О мерах по реализации Федерального закона от 26 июля 2017 г. №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»

С 1 января 2018 г. вступил в силу Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

В соответствии с п. 8 статьи 2 Федерального закона к субъектам критической информационной инфраструктуры Российской Федерации (далее – КИИ) относятся государственные органы, государственные учреждения, российские юридические лица, индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы (далее – ИС), информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в 12 сферах деятельности:

- здравоохранение;
- наука;
- транспорт;
- связь;
- банковская сфера и иные сферы финансового рынка;
- энергетика и топливно-энергетический комплекс;
- атомная энергия;
- оборонная промышленность;
- ракетно-космическая промышленность;
- горнодобывающая промышленность;
- металлургическая промышленность;
- химическая промышленность.

Указом Президента Российской Федерации от 25 ноября 2017 г. № 569 ФСТЭК России определена федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности КИИ.

Перечень Федеральных законов, нормативных правовых актов Президента Российской Федерации, Правительства Российской Федерации и ФСТЭК России, изданных в связи с вступлением в силу Федерального закона от 26 июля 2017 г. № 187-ФЗ, приведен в Приложении 1.

В соответствии с требованиями указанных нормативных правовых актов на первом этапе проведения работ по обеспечению безопасности КИИ необходимо сформировать перечень объектов КИИ, подлежащих последующему категорированию. При этом предлагаем использовать рекомендации, приведенные в Приложении 2.

Приложение 1

Перечень нормативных правовых актов в области безопасности критической информационной инфраструктуры Российской Федерации
(по состоянию на 01.06.2018 г.)

1. Федеральные законы

- Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;

- Федеральный закон от 26 июля 2017 года № 193-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации»;

- Федеральный закон от 26.07.2017 № 194-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации»

2. Указа Президента Российской Федерации

- Указ Президента РФ от 15 января 2013 г. № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» (Выписка);

- Указ Президента РФ №К 1274 от 12.12.2014 «О Концепции государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» (выписка);

- Указ Президента РФ от 25.11.2017 № 569 «О внесении изменений в Положение о Федеральной службе по техническому и экспортному контролю, утвержденное Указом Президента Российской Федерации от 16 августа 2004 г. № 1085»;

- Указ Президента РФ от 22.12.2017 № 620 «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»;

- Указ Президента Российской Федерации от 02.03.2018 № 98 «О внесении изменения в перечень сведений, отнесенных к государственной тайне, утвержденный Указом Президента Российской Федерации от 30.11.1995 № 1203».

3. Постановления Правительства Российской Федерации

- Постановление Правительства РФ от 08.02.2018 № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений»

- Постановление Правительства РФ от 17.02.2018 № 162 «Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»

4. Приказы ФСТЭК России

- Приказ ФСТЭК России от 06.12.2017 № 227 «Об утверждении Порядка ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации»

- Приказ ФСТЭК России от 11.12.2017 № 229 «Об утверждении формы акта проверки, составляемого по итогам проведения государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»

- Приказ ФСТЭК от 21.12.2017 № 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования»

- Приказ ФСТЭК России от 21.12.2017 № 236 «Об утверждении формы направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий»;

- Приказ ФСТЭК России от 25.12.2017 №239 "Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации"

- Приказ ФСТЭК РФ от 14 марта 2014 г. N 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды»

Приложение 2

Рекомендации по формированию перечня объектов критической информационной инфраструктуры

1. Руководитель субъекта критической информационной инфраструктуры своим решением создает комиссию, на которую возлагается задача формирования перечня объектов КИИ. Состав комиссии определяется в соответствии с пунктами 11-13 Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, утвержденных постановлением Правительства Российской Федерации от 8 февраля 2018 г. № 127.

2. Составление перечня управленческих, технологических, производственных, финансово-экономических и (или) иных процессов в рамках выполнения функций (полномочий) или осуществления видов деятельности субъекта критической информационной инфраструктуры.

3. Из состава процессов, включенных в перечень, выявление процессов, нарушение и (или) прекращение которых может привести к негативным социальным, политическим, экономическим, экологическим последствиям, последствиям для обороны страны, безопасности государства и правопорядка. Таким образом, получаем перечень критических процессов.

4. Для каждого процесса определяются объекты, которые обрабатывают информацию, необходимую для обеспечения критических процессов и (или) осуществляют управление, необходимую для обеспечения критических процессов;

5. Определенные объекты включаются в перечень объектов критической информационной инфраструктуры, подлежащих категорированию.

Рекомендуемая форма перечня приведена в Таблице.

Таблица 1

№ п/п	Наименование объекта КИИ	Сфера деятельности	Адреса размещения объекта КИИ	Ориентированный срок категорирования объекта КИИ

Примечание: в случае, если объект КИИ являются распределенным, в третьей колонке указываются адреса подразделений (обособленных подразделений, филиалов, представительств) субъекта КИИ, в которых размещаются сегменты объекта КИИ (серверы, рабочие места, технологическое, производственное оборудование (исполнительные устройства).

6. Перечень объектов критической информационной инфраструктуры утверждается руководителем субъекта критической информационной инфраструктуры. Перечень согласовывается с вышестоящим органом власти или организации (при наличии).

7. Перечень объектов критической информационной инфраструктуры в течении 5 рабочих дней после утверждения направляется в Управление ФСТЭК России по Центральному федеральному округу. Перечень необходимо представить на бумажном носителе (допускается приложение электронной копии на электронном носителе) с сопроводительным письмом, подписанным руководителем субъекта критической информационной инфраструктуры Российской Федерации.

Приложение 3

Ответственность на нарушение законодательства по безопасности КИИ
(по состоянию на 01.06.2018 г.)

Уголовный кодекс Российской Федерации

Статья 274.1. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации

1. Создание, распространение и (или) использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации, в том числе для уничтожения, блокирования, модификации, копирования информации, содержащейся в ней, или нейтрализации средств защиты указанной информации, -

наказываются принудительными работами на срок до пяти лет с ограничением свободы на срок до двух лет или без такового либо лишением свободы на срок от двух до пяти лет со штрафом в размере от пятисот тысяч до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период от одного года до трех лет.

2. Неправомерный доступ к охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации, в том числе с использованием компьютерных программ либо иной компьютерной информации, которые заведомо предназначены для неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации, или иных вредоносных компьютерных программ, если он повлек причинение вреда критической информационной инфраструктуре Российской Федерации, -

наказывается принудительными работами на срок до пяти лет со штрафом в размере от пятисот тысяч до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период от одного года до трех лет и с ограничением свободы на срок до двух лет или без такового либо лишением свободы на срок от двух до шести лет со штрафом в размере от пятисот тысяч до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период от одного года до трех лет.

3. Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации, или информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, сетей электросвязи, относящихся к критической информационной инфраструктуре Российской Федерации, либо правил доступа к указанным информации, информационным системам,

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

наказывается принудительными работами на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового либо лишением свободы на срок до шести лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

4. Деяния, предусмотренные частью первой, второй или третьей настоящей статьи, совершенные группой лиц по предварительному сговору или организованной группой, или лицом с использованием своего служебного положения, -

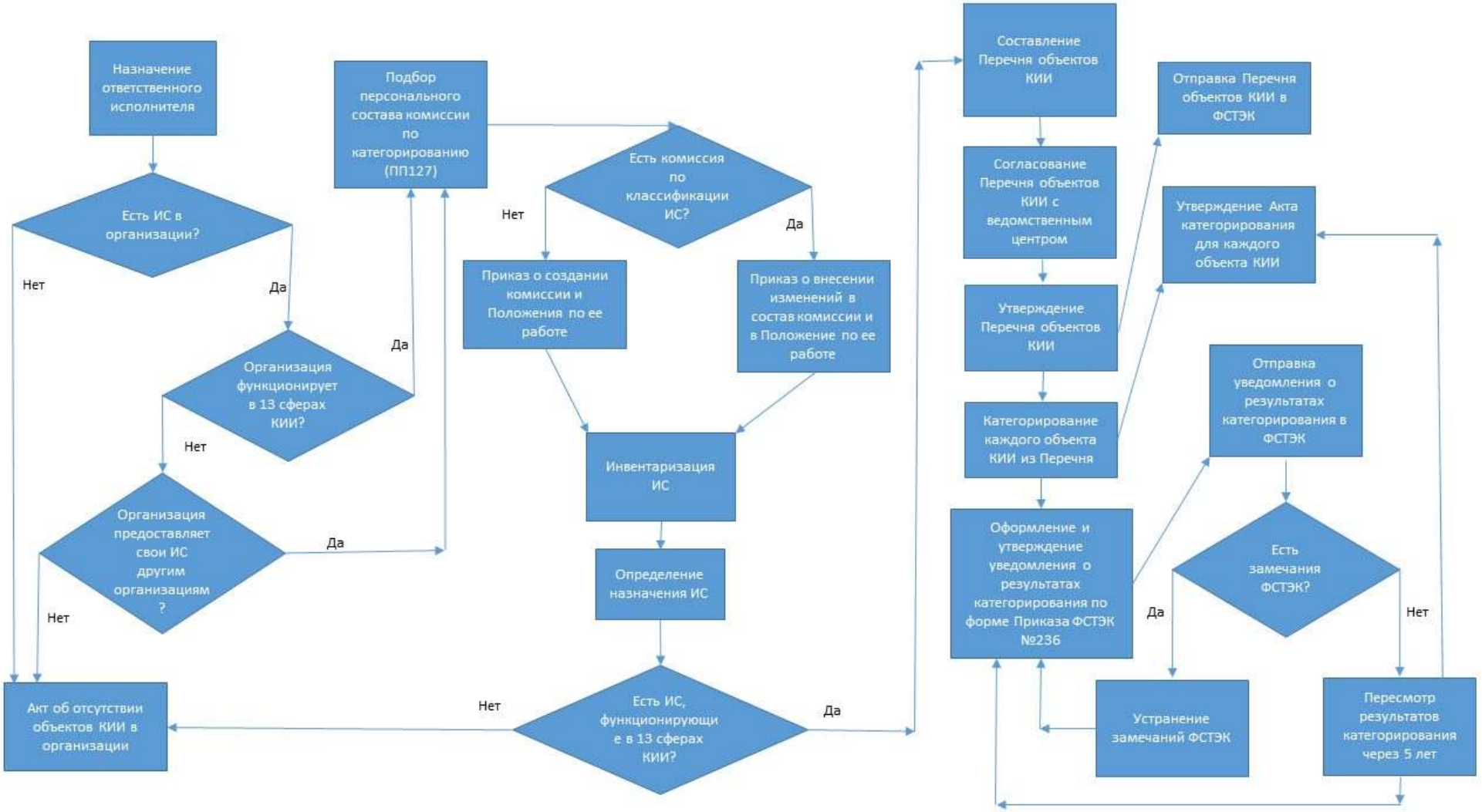
наказываются лишением свободы на срок от трех до восьми лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

5. Деяния, предусмотренные частью первой, второй, третьей или четвертой настоящей статьи, если они повлекли тяжкие последствия, -

наказываются лишением свободы на срок от пяти до десяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет или без такового.

Приложение 4.

Алгоритм организации выполнения требований 187-ФЗ



Пояснения к алгоритму

1. Сведения о том, является ли организация субъектом КИИ, можно получить в следующих источниках:

- уставы, положения организаций (госорганов);
- общероссийский классификатор видов экономической деятельности (ОКВЭД);
- лицензии и иные разрешительные документы на различные виды деятельности;
- другие источники (например ОКОГУ).

2. Наличие ИС в организации определяется через бухгалтерию и приказы о вводе в эксплуатацию. Возможно через распоряжения вышестоящих организаций для подведомственных учреждений о передаче ИС. Не забывайте о сайтах организации в интернет, они то же ИС, если зарегистрированы на организацию.

3. Назначение ИС определять через приказы на создание и ввод в эксплуатацию, проектную документацию, анализ обрабатываемой в ИС информации.

4. Перечень объектов КИИ направляется для согласования в ФСТЭК России в течение пяти дней со дня утверждения руководителем организации.

5. Акт категорирования оформляется на каждую ИС, включенную в перечень, и утверждается руководителем организации.

6. Сведения о результатах категорирования направляются в ФСТЭК России в течение 10 дней со дня утверждения Акта категорирования руководителем организации.