Об утверждении Перечня информации, представляемой в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и Порядка представления информации в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации

В соответствии с пунктом 5 части 4 статьи 6 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»[1]

П Р И К А З Ы В А Ю

утвердить:

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

Перечень информации, представляемой в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (приложение № 1);

Порядок представления информации в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (приложение № 2).

Директор А.Бортников

Приложение № 1
к приказу ФСБ России
от
№

Перечень
информации, представляемой в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации

1. Информация, содержащаяся в реестре значимых объектов критической информационной инфраструктуры Российской Федерации (далее – КИИ).

2. Информация об отсутствии необходимости присвоения объекту КИИ одной из категорий значимости.

3. Информация об исключении объекта КИИ из реестра значимых объектов КИИ, а также об изменении категории значимости значимого объекта КИИ.

4. Информация по итогам проведения государственного контроля в области обеспечения безопасности значимых объектов КИИ о нарушении требований по обеспечению безопасности значимых объектов КИИ, в результате которого создаются предпосылки возникновения компьютерных инцидентов.

5. Информация о компьютерных инцидентах, связанных с функционированием объектов КИИ:

дата, время, фактический адрес или географическое местоположение объекта КИИ, на котором произошел компьютерный инцидент;

наличие причинно-следственной связи между компьютерным инцидентом и компьютерной атакой;

связь с другими компьютерными инцидентами (при наличии);

состав технических параметров компьютерного инцидента;

последствия компьютерного инцидента.

6. Иная информация в области обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, представление которой субъектами КИИ и иными не являющимися субъектами КИИ органами и организациями, в том числе иностранными и международными, согласовано с Национальным координационным центром по компьютерным инцидентам.

Приложение № 2
к приказу ФСБ России
от
№

Порядок
представления информации в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации

1. Информация, указанная в пунктах 1 – 4 Перечня информации, представляемой в государственную систему обнаружения, предупреждения
и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, утвержденного приказом ФСБ России от
№ (далее – Перечень), представляется в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (далее – ГосСОПКА) федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации (далее – уполномоченный орган), путем ее направления в Национальный координационный центр по компьютерным инцидентам (далее – НКЦКИ) в пятидневный срок с момента:

включения объекта критической информационной инфраструктуры Российской Федерации (далее – КИИ) в реестр значимых объектов КИИ;

изменения категории значимости, присвоенной значимому объекту КИИ;

получения информации об отсутствии необходимости присвоения объекту КИИ одной из категорий значимости;

исключения объекта КИИ из реестра значимых объектов КИИ;

утверждения акта проверки по итогам осуществления государственного контроля области обеспечения безопасности значимых объектов КИИ, в котором содержится информация о нарушении требований по обеспечению безопасности значимых объектов КИИ, в результате которого создаются предпосылки возникновения компьютерных инцидентов.

2. Информация, указанная в пунктах 1 – 4 Перечня, направляется уполномоченным органом в НКЦКИ по форме, согласованной с НКЦКИ.

3. Информация, указанная в пункте 5 Перечня, представляется субъектами КИИ в ГосСОПКА путем ее направления в НКЦКИ в соответствии
с установленными НКЦКИ форматами 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 почтовой, факсимильной, электронной и телефонной связи на адреса (телефонные номера) НКЦКИ, указанные на сайте в информационно-телекоммуникационной сети «Интернет» по адресу: «http://cert.gov.ru».

4. Информация, указанная в пункте 5 Перечня, направляется субъектом КИИ в НКЦКИ незамедлительно (не позднее 24 часов с момента обнаружения компьютерного инцидента).

НКЦКИ незамедлительно уведомляет субъект КИИ о получении данной информации с учетом способа ее представления в НКЦКИ.

5. Информация, указанная в пункте 6 Перечня, представляется в ГосСОПКА путем ее направления в НКЦКИ посредством почтовой, факсимильной, электронной и телефонной связи на адреса (телефонные номера) НКЦКИ, указанные на сайте в информационно-телекоммуникационной сети «Интернет» по адресу: «http://cert.gov.ru» (при наличии подключения к технической инфраструктуре НКЦКИ информация может направляться посредством использования данной инфраструктуры) в сроки, согласованные с НКЦКИ и достаточные для своевременного проведения мероприятий по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты.