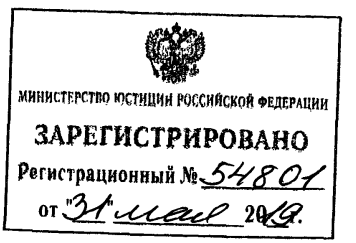
ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКАЗ

6 мая 2019 года Москва № 196



Об утверждении Требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты

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»[1]

П Р И К А З Ы В А Ю

утвердить прилагаемые Требования к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты.

Директор А.Бортников

[1] Собрание законодательства Российской Федерации, 2017, № 31 (ч. I), ст. 4736.

gost.e-ecolog.ru

Приложение
к приказу ФСБ России
от 6 мая 2019 г.
№ 196

Требования
к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты

I. Общие положения

1. Настоящие Требования определяют требования к устанавливаемым и используемым на всей территории Российской Федерации, в дипломатических представительствах и (или) консульских учреждениях Российской Федерации 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 – критическая информационная инфраструктура), предупреждения, ликвидации последствий компьютерных атак и (или) обмена информацией, необходимой субъектам критической информационной инфраструктуры при обнаружении, предупреждении и (или) ликвидации последствий компьютерных атак, а также криптографическим средствам защиты такой информации (далее – средства ГосСОПКА).

2. К средствам ГосСОПКА относятся:

технические, программные, программно-аппаратные и иные средства для обнаружения компьютерных атак (далее – средства обнаружения);

технические, программные, программно-аппаратные и иные средства для предупреждения компьютерных атак (далее – средства предупреждения);

технические, программные, программно-аппаратные и иные средства для ликвидации последствий компьютерных атак (далее – средства ликвидации последствий);

технические, программные, программно-аппаратные и иные средства поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры (далее – средства ППКА);

технические, программные, программно-аппаратные и иные средства обмена информацией, необходимой субъектам критической информационной инфраструктуры при обнаружении, предупреждении и (или) ликвидации последствий компьютерных атак (далее – средства обмена);

криптографические средства защиты информации, необходимой субъектам критической информационной инфраструктуры при обнаружении, предупреждении и (или) ликвидации последствий компьютерных атак.

Средства ГосСОПКА реализуются одним или несколькими техническими, программными и программно-аппаратными средствами.

II. Требования к средствам ГосСОПКА

3. Средства ГосСОПКА должны соответствовать следующим требованиям:

3.1. В средствах ГосСОПКА должна быть исключена возможность удаленного управления со стороны лиц, не являющихся работниками субъекта критической информационной инфраструктуры и (или) работниками привлекаемой в соответствии с законодательством Российской Федерации субъектом критической информационной инфраструктуры организации, осуществляющей лицензируемую деятельность в области защиты информации.

3.2. В средствах ГосСОПКА должна быть исключена возможность несанкционированной передачи обрабатываемой информации лицам, не являющимся работниками субъекта критической информационной

инфраструктуры и (или) работниками привлекаемой в соответствии с законодательством Российской Федерации субъектом критической информационной инфраструктуры организации, осуществляющей лицензируемую деятельность в области защиты информации.

3.3. Средства ГосСОПКА должны иметь возможность модернизации российскими организациями, не находящимися под прямым или косвенным контролем иностранных физических лиц и (или) юридических лиц.

3.4. Средства ГосСОПКА должны быть обеспечены гарантийной и технической поддержкой российскими организациями, не находящимися под прямым или косвенным контролем иностранных физических лиц и (или) юридических лиц.

3.5. Работа средств ГосСОПКА не должна приводить к нарушениям функционирования информационных систем, информационно-телекоммуникационных сетей и автоматизированных систем управления, находящихся на территории Российской Федерации, в дипломатических представительствах и (или) консульских учреждениях Российской Федерации (далее – информационные ресурсы) (должно быть исключено влияние на достижение целей и функционирование объектов критической информационной инфраструктуры).

3.6. В средствах ГосСОПКА должны быть реализованы функции безопасности в соответствии с главой VIII настоящих Требований.

III. Требования к средствам обнаружения

4. Средства обнаружения должны обладать следующими функциями:

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

программного обеспечения, телекоммуникационного оборудования, прикладных сервисов, средств контроля (анализа) защищенности, средств управления телекоммуникационным оборудованием и сетями связи, систем мониторинга состояния телекоммуникационного оборудования, систем мониторинга качества обслуживания, а также иных средств и систем защиты информации и систем мониторинга, эксплуатируемых субъектом критической информационной инфраструктуры (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.

5. При осуществлении сбора и первичной обработки событий ИБ средства обнаружения должны обеспечивать:

удаленный и (или) локальный сбор событий ИБ;

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

обработку поступающих событий ИБ и сохранение результатов их обработки;

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

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

встроенную поддержку различных источников событий ИБ и возможность разработки дополнительных модулей, обеспечивающих получение информации от новых источников событий ИБ.

6. При осуществлении автоматического анализа событий ИБ и выявления компьютерных инцидентов средства обнаружения должны обеспечивать:

отбор и фильтрацию событий ИБ;

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

выявление компьютерных инцидентов, регистрацию методов (способов) их обнаружения;

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

возможность корреляции для последовательности событий ИБ;

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

автоматическое назначение приоритетов событиям ИБ на основании задаваемых пользователем показателей.

7. При осуществлении повторного анализа ранее зарегистрированных событий ИБ и выявления на основе такого анализа не обнаруженных ранее компьютерных инцидентов средства обнаружения должны обеспечивать:

выявление 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);

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

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

возможность настройки параметров проводимого анализа;

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

хранение агрегированных событий ИБ не менее шести месяцев.

IV. Требования к средствам предупреждения

8. Средства предупреждения должны обладать следующими функциями:

сбор и обработка сведений об инфраструктуре контролируемых информационных ресурсов и справочной информации;

сбор и обработка сведений об уязвимостях и недостатках в настройке программного обеспечения (далее – ПО), используемого в контролируемых информационных ресурсах;

формирование рекомендаций по минимизации угроз безопасности информации;

учет угроз безопасности информации.

9. При осуществлении сбора и обработки сведений об инфраструктуре контролируемых информационных ресурсов и справочной информации средства предупреждения должны обеспечивать:

9.1. Сбор и обработку сведений об инфраструктуре контролируемых информационных ресурсов, включающих информацию:

об архитектуре и объектах контролируемых информационных ресурсов (сетевые адреса и имена, наименования и версии используемого ПО);

о выполняющихся на объектах контролируемых информационных ресурсов сетевых службах;

об источниках событий ИБ.

9.2. Сбор и обработку справочной информации:

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;

об известных уязвимостях используемого ПО;

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

9.3. Возможность добавления, просмотра и изменения сведений об инфраструктуре контролируемых информационных ресурсов и справочной информации.

10. При осуществлении сбора и обработки сведений об уязвимостях и недостатках в настройке ПО, используемого в контролируемых информационных ресурсах, средства предупреждения должны обеспечивать:

сбор данных о дате и времени проведения исследования контролируемых информационных ресурсов;

формирование перечня выявленных уязвимостей и недостатков в настройке используемого ПО (для каждого объекта контролируемого информационного ресурса);

возможность статистической и аналитической обработки полученной информации.

11. Формируемые рекомендации по минимизации угроз безопасности информации должны содержать перечень мер, направленных на устранение уязвимостей и недостатков в настройке ПО, используемого в контролируемых информационных ресурсах.

12. При осуществлении учета угроз безопасности информации средства предупреждения должны обеспечивать:

создание и изменение записи, содержащей уведомление об угрозе безопасности информации в форматах, обрабатываемых технической инфраструктурой Национального координационного центра по

компьютерным инцидентам[1] (далее – 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;

создание и изменение инструкций по реагированию на компьютерные инциденты, связанные с угрозами безопасности информации, включающих порядок принятия решений, очередность выполняемых действий и способы организации совместных действий участвующих в мероприятиях по реагированию на компьютерные инциденты и ликвидации последствий компьютерных атак работников субъекта критической информационной инфраструктуры и (или) работников привлекаемой в соответствии с законодательством Российской Федерации субъектом критической информационной инфраструктуры организации, осуществляющей лицензируемую деятельность в области защиты информации;

создание и изменение инструкций по обработке запросов и уведомлений, поступающих из НКЦКИ.

V. Требования к средствам ликвидации последствий

13. Средства ликвидации последствий должны обладать следующими функциями:

учет и обработка компьютерных инцидентов;

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

взаимодействие с НКЦКИ посредством использования технической инфраструктуры НКЦКИ, предназначенной для отправки, получения, обработки и хранения уведомлений и запросов в рамках информационного

[1] Подпункт 4.9 пункта 4 Положения о Национальном координационном центре по компьютерным инцидентам, утвержденного приказом ФСБ России от 24 июля 2018 г. № 366 «О Национальном координационном центре по компьютерным инцидентам» (зарегистрирован Минюстом России 6 сентября 2018 г., регистрационный № 52109).

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;

информационно-аналитическое сопровождение пользователей.

14. При осуществлении учета и обработки компьютерных инцидентов средства ликвидации последствий должны обеспечивать:

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

автоматическое создание 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;

запись 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;

запись о присвоении категорий опасности и (или) определение приоритетов компьютерных инцидентов на основе критериев, задаваемых по значениям полей карточек компьютерных инцидентов;

регистрацию и учет карточек компьютерных инцидентов;

фильтрацию, сортировку и поиск карточек компьютерных инцидентов по значениям полей карточек;

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

15. Для обеспечения управления процессами реагирования на компьютерные инциденты и ликвидации последствий компьютерных атак средства ликвидации последствий должны обеспечивать:

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;

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

формирование электронных сообщений для организации взаимодействия и координации действий работников субъекта критической информационной инфраструктуры и (или) работников привлекаемой в соответствии с законодательством Российской Федерации субъектом критической информационной инфраструктуры организации, осуществляющей лицензируемую деятельность в области защиты информации, участвующих в реагировании на компьютерный инцидент и ликвидации последствий компьютерной атаки.

16. При взаимодействии с НКЦКИ средства ликвидации последствий должны обеспечивать:

автоматизированный обмен информацией, представляемой в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, указанной в пункте 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];

учет карточек компьютерных инцидентов в соответствии с идентификацией НКЦКИ.

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

VI. Требования к средствам ППКА

18. Средства ППКА должны обладать следующими функциями:

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;

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 шести месяцев;

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

---

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

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

уведомление о фактах нарушения режимов функционирования средств ППКА;

наличие интерфейса(ов) 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;

возможность формирования информации, предусмотренной пунктом 5 Перечня, указанного в пункте 16 настоящих Требований.

VII. Требования к средствам обмена и криптографическим средствам защиты информации, необходимой субъектам критической информационной инфраструктуры при обнаружении, предупреждении и (или) ликвидации последствий компьютерных атак

19. Средства обмена должны обеспечивать передачу, прием и целостность при передаче и приеме информации, необходимой субъектам критической информационной инфраструктуры при обнаружении, предупреждении и (или) ликвидации последствий компьютерных атак.

20. Криптографические средства защиты информации, необходимой субъектам критической информационной инфраструктуры при обнаружении, предупреждении и (или) ликвидации последствий компьютерных атак, должны быть сертифицированы в системе сертификации средств криптографической защиты информации.

VIII. Требования к средствам ГосСОПКА в части реализации функций безопасности

21. Средства ГосСОПКА в части реализации функций безопасности должны обеспечивать:

идентификацию и аутентификацию пользователей;

разграничение прав доступа к информации и функциям;

регистрацию событий ИБ;

обновление программных компонентов и служебных баз данных;

резервирование и восстановление своей работоспособности;

синхронизацию системного времени и корректировку временных значений (корректировку настроек часовых поясов);

контроль целостности ПО.

21.1. При осуществлении идентификации и аутентификации пользователей средства ГосСОПКА должны обеспечивать:

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

хранение паролей в зашифрованном виде;

автоматическое информирование о необходимости смены паролей.

21.2. При осуществлении разграничения прав доступа к информации и функциям средства ГосСОПКА должны обеспечивать:

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

возможность блокирования и повторной активации учетных записей;

блокирование сессии доступа при превышении задаваемого значения временного периода отсутствия активности;

уведомление о неудачных попытках доступа к управлению средствами ГосСОПКА;

запись всех действий пользователей с момента авторизации в электронный журнал.

21.3. При осуществлении регистрации событий ИБ средства ГосСОПКА должны обеспечивать:

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 (только для средств ППКА);

защиту электронных журналов от редактирования и удаления содержащейся в них информации (только для средств ППКА);

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

21.4. При осуществлении обновления программных компонентов и служебных баз данных средства ГосСОПКА должны обеспечивать:

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

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

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

21.5. При осуществлении резервирования и восстановления своей работоспособности средства ГосСОПКА должны обеспечивать:

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 (только для средств ППКА).

21.6. При осуществлении контроля целостности ПО средства ГосСОПКА должны обеспечивать:

проверку 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;

регистрацию в электронном журнале результатов проведения контроля целостности ПО.

IX. Требования к средствам обнаружения, средствам предупреждения и средствам ликвидации последствий в части реализации визуализации, построения сводных отчетов и хранения информации

22. К средствам обнаружения, средствам предупреждения и средствам ликвидации последствий предъявляются требования в части реализации визуализации, построения сводных отчетов и хранения информации.

Средства обнаружения, средства предупреждения и средства ликвидации последствий должны обеспечивать:

22.1. Визуализацию в виде таблиц (списков, схем, графиков, диаграмм) сведений:

о событиях ИБ;

об обнаруженных компьютерных инцидентах;

об уязвимостях и недостатках в настройке ПО, используемого в контролируемых информационных ресурсах;

об инфраструктуре контролируемых информационных ресурсов;

хранящихся в базе данных;

содержащих справочную и другую необходимую информацию.

22.2. Построение сводных отчетов путем реализации следующих функций:

создание таблиц (списков, схем, графиков, диаграмм), а также их визуализация на основе полученных данных;

выбор параметров, по которым строятся таблицы (списки, схемы, графики, диаграммы) в отчетах;

экспорт отчетов;

автоматическое формирование отчетов по расписанию, а также их автоматическое направление назначаемым адресатам.

22.3. Хранение загружаемой информации в течение установленного периода времени и постоянный доступ к ней, а также возможность экспорта хранящейся информации, в том числе в исходном виде.

gost.e-ecolog.ru