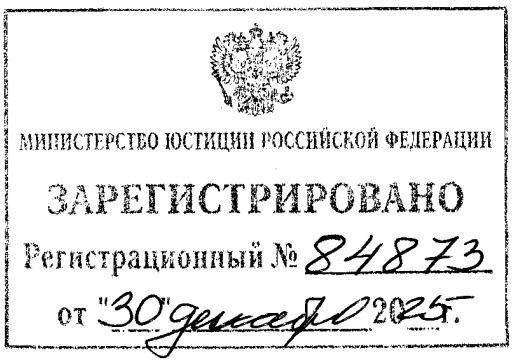
ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКАЗ

26 декабря 2025 года **Москва** **№** 553

Об утверждении Порядка и Технических условий установки и эксплуатации средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, в том числе средств, предназначенных для поиска признаков компьютерных атак, за исключением средств, предназначенных для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры Российской Федерации



В соответствии с пунктом 10 части 4 статьи 6 и частью 5 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»

ПРИКАЗЫВАЮ:

1. Утвердить:

1.1. Порядок установки и эксплуатации средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, в том числе средств, предназначенных для поиска признаков компьютерных атак, за исключением средств, предназначенных для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры Российской Федерации (приложение № 1 к настоящему приказу).

1.2. Технические условия установки и эксплуатации средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, в том числе средств, предназначенных для поиска признаков компьютерных атак, за исключением средств, предназначенных для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры Российской Федерации (приложение № 2 к настоящему приказу).

2. Признать утратившим силу приказ ФСБ России от 19 июня 2019 г. № 281 «Об утверждении Порядка, технических условий установки и эксплуатации средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, за исключением средств, предназначенных для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры Российской Федерации»[1].

Директор А.Бортников

[1] Зарегистрирован Минюстом России 16 июля 2019 г., регистрационный № 55285.

Приложение № 1
к приказу ФСБ России
от 26 декабря 2025 г.
№ 553

Порядок
установки и эксплуатации средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, в том числе средств, предназначенных для поиска признаков компьютерных атак, за исключением средств, предназначенных для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры Российской Федерации

I. Установка и эксплуатация средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты

1. Установка и эксплуатация средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты (далее – средства ГосСОПКА), в том числе в банковской сфере и в иных сферах финансового рынка, включают:

определение необходимости установки средств ГосСОПКА, требуемых субъекту критической информационной инфраструктуры Российской Федерации (далее – КИИ) или органу, организации, указанным в части 4 статьи 9 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (далее – орган (организация);

установку, настройку, проверку работоспособности и подключение средств ГосСОПКА к информационным ресурсам субъекта КИИ или органа (организации);

обеспечение непрерывной работы средств ГосСОПКА.

2. Субъект КИИ или орган (организация) должен самостоятельно определить состав средств ГосСОПКА, необходимых ему для полноценного выполнения мероприятий по обнаружению, предупреждению, ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты в отношении принадлежащих ему информационных ресурсов.

3. Субъект КИИ или орган (организация) должен обеспечить установку в принадлежащих ему информационных ресурсах средств ГосСОПКА, соответствующих требованиям к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, в том числе к средствам, предназначенным для поиска признаков компьютерных атак, устанавливаемым федеральным органом исполнительной власти, уполномоченным в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (далее – ГосСОПКА), на основании пункта 9 части 4 статьи 6 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

4. Установка, настройка, проверка работоспособности и подключение средств ГосСОПКА к информационным ресурсам проводятся субъектом КИИ или органом (организацией) самостоятельно либо с привлечением аккредитованного центра ГосСОПКА или организации, имеющей соглашение с ФСБ России (Национальным координационным центром по компьютерным инцидентам (далее – НКЦКИ) о сотрудничестве (взаимодействии) в области обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты[1].

---

[1] Подпункт «г» пункта 1 Указа Президента Российской Федерации от 1 мая 2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации».

Проведение указанных мероприятий не должно приводить к нарушению функционирования информационных ресурсов субъекта КИИ или органа (организации).

5. В течение 15 календарных дней со дня завершения мероприятий, указанных в пункте 4 настоящего Порядка, субъект КИИ или орган (организация) должен проинформировать об этом НКЦКИ с представлением перечня используемых средств ГосСОПКА.

Субъект КИИ или орган (организация), который осуществляет деятельность в банковской сфере и в иных сферах финансового рынка, дополнительно должен проинформировать в указанный срок Банк России.

6. В случае если по результатам рассмотрения представленной субъектом КИИ или органом (организацией) информации, указанной в пункте 5 настоящего Порядка, НКЦКИ будут обнаружены нарушения выполнения пунктов 3 и 4 настоящего Порядка, НКЦКИ в течение 30 календарных дней со дня получения указанной информации должен направить субъекту КИИ или органу (организации) замечания.

7. Субъект КИИ или орган (организация) должен устранить полученные от НКЦКИ замечания и направить информацию об этом в НКЦКИ в срок, не превышающий 30 календарных дней со дня получения замечаний.

8. Обеспечение непрерывной работы средств ГосСОПКА осуществляется в целях обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, реагирования на компьютерные инциденты и осуществления непрерывного взаимодействия с ГосСОПКА.

9. Субъект КИИ или орган (организация) должен обеспечить круглосуточную и бесперебойную работу средств ГосСОПКА, а также определить порядок доступа к этим средствам и осуществления контроля за их применением.

II. Установка и эксплуатация средств, предназначенных для поиска признаков компьютерных атак, за исключением средств, предназначенных для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов КИИ

10. Установка и эксплуатация средств, предназначенных для поиска признаков компьютерных атак, за исключением средств, предназначенных для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов КИИ (далее – средства ППКА), в том числе в банковской сфере и в иных сферах финансового рынка, включают:

определение необходимости установки средств ППКА;

установку средств ППКА, их подключение к каналам связи, необходимым для управления и получения информации от средств ППКА;

прием в эксплуатацию средств ППКА;

обеспечение непрерывной работы средств ППКА;

проведение технического обслуживания, замену и демонтаж средств ППКА;

обеспечение сохранности средств ППКА;

осуществление мониторинга функционирования средств ППКА.

11. Необходимость установки средств ППКА на информационные ресурсы субъекта КИИ или органа (организации) определяется ФСБ России в соответствии с пунктом 8 части 4 статьи 6 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

12. Для установки средств ППКА ФСБ России должна направить субъекту КИИ или органу (организации) следующую информацию и документы:

уведомление о необходимости установки средств ППКА на информационные ресурсы субъекта КИИ или органа (организации) в целях их устойчивого функционирования при проведении в их отношении компьютерных атак;

условия для размещения средств ППКА;

фамилия, имя, отчество (при наличии) представителя ФСБ России или наименование структурного подразделения ФСБ России, ответственного за организацию работ;

проект регламента взаимодействия по вопросам обнаружения, предупреждения и ликвидации последствий компьютерных атак (далее – регламент).

13. Субъект КИИ или орган (организация) не позднее 10 календарных дней с даты получения уведомления, предусмотренного пунктом 12 настоящего Порядка, должен определить должностных лиц, ответственных за организацию взаимодействия по вопросам обнаружения, предупреждения и ликвидации последствий компьютерных атак.

14. Субъект КИИ или орган (организация) в срок не более 30 календарных дней с даты получения информации, предусмотренной пунктом 12 настоящего Порядка, должен направить в ФСБ России:

согласованный проект регламента;

информацию об информационных ресурсах, включающую описание инфраструктуры, хостов, подсистем, сервисов, доменных имен, средств защиты информации, телекоммуникационного оборудования и его настроек, а также правила межсетевого экранирования;

структурно-функциональную схему информационных ресурсов;

информационно-алгоритмическую модель информационных ресурсов, включающую правила доступа к подсистемам и сервисам, маршрутизацию пользователей, распределение пользователей по подсетям, наличие и расположение контроллера доменов, наличие и расположение сервисов авторизации пользователей, наличие виртуальных сетей и их маршрутизацию, наличие удаленного доступа к подсистемам и сервисам.

15. ФСБ России в течение 45 календарных дней со дня получения документов и информации, предусмотренных пунктом 14 настоящего Порядка, должна определить места установки средств ППКА и направить

субъекту КИИ или органу (организации) утвержденный руководством Центра защиты информации и специальной связи ФСБ России регламент с указанием мест установки средств ППКА или запросить дополнительную информацию, необходимую для определения мест установки средств ППКА.

16. Субъект КИИ или орган (организация) в течение 30 календарных дней со дня получения утвержденного регламента должен направить уведомление в ФСБ России о сроке подготовки своих информационных ресурсов для установки средств ППКА в соответствии со структурно-функциональной схемой информационных ресурсов. Указанный срок не должен превышать 6 месяцев со дня направления уведомления, предусмотренного настоящим пунктом.

17. Установка средств ППКА осуществляется силами и средствами ФСБ России на безвозмездной основе.

18. Прием в эксплуатацию средств ППКА осуществляется после выполнения требований пунктов 12 – 16 настоящего Порядка назначенной субъектом КИИ или органом (организацией) комиссией по приему средств ППКА в эксплуатацию (далее – комиссия). В состав комиссии включаются сотрудники субъекта КИИ или органа (организации) и представители ФСБ России (по согласованию).

19. В ходе приема в эксплуатацию средств ППКА проверяются технические условия установки и эксплуатации средств ППКА, предусмотренные приложением № 2 к настоящему приказу.

20. По результатам приема в эксплуатацию средств ППКА в соответствии с пунктом 19 настоящего Порядка оформляется акт приема средств ППКА в эксплуатацию, в котором указываются:

наименование информационного ресурса;

дата приемки средств ППКА в эксплуатацию;

фамилии, имена, отчества (при наличии) и должности членов комиссии;

состав и серийные номера средств ППКА;

результат проверки выполнения технических условий установки и эксплуатации средств ППКА;

реквизиты утвержденного регламента.

21. Акт приема средств ППКА в эксплуатацию подписывается всеми членами комиссии и хранится у субъекта КИИ или органа (организации). Копия указанного акта направляется в ФСБ России в течение 7 календарных дней со дня его оформления.

Субъект КИИ или орган (организация), который осуществляет деятельность в банковской сфере и в иных сферах финансового рынка, дополнительно должен направить копию акта приема средств ППКА в эксплуатацию в указанный срок в Банк России.

22. Субъект КИИ или орган (организация) должен обеспечить непрерывную работу своей информационной инфраструктуры для корректной работы средств ППКА.

23. Эксплуатация средств ППКА осуществляется ФСБ России.

24. Непрерывность функционирования в круглосуточном режиме и сохранность средств ППКА обеспечиваются субъектом КИИ или органом (организацией) самостоятельно путем соблюдения технических условий установки и эксплуатации средств ППКА, предусмотренных приложением № 2 к настоящему приказу.

25. Техническое обслуживание средств ППКА проводится ФСБ России.

26. Субъект КИИ или орган (организация) не менее чем за 7 календарных дней до дня начала проведения в своей информационной инфраструктуре плановых работ, которые могут повлечь нарушение функционирования средств ППКА, должен уведомить ФСБ России о сроках и продолжительности проведения указанных плановых работ.

27. Замена средств ППКА осуществляется ФСБ России в случае нарушения их функционирования или необходимости их модернизации.

28. После замены средств ППКА осуществляется их прием в эксплуатацию в соответствии с пунктами 18 – 21 настоящего Порядка.

29. Демонтаж средств ППКА проводится ФСБ России в случае необходимости изменения мест установки средств ППКА, в связи с реорганизацией, ликвидацией или прекращением деятельности субъекта КИИ или органа (организации), или по решению ФСБ России.

30. В случае необходимости изменения мест установки средств ППКА демонтаж средств ППКА должен проводиться после выполнения мероприятий, предусмотренных пунктами 12 – 21 настоящего Порядка.

31. Демонтаж средств ППКА в связи с реорганизацией, ликвидацией или прекращением деятельности субъекта КИИ или органа (организации) проводится в сроки, согласованные с ФСБ России, но не позднее чем за 45 календарных дней до дня завершения реорганизации, ликвидации или прекращения деятельности субъекта КИИ или органа (организации).

32. Демонтаж средств ППКА по решению ФСБ России проводится в срок, не превышающий 30 календарных дней со дня уведомления субъекта КИИ или органа (организации) о принятии такого решения.

33. По результатам демонтажа средств ППКА ФСБ России и субъект КИИ или орган (организация) должны составить акт о демонтаже средств ППКА в двух экземплярах, по одному для каждой из сторон, в котором указываются:

полное наименование субъекта КИИ или органа (организации);

дата демонтажа средств ППКА;

фамилия, имя, отчество (при наличии) представителя ФСБ России и субъекта КИИ или органа (организации);

места установки средств ППКА (адрес, помещение), в отношении которых проведен демонтаж;

состав и серийные номера средств ППКА, в отношении которых проведен демонтаж;

реквизиты утвержденного регламента.

34. Мониторинг функционирования средств ППКА осуществляется ФСБ России в круглосуточном режиме.

Приложение № 2
к приказу ФСБ России
от 26 декабря 2025 г.
№ 553

Технические условия
установки и эксплуатации средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, в том числе средств, предназначенных для поиска признаков компьютерных атак, за исключением средств, предназначенных для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры Российской Федерации

1. Технические условия установки и эксплуатации средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты (далее – средства ГосСОПКА), в том числе в банковской сфере и в иных сферах финансового рынка, включают:

выполнение требований эксплуатационной документации к средствам ГосСОПКА;

обеспечение разграничения и контроля доступа к средствам ГосСОПКА;

обеспечение бесперебойным электропитанием средств ГосСОПКА, позволяющим в случаях аварийного отключения электроэнергии поддерживать работу средств ГосСОПКА в текущем режиме или осуществить правильное (корректное) завершение их работы с реализацией функции автоматического оповещения лиц, ответственных за эксплуатацию средств ГосСОПКА.

2. Технические условия установки и эксплуатации средств, предназначенных для поиска признаков компьютерных атак, за исключением средств, предназначенных для поиска признаков компьютерных атак в сетях

электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры Российской Федерации (далее – средства ППКА), в том числе в банковской сфере и в иных сферах финансового рынка, включают:

определение места для установки и непрерывной эксплуатации средств ППКА в круглосуточном режиме;

контроль и ограничение физического доступа персонала к средствам ППКА в целях обеспечения их сохранности;

выделение маршрутизируемых IP-адресов и подключение средств ППКА к каналам связи, необходимым ФСБ России для управления и обмена данными со средствами ППКА;

подключение средств ППКА к линиям связи, за исключением сетей электросвязи, через которые осуществляется взаимодействие объектов критической информационной инфраструктуры Российской Федерации;

обеспечение бесперебойным электропитанием средств ППКА, позволяющим в случаях аварийного отключения электроэнергии поддерживать работу средств ППКА в текущем режиме или осуществить правильное (корректное) завершение их работы с реализацией функции автоматического оповещения лиц, ответственных за эксплуатацию средств ППКА;

поддержание температуры и влажности воздуха, в пределах которых может осуществляться эксплуатация средств ППКА (в соответствии с эксплуатационной документацией на средства ППКА).