации;

з) угрозы пропуска трафика технологических сетей связи, имеющие номер автономной системы собственники или иные владельцы которых не соблюдают требования, предусмотренные подпунктом 3 пункта 9 статьи 56^2 Федерального закона "О связи", и (или) сетей связи, в отношении которых оператором связи не реализованы требования, предусмотренные пунктом 2 статьи 64 Федерального закона "О связи";

и) угрозы предоставления доступа к информации или информационным ресурсам в сети "Интернет", посредством которых создается возможность приобретения средств связи, в отношении которых обязательное подтверждение соответствия в нарушение законодательства Российской Федерации не проводилось;

к) угрозы осуществления деятельности по предоставлению вычислительной мощности для размещения информации в информационной системе, постоянно подключенной к сети "Интернет", провайдером хостинга, сведения о котором не включены в реестр провайдеров хостинга;

л) угрозы осуществления деятельности по предоставлению вычислительной мощности для размещения информации в информационной системе, постоянно подключенной к сети "Интернет", провайдерами хостинга, которые не соблюдают требования, предусмотренные частями 2 - 4 статьи 10^{2-1} Федерального закона "Об информации, информационных технологиях и о защите информации".

5. Под угрозой целостности функционирования на территории Российской Федерации сети "Интернет" и сети связи общего пользования понимается угроза, при которой нарушается способность взаимодействия сетей связи, становятся невозможными соединение и передача информации между пользователями взаимодействующих сетей и доступ

пользователей к информационным ресурсам в сети "Интернет" и к которой относятся следующие виды угроз:

а) угрозы нарушения взаимодействия сети связи общего пользования, расположенной на территории 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 (нескольких) иностранного государства;

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 на территории одного (нескольких) иностранного государства;

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 (нескольких) субъекта Российской Федерации;

г) угрозы нарушения взаимодействия технологических сетей связи лиц, имеющих номер автономной системы, расположенных на территории одного (нескольких) субъекта 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 и меры по их устранению, в том числе случаи управления техническими средствами противодействия угрозам и передачи указаний лицам, участвующим в централизованном управлении

6. 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.

7. 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 3 - 5 настоящих Правил.

8. Информация об угрозах, определенных в соответствии с видами угроз, указанными в пунктах 3 - 5 настоящих Правил, 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.

9. Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций при получении информации, указанной в пункте 8 настоящих Правил, а также в случае самостоятельного определения угроз в соответствии с видами угроз, указанными в пунктах 3 - 5 настоящих Правил, вносит в перечень угроз устойчивости, безопасности и целостности функционирования на территории Российской Федерации сети "Интернет" и сети связи общего пользования (далее - перечень угроз) информацию, указанную в пункте 8 настоящих Правил, информацию об угрозах, самостоятельно определенных в соответствии с видами угроз, указанными в пунктах 3 - 5 настоящих Правил, описание угрозы, определенной в соответствии с видами угроз, указанными в пунктах 3 - 5 настоящих Правил, данные об уязвимости средств и технологий связи, количественные и качественные показатели влияния такой угрозы на функционирование сети "Интернет" и сети связи общего пользования.

Вопросы внесения в перечень угроз информации, указанной в пункте 8 настоящих Правил, данных об уязвимости средств и технологий связи, количественных и качественных показателей влияния угроз, определенных в соответствии с видами угроз, указанными в пунктах 3 - 5 настоящих Правил, на функционирование сети "Интернет" и сети связи общего пользования, а также вопросы формирования модели таких угроз и нарушителей могут быть вынесены на заседание экспертной комиссии, в том числе в случае разногласий по представленной информации с указанными в пункте 8 настоящих Правил федеральными органами исполнительной власти. Состав и порядок деятельности экспертной комиссии утверждает 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.

10. Внесение информации, указанной в пунктах 8 и 9 настоящих Правил, в перечень угроз является основанием для осуществления Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций централизованного управления.

11. 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, определенной в соответствии с видами угроз, указанными в пунктах 3 - 5 настоящих Правил, содержащихся в перечне угроз (далее - регламент реагирования), который должен содержать конкретные мероприятия по устранению таких угроз в соответствии с мерами, указанными в пункте 12 настоящих Правил.

12. 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 угроз устойчивости, безопасности и целостности функционирования на территории Российской Федерации сети "Интернет" и сети связи общего пользования и принимаемых мерах противодействия;

ж) мероприятия по предупреждению возникновения угроз устойчивости, безопасности и целостности функционирования на территории Российской Федерации сети "Интернет" и сети связи общего пользования, в том числе в соответствии с разработанными моделями таких угроз.

13. 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 их запросу. Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций направляет ответ на запрос о предоставлении информации, содержащейся в регламенте реагирования (далее - запрос о предоставлении информации), на электронную почту или иным способом в течение 2 рабочих дней со дня получения запроса о предоставлении информации.

14. 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 4 и 5 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 9 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.

15. 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, в том числе порядок и сроки рассмотрения претензий операторов связи к функционированию технических средств противодействия угрозам и запросов о предоставлении сведений

16. Лица, участвующие в централизованном управлении, определяют должностное лицо (должностных лиц), ответственное за организационно-техническое взаимодействие в рамках централизованного управления (далее - лицо, ответственное за взаимодействие). Лица, участвующие в централизованном управлении, направляют посредством размещения в личном кабинете сведения о лице, ответственном за взаимодействие (фамилия, имя, отчество (при наличии), должность, телефон, адрес электронной почты), в Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций.

17. 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 и автоматического взаимодействия систем управления или средств связи лиц, участвующих в централизованном управлении, с информационной системой мониторинга и управления сетью связи общего пользования.

18. При осуществлении централизованного управления указания могут быть переданы лицу, ответственному за взаимодействие, любым способом, позволяющим установить факт получения указания, в том числе посредством телефонной связи и размещения указания в личном кабинете.

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.

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

20. Оператор связи вправе направить в Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций запрос о предоставлении сведений способом, позволяющим подтвердить факт направления запроса о предоставлении сведений, в том числе посредством его размещения в личном кабинете.

Запрос о предоставлении сведений подлежит рассмотрению Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций в течение 5 рабочих дней со дня регистрации запроса о предоставлении сведений.

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

22. 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 о предоставлении сведений не более чем на 20 рабочих дней, а запрос о предоставлении сведений передается на рассмотрение в комиссию. Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций утверждает состав и положение о комиссии.

23. Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций уведомляет оператора связи о продлении срока рассмотрения запроса о предоставлении сведений и передаче запроса о предоставлении сведений в комиссию в течение 2 рабочих дней со дня принятия решения о продлении срока рассмотрения запроса о предоставлении сведений способом, позволяющим подтвердить

факт направления уведомления, в том числе посредством его размещения в личном кабинете.

24. Комиссия рассматривает запрос о предоставлении сведений в срок, не превышающий 15 рабочих дней со дня передачи запроса о предоставлении сведений в комиссию.

25. По результатам рассмотрения запроса о предоставлении сведений комиссия готовит и передает в Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций в течение 3 рабочих дней 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.

26. Мотивированное заключение, указанное в пункте 25 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 получения, в том числе посредством размещения мотивированного заключения в личном кабинете.

27. Оператор 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.

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

29. 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 претензии.

30. 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.

31. 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.

32. Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций направляет решение, принятое в соответствии с пунктом 31 настоящих Правил, оператору связи в течение 2 рабочих дней со дня принятия такого решения способом, позволяющим подтвердить факт направления решения, в том числе посредством его размещения в личном кабинете.

33. В случае принятия решения, указанного в подпункте "а" пункта 31 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 Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций технической возможности исполнения указаний, передаваемых в рамках централизованного управления

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

35. Техническая возможность исполнения указаний в отношении угроз 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 указанной 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

36. 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 техническое средство противодействия угрозам, при условии соблюдения требований к эксплуатации технических средств противодействия угрозам;

б) нарушение функционирования технического средства противодействия угрозам, при котором параметры пропуска трафика через технические средства противодействия угрозам 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 в соответствии с законодательством Российской Федерации не подлежит ограничению, но ограничивается.

37. Оператор связи вправе не направлять трафик через техническое средство противодействия угрозам в случае, предусмотренном подпунктом "а" пункта 36 настоящих Правил, после размещения информации о нем в личном кабинете.

38. Оператор связи вправе не направлять трафик через техническое средство противодействия угрозам в случаях, предусмотренных подпунктами "б" и "в" пункта 36 настоящих Правил, после размещения информации о них в личном кабинете и получения указания.

39. 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.

40. Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций при подтверждении информации о случаях, предусмотренных подпунктами "а" и "б" пункта 36 настоящих Правил, незамедлительно обеспечивает проведение работ по восстановлению функционирования технических средств противодействия угрозам.

41. При неподтверждении информации о случае, предусмотренном подпунктом "а" пункта 36 настоящих Правил, или после восстановления функционирования технических средств противодействия угрозам Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций незамедлительно доводит любым доступным способом, позволяющим подтвердить факт получения указания, в том числе через личный кабинет, до сведения оператора связи указание, содержащее в том числе информацию о направлении трафика через техническое средство противодействия угрозам.

42. Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций при подтверждении информации о случае, предусмотренном подпунктом "в" пункта 36 настоящих Правил, незамедлительно обеспечивает доступ к информации или информационным ресурсам, доступ к которым в соответствии с законодательством Российской Федерации не подлежит ограничению, но ограничивается, и доводит любым доступным способом, позволяющим подтвердить факт получения указания, в том числе через личный кабинет, до сведения оператора связи указание, содержащее в том числе информацию о направлении трафика через техническое средство противодействия угрозам.

____