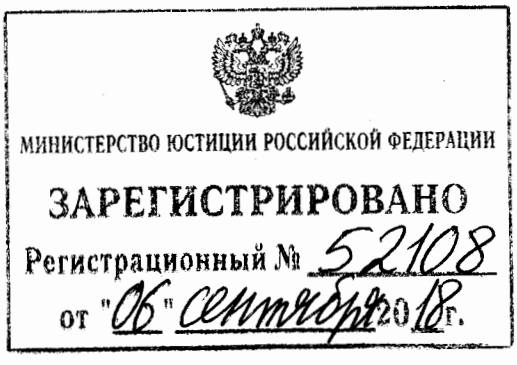
ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКАЗ

24 июля 2018 года **Москва** № 367



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 24 июля 2018 г.
№ 367

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 – критическая информационная инфраструктура).

2. Информация об отсутствии необходимости присвоения объекту критической информационной инфраструктуры одной из категорий значимости.

3. Информация об исключении объекта критической информационной инфраструктуры из реестра значимых объектов критической информационной инфраструктуры, а также об изменении категории его значимости.

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

5. Информация о компьютерных инцидентах, связанных с функционированием объектов критической информационной инфраструктуры:

дата, время, место нахождения или географическое местоположение объекта критической информационной инфраструктуры, 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, предоставляемая субъектами критической информационной инфраструктуры и иными не являющимися субъектами критической информационной инфраструктуры органами и организациями, в том числе иностранными и международными.

Приложение № 2
к приказу ФСБ России
от 24 июля 2018 г.
№ 367

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 24 июля 2018 г.№ 367 (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) не реже раза в месяц и не позднее месячного срока с момента:

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

изменения категории значимости, присвоенной значимому объекту критической информационной инфраструктуры;

получения информации об отсутствии необходимости присвоения объекту критической информационной инфраструктуры одной из категорий значимости;

исключения объекта критической информационной инфраструктуры из реестра значимых объектов критической информационной инфраструктуры;

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

2. Информация, указанная в пунктах 1 – 4 Перечня, направляется уполномоченным органом в НКЦКИ в форматах, определенных уполномоченным органом.

3. Информация, указанная в пункте 5 Перечня, представляется субъектами критической информационной инфраструктуры в ГосСОПКА путем ее направления в НКЦКИ в соответствии с определенными НКЦКИ форматами 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 (далее – техническая инфраструктура НКЦКИ).

4. В случае отсутствия подключения к технической инфраструктуре НКЦКИ информация направляется 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».

5. Информация, указанная в пункте 5 Перечня, направляется субъектом критической информационной инфраструктуры в НКЦКИ не позднее 24 часов с момента обнаружения компьютерного инцидента.

6. НКЦКИ уведомляет субъект критической информационной инфраструктуры о получении информации, направленной в соответствии с пунктом 5 настоящего Порядка не позднее 24 часов с момента ее получения.

7. Информация, указанная в пункте 6 Перечня, представляется в ГосСОПКА путем ее направления в НКЦКИ 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».

8. При наличии подключения к технической инфраструктуре НКЦКИ информация, указанная в пункте 6 Перечня, направляется посредством использования данной инфраструктуры.

9. Информация, указанная в пункте 6 Перечня, представляется в ГосСОПКА в сроки, достаточные для своевременного проведения мероприятий по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты.