ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ
(ФСТЭК России)

П Р И К А З

«____» июня 2024 г. Москва № ___

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 ___ июня 2024 г. №___

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. Организационные и технические меры защиты информации, реализуемые в информационной системе в рамках ее системы защиты информации, в зависимости от угроз безопасности информации, используемых информационных технологий и структурно-функциональных характеристик информационной системы должны обеспечивать:

а) идентификацию и аутентификацию субъектов доступа и объектов доступа;

б) управление доступом субъектов доступа к объектам доступа;

в) ограничение программной среды;

г) защиту машинных носителей информации;

д) регистрацию событий безопасности;

е) антивирусную защиту;

ж) обнаружение (предотвращение) вторжений;

з) контроль (анализ) защищенности информации;

и) целостность информационной системы и информации;

к) доступность информации;

л) защиту среды виртуализации;

м) защиту технических средств;

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

о) защиту информационной системы от угроз типа «отказ в обслуживании».

Состав мер защиты информации и их базовые наборы для соответствующих классов защищенности информационных систем приведены в приложении № 2 к настоящим Требованиям.»;

2) дополнить подпунктом 20.14 следующего содержания:

«20.14. Меры по защите информационной системы от угроз типа «отказ в обслуживании» принимаются в отношении информационной системы, имеющей интерфейсы и сервисы, которые должны быть постоянно доступны из информационно-телекоммуникационной сети «Интернет» (далее - сеть «Интернет»), и должны предусматривать:

а) выявление интерфейсов и сервисов информационной системы, которые должны быть постоянно доступны 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) исключение интерфейсов и сервисов информационных систем, доступных из сети «Интернет», публичных сетевых адресов и доменных имен, не используемых для обеспечения функционирования информационной системы и (или) принадлежность которых не установлена;

г) формирование матрицы коммуникаций информационной системы с сетью «Интернет», содержащей перечень ресурсов сети «Интернет», с которыми может взаимодействовать информационная система, а также исходящий и входящий сетевые трафики и их характеристики, используемые протоколы;

д) определение сетевых адресов, с которыми должно быть обеспечено взаимодействие информационной системы, формирование списка разрешенных сетевых адресов в условиях реализации угроз типа «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 каналов связи, возможность блокирования сетевых запросов, обладающих признаками угроз типа «отказ в обслуживании», на сетевом и прикладном уровнях информационной системы;

ж) наличие двукратного резерва по пропускной способности каналов передачи данных относительно нормальных объемов трафика в условиях отсутствия реализации угроз типа «отказ в обслуживании»;

з) использование данных информационной системы определения страновой принадлежности сетевых адресов центра мониторинга и управления сетями связи общего пользования (GeoIP);

и) обеспечение хранения в течение трех лет следующей информации о фактах реализации угроз типа «отказ в обслуживании»: дата и время начала и окончания реализации угрозы, тип угрозы, объем (Гбит/с, сетевых пакетов/с), перечень сетевых адресов, являющихся источником угроз, и сетевых адресов, подверженных угрозам, принимаемые меры защиты.»;

3) дополнить подпунктом 25.1 следующего содержания:

«25.1. Организационные меры, направленные на защиту информационной системы от угроз типа «отказ в обслуживании», должны предусматривать:

а) взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, а также национальной системой противодействия DdoS-атакам;

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

в) разработку регламента взаимодействия с провайдером хостинга или организацией, предоставляющей услуги связи, по совместному блокированию угроз типа «отказ в обслуживании» и разграничению зон ответственности при таком блокировании;

г) предоставление доступа из сети «Интернет» к интерфейсам и сервисам информационной системы по согласованию со структурным подразделением, должностным лицом (работником), ответственным за защиту информации обладателя информации (заказчика) и оператора после принятия мер по контролю и фильтрации исходящего и входящего сетевого трафика в соответствии с матрицей коммуникаций;

д) возможность размещения информационной системы в информационно-телекоммуникационной инфраструктуре провайдера хостинга, обеспечивающей защиту от угроз типа «отказ в обслуживании» в соответствии с настоящими Требованиями, при отсутствии технической возможности у оператора самостоятельно организовать защиту информационных систем от угроз типа «отказ в обслуживании».».

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 должны быть реализованы следующие организационные и технические меры:

а) идентификация и аутентификация (ИАФ);

б) управление доступом (УПД);

в) ограничение программной среды (ОПС);

г) защита машинных носителей информации (ЗНИ);

д) аудит безопасности (АУД);

е) антивирусная защита (АВЗ);

ж) предотвращение вторжений (компьютерных атак) (СОВ);

з) обеспечение целостности (ОЦЛ);

и) обеспечение доступности (ОДТ);

к) защита технических средств и систем (ЗТС);

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

м) планирование мероприятий по обеспечению безопасности (ПЛН);

н) управление конфигурацией (УКФ);

о) управление обновлениями программного обеспечения (ОПО);

п) реагирование на инциденты информационной безопасности (ИНЦ);

р) обеспечение действий в нештатных ситуациях (ДНС);

с) информирование и обучение персонала (ИПО);

т) защита значимых объектов от угроз типа «отказ в обслуживании».

Состав мер по обеспечению безопасности значимых объектов в зависимости от категории значимости приведен в приложении к настоящим Требованиям.

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. N 1085.».

2) дополнить подпунктом 22.1 следующего содержания:

«22.1. Меры по обеспечению защиты значимых объектов от угроз типа «отказ в обслуживании» принимаются в отношении значимых объектов, имеющих интерфейсы и сервисы, которые должны быть постоянно доступны из информационно-телекоммуникационной сети «Интернет» (далее - сеть «Интернет») и должны предусматривать:

а) выявление интерфейсов и сервисов значимых объектов, которые должны быть постоянно доступны 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) исключение интерфейсов и сервисов значимых объектов, доступных из сети «Интернет», публичных сетевых адресов и доменных имен, не используемых для обеспечения функционирования значимых объектов и (или) принадлежность которых не установлена;

г) формирование матрицы коммуникаций значимых объектов с сетью «Интернет», содержащей перечень ресурсов сети «Интернет», с которыми могут взаимодействовать значимые объекты, а также исходящий и входящий сетевые потоки и их характеристики, используемые протоколы;

д) определение сетевых адресов, с которыми должно быть обеспечено взаимодействие значимых объектов, формирование списка разрешенных сетевых адресов в условиях реализации угроз типа «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 каналов связи, возможность блокирования сетевых запросов, обладающих признаками угроз типа «отказ в обслуживании», на сетевом и прикладном уровнях значимых объектов;

ж) наличие двукратного резерва по пропускной способности каналов передачи данных относительно нормальных объемов трафика в условиях отсутствия реализации угроз типа «отказ в обслуживании»;

з) использование данных информационной системы определения страновой принадлежности сетевых адресов центра мониторинга и управления сетями связи общего пользования (GeoIP);

и) обеспечение хранения в течение трех лет следующей информации о фактах реализации угроз типа «отказ в обслуживании»: дата и время начала и окончания реализации угрозы, тип угрозы, объем (Гбит/с, сетевых пакетов/с), перечень сетевых адресов, являющихся источником угроз, и сетевых адресов, подверженных угрозам, принимаемые меры защиты.»;

3) дополнить подпунктом 26.2 следующего содержания:

«26.2. Организационные меры, направленные на защиту значимых объектов от угроз типа «отказ в обслуживании», должны предусматривать:

а) взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, а также национальной системой

противодействия DdoS-атакам;

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

в) разработку регламента взаимодействия с провайдером хостинга или организацией, предоставляющей услуги связи, по совместному блокированию угроз типа «отказ в обслуживании» и разграничению зон ответственности при таком блокировании;

г) предоставление доступа из сети «Интернет» к интерфейсам и сервисам значимых объектов по согласованию со структурным подразделением субъекта критической информационной инфраструктуры или специалистами, ответственными за обеспечение безопасности значимых объектов, после принятия мер по контролю и фильтрации исходящего и входящего сетевого трафика в соответствии с матрицей коммуникаций;

д) возможность размещения значимых объектов в информационно-телекоммуникационной инфраструктуре провайдера хостинга, обеспечивающей защиту от угроз типа «отказ в обслуживании» в соответствии с настоящими Требованиями, при отсутствии технической возможности у субъекта критической информационной инфраструктуры самостоятельно организовать защиту значимых объектов от угроз типа «отказ в обслуживании».».