ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКАЗ

25 декабря 2025 года **Москва** **№** 546

Об утверждении Порядка обмена информацией о компьютерных атаках и 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

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» и пунктом 1 Указа Президента Российской Федерации от 22 декабря 2017 г. № 620 «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации

последствий компьютерных атак на информационные ресурсы Российской Федерации»

П Р И К А З Ы В А Ю:

1. Утвердить прилагаемый Порядок обмена информацией о компьютерных атаках и 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.

2. Признать утратившим силу приказ ФСБ России от 24 июля 2018 г. № 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»[1].

3. Настоящий приказ вступает в силу с 30 января 2026 г.

Директор А.Бортников

[1] Зарегистрирован Минюстом России 6 сентября 2018 г., регистрационный № 52107.

Утвержден
приказом ФСБ России
от 25 декабря 2025г.
№ 546

Порядок
обмена информацией о компьютерных атаках и 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. Обмен информацией о компьютерных атаках и компьютерных инцидентах осуществляется 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 (далее – иностранные (международные) организации).

2. При проведении мероприятий по реагированию на компьютерные инциденты, связанные с функционированием объектов критической информационной инфраструктуры, субъектами критической информационной инфраструктуры осуществляется обмен информацией о компьютерных атаках и 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 атаках и компьютерных инцидентах осуществляется в сроки, достаточные для оперативного проведения мероприятий по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты.

4. Обмен информацией о компьютерных атаках и компьютерных инцидентах осуществляется субъектами критической информационной инфраструктуры путем взаимного направления уведомлений в соответствии с форматами представления информации о компьютерных атаках и компьютерных инцидентах в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (далее – ГосСОПКА) и составом технических параметров компьютерной атаки и компьютерного инцидента, указываемых при представлении информации в ГосСОПКА, определенными Национальным координационным центром по компьютерным инцидентам (далее – НКЦКИ)[1], а также запросов, уточняющих представляемую информацию.

5. Направление уведомлений и запросов осуществляется посредством почтовой и электронной 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

---

[1] Подпункты 4.9 и 4.10 пункта 4 Положения о Национальном координационном центре по компьютерным инцидентам, утвержденного приказом ФСБ России от 24 июля 2018 г. № 366 (зарегистрирован Минюстом России 6 сентября 2018 г., регистрационный № 52109), с изменениями, внесенными приказом ФСБ России от 24 декабря 2025 г. № 540 (зарегистрирован Минюстом России 25 декабря 2025 г., регистрационный № 84777).

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 атаках и компьютерных инцидентах сведения составляют государственную тайну, обмен осуществляется в соответствии с требованиями законодательства Российской Федерации о государственной тайне.

8. Одновременно с направлением информации о компьютерных атаках и компьютерных инцидентах в рамках обмена субъекты критической информационной инфраструктуры также должны направить такую информацию в НКЦКИ.

9. Информирование НКЦКИ 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 атаках и компьютерных инцидентах в ГосСОПКА и составом технических параметров компьютерной атаки и компьютерного инцидента, указываемых при представлении информации в ГосСОПКА, определенными НКЦКИ.

10. В случае отсутствия подключения к технической инфраструктуре НКЦКИ информирование осуществляется посредством почтовой или электронной связи по адресам НКЦКИ, указанным на официальном сайте в информационно-телекоммуникационной сети «Интернет» (www.cert.gov.ru).

11. Обмен информацией о компьютерных атаках и компьютерных инцидентах с иностранными (международными) организациями осуществляется НКЦКИ, за исключением случаев, когда международным договором Российской Федерации с иностранной (международной) организацией предусмотрен непосредственный обмен такой информацией между субъектом критической информационной инфраструктуры и иностранной (международной) организацией.

12. В случае необходимости осуществления обмена информацией о компьютерной атаке и (или) компьютерном инциденте с иностранной (международной) организацией субъект критической информационной инфраструктуры должен направить в НКЦКИ обращение, содержащее обоснование необходимости обмена такой информацией и указание полного 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 должны направить обращение в НКЦКИ в соответствии с пунктами 9 и 10 настоящего Порядка.

14. НКЦКИ должен незамедлительно информировать субъект критической информационной инфраструктуры о получении его обращения посредством использования технической инфраструктуры НКЦКИ. В случае отсутствия у субъекта критической информационной инфраструктуры подключения к технической инфраструктуре НКЦКИ информация направляется посредством почтовой или электронной связи по адресу, указанному в данном обращении.

15. НКЦКИ в течение 24 часов после получения обращения должен рассмотреть информацию о компьютерной атаке и (или) компьютерном инциденте. В случае принятия решения о передаче этой информации в иностранную (международную) организацию НКЦКИ должен незамедлительно направить ее адресату, о чем одновременно информируется субъект критической информационной инфраструктуры, направивший обращение в соответствии с пунктом 14 настоящего Порядка.

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 с момента принятия такого решения в соответствии с пунктом 14 настоящего Порядка.

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

18. При получении ответа от иностранной (международной) организации НКЦКИ в течение 48 часов с момента получения ответа должен направить его субъекту критической информационной инфраструктуры, направившему обращение, в соответствии с пунктом 14 настоящего Порядка.

19. В случае если международным договором Российской Федерации с иностранной (международной) организацией предусмотрен непосредственный обмен информацией о компьютерных атаках и компьютерных инцидентах, связанных с функционированием объектов критической информационной инфраструктуры, субъекты критической информационной инфраструктуры также должны направить такую информацию в НКЦКИ с указанием реквизитов международного договора Российской Федерации, на основании которого осуществляется данный обмен, в соответствии с пунктами 9 и 10 настоящего Порядка.

20. В случае получения субъектом критической информационной инфраструктуры информации о компьютерной атаке и (или) компьютерном инциденте, связанных с функционированием объекта критической информационной инфраструктуры, инициативно направленной иностранной (международной) организацией, субъект критической информационной инфраструктуры должен направить полученную информацию в НКЦКИ не позднее 24 часов с момента получения такой информации в соответствии с пунктами 9 и 10 настоящего Порядка.

Дальнейший обмен информацией об этих компьютерной атаке и (или) компьютерном инциденте с иностранной (международной) организацией осуществляется в соответствии с пунктами 12 – 18 настоящего Порядка.

21. В случае получения субъектом критической информационной инфраструктуры информации о компьютерной атаке и (или) компьютерном инциденте, связанных с функционированием объекта критической информационной инфраструктуры другого субъекта критической информационной инфраструктуры, субъект критической информационной инфраструктуры должен направить полученную информацию в НКЦКИ не позднее 12 часов с момента получения такой информации в соответствии с пунктами 9 и 10 настоящего Порядка.