Федеральный закон от 7 апреля 2025 г. № 58-ФЗ "О внесении изменений в Федеральный закон "О безопасности критической информационной инфраструктуры Российской Федерации"

Принят
Государственной Думой
25 марта 2025 года

Одобрен
Советом Федерации
2 апреля 2025 года

Статья 1

Внести в Федеральный закон от 26 июля 2017 года N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации" (Собрание законодательства Российской Федерации, 2017, N 31, ст. 4736; 2023, N 29, ст. 5330) следующие изменения:

1) в пункте 8 статьи 2 слова "и (или) индивидуальные предприниматели" исключить;

2) в статье 5:

а) в части 1 слова "В целях настоящей статьи" заменить словами "Для целей настоящего Федерального закона";

б) пункт 3 части 2 после слов "критической информационной инфраструктуры," дополнить словами "а также иных органов и организаций,";

в) часть 3 после слов "субъектам критической информационной инфраструктуры" дополнить словами "и иным не являющимся субъектами критической информационной инфраструктуры органам и организациям";

г) часть 6 после слов "обмен информацией о компьютерных" дополнить словами "атаках и компьютерных";

3) в статье 6:

а) часть 2 дополнить пунктами 4 - 8 следующего содержания:

"4) перечни типовых отраслевых объектов критической информационной инфраструктуры;

5) отраслевые особенности категорирования объектов критической информационной инфраструктуры (по согласованию с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, в банковской сфере и иных сферах финансового рынка - также по согласованию с Центральным банком Российской Федерации), определяющие порядок установления соответствия объекта критической информационной инфраструктуры критериям значимости и показателям их значений в целях присвоения ему одной из категорий значимости и включающие в себя отраслевые признаки значимости объектов критической информационной инфраструктуры, соответствующие критериям значимости и показателям их значений, а также порядок расчета значений показателей критериев значимости с учетом особенностей функционирования объекта критической информационной инфраструктуры;

6) требования к используемым на значимых объектах критической информационной инфраструктуры программно-аппаратным средствам (в банковской сфере и иных сферах финансового рынка - по согласованию с Центральным банком Российской Федерации);

7) порядок и сроки перехода субъектов критической информационной инфраструктуры на использование на значимых объектах критической информационной инфраструктуры программ для электронных вычислительных машин и баз данных (далее - программное обеспечение), указанных в подпункте "а" пункта 5 части 3 статьи 9 настоящего Федерального закона, и программно-аппаратных средств, соответствующих требованиям, указанным в пункте 6 настоящей части;

8) порядок осуществления мониторинга за исполнением субъектами критической информационной инфраструктуры обязанности по использованию на значимых объектах критической информационной инфраструктуры программного обеспечения, указанного в пункте 5 части 3 статьи 9 настоящего Федерального закона, и программно-аппаратных средств, соответствующих требованиям, указанным в пункте 6 настоящей части.";

б) в части 4:

пункт 3 после слов "критической информационной инфраструктуры" дополнить словами "и иных органов и организаций";

пункт 6 изложить в следующей редакции:

"6) утверждает порядок информирования федерального органа исполнительной власти, уполномоченного в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, о компьютерных атаках и компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры и иных информационных ресурсов Российской Федерации, принадлежащих органам и организациям, на которые возложены обязанности, предусмотренные частью 4 статьи 9 настоящего Федерального закона (в банковской сфере и в иных сферах финансового рынка утверждает указанный порядок по согласованию с Центральным банком Российской Федерации);";

пункт 7 после слов "информацией о компьютерных" дополнить словами "атаках и компьютерных";

пункт 8 изложить в следующей редакции:

"8) организует установку на значимых объектах критической информационной инфраструктуры, в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры, и в иных информационных ресурсах Российской Федерации, принадлежащих органам и организациям, на которые возложены обязанности, предусмотренные частью 4 статьи 9 настоящего Федерального закона, средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, в том числе средств, предназначенных для поиска признаков компьютерных атак;";

пункт 9 дополнить словами ", в том числе к средствам, предназначенным для поиска признаков компьютерных атак";

пункт 10 после слов "компьютерные инциденты," дополнить словами "в том числе средств, предназначенных для поиска признаков компьютерных атак,";

4) в статье 7:

а) в части 4 слова "а также" исключить, после слова "категорирования" дополнить словами ", перечнями типовых отраслевых объектов критической информационной инфраструктуры и отраслевыми особенностями категорирования объектов критической информационной инфраструктуры";

б) часть 6 изложить в следующей редакции:

"6. Федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, в тридцатидневный срок со дня получения сведений, указанных в части 5 настоящей статьи, проверяет соблюдение порядка осуществления категорирования с учетом перечней типовых отраслевых объектов критической информационной инфраструктуры, отраслевых особенностей категорирования объектов критической информационной инфраструктуры и правильность присвоения объекту критической информационной инфраструктуры одной из категорий значимости.";

в) часть 7 после слова "категорирования" дополнить словами "с учетом перечней типовых отраслевых объектов критической информационной инфраструктуры, отраслевых особенностей категорирования объектов критической информационной инфраструктуры";

г) часть 8 изложить в следующей редакции:

"8. В случае, если федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, выявлены нарушения порядка осуществления категорирования с учетом перечней типовых отраслевых объектов критической информационной инфраструктуры, отраслевых особенностей категорирования объектов критической информационной инфраструктуры, федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, возвращает представленные сведения субъекту критической информационной инфраструктуры в письменном виде с мотивированным обоснованием причин их возврата.";

д) часть 11 дополнить словами "с указанием срока выполнения данного требования";

е) пункт 2 части 12 после слов "и показателям их значений," дополнить словами "отраслевым особенностям категорирования объектов критической информационной инфраструктуры,";

ж) дополнить частями 13 и 14 следующего содержания:

"13. В перечни типовых отраслевых объектов критической информационной инфраструктуры включаются только типы информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, обладающие признаком значимости.

14. Перечни типовых отраслевых объектов критической информационной инфраструктуры подлежат пересмотру и дополнению на основании предложений федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, или федерального органа исполнительной власти, уполномоченного в области обеспечения функционирования государственной системы обнаружения, предупреждения и

ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.";

5) пункт 1 части 1 статьи 8 изложить в следующей редакции:

"1) сведения о значимом объекте критической информационной инфраструктуры (наименование, доменное имя и сетевой адрес);";

6) в статье 9:

а) наименование дополнить словами ", а также иных органов и организаций в сфере обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации";

б) в части 2:

пункт 1 после слов "о компьютерных" дополнить словами "атаках и компьютерных";

пункт 3 после слов "компьютерные инциденты," дополнить словами "в том числе средств, предназначенных для поиска признаков компьютерных атак,";

в) часть 3 дополнить пунктами 5 - 7 следующего содержания:

"5) использовать на значимых объектах критической информационной инфраструктуры программное обеспечение:

а) сведения о котором включены в единый реестр российских программ для электронных вычислительных машин и баз данных, предусмотренный статьей 12.1 Федерального закона от 27 июля 2006 года N 149-ФЗ "Об информации, информационных технологиях и о защите информации";

б) которое используется в соответствующих требованиям о защите информации, установленным частью 5 статьи 16 Федерального закона от 27 июля 2006 года N 149-ФЗ "Об информации, информационных технологиях и о защите информации", государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений;

6) соблюдать указанные в пункте 6 части 2 статьи 6 настоящего Федерального закона требования к используемым на значимых объектах критической информационной инфраструктуры программно-аппаратным средствам;

7) осуществлять непрерывное взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы

Российской Федерации в порядке, установленном федеральным органом исполнительной власти, уполномоченным в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.";

г) дополнить частями 4 - 6 следующего содержания:

"4. Обязанности, предусмотренные частью 2 и пунктом 7 части 3 настоящей статьи, распространяются также на руководителей государственных органов (за исключением органов федеральной службы безопасности, органов внешней разведки Российской Федерации, органов государственной охраны, федерального органа обеспечения мобилизационной подготовки органов государственной власти Российской Федерации, федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации), государственных унитарных предприятий, государственных учреждений, государственных фондов, государственных корпораций (компаний), иных российских юридических лиц, которые, если иное не предусмотрено международным договором Российской Федерации, находятся под контролем Российской Федерации, и (или) субъекта Российской Федерации, и (или) контролируемых ими совместно или по отдельности лиц, в части информационных ресурсов Российской Федерации, принадлежащих таким органам и юридическим лицам на праве собственности, аренды или ином законном основании. При этом под контролем понимается возможность определять решения, принимаемые юридическим лицом, в силу наличия права прямо или косвенно распоряжаться более чем пятьюдесятью процентами общего количества голосов, приходящихся на голосующие акции (доли), составляющие уставный капитал данного юридического лица.

5. Порядок и технические условия установки и эксплуатации в указанных в части 4 настоящей статьи информационных ресурсах средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, в том числе средств, предназначенных для поиска признаков компьютерных атак, устанавливаются федеральным органом исполнительной власти, уполномоченным в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

6. Порядок информирования руководителями, указанными в части 4 настоящей статьи, федерального органа исполнительной власти, уполномоченного в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, о компьютерных атаках и компьютерных инцидентах, связанных с функционированием информационных ресурсов, устанавливается указанным федеральным органом исполнительной власти.";

7) часть 1 статьи 13 после слов "правовыми актами" дополнить словами ", в том числе правильности отнесения субъектами критической информационной инфраструктуры принадлежащих им на праве собственности, аренды или ином законном основании объектов критической информационной инфраструктуры к значимым объектам критической информационной инфраструктуры".

Статья 2

1. Настоящий Федеральный закон вступает в силу с 1 сентября 2025 года.

2. До установления перечней типовых отраслевых объектов критической информационной инфраструктуры, отраслевых особенностей категорирования объектов критической информационной инфраструктуры, предусмотренных пунктами 4 и 5 части 2 статьи 6 Федерального закона от 26 июля 2017 года N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации", категорирование объектов критической информационной инфраструктуры осуществляется в соответствии с порядком осуществления категорирования, установленным Правительством Российской Федерации.

3. Исполнение обязанностей, установленных пунктами 5 и 6 части 3 статьи 9 Федерального закона от 26 июля 2017 года N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации", осуществляется с учетом положений пункта 7 части 2 статьи 6 Федерального закона от 26 июля 2017 года N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации".

4. Правительство Российской Федерации вправе установить на период до 2030 года особенности применения пунктов 5 и 6 части 3 статьи 9 Федерального закона от 26 июля 2017 года N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации" на территориях субъектов Российской Федерации, названных в Указе Президента Российской Федерации от 19 октября 2022 года N 757 "О мерах, осуществляемых в субъектах Российской Федерации в связи с Указом Президента Российской Федерации от 19 октября 2022 г. N 756".

Президент
Российской Федерации
В.Путин
Москва, Кремль
7 апреля 2025 года
№ 58-ФЗ