ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКАЗ

25 декабря 2025 года Москва № 548

Об утверждении Порядка осуществления непрерывного взаимодействия субъектов критической информационной инфраструктуры Российской Федерации, которым на праве собственности, аренды или ином законном основании принадлежат значимые объекты критической информационной инфраструктуры Российской Федерации, а также руководителей органов и организаций, на которых возложены обязанности, предусмотренные частью 4 статьи 9 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации

В соответствии с пунктом 7 части 3, частью 4 статьи 9 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической

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 осуществления непрерывного взаимодействия субъектов критической информационной инфраструктуры Российской Федерации, которым на праве собственности, аренды или ином законном основании принадлежат значимые объекты критической информационной инфраструктуры Российской Федерации, а также руководителей органов и организаций, на которых возложены обязанности, предусмотренные частью 4 статьи 9 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

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

Директор А.Бортников

Утвержден
приказом ФСБ России
от 25 декабря 2025г.
№ 548

Порядок
осуществления непрерывного взаимодействия субъектов критической информационной инфраструктуры Российской Федерации, которым на праве собственности, аренды или ином законном основании принадлежат значимые объекты критической информационной инфраструктуры Российской Федерации, а также руководителей органов и организаций, на которых возложены обязанности, предусмотренные частью 4 статьи 9 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации

1. Непрерывное взаимодействие субъектов критической информационной инфраструктуры Российской Федерации (далее – критическая информационная инфраструктура), которым на праве собственности, аренды или ином законном основании принадлежат значимые объекты критической информационной инфраструктуры, а также руководителей органов и организаций, на которых возложены обязанности, предусмотренные частью 4 статьи 9 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (далее – руководители органов (организаций), с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (далее – ГосСОПКА) 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 и организациями, в том числе иностранными и международными[1] (далее – техническая инфраструктура НКЦКИ).

2. Непрерывное взаимодействие осуществляется в целях направления субъектами критической информационной инфраструктуры и руководителями органов (организаций) в НКЦКИ информации о компьютерных атаках и компьютерных инцидентах, связанных с нарушением функционирования принадлежащих им на праве собственности, аренды или ином законном основании значимых объектов критической информационной инфраструктуры или информационных ресурсов Российской Федерации (далее – информация о компьютерных атаках и компьютерных инцидентах), и реагирования на компьютерные инциденты, а также в целях информирования НКЦКИ субъектов критической информационной инфраструктуры и руководителей органов (организаций) 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 значимых объектов критической информационной инфраструктуры или информационных ресурсов Российской Федерации, и необходимых мерах по противодействию им.

3. Субъекты критической информационной инфраструктуры и руководители органов (организаций) обязаны направлять информацию о компьютерных атаках и 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 значимых объектов критической информационной инфраструктуры или информационных ресурсов

---

[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).

Российской Федерации, 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[1].

В случаях технических сбоев и (или) отсутствия связи с личным кабинетом информация о компьютерных атаках и компьютерных инцидентах должна быть направлена в НКЦКИ с использованием резервных каналов связи (почтовый адрес и адрес электронной почты), указанных субъектами критической информационной инфраструктуры и руководителями органов (организаций) 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 непрерывного 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, на которые возложены обязанности, предусмотренные частью 4 статьи 9 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»[2].

5. Информация о компьютерных атаках и компьютерных инцидентах направляется в НКЦКИ субъектами критической информационной инфраструктуры и руководителями органов (организаций) в сроки,

---

[1] Подпункт 4.9 пункта 4 Положения о НКЦКИ.
[2] Подпункт 5.8 пункта 5 Положения о НКЦКИ.

установленные в порядке информирования ФСБ России о компьютерных атаках и компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации и иных информационных ресурсов Российской Федерации, принадлежащих органам и организациям, на которые возложены обязанности, предусмотренные частью 4 статьи 9 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», утверждаемом приказом ФСБ России в соответствии с пунктом 6 части 4 статьи 6 и частью 6 статьи 9 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

6. Передача субъектом критической информационной инфраструктуры и руководителем органа (организации) в НКЦКИ информации о компьютерных атаках и компьютерных инцидентах подтверждается посредством присвоения НКЦКИ компьютерной атаке и (или) компьютерному инциденту идентификатора.

Идентификатор присваивается компьютерным атакам и (или) компьютерным инцидентам в течение 24 часов с момента получения информации о компьютерной атаке и компьютерном инциденте в личном кабинете.

7. Субъекты критической информационной инфраструктуры и руководители органов (организаций) вправе посредством личного кабинета обратиться в НКЦКИ для оказания им содействия в реагировании на компьютерные инциденты и привлечения сил ГосСОПКА.

8. НКЦКИ в целях информирования субъектов критической информационной инфраструктуры и руководителей органов (организаций), предусмотренного пунктом 2 настоящего Порядка, и оказания им содействия в реагировании на компьютерные инциденты, предусмотренного пунктом 7 настоящего Порядка, осуществляется:

доведение до субъектов критической информационной инфраструктуры и руководителей органов (организаций) 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 значимых объектов критической информационной инфраструктуры или информационных ресурсов Российской Федерации, и необходимых мерах по противодействию им;

доведение до субъектов критической информационной инфраструктуры и руководителей органов (организаций) информации о средствах и способах проведения компьютерных атак и методах их обнаружения и предупреждения;

направление субъектам критической информационной инфраструктуры и руководителям органов (организаций) 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 значимых объектов критической информационной инфраструктуры или информационных ресурсов Российской Федерации, и вредоносной активности;

оказание содействия субъектам критической информационной инфраструктуры и руководителям органов (организаций) в реагировании на компьютерные инциденты при наличии такой необходимости;

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

9. Субъект критической информационной инфраструктуры и руководитель органа (организации) 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 значимых объектов критической информационной инфраструктуры или информационных ресурсов Российской Федерации, обязаны направить в НКЦКИ информацию о проводимых мероприятиях по их предупреждению.

10. В случае получения запроса, указанного в абзаце четвертом пункта 8 настоящего Порядка, субъект критической информационной инфраструктуры и руководитель органа (организации) 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.