

Об утверждении Порядка ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации

Приказ Федеральной службы по техническому и экспортному контролю · № 227 · от 06.12.2017 · Действует с изменениями

ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

ПРИКАЗ

МОСКВА

6 декабря 2017 г. № 227

Об утверждении Порядка ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации

Зарегистрирован Минюстом России 8 февраля 2018 г.

Регистрационный № 49966

В соответствии с пунктом 2 части 3 статьи 6 Федерального закона от 26 июля 2017 г. № 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации" (Собрание законодательства Российской Федерации, 2017, № 31, ст. 4736) ПРИКАЗЫВАЮ:

Утвердить прилагаемый Порядок ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации.

ДИРЕКТОР ФЕДЕРАЛЬНОЙ СЛУЖБЫ
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ
КОНТРОЛЮ В.СЕЛИН

УТВЕРЖДЕН
приказом ФСТЭК России
от 6 декабря 2017 г. № 227

Порядок

ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации

1. Настоящий Порядок определяет правила формирования и ведения Реестра значимых объектов критической информационной инфраструктуры Российской Федерации (далее - Реестр) с целью учета значимых объектов критической информационной инфраструктуры Российской Федерации (далее - критическая информационная инфраструктура) в ходе межотраслевой координации деятельности по обеспечению значимых объектов критической информационной инфраструктуры, осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры, а также проведения иных мероприятий в области обеспечения безопасности критической информационной инфраструктуры в соответствии с Федеральным законом от 26 июля 2017 г. № 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации" (далее - Федеральный закон "О безопасности критической информационной инфраструктуры Российской Федерации").

2. Ведение Реестра осуществляется в целях учета, хранения и предоставления информации в бумажном и электронном виде о значимых объектах критической информационной инфраструктуры, принадлежащих на праве собственности, аренды или ином законном основании субъектам критической информационной инфраструктуры*.

* Пункт 8 статьи 2 Федерального закона от 26 июля 2017 г. № 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации"

3. Реестр формируется и ведется Федеральной службой по техническому и экспортному контролю на основе сведений, представляемых субъектами критической информационной инфраструктуры в соответствии с частью 5 статьи 7 Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации" (далее - сведения об объектах критической информационной инфраструктуры).

Субъекты критической информационной инфраструктуры должны обеспечивать достоверность и актуальность представляемых сведений об объектах критической информационной инфраструктуры.

4. Решение о включении сведений о значимом объекте критической информационной инфраструктуры в Реестр принимается в течение 30 дней со дня получения ФСТЭК России сведений от субъекта критической информационной инфраструктуры.

5. В соответствии с частью 1 статьи 8 Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации" в Реестр вносятся следующие сведения о значимом объекте критической информационной инфраструктуры:

- а) наименование значимого объекта критической информационной инфраструктуры;
- б) наименование субъекта критической информационной инфраструктуры;
- в) сведения о взаимодействии значимого объекта критической информационной инфраструктуры и сетей электросвязи;
- г) сведения о лице, эксплуатирующем значимый объект критической информационной инфраструктуры;
- д) категория значимости, которая присвоена объекту критической информационной инфраструктуры субъектом критической информационной инфраструктуры;
- е) сведения о программных и программно-аппаратных средствах, используемых на значимом объекте критической информационной инфраструктуры;
- ж) меры, применяемые для обеспечения безопасности значимого объекта критической информационной инфраструктуры.

6. Каждому значимому объекту критической информационной инфраструктуры, включенному в Реестр, присваивается регистрационный номер, состоящий из групп цифр и прописных букв, разделенных косыми чертами, который имеет вид: XXXXXX/X/XX/X.

Первая группа знаков содержит число от 000001 до 999999, указывающее на порядковый номер значимого объекта критической информационной инфраструктуры в Реестре.

Вторая группа знаков содержит число, обозначающее федеральный округ, на территории которого находится значимый объект критической информационной инфраструктуры:

- 1 - Центральный федеральный округ;
- 2 - Северо-Западный федеральный округ;
- 3 - Южный федеральный округ;
- 4 - Северо-Кавказский федеральный округ;
- 5 - Приволжский федеральный округ;
- 6 - Уральский федеральный округ;
- 7 - Сибирский федеральный округ;
- 8 - Дальневосточный федеральный округ.

Третья группа знаков содержит двузначное число, обозначающее сферу (область) деятельности, в которой функционирует значимый объект критической информационной инфраструктуры, определенную в соответствии с пунктом 8 статьи 2 Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации":

- 1 - здравоохранение;
- 2 - наука;
- 3 - транспорт;
- 4 - связь;
- 5 - банковская сфера и иные сферы финансового рынка;
- 6 - энергетика;
- 7 - атомная энергия;
- 8 - оборонная промышленность;
- 9 - ракетно-космическая промышленность;
- 10 - горнодобывающая промышленность;
- 11 - металлургическая промышленность;
- 12 - химическая промышленность;
- 13 - топливно-энергетический комплекс (за исключением энергетики).

Четвертая группа знаков содержит прописную букву, которая обозначает тип значимого объекта критической информационной инфраструктуры:

"А" - информационная система;

"Б" - автоматизированная система управления технологическими (производственными) процессами;

"В" - информационно-телекоммуникационная сеть.

В случае если значимый объект критической информационной инфраструктуры функционирует в нескольких сферах (областях) деятельности или расположен на территории нескольких федеральных округов, второй и третьей группам цифр присваивается обозначение сферы (области) деятельности или территории, указанные субъектом критической информационной инфраструктуры первыми. Обозначение других сфер (областей) деятельности, в которых функционирует значимый объект критической информационной инфраструктуры, или территорий федеральных округов, на которых он располагается, вносится в графу Реестра, содержащую дополнительные сведения о значимом объекте критической информационной инфраструктуры.

(Пункт в редакции Приказа Федеральной службы по техническому и экспортному контролю от 10.02.2022 № 26)

7. Записи о значимых объектах критической информационной инфраструктуры в Реестре ведутся последовательно в соответствии с датой включения в него сведений о значимом объекте критической информационной инфраструктуры.

8. В случае изменения сведений, указанных в подпунктах "а" - "е" пункта 17 Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, утвержденных постановлением Правительства Российской Федерации от 8 февраля 2018 г. № 127 (Собрание законодательства Российской Федерации, 2018, № 8, ст. 1204; 2019, № 16, ст. 1955), субъекты критической информационной инфраструктуры должны направить измененные сведения в ФСТЭК России не позднее 20 рабочих дней со дня их изменения на бумажном и электронном носителях. Изменения в Реестр вносятся только на основе сведений, представляемых субъектами критической информационной инфраструктуры.

9. В случае внесения изменений в сведения о значимом объекте критической информационной инфраструктуры, регистрационный номер значимого объекта критической информационной инфраструктуры, включенного в Реестр, не изменяется.

10. В случае изменения значимого объекта критической информационной инфраструктуры, в результате которого такой объект перестал соответствовать критериям значимости и показателям их значений, и ему не может быть присвоена ни одна из категорий значимости, субъект критической информационной инфраструктуры должен направить об этом сведения в ФСТЭК России.

На основании сведений, представленных субъектом критической информационной инфраструктуры, объект критической информационной инфраструктуры исключается из Реестра.

11. В случае исключения значимого объекта критической информационной инфраструктуры из Реестра, ранее присвоенный такому объекту регистрационный номер в дальнейшем не используется.

12. Сведения из Реестра не реже, чем один раз в месяц направляются в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации в соответствии со статьей 5 Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации".

Сведения из Реестра могут предоставляться государственным органам или российским юридическим лицам, выполняющим функции по разработке, проведению или реализации государственной политики и (или) нормативно-правовому регулированию в установленной сфере, указанным в части 2 статьи 11 Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации" ежеквартально, либо по их запросам только в части субъектов критической информационной инфраструктуры, выполняющих функции (полномочия) или осуществляющих деятельность в областях (сферах), отнесенных в компетенции этих государственных органов или российских юридических лиц.

13. В ходе формирования и ведения Реестра ФСТЭК России должны быть обеспечены: безопасность информации ограниченного доступа, содержащейся в Реестре, в соответствии с законодательством Российской Федерации о государственной тайне; поддержание содержащихся в Реестре сведений о значимых объектах критической информационной инфраструктуры в актуальном состоянии в соответствии с представленными субъектами критической информационной инфраструктуры сведениями; использование содержащихся в Реестре сведений о значимых объектах критической информационной инфраструктуры только в рамках предоставленных ФСТЭК России полномочий в области обеспечения безопасности критической информационной инфраструктуры; полнота и актуальность сведений о значимых объектах критической информационной инфраструктуры, предоставляемых в соответствии с пунктом 12 настоящего Порядка; информирование субъектов критической информационной инфраструктуры о внесении в Реестр сведений о значимых объектах критической информационной инфраструктуры в сроки, установленные частью 7 статьи 7 Федерального закона "О безопасности критической информационной инфраструктуры", с указанием дат внесения сведений в Реестр и присвоенных регистрационных номеров.

14. В целях сохранности сведений о значимых объектах критической информационной инфраструктуры, включенных в Реестр, ФСТЭК России обеспечивается резервирование Реестра. Резервная копия Реестра формируется не реже одного раза в месяц путем записи на учетные съемные машинные носители информации. Срок хранения машинных носителей информации составляет не менее 5 лет.