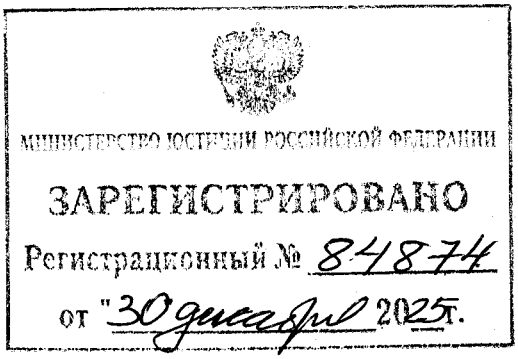
ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКАЗ

26 декабря 2025 года **Москва** **№** 554

Об установлении Требований 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



В соответствии с пунктом 9 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. Установить Требования 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, согласно приложению к настоящему приказу.

2. Признать утратившим силу приказ ФСБ России от 6 мая 2019 г. № 196 «Об утверждении Требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты»[1].

Директор А.Бортников

[1] Зарегистрирован Минюстом России 31 мая 2019 г., регистрационный № 54801.

Приложение
к приказу ФСБ России
от 26 декабря 2025 г.
№ 554

Требования
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

I. Общие положения

1. Настоящие Требования предъявляются к техническим, программным, программно-аппаратным и иным средствам для обнаружения (в том числе для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры Российской Федерации (далее – КИИ), предупреждения, ликвидации последствий компьютерных атак и (или) обмена информацией, необходимой субъектам КИИ и иным не являющимся субъектами КИИ органам и организациям (далее – органы (организации) при обнаружении, предупреждении и (или) ликвидации последствий компьютерных атак, а также средствам криптографической защиты такой информации, в том числе средствам, предназначенным для поиска признаков компьютерных атак (далее – средства ГосСОПКА).

2. Требования предъявляются к следующим средствам ГосСОПКА[1]:

техническим, программным, программно-аппаратным и иным средствам для обнаружения компьютерных атак (далее – средства обнаружения);

---

[1] Часть 3 статьи 5 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

техническим, программным, программно-аппаратным и иным средствам для предупреждения компьютерных атак (далее – средства предупреждения);

техническим, программным, программно-аппаратным и иным средствам для ликвидации последствий компьютерных атак (далее – средства ликвидации последствий);

техническим, программным, программно-аппаратным и иным средствам поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов КИИ (далее – средства ППКА в сетях электросвязи);

средствам, предназначенным для поиска признаков компьютерных атак (далее – средства ППКА);

техническим, программным, программно-аппаратным и иным средствам обмена информацией, необходимой субъектам КИИ и органам (организациям) при обнаружении, предупреждении и (или) ликвидации последствий компьютерных атак (далее – средства обмена);

средствам криптографической защиты информации, необходимой субъектам КИИ и органам (организациям) при обнаружении, предупреждении и (или) ликвидации последствий компьютерных атак.

3. Средства ГосСОПКА реализуются в том числе одним или несколькими техническими, программными и программно-аппаратными средствами.

II. Требования к средствам ГосСОПКА

4. Средства ГосСОПКА должны быть произведены, обеспечены гарантийной и технической поддержкой, модернизироваться исключительно российскими юридическими лицами, не находящимися под прямым или косвенным контролем иностранных физических лиц и (или) юридических лиц.

5. В средствах ГосСОПКА должна быть исключена возможность удаленного управления со стороны лиц, не являющихся работниками субъекта КИИ, органа (организации) и (или) работниками привлекаемого в соответствии с законодательством Российской Федерации аккредитованного центра государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (далее – ГосСОПКА) или организации, осуществляющей лицензируемую деятельность в области защиты информации.

6. В средствах ГосСОПКА должна быть исключена возможность несанкционированной передачи обрабатываемой информации лицам, не являющимся работниками субъекта КИИ, органа (организации) и (или) работниками привлекаемого в соответствии с законодательством Российской Федерации аккредитованного центра ГосСОПКА или организации, осуществляющей лицензируемую деятельность в области защиты информации.

В случае наличия в средствах ГосСОПКА функций мониторинга пользовательской активности, предусмотренных производителем, данные функции должны реализовывать возможность принудительного отключения пользователем.

7. В средствах ГосСОПКА должны быть реализованы функции безопасности в соответствии с главой IX настоящих Требований.

III. Требования к средствам обнаружения

8. Средства обнаружения должны реализовывать следующие функции:

сбор и первичная обработка событий, связанных с нарушением информационной безопасности (далее – события ИБ), поступающих от операционных систем, средств и систем защиты информации и систем мониторинга, в том числе от средств обнаружения вторжений, межсетевых экранов, средств предотвращения утечек данных, антивирусного

программного обеспечения (далее – ПО), телекоммуникационного оборудования, прикладных сервисов, средств контроля (анализа) защищенности, средств управления телекоммуникационным оборудованием и сетями связи, систем мониторинга состояния телекоммуникационного оборудования, систем мониторинга качества обслуживания (далее – источники событий ИБ);

автоматический анализ событий ИБ и выявление компьютерных инцидентов;

повторный анализ ранее зарегистрированных событий ИБ и выявление на основе такого анализа не обнаруженных ранее компьютерных инцидентов.

9. Для осуществления сбора и первичной обработки событий ИБ в средствах обнаружения должна быть реализована возможность:

удаленного и (или) локального сбора событий ИБ;

сбора событий ИБ в непрерывном режиме функционирования либо по расписанию, в случае потери связи с источниками событий ИБ – сразу после ее восстановления;

обработки поступающих событий ИБ и сохранение результатов их обработки;

сохранения информации о событиях ИБ, в том числе в исходном виде;

сбора информации непосредственно от источников событий ИБ, из файлов либо посредством агентов, размещенных на отдельных источниках событий ИБ;

встроенной поддержки различных источников событий ИБ и разработки дополнительных модулей, посредством использования которых должно обеспечиваться получение информации от новых источников событий ИБ.

10. Для осуществления автоматического анализа событий ИБ и выявления компьютерных инцидентов в средствах обнаружения должна быть реализована возможность:

отбора и фильтрации событий ИБ;

выявления последовательностей разнородных событий ИБ, имеющих логическую связь, которые могут быть значимы для выявления возможных нарушений безопасности информации (корреляция), и объединения однородных данных о событиях ИБ (агрегация);

выявления компьютерных инцидентов, регистрации методов (способов) их обнаружения;

корреляции для распределенных по времени и (или) месту возникновения событий ИБ;

корреляции для последовательности событий ИБ;

просмотра и редактирования правил корреляции, а также для обновления и загрузки новых правил;

автоматического назначения приоритетов событиям ИБ на основании задаваемых пользователем показателей.

11. Для осуществления повторного анализа ранее зарегистрированных событий ИБ и выявления на основе такого анализа не обнаруженных ранее компьютерных инцидентов в средствах обнаружения должна быть реализована возможность:

выявления связей и зависимостей между событиями ИБ, зарегистрированными в установленном интервале времени, и вновь появившейся любой дополнительной информацией, позволяющей идентифицировать контролируемые информационные ресурсы (далее – справочная информация);

выявления связей и зависимостей между событиями ИБ, зарегистрированными в установленном пользователем интервале времени, и новыми или измененными методами (способами) выявления компьютерных инцидентов;

выявления связей и зависимостей между событиями ИБ и полученными ранее сведениями о контролируемых информационных ресурсах и (или) состоянии защищенности;

настройки параметров проводимого анализа;

проведения поиска не обнаруженных ранее компьютерных инцидентов с использованием новых методов (способов) выявления компьютерных инцидентов;

хранения агрегированных событий ИБ не менее 6 месяцев.

12. Средства обнаружения должны иметь сертификат соответствия требованиям ФСБ России к средствам обнаружения компьютерных атак, разрабатываемым в соответствии с пунктом 1.4 Положения о системе сертификации средств защиты информации по требованиям безопасности для сведений, составляющих государственную тайну (система сертификации СЗИ-ГТ), утвержденного приказом ФСБ России от 13 ноября 1999 г. № 564[1].

IV. Требования к средствам предупреждения

13. Средства предупреждения должны реализовывать следующие функции:

сбор и обработка сведений об уязвимостях и недостатках в настройке ПО, а также справочной информации;

поддержка статистической и аналитической обработки получаемой информации;

формирование рекомендаций по минимизации угроз безопасности информации.

14. Для осуществления сбора и обработки сведений об уязвимостях и недостатках в настройке ПО, а также справочной информации в средствах предупреждения должна быть реализована возможность сбора и обработки следующих сведений:

о потенциальных и известных уязвимостях и недостатках в настройке ПО;

об индикаторах компрометации;

о вредоносном ПО;

---

[1] Зарегистрирован Минюстом России 27 декабря 1999 г., регистрационный № 2028.

о показателе доверия (репутации) сетевых адресов, доменных имен, серверов электронной почты, серверов доменных имен;

о владельцах сетевых адресов, доменных имен, серверов электронной почты, серверов доменных имен;

о местоположении и географической принадлежности сетевых адресов;

о компьютерных сетях, состоящих из управляемых с использованием вредоносного ПО средств вычислительной техники, включая сведения об их управляющих серверах;

об инструментах, о тактиках, техниках и процедурах проведения компьютерных атак.

15. Для поддержки статистической и аналитической обработки получаемой информации в средствах предупреждения должна быть реализована возможность:

анализа и агрегации сведений, предусмотренных пунктом 14 настоящих Требований;

корреляции событий ИБ и визуализации корреляционных связей в форме графов;

установления степени доверия к источникам сведений, предусмотренных пунктом 14 настоящих Требований, а также контроля их актуальности.

16. Для формирования рекомендаций по минимизации угроз безопасности информации в средствах предупреждения должна быть реализована возможность вывода пользователю перечня актуальных мер, направленных на устранение уязвимостей и недостатков в настройке ПО, используемого в контролируемых информационных ресурсах, а также мер, направленных на снижение негативных последствий реализации угроз безопасности информации.

17. При реализации своих функций в средствах предупреждения должны быть реализованы:

поддержка актуальности предоставляемых данных путем проверки наличия обновлений в источниках сведений, предусмотренных пунктом 14

настоящих Требований, не реже одного раза в 24 часа и загрузки таких обновлений при их наличии;

поддержка структурированной передачи данных киберразведки;

возможность интеграции и обмена информацией со средствами обнаружения и средствами ликвидации последствий, а также наличие программного интерфейса приложений (API).

V. Требования к средствам ликвидации последствий

18. Средства ликвидации последствий должны реализовывать следующие функции:

учет и обработка компьютерных инцидентов;

управление процессами реагирования на компьютерные инциденты и ликвидации последствий компьютерных атак;

взаимодействие с Национальным координационным центром по компьютерным инцидентам (далее – НКЦКИ) посредством использования технической инфраструктуры НКЦКИ, предназначенной для отправки, получения, обработки и хранения уведомлений и запросов в рамках информационного взаимодействия с субъектами КИИ, а также с иными не являющимися субъектами КИИ органами и организациями, в том числе иностранными и международными[1];

информационно-аналитическое сопровождение пользователей.

19. Для осуществления учета и обработки компьютерных инцидентов в средствах ликвидации последствий должна быть реализована возможность:

создания и изменения формализованных описаний (далее – карточка) компьютерных инцидентов, определения типов компьютерных инцидентов, определения состава полей карточек компьютерных инцидентов и требований к их заполнению в соответствии с типом компьютерного инцидента;

---

[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).

автоматического создания карточки компьютерного инцидента на основе уведомления об угрозе безопасности информации либо при выявлении события ИБ, в котором содержатся признаки компьютерных атак для контролируемых информационных ресурсов;

формирования записи о текущей стадии процесса реагирования на компьютерные инциденты (стадия приема сообщения о компьютерном инциденте, стадия сбора первичных сведений о компьютерном инциденте, стадия локализации компьютерного инцидента, стадия сбора сведений для расследования компьютерного инцидента) в зависимости от типа компьютерного инцидента;

формирования записи о присвоении категории опасности и (или) определения приоритетов компьютерных инцидентов на основе критериев, задаваемых по значениям полей карточек компьютерных инцидентов;

регистрации и учета карточек компьютерных инцидентов;

фильтрации, сортировки и поиска карточек компьютерных инцидентов по значениям полей карточек;

объединения карточек компьютерных инцидентов на основе критериев, применяемых к значениям полей карточек.

20. Для обеспечения управления процессами реагирования на компьютерные инциденты и ликвидации последствий компьютерных атак в средствах ликвидации последствий должна быть реализована возможность:

включения в карточку компьютерного инцидента дополнительных сведений, связанных с компьютерным инцидентом и зарегистрированных в процессе реагирования на компьютерный инцидент и ликвидации последствий компьютерной атаки, в том числе сообщений пользователей контролируемых информационных ресурсов, сведений о предпринятых действиях, технических данных, необходимых для расследования обстоятельств компьютерного инцидента;

назначения для карточки компьютерного инцидента инструкций по реагированию на компьютерный инцидент, а также задания правил их применимости на основании сведений о компьютерном инциденте;

формирования электронных сообщений для организации взаимодействия и координации действий по реагированию на компьютерные инциденты и ликвидации последствий компьютерных атак.

21. Для взаимодействия с НКЦКИ в средствах ликвидации последствий должна быть реализована возможность:

автоматизированного обмена информацией о компьютерных атаках и компьютерных инцидентах в соответствии с определенными НКЦКИ форматами представления информации о компьютерных атаках и компьютерных инцидентах в ГосСОПКА[1];

автоматизированного получения в соответствии с определенными НКЦКИ форматами представления информации об угрозах безопасности информации, в том числе о признаках компьютерных инцидентов;

учета карточек компьютерных инцидентов в соответствии с идентификацией НКЦКИ.

22. При осуществлении информационно-аналитического сопровождения средства ликвидации последствий должны реализовывать формирование выборок данных, основанных на значениях полей карточек компьютерных инцидентов, уведомлений об актуальных угрозах безопасности информации и справочной информации.

VI. Требования к средствам ППКА в сетях электросвязи

23. Средства ППКА в сетях электросвязи должны реализовывать следующие функции:

обнаружение признаков компьютерных атак в сети электросвязи по значениям служебных полей протоколов сетевого взаимодействия, а также осуществление сбора, накопления и статистической обработки результатов такого обнаружения;

обнаружение в сети электросвязи признаков управления телекоммуникационным оборудованием;

---

[1] Подпункт 4.9 пункта 4 Положения о НКЦКИ.

обнаружение изменений параметров настроек телекоммуникационного оборудования сети электросвязи;

обнаружение изменений параметров настроек систем управления телекоммуникационным оборудованием и сетями электросвязи;

хранение копий сетевого трафика, в котором были обнаружены признаки компьютерных атак в сети электросвязи и (или) признаки управления телекоммуникационным оборудованием, не менее 6 месяцев;

анализ и экспорт фрагментов копий сетевого трафика, в котором были обнаружены признаки компьютерных атак в сети электросвязи и (или) признаки управления телекоммуникационным оборудованием;

уведомление о фактах обнаружения признаков компьютерных атак в сети электросвязи и (или) признаков управления телекоммуникационным оборудованием;

уведомление о фактах нарушения режимов функционирования средства ППКА в сетях электросвязи;

возможность формирования информации, предусмотренной пунктом 5 Перечня информации, представляемой в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, утвержденного приказом ФСБ России от 24 июля 2018 г. № 367[1].

24. В средствах ППКА должен быть предусмотрен интерфейс (интерфейсы) передачи фрагментов копий сетевого трафика, в котором обнаружены признаки компьютерных атак в сети электросвязи и (или) признаки управления телекоммуникационным оборудованием, а также результатов сбора, накопления и статистической обработки такой информации.

VII. Требования к средствам ППКА

25. Средства ППКА должны реализовывать следующие функции:

обнаружение признаков компьютерных атак по значениям служебных

[1] Зарегистрирован Минюстом России 6 сентября 2018 г., регистрационный № 52108.

полей протоколов сетевого взаимодействия, а также осуществление сбора, накопления и статистической обработки результатов такого обнаружения;

хранение копий сетевого трафика, в котором были обнаружены признаки компьютерных атак, не менее 7 календарных дней;

анализ и экспорт фрагментов копий сетевого трафика, в котором были обнаружены признаки компьютерных атак;

уведомление о фактах обнаружения признаков компьютерных атак;

уведомление о фактах нарушения режимов функционирования средств ППКА;

наличие интерфейса (интерфейсов) передачи фрагментов копий сетевого трафика, в котором обнаружены признаки компьютерных атак;

получение информации об индикаторах компрометации от ГосСОПКА в целях их применения для обнаружения признаков компьютерных атак.

26. Средства ППКА должны иметь сертификат соответствия требованиям ФСБ России к средствам обнаружения компьютерных атак, разрабатываемым в соответствии с пунктом 1.4 Положения о системе сертификации средств защиты информации по требованиям безопасности для сведений, составляющих государственную тайну (система сертификации СЗИ-ГТ), утвержденного приказом ФСБ России от 13 ноября 1999 г. № 564.

VIII. Требования к средствам обмена и средствам криптографической защиты информации, необходимой субъектам КИИ и органам (организациям) при обнаружении, предупреждении и (или) ликвидации последствий компьютерных атак

27. В средствах обмена должна быть реализована возможность передачи, приема и обеспечена целостность при передаче и приеме информации, необходимой субъектам КИИ и органам (организациям) при обнаружении, предупреждении и (или) ликвидации последствий компьютерных атак.

28. Средства криптографической защиты информации, необходимой субъектам КИИ и органам (организациям) при обнаружении,

предупреждении и (или) ликвидации последствий компьютерных атак, должны быть сертифицированы ФСБ России[1].

IX. Требования к средствам ГосСОПКА в части реализации функций безопасности

29. В средствах ГосСОПКА в части реализации функций безопасности должны быть реализованы:

идентификация и аутентификация пользователей;

разграничение прав доступа к информации и функциям;

регистрация событий ИБ;

обновление программных компонентов и служебных баз данных;

резервирование и восстановление своей работоспособности;

синхронизация системного времени и корректировка временных значений (корректировка настроек часовых поясов);

контроль целостности ПО.

30. При осуществлении идентификации и аутентификации пользователей в средствах ГосСОПКА должны быть реализованы:

аутентификация пользователей с использованием паролей (в том числе временного действия) и (или) аппаратных средств аутентификации;

возможность хранения паролей в шифрованном или хешированном виде;

автоматическое информирование о необходимости смены паролей.

31. При осуществлении разграничения прав доступа к информации и функциям в средствах ГосСОПКА должны быть реализованы:

поддержка функций создания, редактирования и удаления пользовательских ролей и возможность настройки прав доступа для каждой роли;

возможность блокирования сессии доступа при превышении задаваемого значения временного периода отсутствия активности;

---

[1] Подпункт 21 пункта 9 Положения о Федеральной службе безопасности Российской Федерации, утвержденного Указом Президента Российской Федерации от 11 августа 2003 г. № 960.

возможность блокирования и повторной активации учетных записей;

формирование уведомлений о неудачных попытках доступа к управлению средствами ГосСОПКА;

запись всех действий пользователей с момента авторизации в электронный журнал.

32. При осуществлении регистрации событий ИБ в средствах ГосСОПКА должны быть реализованы:

возможность определения перечня событий ИБ, подлежащих регистрации, и хранения соответствующих записей в электронных журналах с возможностью корректировки сроков;

возможность регистрации следующих связанных с функционированием средств ГосСОПКА сведений: идентификатора пользователя, времени авторизации, запуска (завершения) программ и процессов, связанных с реализацией функций безопасности средств ГосСОПКА, команды управления, неудачных попыток аутентификации, данных о сбоях и неисправностях в работе средств ГосСОПКА;

ведение электронных журналов учета технического состояния, содержащих следующие поля: информация о состоянии интерфейсов (портов), информация об ошибках в работе средств ГосСОПКА с их классификацией, информация о загрузке и инициализации средств ГосСОПКА и их остановке (для средств ППКА в сетях электросвязи);

защита электронных журналов от редактирования и удаления содержащейся в них информации (для средств ППКА в сетях электросвязи);

автоматическое уведомление о заполнении электронного журнала и возможность его сохранения на внешнем носителе информации (для средств ППКА в сетях электросвязи).

33. При осуществлении обновления программных компонентов и служебных баз данных в средствах ГосСОПКА должны быть реализованы:

возможность обновления без потери информации, необходимой для функционирования средств, а также информации о компьютерных инцидентах и событиях ИБ;

возможность обновления только пользователями, ответственными за управление (администрирование) средств ГосСОПКА;

возможность восстановления работоспособности в случае сбоя процесса обновления (в том числе осуществление предварительного резервного копирования и последующее восстановление).

34. При осуществлении резервирования и восстановления своей работоспособности в средствах ГосСОПКА должны быть реализованы:

возможность создания резервной копии конфигурационных данных на внешнем носителе;

возможность создания резервной копии ПО на внешнем носителе;

возможность самовосстановления работоспособности при обнаружении критических ошибок в процессе функционирования (для средств ППКА в сетях электросвязи).

35. При осуществлении контроля целостности ПО в средствах ГосСОПКА должны быть реализованы:

проверка целостности ПО и конфигурационных файлов при загрузке, во время функционирования и по команде пользователя, ответственного за управление (администрирование) средством ГосСОПКА;

возможность штатного самотестирования ПО в процессе функционирования;

регистрация в электронном журнале результатов проведения контроля целостности ПО.