ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКАЗ

_____ **Москва** **№** _____

Об утверждении Порядка взаимодействия операторов государственных информационных систем, иных информационных систем государственных органов, государственных унитарных предприятий, государственных учреждений с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, включая информирование ФСБ России о компьютерных инцидентах, повлекших неправомерную передачу содержащейся в указанных информационных системах информации

В соответствии с частью 7 статьи 16 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и пунктом 1 Положения о Федеральной службе безопасности Российской Федерации, утвержденного Указом Президента Российской Федерации от 11 августа 2003 г. № 960,

П Р И К А З Ы В А Ю:

1. Утвердить прилагаемый Порядок взаимодействия операторов государственных информационных систем, иных информационных систем государственных органов, государственных унитарных предприятий, государственных учреждений с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, включая информирование ФСБ России о компьютерных инцидентах, повлекших неправомерную передачу содержащейся в указанных информационных системах информации

2. Настоящий приказ вступает в силу с 1 сентября 2026 г.

Директор А.Бортников

Утвержден
приказом ФСБ России
от
№

Порядок
взаимодействия операторов государственных информационных систем, иных информационных систем государственных органов, государственных унитарных предприятий, государственных учреждений с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, включая информирование ФСБ России о компьютерных инцидентах, повлекших неправомерную передачу содержащейся в указанных информационных системах информации

1. Взаимодействие операторов государственных информационных систем, иных информационных систем государственных органов, государственных унитарных предприятий, государственных учреждений[1] (далее – операторы и информационные системы соответственно) с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (далее – ГосСОПКА), включая информирование ФСБ России о компьютерных инцидентах, повлекших неправомерную передачу содержащейся в информационных системах информации, осуществляется через Национальный координационный центр по компьютерным инцидентам (далее – НКЦКИ) посредством 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

[1] Часть 2 статьи 13 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

и организациями, в том числе иностранными и международными[1] (далее – техническая инфраструктура НКЦКИ).

2. Взаимодействие осуществляется в целях направления операторами в НКЦКИ информации о компьютерных инцидентах, связанных с нарушением функционирования принадлежащих им на праве собственности, аренды или ином законном основании технических средств информационных систем, используемых для обработки содержащейся в базах данных информационных систем информации, и реагирования на компьютерные инциденты, а также в целях информирования НКЦКИ операторов об угрозах безопасности информации, в том числе о готовящихся компьютерных атаках и признаках компьютерных инцидентов, связанных с функционированием принадлежащих им на праве собственности, аренды или ином законном основании технических средств информационных систем, используемых для обработки содержащейся в базах данных информационных систем информации, и необходимых мерах по противодействию им.

3. Операторы обязаны направлять информацию о компьютерных инцидентах и получать информацию об угрозах безопасности информации, в том числе о готовящихся компьютерных атаках и признаках компьютерных инцидентов, связанных с функционированием принадлежащих им на праве собственности, аренды или ином законном основании технических средств информационных систем, используемых для обработки содержащейся в базах данных информационных систем информации, и необходимых мерах по противодействию им с использованием личного кабинета субъекта ГосСОПКА, зарегистрированного в технической инфраструктуре НКЦКИ (далее – личный кабинет), в соответствии с определенными НКЦКИ форматами представления информации о компьютерных атаках и компьютерных инцидентах в ГосСОПКА[2].

---

[1] Подпункт 4.2 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) (далее – Положение о НКЦКИ).

[2] Подпункт 4.9 пункта 4 Положения о НКЦКИ.

В случаях технических сбоев и (или) отсутствия связи с личным кабинетом информация о компьютерных инцидентах должна быть направлена в НКЦКИ с использованием резервных каналов связи (почтовый адрес и адрес электронной почты), указанных операторами в личном кабинете, в соответствии с определенными НКЦКИ форматами представления информации о компьютерных атаках и компьютерных инцидентах в ГосСОПКА[1].

4. Подключение к личному кабинету, осуществляемое в целях взаимодействия, организуется после заключения регламента взаимодействия НКЦКИ и владельцев информационных ресурсов Российской Федерации при информировании ФСБ России о компьютерных атаках и компьютерных инцидентах, реагировании на компьютерные инциденты и принятии мер по ликвидации последствий компьютерных атак в отношении значимых объектов критической информационной инфраструктуры и иных информационных ресурсов Российской Федерации, принадлежащих органам и организациям[1].

5. Информация о компьютерных инцидентах направляется в НКЦКИ операторами в срок не позднее 24 часов с момента их обнаружения.

6. Передача операторами в НКЦКИ информации о компьютерных инцидентах подтверждается посредством присвоения НКЦКИ компьютерному инциденту идентификатора.

Идентификатор присваивается компьютерным инцидентам в течение 24 часов с момента получения информации о компьютерном инциденте в личном кабинете.

7. Операторы вправе посредством личного кабинета обратиться в НКЦКИ для оказания им содействия в реагировании на компьютерные инциденты и привлечения сил ГосСОПКА.

---

[1] Подпункт 5.8 пункта 5 Положения о НКЦКИ.

8. НКЦКИ в целях информирования операторов, предусмотренного пунктом 2 настоящего Порядка, и оказания им содействия в реагировании на компьютерные инциденты, предусмотренного пунктом 7 настоящего Порядка, осуществляется:

доведение до операторов информации об угрозах безопасности информации, в том числе о готовящихся компьютерных атаках и признаках компьютерных инцидентов, связанных с функционированием принадлежащих им на праве собственности, аренды или ином законном основании технических средств информационных систем, используемых для обработки содержащейся в базах данных информационных систем информации, и необходимых мерах по противодействию им;

доведение до операторов информации о средствах и способах проведения компьютерных атак и методах их обнаружения и предупреждения;

направление операторам запросов о представлении дополнительных сведений об угрозах безопасности информации, в том числе о признаках компьютерных инцидентов, связанных с функционированием принадлежащих им на праве собственности, аренды или ином законном основании технических средств информационных систем, используемых для обработки содержащейся в базах данных информационных систем информации, и вредоносной активности;

оказание содействия операторам в реагировании на компьютерные инциденты при наличии такой необходимости;

обеспечение методической и экспертной поддержки по вопросам реагирования на компьютерные инциденты.

9. Операторы в течение 24 часов с момента получения от НКЦКИ информации о готовящихся компьютерных атаках и признаках компьютерных инцидентов, связанных с функционированием принадлежащих им на праве собственности, аренды или ином законном основании технических средств информационных систем, используемых для обработки содержащейся в базах

данных информационных систем информации, обязаны направить в НКЦКИ информацию о проводимых мероприятиях по их предупреждению.

10. В случае получения запроса, указанного в абзаце четвертом пункта 8 настоящего Порядка, операторы в течение 24 часов с момента получения указанного запроса обязаны направить в НКЦКИ запрашиваемые сведения или уведомление о невозможности их представления с указанием причин и срока, в который данные сведения будут представлены.