ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ
(ФСТЭК России)

П Р И К А З

«28» августа 2024 г. Москва № 159

О внесении изменений в Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. № 17, и Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 25 декабря 2017 г. № 239

В соответствии с частью 5 статьи 16 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», пунктом 4 части 3 статьи 6 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», пунктом 2, подпунктом 9.1 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085,
П Р И К А З Ы В А Ю:

Внести в Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. № 17 (зарегистрирован Министерством юстиции Российской Федерации 31 мая 2013 г., регистрационный № 28608) (с изменениями, внесенными приказами Федеральной службы

по техническому и экспортному контролю от 15 февраля 2017 г. № 27 (зарегистрирован Министерством юстиции Российской Федерации 14 марта 2017 г., регистрационный № 45933), от 28 мая 2019 г. № 106 (зарегистрирован Министерством юстиции Российской Федерации 13 сентября 2019 г., регистрационный № 55924), и в Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 25 декабря 2017 г. № 239 (зарегистрирован Министерством юстиции Российской Федерации 26 марта 2018 г., регистрационный № 50524) (с изменениями, внесенными приказами Федеральной службы по техническому и экспортному контролю от 9 августа 2018 г. № 138 (зарегистрирован Министерством юстиции Российской Федерации 5 сентября 2018 г., регистрационный № 52071), от 26 марта 2019 г. № 60 (зарегистрирован Министерством юстиции Российской Федерации 18 апреля 2019 г., регистрационный № 54443), от 20 февраля 2020 г. № 35 (зарегистрирован Министерством юстиции Российской Федерации 11 сентября 2020 г., регистрационный № 59793), изменения согласно приложению к настоящему приказу.

ДИРЕКТОР ФЕДЕРАЛЬНОЙ СЛУЖБЫ
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

В.СЕЛИН

ПРИЛОЖЕНИЕ
к приказу ФСТЭК России
от 28 августа 2024 г. № 159

Изменения, которые вносятся в Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. № 17, и в Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 25 декабря 2017 г. № 239

1. В Требованиях о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. № 17:

1) пункт 20 изложить в следующей редакции:

«20. Посредством исполнения организационных и технических мер защиты информации, определяемых в соответствии с приложением № 2 к настоящим Требованиям и реализуемых в информационной системе в рамках ее системы защиты информации, в зависимости от угроз безопасности информации, используемых информационных технологий и структурно-функциональных характеристик информационной системы осуществляются:

а) идентификация и аутентификация субъектов доступа и объектов доступа;

б) управление доступом субъектов доступа к объектам доступа;

в) ограничение программной среды;

г) защита машинных носителей информации;

д) регистрация событий безопасности;

е) антивирусная защита;

ж) обнаружение (предотвращение) вторжений;

з) контроль (анализ) защищенности информации;

и) целостность информационной системы и информации;

к) доступность информации;

л) защита среды виртуализации;

м) защита технических средств;

н) защита информационной системы, ее средств, систем связи и передачи данных;

о) защита информационной системы от атак, направленных на отказ в обслуживании.»;

2) после пункта 20.13 дополнить пунктом 20.14 следующего содержания:

«20.14. Меры по защите информационной системы от атак, направленных на отказ в обслуживании, должны приниматься в отношении информационной системы, имеющей интерфейсы и сервисы, к которым должен быть обеспечен постоянный доступ из информационно-телекоммуникационной сети «Интернет» (далее — сеть «Интернет»), и должны предусматривать:

а) выявление интерфейсов и сервисов информационной системы, к которым должен быть обеспечен постоянный доступ из сети «Интернет», определение их принадлежности и назначения;

б) выявление публичных сетевых адресов, зарегистрированных за оператором и (или) полученных от провайдера хостинга, и доменных имен, используемых для обеспечения функционирования информационной системы, определение их назначения;

в) выявление и исключение из информационной системы интерфейсов и сервисов информационных систем, к которым обеспечен доступ из сети «Интернет», публичных сетевых адресов и доменных имен, не используемых для обеспечения функционирования информационной системы и (или) принадлежность которых не установлена;

г) формирование перечня ресурсов сети «Интернет», с которыми может взаимодействовать информационная система, включающего исходящий и входящий сетевые потоки, их характеристики и используемые протоколы (далее — матрица коммуникаций информационной системы с сетью «Интернет»);

д) определение сетевых адресов, с которыми должно быть обеспечено взаимодействие информационной системы, формирование списка разрешенных сетевых адресов в условиях реализации атак, направленных на отказ в обслуживании;

е) использование программных, программно-аппаратных средств, обеспечивающих анализ и фильтрацию сетевых запросов в соответствии с матрицей коммуникаций информационной системы с сетью «Интернет» на максимально возможной скорости для этих каналов связи и возможность блокирования сетевых запросов, обладающих признаками атак, направленных на отказ в обслуживании, на сетевом и прикладном уровнях информационной системы;

ж) наличие двукратного резерва пропускной способности каналов передачи данных относительно объемов трафика в условиях отсутствия реализации атак, направленных на отказ в обслуживании;

з) использование данных, полученных при взаимодействии с Центром мониторинга и управления сетью связи общего пользования[1(1)];

и) обеспечение хранения в течение трех лет следующей информации о фактах реализации атак, направленных на отказ в обслуживании: дата и время начала и окончания реализации атаки, тип атаки, объем (Гбит/с, сетевых пакетов/с), перечень сетевых адресов, являющихся источником атак, и сетевых адресов, подверженных атакам, принимаемые меры.»;

3) дополнить сноской 1(1) к пункту 20.14 следующего содержания:

«[1(1)] Пункт 4 Положения о Центре мониторинга и управления сетью связи общего пользования, утвержденного приказом Роскомнадзора от 31 июля 2019 г. № 225 (зарегистрирован Минюстом России 22 ноября 2019 г., регистрационный № 56583), с изменениями, внесенными приказом Роскомнадзора от 24 апреля 2024 г. № 73 (зарегистрирован Минюстом России 6 июня 2024 г., регистрационный № 78486) (далее — Положение о Центре мониторинга).»;

4) дополнить пунктом 25^1 следующего содержания:

«25^1. Организационные меры, направленные на защиту информационной системы от атак, направленных на отказ в обслуживании, должны предусматривать:

а) взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации[1(2)];

б) взаимодействие в автоматизированном режиме с Центром мониторинга и управления сетью связи общего пользования[1(3)] в рамках противодействия атакам, направленным на отказ в обслуживании;

в) взаимодействие с провайдером хостинга или организацией, предоставляющей услуги связи;

г) определение порядка взаимодействия с провайдером хостинга или организацией, предоставляющей услуги связи, по совместному блокированию атак, направленных на отказ в обслуживании, и разграничению зон ответственности при таком блокировании;

д) обеспечение доступности из сети «Интернет» интерфейсов и сервисов информационной системы, подлежащих защите от атак, направленных на отказ в обслуживании, по согласованию со структурным подразделением, специалистами по защите информации после принятия мер по контролю и фильтрации исходящего и входящего сетевого трафика в соответствии с матрицей коммуникаций информационной системы с сетью «Интернет»;

е) возможность размещения информационной системы в информационно-телекоммуникационной инфраструктуре провайдера хостинга, обеспечивающего защиту от атак, направленных на отказ в обслуживании, или осуществление защиты информационных систем путем перенаправления сетевого трафика на программно-аппаратные средства организации, оказывающей услуги

по контролю, фильтрации и блокированию сетевых запросов, обладающих признаками атак, направленных на отказ в обслуживании, при отсутствии технической возможности у оператора самостоятельно организовать защиту информационных систем от атак, направленных на отказ в обслуживании.»;

5) дополнить сносками 1(2) и 1(3) к пункту 25^1 следующего содержания:

«[1(2)] Подпункт «б» пункта 2 Указа Президента Российской Федерации от 22 декабря 2017 г. № 620 «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации».

[1(3)] Пункт 5 Положения о Центре мониторинга.»;

6) дополнить пунктом 25^2 следующего содержания:

«25^2. Программно-аппаратные средства, используемые для осуществления контроля, фильтрации и блокирования сетевых запросов, обладающих признаками атак, направленных на отказ в обслуживании, должны быть расположены на территории Российской Федерации.»;

7) в пункте 26.1 слова «информационно-телекоммуникационной» исключить.

2. В Требованиях по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденных приказом Федеральной службы по техническому и экспортному контролю от 25 декабря 2017 г. № 239:

1) пункт 22 изложить в следующей редакции:

«22. В значимых объектах в зависимости от их категории значимости и угроз безопасности информации посредством исполнения организационных и технических мер, определяемых в соответствии с приложением к настоящим Требованиям, осуществляются:

а) идентификация и аутентификация субъектов доступа и объектов доступа;

б) управление доступом субъектов доступа к объектам доступа;

в) ограничение программной среды;

г) защита машинных носителей информации;

д) аудит безопасности;

е) антивирусная защита;

ж) предотвращение вторжений (компьютерных атак);

з) обеспечение целостности;

и) обеспечение доступности;

к) защита технических средств и систем;

л) защита информационной (автоматизированной) системы и ее компонентов;

м) планирование мероприятий по обеспечению безопасности;

н) управление конфигурацией;

о) управление обновлениями программного обеспечения;

п) реагирование на инциденты информационной безопасности;

р) обеспечение действий в нештатных ситуациях;

с) информирование и обучение персонала;

т) защита значимых объектов от атак, направленных на отказ в обслуживании.».

2) дополнить пунктом 22^1 следующего содержания:

«22^1. При реализации мер по обеспечению безопасности значимых объектов применяются методические документы, разработанные ФСТЭК России в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085.»;

3) дополнить пунктом 22^2 следующего содержания:

«22^2. Меры по обеспечению защиты значимых объектов от атак, направленных на отказ в обслуживании, должны приниматься в отношении значимых объектов, имеющих интерфейсы и сервисы, к которым должен быть обеспечен постоянный доступ из информационно-телекоммуникационной сети «Интернет» (далее — сеть «Интернет»), и должны предусматривать:

а) выявление интерфейсов и сервисов значимых объектов, к которым должен быть обеспечен постоянный доступ из сети «Интернет», определение их принадлежности и назначения;

б) выявление публичных сетевых адресов, зарегистрированных за субъектом критической информационной инфраструктуры и (или) полученных от провайдера хостинга, и доменных имен, используемых для обеспечения функционирования значимых объектов, определение их назначения;

в) выявление и исключение из значимых объектов интерфейсов и сервисов значимых объектов, к которым обеспечен доступ из сети «Интернет», публичных сетевых адресов и доменных имен, не используемых для обеспечения функционирования значимых объектов и (или) принадлежность которых не установлена;

г) формирование перечня ресурсов сети «Интернет», с которыми могут взаимодействовать значимые объекты, включающего исходящий и входящий сетевые потоки, их характеристики и используемые протоколы (далее — матрица коммуникаций значимых объектов с сетью «Интернет»);

д) определение сетевых адресов, с которыми должно быть обеспечено взаимодействие значимых объектов, формирование списка разрешенных сетевых адресов в условиях реализации атак, направленных на отказ в обслуживании;

е) использование программных, программно-аппаратных средств, обеспечивающих анализ и фильтрацию сетевых запросов в соответствии с матрицей коммуникаций значимых объектов с сетью «Интернет» на максимально возможной скорости для этих каналов связи и возможность блокирования сетевых запросов, обладающих признаками атак, направленных на отказ в обслуживании, на сетевом и прикладном уровнях значимых объектов;

ж) наличие двукратного резерва пропускной способности каналов передачи данных относительно объемов трафика в условиях отсутствия реализации атак, направленных на отказ в обслуживании;

з) использование данных, полученных при взаимодействии с Центром мониторинга и управления сетью связи общего пользования[1];

и) обеспечение хранения в течение трех лет следующей информации о фактах реализации атак, направленных на отказ в обслуживании: дата и время начала и окончания реализации атаки, тип атаки, объем (Гбит/с, сетевых пакетов/с), перечень сетевых адресов, являющихся источником атак, и сетевых адресов, подверженных атакам, принимаемые меры.»;

4) дополнить сноской 1 к пункту 22^2 следующего содержания:

«[1] Пункт 4 Положения о Центре мониторинга и управления сетью связи общего пользования, утвержденного приказом Роскомнадзора от 31 июля 2019 г. № 225 (зарегистрирован Минюстом России 22 ноября 2019 г., регистрационный № 56583), с изменениями, внесенными приказом Роскомнадзора от 24 апреля 2024 г. № 73 (зарегистрирован Минюстом России 6 июня 2024 г., регистрационный № 78486) (далее — Положение о Центре мониторинга).»;

5) дополнить пунктом 26^2 следующего содержания:

«26^2. Организационные меры, направленные на защиту значимых объектов от атак, направленных на отказ в обслуживании, должны предусматривать:

а) взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации[2];

б) взаимодействие в автоматизированном режиме с Центром мониторинга и управления сетью связи общего пользования[3] в рамках противодействия атакам, направленным на отказ в обслуживании;

в) взаимодействие с провайдером хостинга или организацией, предоставляющей услуги связи, программно-аппаратные средства которых, участвующие в контроле, фильтрации и блокировании сетевых запросов, обладающих признаками атак, направленных на отказ в обслуживании, должны быть расположены на территории Российской Федерации;

г) определение порядка взаимодействия с провайдером хостинга или организацией, предоставляющей услуги связи, по совместному блокированию

атак, направленных на отказ в обслуживании, и разграничению зон ответственности при таком блокировании;

д) обеспечение доступности из сети «Интернет» интерфейсов и сервисов значимых объектов, подлежащих защите от атак, направленных на отказ в обслуживании, по согласованию со структурным подразделением, специалистами по защите информации после принятия мер по контролю и фильтрации исходящего и входящего сетевого трафика в соответствии с матрицей коммуникаций значимых объектов с сетью «Интернет»;

е) возможность размещения значимых объектов в информационно-телекоммуникационной инфраструктуре провайдера хостинга, обеспечивающего защиту от атак, направленных на отказ в обслуживании, или осуществление защиты значимых объектов путем перенаправления сетевого трафика на программно-аппаратные средства организации, оказывающей услуги по контролю, фильтрации и блокированию сетевых запросов, обладающих признаками атак, направленных на отказ в обслуживании, при отсутствии технической возможности у субъекта критической информационной инфраструктуры самостоятельно организовать защиту значимых объектов от атак, направленных на отказ в обслуживании.»;

6) дополнить сносками 2 и 3 к пункту 26^2 следующего содержания:

«[2] Подпункт «б» пункта 2 Указа Президента Российской Федерации от 22 декабря 2017 г. № 620 «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации».

[3] Пункт 5 Положения о Центре мониторинга.»;

7) дополнить пунктом 26^3 следующего содержания:

«26^3. Программно-аппаратные средства, используемые для осуществления контроля, фильтрации и блокирования сетевых запросов, обладающих признаками атак, направленных на отказ в обслуживании, должны быть расположены на территории Российской Федерации.»;

8) в абзаце первом пункта 29.1 слова «информационно-телекоммуникационной» исключить.