



КонсультантПлюс

Приказ ФСБ России от 24.07.2018 N 368
"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"
(Зарегистрировано в Минюсте России 06.09.2018 N
52107)

Документ предоставлен **КонсультантПлюс**

www.consultant.ru

Дата сохранения: 04.10.2024

Зарегистрировано в Минюсте России 6 сентября 2018 г. N 52107

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКАЗ
от 24 июля 2018 г. N 368

**ОБ УТВЕРЖДЕНИИ ПОРЯДКА
ОБМЕНА ИНФОРМАЦИЕЙ О КОМПЬЮТЕРНЬ Х ИНЦИДЕНТАХ
МЕЖДУ СУБЪЕКТАМИ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ
ИНФРАСТРУКТУРЬ
РОССИЙСКОЙ ФЕДЕРАЦИИ, МЕЖДУ СУБЪЕКТАМИ КРИТИЧЕСКОЙ
ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЬ РОССИЙСКОЙ ФЕДЕРАЦИИ
И УПОЛНОМОЧЕННЬ МИ ОРГАНАМИ ИНОСТРАННЬ Х ГОСУДАРСТВ,
МЕЖДУНАРОДНЬ МИ, МЕЖДУНАРОДНЬ МИ НЕПРАВИТЕЛЬСТВЕННЬ МИ
ОРГАНИЗАЦИЯМИ И ИНОСТРАННЬ МИ ОРГАНИЗАЦИЯМИ,
ОСУЩЕСТВЛЯЮЩИМИ
ДЕЯТЕЛЬНОСТЬ В ОБЛАСТИ РЕАГИРОВАНИЯ НА КОМПЬЮТЕРНЬ Е
ИНЦИДЕНТЬ , И ПОРЯДКА ПОЛУЧЕНИЯ СУБЪЕКТАМИ КРИТИЧЕСКОЙ
ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЬ РОССИЙСКОЙ ФЕДЕРАЦИИ
ИНФОРМАЦИИ О СРЕДСТВАХ И СПОСОБАХ ПРОВЕДЕНИЯ
КОМПЬЮТЕРНЬ Х
АТАК И О МЕТОДАХ ИХ ПРЕДУПРЕЖДЕНИЯ И ОБНАРУЖЕНИЯ**

В соответствии с [пунктом 7 части 4 статьи 6](#) Федерального закона от 26 июля 2017 г. N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации" <1> приказываю

<1> [Собрание законодательства Российской Федерации, 2017, N 31 \(ч. I\), ст. 4736.](#)

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 N 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 N 2).

Директор
А.БОРТНИКОВ

Приложение N 1
к приказу ФСБ России
от 24 июля 2018 г. N 368

**ПОРЯДОК
ОБМЕНА ИНФОРМАЦИЕЙ О КОМПЬЮТЕРНЬ Х
ИНЦИДЕНТАХ МЕЖДУ СУБЪЕКТАМИ КРИТИЧЕСКОЙ
ИНФОРМАЦИОННОЙ
ИНФРАСТРУКТУРЬ РОССИЙСКОЙ ФЕДЕРАЦИИ, МЕЖДУ СУБЪЕКТАМИ
КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЬ РОССИЙСКОЙ
ФЕДЕРАЦИИ И УПОЛНОМОЧЕННЬ МИ ОРГАНАМИ ИНОСТРАННЬ Х
ГОСУДАРСТВ, МЕЖДУНАРОДНЬ МИ, МЕЖДУНАРОДНЬ МИ
НЕПРАВИТЕЛЬСТВЕННЬ МИ ОРГАНИЗАЦИЯМИ И ИНОСТРАННЬ МИ
ОРГАНИЗАЦИЯМИ, ОСУЩЕСТВЛЯЮЩИМИ ДЕЯТЕЛЬНОСТЬ В ОБЛАСТИ
РЕАГИРОВАНИЯ НА КОМПЬЮТЕРНЬ Е ИНЦИДЕНТЬ**

1. Настоящий Порядок определяет правила обмена информацией о компьютерных инцидентах между субъектами критической информационной инфраструктуры Российской Федерации (далее - критическая информационная инфраструктура), между субъектами критической информационной инфраструктуры и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты.

2. При проведении мероприятий по реагированию на компьютерные инциденты, связанные с функционированием объектов критической информационной инфраструктуры, субъекты критической информационной инфраструктуры осуществляют обмен информацией о таких компьютерных инцидентах с другими субъектами критической информационной инфраструктуры в целях минимизации последствий компьютерных инцидентов и предотвращения компьютерных инцидентов на других объектах

критической информационной инфраструктуры.

Субъекты критической информационной инфраструктуры вправе самостоятельно определять круг субъектов критической информационной инфраструктуры, с которыми осуществляется такой обмен.

3. 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.

4. Обмен информацией о компьютерных инцидентах осуществляется субъектами критической информационной инфраструктуры 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, определенными Национальным координационным центром по компьютерным инцидентам (далее - НКЦКИ), а также запросов, уточняющих представляемую информацию.

5. Направление уведомлений и запросов осуществляется посредством почтовой, факсимильной, электронной или телефонной связи.

6. При наличии подключения к технической инфраструктуре 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), уведомления и запросы направляются посредством использования данной инфраструктуры.

7. В случае если передаваемые в рамках обмена информацией о компьютерных инцидентах сведения составляют государственную тайну, обмен осуществляется в соответствии с требованиями законодательства Российской Федерации в области защиты государственной тайны.

8. Одновременно с направлением информации о компьютерных инцидентах в рамках обмена субъекты критической информационной инфраструктуры информируют об этом НКЦКИ.

9. Информирование в соответствии с [пунктом 8](#) настоящего Порядка осуществляется субъектами критической информационной инфраструктуры 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, определенными НКЦКИ.

10. В случае отсутствия подключения к технической инфраструктуре НКЦКИ информирование осуществляется 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".

11. 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 случаев, когда обмен субъекта критической информационной инфраструктуры такой информацией напрямую с иностранной (международной) организацией предусмотрен международным договором Российской Федерации.

12. В случае необходимости осуществления обмена информацией о компьютерном инциденте с иностранной (международной) организацией субъект критической информационной инфраструктуры направляет в НКЦКИ обращение, содержащее обоснование необходимости обмена этой информацией и указание наименования, места нахождения, адреса иностранной (международной) организации и иных необходимых для передачи информации сведений с приложением составляющей предмет обмена информации (далее - обращение).

13. Субъекты критической информационной инфраструктуры направляют обращение в НКЦКИ в порядке, установленном [пунктами 9 и 10](#) настоящего Порядка.

14. НКЦКИ незамедлительно информирует субъект критической информационной инфраструктуры о получении его обращения.

15. НКЦКИ в течение 24 часов после получения обращения рассматривает информацию о компьютерном инциденте. В случае принятия решения о передаче этой информации в иностранную (международную) организацию, незамедлительно направляет ее адресату, о чем одновременно информируется субъект критической информационной инфраструктуры, направивший обращение.

16. При принятии НКЦКИ решения об отказе в передаче информации о компьютерном инциденте иностранной (международной) организации

субъект критической информационной инфраструктуры, направивший обращение, информируется об этом в течение 24 часов.

17. 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, определенными НКЦКИ.

18. При получении ответа от иностранной (международной) организации НКЦКИ в течение 12 часов направляет данный ответ субъекту критической информационной инфраструктуры, направившему обращение.

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

20. В случае получения субъектом критической информационной инфраструктуры информации о компьютерном инциденте, связанном с функционированием объекта критической информационной инфраструктуры, инициативно направленной иностранной (международной) организацией, субъект критической информационной инфраструктуры направляет полученную информацию в НКЦКИ 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 12 - 18](#) настоящего Порядка.

Приложение N 2
к приказу ФСБ России
от 24 июля 2018 г. N 368

**ПОРЯДОК
ПОЛУЧЕНИЯ СУБЪЕКТАМИ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ
ИНФРАСТРУКТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ ИНФОРМАЦИИ О
СРЕДСТВАХ
И СПОСОБАХ ПРОВЕДЕНИЯ КОМПЬЮТЕРНЫХ АТАК И О МЕТОДАХ**

ИХ ПРЕДУПРЕЖДЕНИЯ И ОБНАРУЖЕНИЯ

1. Настоящий Порядок определяет правила получения субъектами критической информационной инфраструктуры Российской Федерации (далее - критическая информационная инфраструктура) информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения.

2. Субъекты критической информационной инфраструктуры получают информацию о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения путем:

2.1. Обращения к официальному сайту в информационно-телекоммуникационной сети "Интернет" по адресу: "http://cert.gov.ru".

2.2. 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 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), либо, при отсутствии подключения к ней, 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".

2.3. Направления обращений в ФСБ России.

2.4. Направления запросов другим субъектам критической информационной инфраструктуры, иностранным (международным) организациям, если такой запрос не содержит сведений о компьютерных инцидентах, связанных с функционированием объектов критической информационной инфраструктуры.

3. В случае направления запроса, предусмотренного **подпунктом 2.2** настоящего Порядка, ответ субъекту критической информационной инфраструктуры предоставляется в пятидневный срок с момента получения такого запроса.

4. Получение субъектами критической информационной инфраструктуры 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

критической информационной инфраструктуры, 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 24 июля 2018 г. N 368.

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

6. Направление информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения осуществляется посредством использования технической инфраструктуры НКЦКИ.

7. В случае отсутствия у субъекта критической информационной инфраструктуры подключения к технической инфраструктуре НКЦКИ, информация направляется посредством почтовой, факсимильной или электронной связи.

8. Направление информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения субъекту критической информационной инфраструктуры осуществляется в срок не позднее 24 часов с момента получения НКЦКИ такой информации.
