Об утверждении Порядка обмена информацией о компьютерных инцидентах между субъектами критической информационной инфраструктуры Российской Федерации, между субъектами критической информационной инфраструктуры Российской Федерации и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты, и Порядка получения субъектами критической информационной инфраструктуры Российской Федерации информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения

В соответствии с пунктом 7 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:

Порядок обмена информацией о компьютерных инцидентах между субъектами критической информационной инфраструктуры Российской Федерации, между субъектами критической информационной инфраструктуры Российской Федерации и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты (приложение № 1);

Порядок получения субъектами критической информационной инфраструктуры Российской Федерации информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения (приложение № 2).

Директор А.Бортников

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

Приложение № 1
к приказу ФСБ России
от
№

Порядок
обмена информацией о компьютерных инцидентах между субъектами критической информационной инфраструктуры Российской Федерации, между субъектами критической информационной инфраструктуры Российской Федерации и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты

1. В ходе проведения мероприятий по реагированию на компьютерные инциденты, связанные с функционированием объектов критической информационной инфраструктуры Российской Федерации (далее – КИИ), субъекты КИИ осуществляют обмен информацией о таких компьютерных инцидентах с другими субъектами КИИ в целях минимизации последствий компьютерных инцидентов и предотвращения компьютерных инцидентов на других объектах КИИ.

Круг субъектов КИИ, с которыми осуществляется такой обмен, определяется субъектами КИИ самостоятельно.

2. Обмен информацией о компьютерных инцидентах осуществляется в сроки, достаточные для своевременного проведения мероприятий по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты, но, как правило, не позднее 24 часов с момента обнаружения компьютерного инцидента.

3. Обмен информацией о компьютерных инцидентах осуществляется субъектами КИИ путем взаимного направления уведомлений в соответствии с форматами представления информации о компьютерных инцидентах в государственную систему обнаружения, предупреждения

и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (далее – ГосСОПКА) и составом технических параметров компьютерного инцидента, указываемых при представлении информации в ГосСОПКА, установленными Национальным координационным центром по компьютерным инцидентам (далее – НКЦКИ), а также запросов, уточняющих представляемую информацию.

4. Направление уведомлений и запросов осуществляется посредством почтовой, факсимильной, электронной и телефонной связи (при наличии подключения к технической инфраструктуре 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 (далее – техническая инфраструктура НКЦКИ), информация передается посредством использования данной инфраструктуры).

5. В случае, если передаваемые в рамках обмена информацией о компьютерных инцидентах сведения составляют государственную или иную охраняемую законом тайну, обмен осуществляется в соответствии с требованиями законодательства Российской Федерации.

6. Одновременно с направлением информации о компьютерных инцидентах в рамках обмена субъекты КИИ уведомляют об этом НКЦКИ.

7. Уведомление в соответствии с пунктом 6 настоящего Порядка осуществляется субъектами КИИ с использованием технической инфраструктуры НКЦКИ в соответствии с форматами представления информации о компьютерных инцидентах в ГосСОПКА и составом технических параметров компьютерного инцидента, указываемых при представлении информации в ГосСОПКА, установленными НКЦКИ.

В случае отсутствия подключения к данной инфраструктуре уведомление осуществляется 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».

8. Обмен информацией о компьютерных инцидентах с уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты (далее – иностранные (международные) организации), осуществляется НКЦКИ, за исключением случая, когда международным договором Российской Федерации предусмотрен обмен такой информацией напрямую между субъектом КИИ и иностранной (международной) организацией.

9. В случае необходимости осуществления обмена информацией о компьютерном инциденте с иностранной (международной) организацией субъект КИИ направляет в НКЦКИ мотивированное обращение с приложением составляющей предмет обмена информации и указанием наименования, места нахождения, адреса иностранной (международной) организации и иных необходимых сведений (далее – обращение).

10. Субъекты КИИ направляют обращение в НКЦКИ в порядке, установленном пунктом 7 настоящего Порядка.

11. НКЦКИ в течение 12 часов после получения обращения оценивает целесообразность передачи информации о компьютерном инциденте в иностранную (международную) организацию и, в случае принятия положительного решения, незамедлительно направляет ее адресату.

12. При принятии НКЦКИ отрицательного решения в отношении передачи информации о компьютерном инциденте иностранной (международной) организации субъект КИИ, направивший обращение, уведомляется об этом в течение 24 часов.

13. Направление информации в иностранную (международную) организацию осуществляется НКЦКИ в соответствии с форматами представления информации о компьютерных инцидентах в ГосСОПКА и составом технических параметров компьютерного инцидента, указываемых при представлении информации в ГосСОПКА, установленными НКЦКИ.

14. При получении ответа от иностранной (международной) организации НКЦКИ в течение 12 часов направляет данный ответ субъекту КИИ, направившему обращение, с учетом способа направления в НКЦКИ обращения.

15. В случае, если обмен информацией о компьютерных инцидентах, связанных с функционированием объектов КИИ, напрямую с иностранной (международной) организацией предусмотрен международным договором Российской Федерации, субъекты КИИ также направляют такую информацию в НКЦКИ с указанием реквизитов международного договора Российской Федерации, в соответствии с которым осуществляется данный обмен.

16. В случае получения субъектом КИИ информации о компьютерном инциденте, связанном с функционированием объекта КИИ, инициативно направленной иностранной (международной) организацией, субъект КИИ направляет полученную информацию в НКЦКИ в возможно короткие сроки, но не позднее 24 часов с момента получения такой информации.

Дальнейший обмен информацией об этом компьютерном инциденте с иностранной (международной) организацией осуществляется в соответствии с пунктами 9 – 14 настоящего Порядка.

Приложение № 2
к приказу ФСБ России
от
№

Порядок
получения субъектами критической информационной инфраструктуры Российской Федерации информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения

1. Субъекты критической информационной инфраструктуры Российской Федерации (далее – КИИ) получают информацию о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения путем:

1.1. Обращения к сайту в информационно-телекоммуникационной сети «Интернет» по адресу: «http://cert.gov.ru», где такая информация, полученная в результате ее сбора и анализа силами государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, публикуется ежемесячно.

1.2. Направления запросов в Национальный координационный центр по компьютерным инцидентам (далее – НКЦКИ) с использованием технической инфраструктуры НКЦКИ, предназначенной для отправки, получения, обработки и хранения уведомлений и запросов в рамках информационного обмена с субъектами КИИ, а также с иными не являющимися субъектами КИИ органами и организациями, в том числе иностранными и международными (далее – техническая инфраструктура НКЦКИ), либо, при отсутствии подключения к технической инфраструктуре НКЦКИ, посредством почтовой, факсимильной и электронной связи, позволяющей достоверно установить отправителя и факт направления обращения, на адреса НКЦКИ, указанные на сайте в информационно-телекоммуникационной сети «Интернет» по адресу: «http://cert.gov.ru».

1.3. Направления обращений в ФСБ России в соответствии с законодательством Российской Федерации.

1.4. Направления запросов другим субъектам КИИ и уполномоченным органам иностранных государств, международным, международным неправительственным организациям и иностранным организациям, осуществляющим деятельность в области реагирования на компьютерные инциденты, если такой запрос не содержит сведений о компьютерных инцидентах, связанных с функционированием объектов КИИ.

2. В случае направления запроса, предусмотренного подпунктом 1.2 настоящего порядка, ответ субъекту КИИ предоставляется в пятидневный срок с момента получения такого запроса.

3. Получение субъектами КИИ информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения в рамках обмена информацией о компьютерных инцидентах, связанных с функционированием объектов КИИ, осуществляется в соответствии с Порядком обмена информацией о компьютерных инцидентах между субъектами критической информационной инфраструктуры Российской Федерации, между субъектами критической информационной инфраструктуры Российской Федерации и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты, утвержденным приказом ФСБ России от
№ .

4. НКЦКИ осуществляет направление субъектам КИИ информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения с учетом особенностей функционирования объектов КИИ, принадлежащих данным субъектам КИИ на праве собственности, аренды или ином законном основании.

Направление такой информации субъекту КИИ осуществляется в сроки, достаточные для своевременного проведения мероприятий по обнаружению,

предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты, но не позднее 24 часов с момента получения НКЦКИ такой информации.