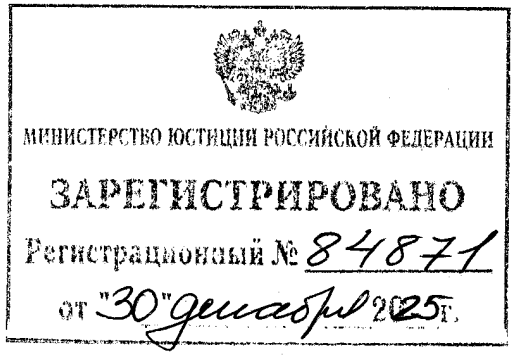
ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКАЗ

25 декабря 2025 года **Москва** **№** 547

Об утверждении Порядка 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»



В соответствии с пунктом 6 части 4 статьи 6, частью 6 статьи 9 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 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».

2. Признать утратившими силу приказы ФСБ России:

от 19 июня 2019 г. № 282 «Об утверждении Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации»[1];

от 7 июля 2022 г. № 348 «О внесении изменений в Порядок информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденный приказом ФСБ России от 19 июня 2019 г. № 282»[2].

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

Директор А.Бортников

[1] Зарегистрирован Минюстом России 16 июля 2019 г., регистрационный № 55284.
[2] Зарегистрирован Минюстом России 5 августа 2022 г., регистрационный № 69513.

Утвержден
приказом ФСБ России
от 25 декабря 2025г.
№ 547

Порядок
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»

1. Субъекты критической информационной инфраструктуры Российской Федерации[1] обязаны информировать ФСБ России обо всех компьютерных атаках и компьютерных инцидентах, реагировать на них и принимать меры по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры, принадлежащих им на праве собственности, аренды или ином законном основании.

Руководители государственных органов (за исключением органов внешней разведки Российской Федерации, органов государственной охраны, федерального органа обеспечения мобилизационной подготовки органов государственной власти Российской Федерации, федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации), государственных унитарных предприятий, государственных учреждений, государственных фондов, государственных корпораций (компаний), иных российских юридических лиц, которые, если иное

[1] Далее – критическая информационная инфраструктура.

не предусмотрено международным договором Российской Федерации, находятся под контролем Российской Федерации, и (или) субъекта Российской Федерации, и (или) контролируемых ими совместно или по отдельности лиц, в части информационных ресурсов Российской Федерации, принадлежащих таким органам и юридическим лицам на праве собственности, аренды или ином законном основании[1], обязаны информировать ФСБ России обо всех компьютерных атаках и компьютерных инцидентах, связанных с функционированием принадлежащих им информационных ресурсов Российской Федерации.

2. Информирование ФСБ России осуществляется путем направления информации в Национальный координационный центр по компьютерным инцидентам[2] в соответствии с определенными НКЦКИ форматами представления информации о компьютерных атаках и компьютерных инцидентах в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации[3] 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. В случае отсутствия подключения к данной технической инфраструктуре информирование ФСБ России субъектом критической информационной инфраструктуры, а также руководителем органа (организации) осуществляется посредством почтовой связи или электронной

---

[1] Далее – органы (организации). Часть 4 статьи 9 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

[2] Далее – НКЦКИ. Положение о Национальном координационном центре по компьютерным инцидентам утверждено 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).

[3] Подпункт 4.9 пункта 4 Положения о НКЦКИ.

связи по адресам НКЦКИ, указанным на официальном сайте в информационно-телекоммуникационной сети «Интернет» (www.cert.gov.ru).

3. Информация о компьютерном инциденте в значимом объекте критической информационной инфраструктуры направляется субъектами критической информационной инфраструктуры в НКЦКИ в срок не позднее 3 часов с момента обнаружения компьютерного инцидента, а в иных объектах критической информационной инфраструктуры – в срок не позднее 24 часов с момента его обнаружения.

Информация о компьютерном инциденте на информационном ресурсе Российской Федерации органа (организации) направляется руководителем этого органа (организации) в НКЦКИ в срок не позднее 24 часов с момента его обнаружения.

Информация о компьютерной атаке, проведенной в отношении объекта критической информационной инфраструктуры или информационного ресурса Российской Федерации органа (организации), направляется субъектом критической информационной инфраструктуры или руководителем органа (организации) в НКЦКИ в срок не позднее 24 часов с момента обнаружения компьютерной атаки.

4. В случае если компьютерная атака и (или) компьютерный инцидент связаны с функционированием объекта критической информационной инфраструктуры, принадлежащего на праве собственности, аренды или ином законном основании субъекту критической информационной инфраструктуры, который осуществляет деятельность в банковской сфере и в иных сферах финансового рынка, информация о компьютерной атаке и (или) компьютерном инциденте также направляется в Банк России с использованием технической инфраструктуры (автоматизированной системы) Банка России или резервного способа взаимодействия (при технической невозможности использования технической инфраструктуры (автоматизированной системы) Банка России в сроки, установленные пунктом 3 настоящего Порядка. Информация о технической инфраструктуре

(автоматизированной системе) Банка России или резервного способа взаимодействия размещается на официальном сайте Банка России в информационно-телекоммуникационной сети «Интернет».

5. Для подготовки к реагированию на компьютерные инциденты и принятию мер по ликвидации последствий компьютерных атак субъектом критической информационной инфраструктуры, которому на праве собственности, аренды или ином законном основании принадлежит значимый объект критической информационной инфраструктуры, в срок, не превышающий 90 календарных дней со дня включения данного объекта в реестр значимых объектов критической информационной инфраструктуры Российской Федерации[1] разрабатывается план реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак (далее – план реагирования), который должен содержать:

технические характеристики и состав значимых объектов критической информационной инфраструктуры;

события (условия), при наступлении которых начинается реализация предусмотренных планом реагирования мероприятий;

мероприятия, проводимые в ходе реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак, а также время, отводимое на их реализацию;

описание состава подразделений и должностных лиц субъекта критической информационной инфраструктуры, ответственных за проведение мероприятий по реагированию на компьютерные инциденты и принятию мер по ликвидации последствий компьютерных атак.

6. План реагирования утверждается руководителем субъекта критической информационной инфраструктуры, которому на праве

---

[1] Порядок ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации утвержден приказом ФСТЭК России от 6 декабря 2017 г. № 227 (зарегистрирован Минюстом России 8 февраля 2018 г., регистрационный № 49966), с изменениями, внесенными приказами ФСТЭК России от 10 февраля 2022 г. № 26 (зарегистрирован Минюстом России 1 апреля 2022 г., регистрационный № 68031), от 1 сентября 2023 г. № 177 (зарегистрирован Минюстом России 3 октября 2023 г., регистрационный № 75437) и от 17 июля 2025 г. № 254 (зарегистрирован Минюстом России 20 августа 2025 г., регистрационный № 83245).

собственности, аренды или ином законном основании принадлежат значимые объекты критической информационной инфраструктуры.

Копия утвержденного плана реагирования в срок, не превышающий 7 календарных дней со дня его утверждения, направляется в НКЦКИ.

7. В план реагирования могут включаться:

условия привлечения подразделений и должностных лиц ФСБ России к проведению мероприятий по реагированию на компьютерные инциденты и принятию мер по ликвидации последствий компьютерных атак;

порядок проведения субъектом критической информационной инфраструктуры, которому на праве собственности, аренды или ином законном основании принадлежат значимые объекты критической информационной инфраструктуры, мероприятий по реагированию на компьютерные инциденты и принятию мер по ликвидации последствий компьютерных атак в отношении значимых объектов критической информационной инфраструктуры совместно с привлекаемыми подразделениями и должностными лицами ФСБ России.

8. Проект плана реагирования, содержащий положения, предусмотренные пунктом 7 настоящего Порядка, и проект о внесении изменений в него разрабатываются субъектом критической информационной инфраструктуры при методическом обеспечении НКЦКИ[1] и до их утверждения направляются на согласование в Центр защиты информации и специальной связи ФСБ России.

Центром защиты информации и специальной связи ФСБ России проект плана реагирования или проект о внесении изменений в него рассматривается в срок до 30 календарных дней со дня поступления и по результатам рассмотрения при отсутствии замечаний согласовывается или возвращается без согласования для доработки.

9. В план реагирования, разрабатываемый субъектами критической информационной инфраструктуры, осуществляющими деятельность в банковской сфере и в иных сферах финансового рынка, которым на праве

[1] Подпункт 4.3 пункта 4 Положения о НКЦКИ.

собственности, аренды или ином законном основании принадлежат значимые объекты критической информационной инфраструктуры, помимо положений, указанных в пунктах 5 и 7 настоящего Порядка, могут включаться условия привлечения подразделений и должностных лиц Банка России к проведению мероприятий по реагированию на компьютерные инциденты и принятию мер по ликвидации последствий компьютерных атак.

Проект плана реагирования и проекты о внесении изменений в него разрабатываются субъектом критической информационной инфраструктуры, который осуществляет деятельность в банковской сфере и в иных сферах финансового рынка, и до их утверждения направляются в Банк России на согласование. После согласования Банком России и утверждения проекта плана реагирования или проекта о внесении изменений в него руководителем субъекта критической информационной инфраструктуры план реагирования или проект о внесении изменений в него направляется в НКЦКИ в соответствии с пунктом 6 настоящего Порядка.

В случае включения в проект плана реагирования или в проекты о внесении изменений в него положений, предусмотренных пунктом 7 настоящего Порядка, проект плана реагирования и проекты о внесении изменений в него до их утверждения направляются в Банк России исключительно после выполнения действий, предусмотренных пунктом 8 настоящего Порядка.

Банком России рассматривается проект плана реагирования или проект о внесении изменений в него в срок до 30 календарных дней со дня поступления и по результатам рассмотрения при отсутствии замечаний согласовывается или возвращается без согласования для доработки.

10. Субъект критической информационной инфраструктуры, которому на праве собственности, аренды или ином законном основании принадлежат значимые объекты критической информационной инфраструктуры, не реже одного раза в год обязан организовывать и проводить тренировки по отработке мероприятий плана реагирования. Объем и содержание тренировки

определяются субъектом критической информационной инфраструктуры исходя из мероприятий, содержащихся в плане реагирования.

Организация и проведение тренировок возлагаются на подразделения и должностных лиц субъекта критической информационной инфраструктуры, ответственных за проведение мероприятий по реагированию на компьютерные инциденты и принятию мер по ликвидации последствий компьютерных атак.

По результатам тренировок в план реагирования вносятся изменения в случае выявления недостатков, предусмотренных планом реагирования мероприятий.

11. Субъектом критической информационной инфраструктуры, которому на праве собственности, аренды или ином законном основании принадлежат значимые объекты критической информационной инфраструктуры, в ходе реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак осуществляются:

анализ компьютерных инцидентов (включая определение очередности реагирования на них), установление их связи с компьютерными атаками;

проведение мероприятий в соответствии с планом реагирования;

определение в соответствии с планом реагирования необходимости привлечения к реагированию на компьютерные инциденты и принятию мер по ликвидации последствий компьютерных атак подразделений и должностных лиц ФСБ России и Банка России.

12. В целях принятия мер по ликвидации последствий компьютерных атак субъектом критической информационной инфраструктуры, которому на праве собственности, аренды или ином законном основании принадлежат значимые объекты критической информационной инфраструктуры, определяются:

состав подразделений и должностных лиц, ответственных за проведение мероприятий по реагированию на компьютерные инциденты и принятию мер

по ликвидации последствий компьютерных атак, и их задачи в рамках принимаемых мер;

перечень средств, необходимых для принятия мер по ликвидации последствий компьютерных атак;

очередность значимых объектов критической информационной инфраструктуры (их структурных элементов), в отношении которых будут приниматься меры по ликвидации последствий компьютерных атак;

перечень мер по восстановлению функционирования значимого объекта критической информационной инфраструктуры.

13. В ходе ликвидации последствий компьютерных атак субъектом критической информационной инфраструктуры, которому на праве собственности, аренды или ином законном основании принадлежат значимые объекты критической информационной инфраструктуры, принимаются меры по восстановлению функционирования и проверке работоспособности значимого объекта критической информационной инфраструктуры.

14. Субъект критической информационной инфраструктуры, которому на праве собственности, аренды или ином законном основании принадлежат значимые объекты критической информационной инфраструктуры, обязан информировать НКЦКИ в срок не позднее 48 часов после завершения мероприятий по реагированию на компьютерные инциденты и принятию мер по ликвидации последствий компьютерных атак о результатах таких мероприятий в соответствии с пунктом 2 настоящего Порядка.

Субъекты критической информационной инфраструктуры, которым на праве собственности, аренды или ином законном основании принадлежат значимые объекты критической информационной инфраструктуры, осуществляющие деятельность в банковской сфере и в иных сферах финансового рынка, наряду с НКЦКИ, обязаны информировать о результатах мероприятий по реагированию на компьютерные инциденты и принятию мер по ликвидации последствий компьютерных атак Банк России в срок не позднее

48 часов после завершения таких мероприятий в соответствии с пунктом 4 настоящего Порядка.

15. Органами (организациями) в ходе реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак, связанных с функционированием принадлежащих им информационных ресурсов Российской Федерации, осуществляются анализ компьютерных инцидентов (включая определение очередности реагирования на них), установление их связи с компьютерными атаками, а также оценивается необходимость привлечения к реагированию на компьютерные инциденты и принятию мер по ликвидации последствий компьютерных атак подразделений и должностных лиц ФСБ России.

Информацию о результатах реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак, связанных с функционированием принадлежащих органам (организациям) информационных ресурсов Российской Федерации, органы (организации) в течение 24 часов с момента окончания мероприятий по реагированию на компьютерные инциденты и принятию мер по ликвидации компьютерных атак направляют в НКЦКИ в соответствии с пунктом 2 настоящего Порядка.

16. Органы (организации) в целях принятия мер по ликвидации последствий компьютерных атак, связанных с функционированием принадлежащих им информационных ресурсов Российской Федерации, обязаны определить состав подразделений и должноетных лиц, ответственных за проведение мероприятий по реагированию на компьютерные инциденты и принятию мер по ликвидации последствий компьютерных атак, их задачи в рамках принимаемых мер, очередность информационных ресурсов Российской Федерации (их структурных элементов), в отношении которых будут приниматься меры по ликвидации последствий компьютерных атак, перечень мер по восстановлению функционирования информационного ресурса Российской Федерации и направить указанную информацию в НКЦКИ в соответствии с пунктом 2 настоящего Порядка.

17. Органы (организации) после ликвидации последствий компьютерных атак и принятия мер по восстановлению функционирования и проверке работоспособности информационных ресурсов Российской Федерации обязаны информировать об этом НКЦКИ в течение 24 часов с момента завершения таких мер в соответствии с пунктом 2 настоящего Порядка.