ПРОЕКТ

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ
(ФСТЭК России)

П Р И К А З

«____» _____ 2017 г. Москва № _____

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

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) **П Р И К А З Ы В А Ю:**

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

2. Настоящий приказ вступает в силу с 1 января 2018 г.

ДИРЕКТОР ФЕДЕРАЛЬНОЙ СЛУЖБЫ
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

В.СЕЛИН

УТВЕРЖДЕН
приказом ФСТЭК России
от «___» _____ 2017 г. №___

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 26июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (Собрание законодательства Российской Федерации, 2017, № 31, ст. 4736).

2. Реестр представляет собой единую систему учета, хранения и представления информации в бумажном или электронном виде о значимых объектах критической информационной инфраструктуры, принадлежащих на праве собственности, аренды или ином законном основании субъектами критической информационной инфраструктуры.

3. Реестр формируется и ведется Федеральной службой по техническому и экспортному контролю (ФСТЭК России) на основе сведений, предоставляемых 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 обеспечивают достоверность и актуальность предоставляемых сведений об объектах критической информационной инфраструктуры.

4. В ходе формирования и ведения Реестра осуществляются:

оценка полноты и достаточности сведений об объектах критической информационной инфраструктуры в соответствии с Порядком и сроками категорирования объектов критической информационной инфраструктуры Российской Федерации, утвержденными постановлением Правительства Российской Федерации от ___ декабря 2017 г. № ___ (Собрание

законодательства Российской Федерации, 2017, № __, ст. ___) (далее – порядок категорирования);

проверка соблюдения субъектами критической информационной инфраструктуры порядка категорирования;

проверка правильности присвоения объектам критической информационной инфраструктуры одной из категорий значимости либо неприсвоения им ни одной из таких категорий.

5. В Реестр вносятся сведения о значимом объекте критической информационной инфраструктуры в случае, если соблюден порядок категорирования и объекту критической информационной инфраструктуры правильно присвоена одна из категорий значимости.

6. 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.

7. 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;

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.

8. Каждому значимому объекту критической информационной инфраструктуры, включенному в Реестр, присваивается регистрационный номер, состоящий из групп цифр и прописных букв, разделенных косой чертой, который имеет вид: XXXXXX/XX/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 двузначное число, обозначающее федеральный округ, на территории которого находится субъект критической информационной инфраструктуры или лицо, эксплуатирующее значимый объект критической информационной инфраструктуры:

01 – Центральный федеральный округ;

02 – Северо-Западный федеральный округ;

03 – Южный федеральный округ;

04 – Северо-Кавказский федеральный округ;
05 – Приволжский федеральный округ;
06 – Уральский федеральный округ;
07 – Сибирский федеральный округ;
08 – Дальневосточный федеральный округ.

Третья группа знаков содержит двузначное число, обозначающее сферу (область) деятельности, в которой функционирует значимый объект критической информационной инфраструктуры:

01 - здравоохранение;
02 - наука;
03 - транспорт;
04 - связь;
05 - банковская сфера и иные сферы финансового рынка;
06 - энергетика и топливно-энергетический комплекс;
07 - атомная энергия;
08 - оборонная промышленность;
09 - ракетно-космическая промышленность;
10 - горнодобывающая промышленность;
11 - металлургическая промышленность;
12 - химическая промышленность.

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.

9. Записи о значимых объектах критической информационной инфраструктуры в Реестре ведутся в хронологическом порядке.

10. В случае изменений сведений о значимых объектах критической информационной инфраструктуры, включенных в Реестр, субъекты критической информационной инфраструктуры направляют измененные сведения в ФСТЭК России.

Изменения в Реестр вносятся только на основе сведений, представляемых субъектами критической информационной инфраструктуры.

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

12. Исключение значимых объектов критической информационной инфраструктуры из Реестра осуществляется в случае утраты ими категорий значимости на основании сведений, предоставляемых субъектами критической информационной инфраструктуры, которым на праве собственности, аренды или ином законном основании принадлежат эти объекты критической информационной инфраструктуры.

13. В случае утраты значимым объектом критической информационной инфраструктуры категории значимости и исключения их из Реестра, ранее присвоенный такому объекту регистрационный номер в дальнейшем не используется.

14. 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.

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, по их запросам только в части значимых объектов критической информационной инфраструктуры, функционирующих в сферах, отнесенных в компетенции этих государственных органов или российских юридических лиц.

15. В ходе формирования и ведения Реестра ФСТЭК России обеспечиваются:

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;

достоверность и актуальность сведений о значимых объектах критической информационной инфраструктуры, предоставляемых в соответствии с пунктом 14 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.

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