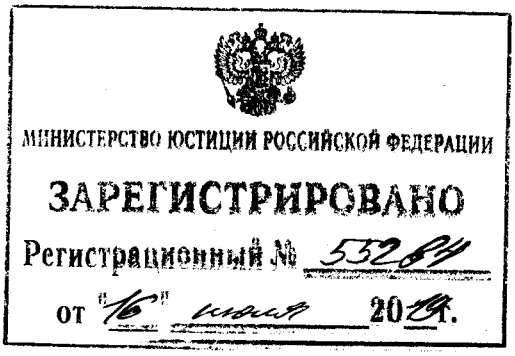
ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКАЗ

19 июня 2019 года Москва № 282

Об утверждении Порядка 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



В соответствии с пунктом 6 части 4 статьи 6 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»[1]

ПРИКАЗЫВАЮ

утвердить прилагаемый Порядок информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении

[1] Собрание законодательства Российской Федерации, 2017, № 31 (ч. I), ст. 4736.

значимых объектов критической информационной инфраструктуры Российской Федерации.

Директор А.Бортников

Приложение
к приказу ФСБ России
от 19 июня 2019 г.
№ 282

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. Настоящий Порядок определяет процедуру информирования ФСБ России субъектами критической информационной инфраструктуры Российской Федерации (далее – критическая информационная инфраструктура) о компьютерных инцидентах, а также реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры, в том числе в банковской сфере и в иных сферах финансового рынка.

2. Субъекты критической информационной инфраструктуры информируют ФСБ России обо всех компьютерных инцидентах, связанных с функционированием принадлежащих им на праве собственности, аренды или ином законном основании объектов критической информационной инфраструктуры.

3. Информирование осуществляется путем направления информации в Национальный координационный центр по компьютерным инцидентам[1] (далее – НКЦКИ) в соответствии с определенными НКЦКИ форматами[2] представления информации о компьютерных инцидентах в государственную

---

[1] Положение о Национальном координационном центре по компьютерным инцидентам, утвержденное приказом ФСБ России от 24 июля 2018 г. № 366 «О Национальном координационном центре по компьютерным инцидентам» (зарегистрирован Минюстом России 6 сентября 2018 г., регистрационный № 52109).

[2] Подпункт 4.9 пункта 4 Положения о Национальном координационном центре по компьютерным инцидентам. Утвержденного приказом ФСБ России от 24 июля 2018 г. № 366 «О Национальном координационном центре по компьютерным инцидентам» (зарегистрирован Минюстом России 6 сентября 2018 г., регистрационный № 52109).

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 критической информационной инфраструктуры, а также с иными, не являющимися субъектами критической информационной инфраструктуры, органами и организациями, в том числе иностранными и международными.

В случае отсутствия подключения к данной технической инфраструктуре информация передается субъектом критической информационной инфраструктуры посредством почтовой, факсимильной или электронной связи на адреса (телефонные номера) НКЦКИ, указанные на официальном сайте в информационно-телекоммуникационной сети «Интернет» по адресу: «http://cert.gov.ru».

4. Информация о компьютерном инциденте, связанном с функционированием значимого объекта критической информационной инфраструктуры, направляется субъектом критической информационной инфраструктуры в НКЦКИ в срок не позднее 3 часов с момента обнаружения компьютерного инцидента, а в отношении иных объектов критической информационной инфраструктуры – в срок не позднее 24 часов с момента его обнаружения.

5. В случае если компьютерный инцидент связан с функционированием объекта критической информационной инфраструктуры, принадлежащего на праве собственности, аренды или ином законном основании субъекту критической информационной инфраструктуры, который осуществляет деятельность в банковской сфере и в иных сферах финансового рынка, информация о компьютерном инциденте также направляется в Банк России с использованием технической

инфраструктуры Банка России в сроки, установленные пунктом 4 настоящего Порядка.

В случае отсутствия возможности уведомления субъектом критической информационной инфраструктуры, который осуществляет деятельность в банковской сфере и в иных сферах финансового рынка, посредством технической инфраструктуры Банка России информация передается субъектом критической информационной инфраструктуры в Банк России посредством почтовой, факсимильной или электронной связи на адреса (телефонные номера), указанные на официальном сайте Банка России в информационно-телекоммуникационной сети «Интернет».

6. Для подготовки к реагированию на компьютерные инциденты и принятию мер по ликвидации последствий компьютерных атак субъектом критической информационной инфраструктуры, которому на праве собственности, аренды или ином законном основании принадлежит значимый объект критической информационной инфраструктуры, в срок до 90 календарных дней со дня включения данного объекта в реестр значимых объектов критической информационной инфраструктуры Российской Федерации[1] разрабатывается план реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак (далее – План), содержащий:

технические характеристики и состав значимых объектов критической информационной инфраструктуры;

события (условия), при наступлении которых начинается реализация предусмотренных Планом мероприятий;

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

---

[1] Порядок ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденный приказом ФСТЭК России от 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).

описание состава подразделений и должностных лиц субъекта критической информационной инфраструктуры, ответственных за проведение мероприятий по реагированию на компьютерные инциденты и принятие мер по ликвидации последствий компьютерных атак.

7. При необходимости в План включаются:

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 критической информационной инфраструктуры, которому на праве собственности, аренды или ином законном основании принадлежат значимые объекты критической информационной инфраструктуры, мероприятий по реагированию на компьютерные инциденты и принятию мер по ликвидации последствий компьютерных атак в отношении значимых объектов критической информационной инфраструктуры совместно с привлекаемыми подразделениями и должностными лицами ФСБ России.

8. Проект Плана, содержащий положения, предусмотренные пунктом 7 настоящего Порядка, разрабатывается субъектом критической информационной инфраструктуры совместно с НКЦКИ и направляется на согласование в ФСБ России.

ФСБ России рассматривает проект Плана в срок до 30 календарных дней и по результатам рассмотрения согласовывает его или возвращает без согласования для доработки.

9. План, разрабатываемый субъектами критической информационной инфраструктуры, которым на праве собственности, аренды или ином законном основании принадлежат значимые объекты критической информационной инфраструктуры, осуществляющими деятельность в банковской сфере и в иных сферах финансового рынка, должен включать, помимо положений, указанных в пунктах 6 и 7 настоящего Порядка, условия привлечения

подразделений и должностных лиц Банка России к проведению мероприятий по реагированию на компьютерные инциденты и принятию мер по ликвидации последствий компьютерных атак. Такой План и изменения в него согласовываются с Банком России.

10. Субъект критической информационной инфраструктуры, которому на праве собственности, аренды или ином законном основании принадлежат значимые объекты критической информационной инфраструктуры, не реже одного раза в год организует и проводит тренировки по отработке мероприятий Плана. Объем и содержание тренировки определяются субъектом критической информационной инфраструктуры с учетом мероприятий, содержащихся в Плане.

Организация и проведение тренировок возлагаются на подразделения и должностных лиц субъекта критической информационной инфраструктуры, ответственных за проведение мероприятий по реагированию на компьютерные инциденты и принятие мер по ликвидации последствий компьютерных атак.

При необходимости по результатам тренировок в План вносятся изменения.

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

анализ компьютерных инцидентов (включая определение очередности реагирования на них), установление их связи с компьютерными атаками;

проведение мероприятий в соответствии с Планом;

определение в соответствии с Планом необходимости привлечения к реагированию на компьютерные инциденты и принятию мер по ликвидации последствий компьютерных атак подразделений

и должностных лиц ФСБ России и Банка России.

12. Перед принятием мер по ликвидации последствий компьютерных атак субъект критической информационной инфраструктуры, которому на праве собственности, аренды или ином законном основании принадлежат значимые объекты критической информационной инфраструктуры, определяет:

состав подразделений и должностных лиц субъекта критической информационной инфраструктуры, ответственных за проведение мероприятий по реагированию на компьютерные инциденты и принятие мер по ликвидации последствий компьютерных атак, и их задачи в рамках принимаемых мер;

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

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

перечень мер по восстановлению функционирования значимого объекта критической информационной инфраструктуры.

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

14. О результатах мероприятий по реагированию на компьютерные инциденты и принятию мер по ликвидации последствий компьютерных атак субъект критической информационной инфраструктуры, которому на праве собственности, аренды или ином законном основании принадлежат значимые объекты критической информационной инфраструктуры, информирует

НКЦКИ в срок не позднее 48 часов после завершения таких мероприятий в соответствии с пунктом 3 настоящего Порядка.

Субъекты критической информационной инфраструктуры, которым на праве собственности, аренды или ином законном основании принадлежат значимые объекты критической информационной инфраструктуры, осуществляющие деятельность в банковской сфере и в иных сферах финансового рынка, наряду с НКЦКИ информируют о результатах мероприятий по реагированию на компьютерные инциденты и принятию мер по ликвидации последствий компьютерных атак Банк России в срок не позднее 48 часов после завершения таких мероприятий в соответствии с пунктом 5 настоящего Порядка.