ГОСУДАРСТВЕННАЯ ДУМА
ФЕДЕРАЛЬНОГО СОБРАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
СЕДЬМОГО СОЗЫВА

ПОСТАНОВЛЕНИЕ
ГОСУДАРСТВЕННОЙ ДУМЫ

О проекте федерального закона № 1048574-7 «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях в части установления административной ответственности за нарушение законодательства в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации»

Государственная Дума Федерального Собрания Российской Федерации **п о с т а н о в л я е т:**

1. Принять в первом чтении проект федерального закона № 1048574-7 «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях в части установления административной ответственности за нарушение законодательства в области обеспечения безопасности критической информационной

инфраструктуры Российской Федерации», внесенный Правительством Российской Федерации.

2. Направить указанный законопроект Президенту Российской Федерации, в Совет Федерации Федерального Собрания Российской Федерации, комитеты и комиссии Государственной Думы, во фракции в Государственной Думе, в Правительство Российской Федерации, законодательные (представительные) органы государственной власти субъектов Российской Федерации, Верховный Суд Российской Федерации.

Установить, что поправки к указанному законопроекту направляются в Комитет Государственной Думы по государственному строительству и законодательству в тридцатидневный срок со дня принятия настоящего Постановления.

3. Комитету Государственной Думы по государственному строительству и законодательству доработать указанный законопроект с учетом поступивших поправок и внести его на рассмотрение Государственной Думы во втором чтении.

4. Настоящее Постановление вступает в силу со дня его принятия.

Председатель Государственной Думы
Федерального Собрания
Российской Федерации В.В.Володин

Москва
27 января 2021 года
№ 9721-7 ГД

Вносится Правительством
Российской Федерации

№1048574-7 Проект

ФЕДЕРАЛЬНЫЙ ЗАКОН

О внесении изменений в Кодекс Российской Федерации об административных правонарушениях в части установления административной ответственности за нарушение законодательства в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации

Статья 1

Внести в Кодекс Российской Федерации об административных правонарушениях (Собрание законодательства Российской Федерации, 2002, № 1, ст. 1; № 44, ст. 4295; 2003, № 27, ст. 2700, 2708, 2717; № 46, ст. 4434; № 50, ст. 4847, 4855; 2004, № 31, ст. 3229; № 34, ст. 3529, 3533; № 44, ст. 4266; 2005, № 1, ст. 9, 13, 40; № 10, ст. 762, 763; № 13, ст. 1077; № 19, ст. 1752; № 27, ст. 2719, 2721; № 30, ст. 3104, 3131; № 52, ст. 5574, 5596; 2006, № 1, ст. 4, 10; № 2, ст. 172; № 6, ст. 636; № 10, ст. 1067; № 12, ст. 1234; № 17, ст. 1776; № 18, ст. 1907; № 19, ст. 2066; № 23, ст. 2380; № 28, ст. 2975; № 31, ст. 3420, 3438, 3452; № 45, ст. 4633, 4634, 4641; № 50, ст. 5279, 5281; № 52, ст. 5498; 2007, № 1, ст. 21, 29; № 16, ст. 1825;

№ 26, ст. 3089; № 30, ст. 3755; № 31, ст. 4007; № 41, ст. 4845; № 43, ст. 5084; № 50, ст. 6246; 2008, № 18, ст. 1941; № 20, ст. 2259; № 29, ст. 3418; № 30, ст. 3601, 3604; № 49, ст. 5748; № 52, ст. 6235, 6236; 2009, № 1, ст. 17; №7, ст. 777; № 23, ст. 2759; № 26, ст. 3120, 3122; № 29, ст. 3597, 3635, 3642; № 30, ст. 3735, 3739; № 52, ст. 6412; 2010, № 1, ст. 1; № 19, ст. 2291; № 21, ст. 2525; № 23, ст. 2790; № 30, ст. 4006, 4007; № 31, ст. 4155, 4164, 4193, 4195, 4207, 4208; № 49, ст. 6409; № 52, ст. 6995; 2011, № 1, ст. 10, 23, 47, 54; № 7, ст. 901; № 17, ст. 2310; № 19, ст. 2714; № 23, ст. 3260; № 27, ст. 3873; № 29, ст. 4298; № 30, ст. 4573, 4585, 4590, 4598, 4600, 4605; № 46, ст. 6406; № 47, ст. 6602; № 48, ст. 6732; № 50, ст. 7342, 7345, 7351, 7352, 7355, 7362, 7366; 2012, № 10, ст. 1166; № 19, ст. 2278, 2281; № 24, ст. 3068, 3082; № 31, ст. 4320, 4330; № 47, ст. 6402, 6403, 6404, 6405; № 49, ст. 6757; № 53, ст. 7577, 7602, 7639, 7640; 2013, № 14, ст. 1651, 1666; № 19, ст. 2318, 2323; № 26, ст. 3207, 3208, 3209; № 27, ст. 3442, 3454, 3465, 3469, 3477; № 30, ст. 4025, 4029, 4030, 4031, 4032, 4034, 4036, 4040, 4044, 4059, 4078, 4082; № 31, ст. 4191; № 43, ст. 5443, 5444, 5452; № 44, ст. 5624, 5643; № 48, ст. 6161, 6163, 6165; № 49, ст. 6327, 6341, 6343; № 51, ст. 6683, 6685, 6695, 6696; № 52, ст. 6961, 6980, 6986, 6994, 7002; 2014, № 6, ст. 557, 559, 566; № 11, ст. 1092, 1096; № 14, ст. 1553, 1562; № 19, ст. 2302, 2306, 2310, 2317, 2324, 2325, 2326, 2327,

2330, 2335; № 26, ст. 3366, 3377, 3379; № 30, ст. 4211, 4214, 4218, 4220, 4228, 4233, 4248, 4256, 4259, 4264, 4278; № 42, ст. 5615; № 43, ст. 5799; № 48, ст. 6636, 6638, 6642, 6643, 6651, 6653; № 52, ст. 7541, 7548; 2015, № 1, ст. 35, 67, 74, 83, 85; № 10, ст. 1405, 1416; № 13, ст. 1811; № 18, ст. 2614, 2620, 2623; № 21, ст. 2981; № 24, ст. 3370; № 27, ст. 3950; № 29, ст. 4354, 4359, 4374, 4391; № 41, ст. 5637; № 44, ст. 6046; № 45, ст. 6208; № 48, ст. 6706, 6710, 6716; № 51, ст. 7249, 7250; 2016, № 1, ст. 11, 28, 59, 63, 84; № 10, ст. 1323; № 11, ст. 1481, 1490, 1493; № 15, ст. 2066; № 26, ст. 3871, 3877, 3884, 3887, 3891; № 27, ст. 4160, 4164, 4183, 4197, 4205, 4206, 4223, 4238, 4251, 4259, 4286, 4287, 4305; № 28, ст. 4558; № 50, ст. 6975; 2017, № 1, ст. 12, 31, 47; № 7, ст. 1030, 1032; № 9, ст. 1278; № 11, ст. 1535; № 17, ст. 2456, 2457; № 18, ст. 2664; № 22, ст. 3069; № 23, ст. 3227; № 27, ст. 3947; № 30, ст. 4455; № 31, ст. 4738, 4755, 4812, 4814, 4815, 4816, 4827, 4828; № 47, ст. 6844, 6851; № 49, ст. 7308; № 50, ст. 7562; № 52, ст. 7919, 7925, 7937; 2018, № 1, ст. 21, 30, 35, 48; № 7, ст. 973; № 11, ст. 1577; № 18, ст. 2562; № 31, ст. 4824, 4825, 4826, 4828, 4851; № 41, ст. 6187; № 42, ст. 6378; № 45, ст. 6832, 6843; № 47, ст. 7125, 7128; № 53, ст. 8436, 8447; 2019, № 6, ст. 465; № 10, ст. 893; № 12, ст. 1216, 1217, 1218, 1219; № 16, ст. 1819, 1821; № 22, ст. 2669; № 25, ст. 3161; № 29, ст. 3847; № 30, ст. 4119, 4122, 4125, 4131; № 42, ст. 5803;

№ 44, ст. 6178, 6182; № 49, ст. 6964; № 51, ст. 7493, 7494, 7495; № 52, ст. 7766, 7811, 7819; 2020, № 14, ст. 2002, 2019, 2020, 2029; № 17, ст. 2710) следующие изменения:

1) часть 1 статьи 4.5 после слов "частью 2 статьи 12.30 настоящего Кодекса)," дополнить словами "законодательства в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации (в части административных правонарушений, предусмотренных статьями 13.12^{1} и 19.7^{15} настоящего Кодекса),";

2) дополнить статьей 13.12^{1} следующего содержания:

"Статья 13.12^{1}. **Нарушение требований в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации**

1. Нарушение требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования либо требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, установленных федеральными законами и принятыми в соответствии с ними иными нормативными правовыми актами Российской Федерации, если такие действия (бездействие) не содержат уголовно наказуемого деяния, -

влечет наложение административного штрафа на должностных лиц в размере от десяти тысяч до пятидесяти тысяч рублей; на юридических лиц - от пятидесяти тысяч до ста тысяч рублей.

2. Нарушение порядка информирования о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации, установленного федеральными законами и принятыми в соответствии с ними иными нормативными правовыми актами Российской Федерации, -

влечет наложение административного штрафа на должностных лиц в размере от десяти тысяч до пятидесяти тысяч рублей; на юридических лиц - от ста тысяч до пятисот тысяч рублей.

3. Нарушение порядка обмена информацией о компьютерных инцидентах между субъектами критической информационной инфраструктуры Российской Федерации, между субъектами критической информационной инфраструктуры Российской Федерации и уполномоченными органами иностранных государств, международными организациями, международными неправительственными и

иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты, -

влечет наложение административного штрафа на должностных лиц в размере от двадцати тысяч до пятидесяти тысяч рублей; на юридических лиц - от ста тысяч до пятисот тысяч рублей.";

3) абзац первый статьи 19.7 после цифр "19.7[14]," дополнить цифрами "19.7[15],";

4) дополнить статьей 19.7[15] следующего содержания:

"Статья 19.7[15]. **Непредставление сведений, предусмотренных законодательством в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации**

1. Непредставление или нарушение сроков представления в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, сведений о результатах присвоения объекту критической информационной инфраструктуры Российской Федерации одной из категорий значимости, предусмотренных законодательством в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, либо об отсутствии необходимости присвоения ему одной из таких категорий -

влечет наложение административного штрафа на должностных лиц в размере от десяти тысяч до пятидесяти тысяч рублей; на юридических лиц - от пятидесяти тысяч до ста тысяч рублей.

2. Непредставление или нарушение порядка либо сроков представления в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации информации, предусмотренной законодательством в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, за исключением случаев, предусмотренных частью 2 статьи 13.12^{1} настоящего Кодекса, -

влечет наложение административного штрафа на должностных лиц в размере от десяти тысяч до пятидесяти тысяч рублей; на юридических лиц - от ста тысяч до пятисот тысяч рублей.";

5) в части 2 статьи 23.1 слова "статьей 13.13" заменить словами "статьями 13.12^{1}, 13.13", слова "статьей 19.7^{11}" заменить словами "статьями 19.7^{11}, 19.7^{15}";

6) пункт 5 части 2 статьи 23.45 после слов "его заместители," дополнить словами "начальники структурных подразделений указанного федерального органа исполнительной власти,", после слов "их

заместители" дополнить словами ", начальники структурных подразделений территориальных органов указанного федерального органа исполнительной власти";

7) пункт 2 части 2 статьи 23.46 после слов "его заместители," дополнить словами "начальники структурных подразделений указанного федерального органа исполнительной власти,", после слов "их заместители" дополнить словами ", начальники структурных подразделений территориальных органов указанного федерального органа исполнительной власти";

8) главу 23 дополнить статьями 23.90 и 23.91 следующего содержания:

"Статья 23.90. **Федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации**

1. Федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, рассматривает дела об административных правонарушениях, предусмотренных частью 1 статьи 13.12^{1}, частью 1 статьи 19.7^{15} настоящего Кодекса.

2. Рассматривать дела об административных правонарушениях от имени органа, указанного в части 1 настоящей статьи, вправе

руководитель федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, его заместители, начальники структурных подразделений указанного федерального органа исполнительной власти, руководители территориальных органов указанного федерального органа исполнительной власти, их заместители, начальники структурных подразделений территориальных органов указанного федерального органа исполнительной власти.

Статья 23.91. **Федеральный орган исполнительной власти, уполномоченный в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации**

1. Федеральный орган исполнительной власти, уполномоченный в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, рассматривает дела об административных правонарушениях, предусмотренных частями 2 и 3 статьи 13.12^{1}, частью 2 статьи 19.7^{15} настоящего Кодекса.

2. Рассматривать дела об административных правонарушениях от имени органа, указанного в части 1 настоящей статьи, вправе

руководитель федерального органа исполнительной власти, уполномоченного в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, его заместители, начальники структурных подразделений указанного федерального органа исполнительной власти, их заместители, руководители территориальных органов указанного федерального органа исполнительной власти, их заместители, начальники структурных подразделений территориальных органов указанного федерального органа исполнительной власти.";

9) часть 2 статьи 28.3 дополнить пунктом 114 следующего содержания:

"114) должностные лица федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, его территориальных органов - об административных правонарушениях, предусмотренных частью 1 статьи 19.4, частью 1 статьи 19.5, статьей 19.6 настоящего Кодекса.".

Статья 2

1. Настоящий Федеральный закон вступает в силу по истечении десяти дней после дня его официального опубликования, за исключением положений, для которых настоящей статьей предусмотрены иные сроки вступления их в силу.

2. Абзацы третий и четвертый пункта 2 статьи 1 настоящего Федерального закона вступают в силу с 1 сентября 2021 года.

Президент
Российской Федерации

В.С Анотаилов

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

к проекту федерального закона "О внесении изменений в Кодекс Российской Федерации об административных правонарушениях в части установления административной ответственности за нарушение законодательства в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации"

Проектом федерального закона "О внесении изменений в Кодекс Российской Федерации об административных правонарушениях в части установления административной ответственности за нарушение законодательства в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации" (далее - законопроект) предусматривается дополнение Кодекса Российской Федерации об административных правонарушениях (далее - Кодекс) статьями 13.12^{1} и 19.7^{15}, устанавливающими административную ответственность за нарушение требований в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации (далее - критическая информационная инфраструктура) и за неисполнение обязанности по представлению сведений, предусмотренных законодательством в области обеспечения безопасности критической информационной инфраструктуры.

Законопроект направлен на правовое регулирование обеспечения безопасности объектов критической информационной инфраструктуры, нарушение функционирования которых может привести к выходу из строя объектов обеспечения жизнедеятельности населения, транспортной инфраструктуры, сетей связи, прекращению или нарушению оказания государственных услуг, нанесению ущерба жизни и здоровью людей, возникновению ущерба субъектам критической информационной инфраструктуры и бюджетам Российской Федерации.

В настоящее время статьей 274^{1} Уголовного кодекса Российской Федерации предусмотрена уголовная ответственность за неправомерное воздействие на критическую информационную инфраструктуру, в том числе за нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре, или информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, сетей электросвязи, относящихся к критической информационной инфраструктуре, либо правил доступа к указанным информации,

информационным системам, информационно-телекоммуникационным сетям, автоматизированным системам управления, сетям электросвязи, если оно повлекло причинение вреда критической информационной инфраструктуре.

В соответствии с Федеральным законом от 26 июля 2017 г. № 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации" (далее - Федеральный закон № 187-ФЗ) субъекты критической информационной инфраструктуры, являющиеся правообладателями значимых объектов критической информационной инфраструктуры, обязаны соблюдать требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры.

Требования в области обеспечения безопасности значимых объектов критической информационной инфраструктуры установлены Федеральным законом № 187-ФЗ и принятыми в соответствии с ним нормативными правовыми актами (Правилами категорирования объектов критической информационной инфраструктуры Российской Федерации, утвержденными постановлением Правительства Российской Федерации от 8 февраля 2018 г. № 127, Требованиями к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования, утвержденными приказом ФСТЭК России от 21 декабря 2017 г. № 235, Требованиями по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденными приказом ФСТЭК России от 25 декабря 2017 г. № 239, Порядком информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденным приказом ФСБ России от 19 июня 2019 г. № 282, Порядком представления информации в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, утвержденными приказом ФСБ России от 24 июля 2018 г. № 367 и Порядком обмена информацией о компьютерных инцидентах между субъектами критической информационной инфраструктуры Российской Федерации, между субъектами критической информационной инфраструктуры Российской Федерации и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования

на компьютерные инциденты, утвержденным приказом ФСБ России от 24 июля 2018 г. № 368).

Ответственность за несоблюдение указанных требований, создающее предпосылки к нанесению ущерба критической информационной инфраструктуре в случае совершения компьютерной атаки, но не повлекшее причинение вреда критической информационной инфраструктуре, не установлена.

Вместе с тем невыполнение требований законодательства о безопасности критической информационной инфраструктуры может привести к нарушению штатного функционирования значимых объектов критической информационной инфраструктуры, создавая реальную угрозу жизни и здоровью граждан, приводить к дестабилизации финансовой системы страны, создавать предпосылки для нарушения безопасности государства.

Так, в 2017 году была осуществлена масштабная компьютерная атака с использованием вируса-шифровальщика WannaCry, в том числе на отдельные субъекты критической информационной инфраструктуры. Анализ последствий указанной атаки на примере 3 государственных компаний, в состав информационной инфраструктуры каждой из которых на момент атаки входило около 50 000 средств вычислительной техники, показал, что заражению в этих организациях подверглись около 33% автоматизированных рабочих мест и 50% серверов, восстановление работоспособности которых заняло от 1 до 3 суток. Около 25% работников указанных организаций в течение этого времени не могли в полной мере исполнять свои должностные обязанности.

Причиной заражения средств вычислительной техники являлась нереализация мер по обеспечению информационной безопасности, предусмотренных законодательством Российской Федерации о безопасности критической информационной инфраструктуры, в частности, невыполнение требований по своевременному обновлению программного обеспечения, отсутствие регламентов и правил работы с электронной почтой, невыполнение минимальных требований по защите периметра информационных и автоматизированных систем.

Для разработки и реализации мер, направленных на ликвидацию последствий компьютерной атаки, каждой из указанных государственных компаний была привлечена внешняя организация, имеющая соответствующие компетенции. Стоимость затрат на услуги этой организации для каждой государственной компании составила от 3 до 5 миллионов рублей в зависимости от масштаба последствий компьютерной атаки и применяемого

компаниями программного обеспечения. В эту сумму не включена стоимость услуг по восстановлению инфраструктурного, прикладного программного обеспечения и информации, содержавшихся на средствах вычислительной техники.

Кроме того, согласно информации, представленной в обзоре несанкционированных переводов денежных средств за 2018 год, подготовленном Центром мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере, в результате воздействия вредоносного кода на объекты информационной инфраструктуры одного субъекта критической информационной инфраструктуры - оператора по переводу денежных средств злоумышленникам удалось осуществить несанкционированные операции по переводу денежных средств с корреспондентских счетов на общую сумму 79,9 млн. рублей.

Размеры предлагаемых штрафов учитывают размер средней заработной платы руководителей структурных подразделений по обеспечению информационной безопасности в Российской Федерации, который составляет 80 - 100 тыс. рублей (по результатам анализа вакансий, представленных на сайте www.hh.ru), и стоимость возможных затрат субъектов критической информационной инфраструктуры на устранение последствий компьютерных атак.

В настоящее время в соответствии с Федеральным законом № 187-ФЗ более чем 5 000 субъектов критической информационной инфраструктуры определили свыше 50 тыс. принадлежащих им объектов критической информационной инфраструктуры, подлежащих категорированию. Вместе с тем на сегодняшний день более чем по 1 700 объектам не соблюдены сроки представления сведений о результатах их категорирования, установленные в пункте 17 Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, утвержденных постановлением Правительства Российской Федерации от 8 февраля 2018 г. № 127.

По результатам анализа поступивших сведений о более чем 8 500 объектах, для которых определена категория значимости, сделан вывод о том, что более чем у 60% из 860 субъектов, владеющих значимыми объектами критической информационной инфраструктуры, системы обеспечения безопасности значимых объектов не соответствуют требованиям к созданию систем безопасности значимых объектов критической информационной инфраструктуры и обеспечению их функционирования (приказ ФСТЭК России от 21 декабря 2017 г. № 235) и требованиям по обеспечению безопасности

значимых объектов критической информационной инфраструктуры Российской Федерации (приказ ФСТЭК России от 25 декабря 2017 г. № 239).

В 2019 году Национальным координационным центром по компьютерным инцидентам выявлено 120 компьютерных инцидентов. При этом в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации о компьютерных инцидентах не поступило ни одного сообщения.

Таким образом, в настоящее время законодательство Российской Федерации о безопасности критической информационной инфраструктуры выполняется не в полной мере, что создает угрозу безопасности критической информационной инфраструктуры.

Кроме этого, законопроектом предусматривается установить специальный срок давности привлечения к административной ответственности по проектируемым статьям 13.12^{1} и 19.7^{15} - один год.

Необходимость установления такого срока связана с тем, что в соответствии с пунктом 2 части 3 статьи 13 Федерального закона № 187-ФЗ возникновение компьютерного инцидента, повлекшего негативные последствия, на значимом объекте критической информационной инфраструктуры является основанием для проведения внеплановой проверки в целях осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры.

Факт невыполнения требований, установленных законодательством в области обеспечения безопасности критической информационной инфраструктуры, на момент возникновения соответствующего компьютерного инцидента в соответствии с Правилами осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденных постановлением Правительства Российской Федерации от 17 февраля 2018 г. № 162, может быть установлен только в ходе выездной проверки. При этом срок проведения проверки в отношении субъекта критической информационной инфраструктуры, который осуществляет свою деятельность на территориях нескольких субъектов Российской Федерации, устанавливается отдельно по каждому филиалу, представительству и обособленному структурному подразделению субъекта критической информационной инфраструктуры и может составлять 60 рабочих дней.

Истечение сроков давности привлечения к административной ответственности является обстоятельством, исключающим производство по делу об административном правонарушении (пункт 6 части 1 статьи 24.5 Кодекса).

Полномочиями по рассмотрению дел об административных правонарушениях, предусмотренных проектируемыми частью 1 статьи 13.12^{1} и частью 1 статьи 19.7^{15} Кодекса, предлагается наделить федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры (ФСТЭК России).

Полномочиями по рассмотрению дел об административных правонарушениях, предусмотренных проектируемыми частями 2 и 3 статьи 13.12^{1} и частью 2 статьи 19.7^{15} Кодекса, предлагается наделить федеральный орган исполнительной власти, уполномоченный в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ФСБ России).

Одновременно вносятся изменения в пункт 5 части 2 статьи 23.45 и в пункт 2 части 2 статьи 23.46 Кодекса, предусматривающие возможность рассмотрения дел об административных правонарушениях, предусмотренных статьями 13.12 (нарушение правил защиты информации) и 13.13 (незаконная деятельность в области защиты информации) Кодекса, начальниками структурных подразделений ФСТЭК России и начальниками структурных подразделений территориальных органов ФСТЭК России.

Указанные изменения направлены на оптимизацию расходов, необходимых для осуществления комплексных выездных проверок, проводимых ФСТЭК России в соответствии с поручениями Президента Российской Федерации или Правительства Российской Федерации, в рамках которых наряду с вопросами обеспечения безопасности критической информационной инфраструктуры осуществляется проверка состояния технической защиты информации ограниченного доступа.

Учитывая, что территориальные органы ФСТЭК России являются территориальными органами межрегионального уровня и расположены в столицах федеральных округов, а также значительную удаленность и распределенность проверяемых субъектов по территории федерального округа, наделение начальников структурных подразделений соответствующими полномочиями будет способствовать оперативному рассмотрению дел об административных правонарушениях и сокращению расходов бюджетных средств на проведение проверочных мероприятий.

Кроме того, в целях нивелирования возможных негативных последствий предлагаемого регулирования для бюджетов бюджетной системы Российской Федерации, а также планомерного и поступательного исполнения установленных требований субъектами предпринимательской деятельности без избыточной финансовой нагрузки законопроектом предусмотрен переходный период в отношении трудозатратных мероприятий, ответственность за которые устанавливается проектируемой частью 1 статьи 13.12^1 Кодекса.

Учитывая, что производство по делам об административных правонарушениях, предусмотренных Законопроектом, будет осуществляться должностными лицами ФСТЭК России и ФСБ России в рамках реализации их полномочий в области обеспечения безопасности критической информационной инфраструктуры и в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, а также наличие у этих лиц механизмов и опыта производства по делам об административных правонарушениях, предусмотренных статьями 13.12 (нарушение правил защиты информации) и 13.13 (незаконная деятельность в области защиты информации) Кодекса, дополнительная нагрузка на них будет отсутствовать.

Реализация Законопроекта не повлечет за собой дополнительных затрат, необходимых для осуществления производства по делам о предусмотренных им административных правонарушениях.

ФИНАНСОВО-ЭКОНОМИЧЕСКОЕ ОБОСНОВАНИЕ

к проекту федерального закона "О внесении изменений в Кодекс Российской Федерации об административных правонарушениях в части установления административной ответственности за нарушение законодательства в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации"

Принятие и реализация проекта федерального закона "О внесении изменений в Кодекс Российской Федерации об административных правонарушениях в части установления административной ответственности за нарушение законодательства в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации" не потребует расходов, покрываемых за счет федерального бюджета.

20062081.doc

ПЕРЕЧЕНЬ

федеральных законов, подлежащих принятию, изменению, приостановлению или признанию утратившими силу в связи с проектом федерального закона "О внесении изменений в Кодекс Российской Федерации об административных правонарушениях в части установления административной ответственности за нарушение законодательства в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации"

В связи с проектом федерального закона "О внесении изменений в Кодекс Российской Федерации об административных правонарушениях в части установления административной ответственности за нарушение законодательства в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации" не потребует признания утратившими силу, приостановления, изменения или принятия федеральных законов.

20062084.doc

ПЕРЕЧЕНЬ

нормативных правовых актов Президента Российской Федерации, Правительства Российской Федерации и федеральных органов исполнительной власти, подлежащих признанию утратившими силу, приостановлению, изменению или принятию в связи с проектом федерального закона "О внесении изменений в Кодекс Российской Федерации об административных правонарушениях в части установления административной ответственности за нарушение законодательства в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации"

В связи с проектом федерального закона "О внесении изменений в Кодекс Российской Федерации об административных правонарушениях в части установления административной ответственности за нарушение законодательства в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации" не потребуется признания утратившими силу, приостановления, изменения или принятия актов Президента Российской Федерации, Правительства Российской Федерации и федеральных органов исполнительной власти.