Приложение
к приказу ФСБ России
от
№

Порядок
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

1. Субъекты критической информационной инфраструктуры Российской Федерации (далее – КИИ) информируют ФСБ России обо всех компьютерных инцидентах, связанных с функционированием принадлежащих им на праве собственности, аренды или ином законном основании объектов КИИ.

2. Информирование осуществляется путем направления субъектом КИИ информации в Национальный координационный центр по компьютерным инцидентам (далее – НКЦКИ) в соответствии с определенными НКЦКИ форматами представления информации о компьютерных инцидентах в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации с использованием технической инфраструктуры НКЦКИ, предназначенной для отправки, получения, обработки и хранения уведомлений и запросов в рамках информационного взаимодействия с субъектами КИИ, а также с иными не являющимися субъектами КИИ органами и организациями, в том числе иностранными и международными.

В случае отсутствия подключения к данной технической инфраструктуре информация направляется посредством факсимильной,

электронной и телефонной связи на адреса (телефонные номера) НКЦКИ, указанные на сайте в информационно-телекоммуникационной сети «Интернет» по адресу: «http://cert.gov.ru».

3. Информация о компьютерном инциденте направляется субъектом КИИ в НКЦКИ незамедлительно.

4. В случае, если компьютерный инцидент связан с функционированием объекта КИИ, принадлежащего на праве собственности, аренды или ином законном основании субъекту КИИ, который осуществляет деятельность в банковской сфере и в иных сферах финансового рынка, одновременно с информированием ФСБ России о таком компьютерном инциденте также информируется Центральный банк Российской Федерации.

5. Субъект КИИ осуществляет реагирование на компьютерные инциденты, связанные с функционированием принадлежащих ему на праве собственности, аренды или ином законном основании значимых объектов КИИ, и принимает меры по ликвидации последствий проведенных в отношении этих объектов компьютерных атак силами подразделений и должностных лиц, которые принимают участие в обнаружении, предупреждении и ликвидации последствий компьютерных атак и в реагировании на компьютерные инциденты (далее – силы субъекта КИИ), а в случаях, предусмотренных регламентом взаимодействия при реагировании на компьютерные инциденты и принятии мер по ликвидации последствий компьютерных атак (далее – Регламент) – с привлечением подразделений и должностных лиц ФСБ России.

6. В целях подготовки к реагированию на компьютерные инциденты и принятию мер по ликвидации последствий компьютерных атак субъектом КИИ, которому на праве собственности, аренды или ином законном основании принадлежат значимые объекты КИИ, разрабатывается план

реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак (далее – План), включающий:

технические характеристики и состав значимых объектов КИИ;

события (условия), при наступлении которых осуществляется ввод в действие Плана;

мероприятия, проводимые в ходе реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак, а также время, отводимое на их реализацию;

силы субъекта КИИ, ответственные за проведение мероприятий по реагированию на компьютерные инциденты и принятие мер по ликвидации последствий компьютерных атак.

7. Субъект КИИ, которому на праве собственности, аренды или ином законном основании принадлежат значимые объекты КИИ, не реже одного раза в год организует и проводит тренировки по отработке мероприятий Плана. По результатам тренировок в План вносятся необходимые коррективы.

8. Для организации мероприятий по реагированию на компьютерные инциденты и принятию мер по ликвидации последствий компьютерных атак с привлечением подразделений и должностных лиц ФСБ России субъектом КИИ, которому на праве собственности, аренды или ином законном основании принадлежат значимые объекты КИИ, во взаимодействии с НКЦКИ разрабатывается, согласовывается с 8 Центром ФСБ России и утверждается Регламент.

9. В Регламенте определяются:

условия привлечения подразделений и должностных лиц ФСБ России к проведению мероприятий по реагированию на компьютерные инциденты и принятию мер по ликвидации последствий компьютерных атак;

порядок проведения субъектом КИИ, которому на праве собственности, аренды или ином законном основании принадлежат значимые

объекты КИИ, совместно с привлекаемыми подразделениями и должностными лицами ФСБ России мероприятий по реагированию на компьютерные инциденты и принятию мер по ликвидации последствий компьютерных атак в отношении значимых объектов КИИ.

10. Субъект КИИ, которому на праве собственности, аренды или ином законном основании принадлежат значимые объекты КИИ, в ходе реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак осуществляет:

первичный анализ компьютерных инцидентов, установление их связи с компьютерными атаками;

проведение мероприятий в соответствии с Планом;

определение в соответствии с Регламентом необходимости привлечения к реагированию на компьютерные инциденты и принятию мер по ликвидации последствий компьютерных атак подразделений и должностных лиц ФСБ России.

11. Непосредственно перед принятием мер по ликвидации последствий компьютерных атак субъект КИИ, которому на праве собственности, аренды или ином законном основании принадлежат значимые объекты КИИ, определяет:

очередность значимых объектов КИИ (их структурных элементов), в отношении которых будут приниматься меры по ликвидации последствий компьютерных атак;

состав сил субъекта КИИ и их задачи в рамках принимаемых мер;

возможность восстановления функционирования значимого объекта КИИ;

перечень средств, необходимых для принятия мер по ликвидации последствий компьютерных атак.

12. В ходе ликвидации последствий компьютерных атак субъектом КИИ, которому на праве собственности, аренды или ином законном основании принадлежат значимые объекты КИИ, принимаются меры по восстановлению функционирования и проверке работоспособности значимого объекта КИИ.

13. О результатах мероприятий по реагированию на компьютерные инциденты и принятию мер по ликвидации последствий компьютерных атак субъект КИИ, которому на праве собственности, аренды или ином законном основании принадлежат значимые объекты КИИ, информирует НКЦКИ в срок не позднее 48 часов после завершения таких мероприятий в соответствии с пунктом 2 настоящего Порядка.