УТВЕРЖДЕНЫ
приказом ФСТЭК России
от «26» февраля 2025 г. № 58

# Требования по безопасности информации к средствам обнаружения и реагирования на уровне узла (Выписка)

1. Требования по безопасности информации к средствам обнаружения и реагирования на уровне узла являются обязательными в области технического регулирования к продукции, используемой в целях защиты информации ограниченного доступа[1] (далее – Требования), предъявляемыми к программным средствам, предназначенным для обнаружения на узлах информационной (автоматизированной) системы (далее – узлах) признаков вредоносного программного обеспечения и компьютерных атак, а также их нейтрализации (далее – средства обнаружения и реагирования на уровне узла).

2. Выполнение настоящих Требований является обязательным при проведении работ по оценке соответствия (включая работы по сертификации) средств технической защиты информации и средств обеспечения безопасности информационных технологий, организуемых ФСТЭК России в пределах своих полномочий в соответствии с Положением о системе сертификации средств защиты информации, утвержденным приказом ФСТЭК России от 3 апреля 2018 г. № 55 (зарегистрирован Минюстом России 11 мая 2018 г., регистрационный № 51063) (с изменениями, внесенными приказом ФСТЭК России от 5 августа 2021 г. № 121 (зарегистрирован Минюстом России 27 октября 2021 г., регистрационный № 65594) и от 19 сентября 2022 г. № 172 (зарегистрирован Минюстом России 19 октября 2022 г., регистрационный № 70614).

3. К средствам обнаружения и реагирования на уровне узла устанавливается 3 класса защиты.

Средства обнаружения и реагирования на уровне узла, соответствующие 6 классу защиты, применяются в значимых объектах критической информационной инфраструктуры третьей категории значимости[2], в

[1] Статья 5 Федерального закона от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».

[2] Статья 7 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», Правила категорирования объектов критической информационной инфраструктуры Российской Федерации, утвержденные постановлением Правительства Российской Федерации от 8 февраля 2018 г. № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации».

государственных информационных системах 3 класса защищенности[3], в автоматизированных системах управления производственными и технологическими процессами 3 класса защищенности[4], в информационных системах персональных данных при необходимости обеспечения 3 и 4 уровня защищенности персональных данных[5].

Средства обнаружения и реагирования на уровне узла, соответствующие 5 классу защиты, применяются в значимых объектах критической информационной инфраструктуры второй категории значимости, в государственных информационных системах 2 класса защищенности, в автоматизированных системах управления производственными и технологическими процессами 2 класса защищенности, в информационных системах персональных данных при необходимости обеспечения 2 уровня защищенности персональных данных.

Средства обнаружения и реагирования на уровне узла, соответствующие 4 классу защиты, применяются в значимых объектах критической информационной инфраструктуры первой категории значимости, в государственных информационных системах 1 класса защищенности, в автоматизированных системах управления производственными и технологическими процессами 1 класса защищенности, в информационных системах персональных данных при необходимости обеспечения 1 уровня защищенности персональных данных, в информационных системах общего пользования II класса[6].

4. Требования по безопасности информации предъявляются к:

уровню доверия средства обнаружения и реагирования на уровне узла;

управлению доступом в средстве обнаружения и реагирования на уровне узла;

идентификации и аутентификации пользователей средства обнаружения и реагирования на уровне узла;

получению данных мониторинга средством обнаружения и реагирования

---

[3] Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденные приказом ФСТЭК России от 11 февраля 2013 г. № 17 (зарегистрирован Минюстом России 31 мая 2013 г., регистрационный № 28608), (с изменениями, внесенными приказом ФСТЭК России от 15 февраля 2017 г. № 27 (зарегистрирован Минюстом России 14 марта 2017 г., регистрационный № 45933), приказом ФСТЭК России от 28 мая 2019 г. № 106 (зарегистрирован Минюстом России 13 сентября 2019 г., регистрационный № 55924) и приказом ФСТЭК России от 28 августа 2024 г. № 159 (зарегистрирован Минюстом России 24 октября 2024 г., регистрационный № 79900).

[4] Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, утвержденные приказом ФСТЭК России от 14 марта 2014 г. № 31 (зарегистрирован Минюстом России 30 июня 2014 г., регистрационный № 32919), (с изменениями, внесенными приказом ФСТЭК России от 23 марта 2017 г. № 49 (зарегистрирован Минюстом России 25 апреля 2017 г., регистрационный № 46487), приказом ФСТЭК России от 9 августа 2018 г. № 138 (зарегистрирован Минюстом России 5 сентября 2018 г., регистрационный № 52071) и приказом ФСТЭК России от 15 марта 2021 г. № 46 (зарегистрирован Минюстом России 1 июля 2021 г., регистрационный № 64063).

[5] Требования к защите персональных данных при их обработке в информационных системах персональных данных, утвержденные постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119.

[6] Требования о защите информации, содержащейся в информационных системах общего пользования, утвержденные приказом ФСБ России и ФСТЭК России от 31 августа 2010 г. № 416/489 (зарегистрирован Минюстом России 13 октября 2010 г., регистрационный № 18704).

на уровне узла;

обнаружению признаков вредоносного программного обеспечения и компьютерных атак средством обнаружения и реагирования на уровне узла;

реагированию средства обнаружения и реагирования на уровне узла;

тестированию средства обнаружения и реагирования на уровне узла;

управлению установкой обновлений (актуализации) служебных баз данных средства обнаружения и реагирования на уровне узла;

регистрации событий безопасности в средстве обнаружения и реагирования на уровне узла;

взаимодействию с иными средствами защиты информации;

централизованному управлению средством обнаружения и реагирования на уровне узла.

5. Средство обнаружения и реагирования на уровне узла должно соответствовать Требованиям по безопасности информации, устанавливающим уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий, утвержденным приказом ФСТЭК России от 2 июня 2020 г. № 76 (зарегистрирован Минюстом России 11 сентября 2020 г., регистрационный № 59772) (с изменениями, внесенными приказом ФСТЭК России от 18 апреля 2022 г. № 68 (зарегистрирован Минюстом России 20 июля 2022 г., регистрационный № 69318).

Устанавливается следующее соответствие классов защиты средств обнаружения и реагирования на уровне узла уровням доверия:

средства обнаружения и реагирования на уровне узла 6 класса защиты должны соответствовать 6 уровню доверия;

средства обнаружения и реагирования на уровне узла 5 класса защиты должны соответствовать 5 уровню доверия;

средства обнаружения и реагирования на уровне узла 4 класса защиты должны соответствовать 4 уровню доверия.

6. К управлению доступом в средстве обнаружения и реагирования на уровне узла предъявляются следующие требования:

6.1. В средстве обнаружения и реагирования на уровне узла 6, 5, 4 классов защиты должен быть реализован ролевой метод управления доступом с двумя ролями пользователей средства обнаружения и реагирования на уровне узла: администратор безопасности информационной (автоматизированной) системы и администратор средства обнаружения и реагирования на уровне узла.

6.2. В средстве обнаружения и реагирования на уровне узла 6, 5, 4 классов защиты должна быть реализована возможность наделения администратора безопасности информационной (автоматизированной) системы следующими

правами:

выбирать события безопасности, подлежащие регистрации в журнале (журналах) событий безопасности средства обнаружения и реагирования на уровне узла;

осуществлять управление журналом (журналами) событий безопасности;

получать оповещения о событиях обнаружения признаков вредоносного программного обеспечения на узле;

получать оповещения о событиях обнаружения признаков компьютерных атак на узле;

настраивать параметры выгрузки информации о событиях безопасности, зарегистрированных в средстве обнаружения и реагирования на уровне узла, в том числе в системы управления событиями безопасности;

осуществлять выборочный просмотр событий безопасности (поиск, сортировка событий безопасности) в средстве обнаружения и реагирования на уровне узла;

изменять назначенный своей учетной записи пароль.

6.3. В средстве обнаружения и реагирования на уровне узла 6, 5, 4 классов защиты должна быть реализована возможность наделения администратора средства обнаружения и реагирования на уровне узла следующими правами:

создавать учетные записи других пользователей средства обнаружения и реагирования на уровне узла;

управлять (изменять, блокировать, разблокировать и уничтожать) учетными записями пользователей средства обнаружения и реагирования на уровне узла;

назначать права пользователям средства обнаружения и реагирования на уровне узла, определяемые их ролями;

изменять назначенный своей учетной записи пароль;

устанавливать обновления (актуализировать) служебных баз данных, необходимые для функционирования средства обнаружения и реагирования на уровне узла;

создавать, редактировать и удалять задания по проверке узла, определяющие перечень объектов контроля, подлежащих проверке, действия по реагированию, принимаемые в случае выявления признаков вредоносного программного обеспечения и компьютерных атак, и расписание запуска задания;

включать и отключать задания по проверке узла;

создавать, изменять и удалять правила выявления признаков вредоносного программного обеспечения и компьютерных атак;

включать и отключать правила выявления признаков вредоносного программного обеспечения и компьютерных атак;

выполнять действия по реагированию;

получать данные об узле для проведения дополнительного анализа выявленного признака вредоносного программного обеспечения или компьютерной атаки;

осуществлять выборочный просмотр событий безопасности (поиск, сортировка событий безопасности) в средстве обнаружения и реагирования на уровне узла;

обновлять программное обеспечение средства обнаружения и реагирования на уровне узла;

тестировать средство обнаружения и реагирования на уровне узла;

обеспечивать возможность управления сетевыми настройками для организации взаимодействия между компонентами средства обнаружения и реагирования на уровне узла;

обеспечивать возможность управления сетевыми настройками для организации взаимодействия средства обнаружения и реагирования на уровне узла с системой управления событиями безопасности информации;

обеспечивать возможность управления сетевыми настройками для организации взаимодействия средства обнаружения и реагирования на уровне узла с замкнутой системой (средой) предварительного выполнения программ;

обеспечивать возможность управления сетевыми настройками для организации получения индикаторов компрометации и индикаторов компьютерных атак из баз данных, содержащих сведения об угрозах безопасности информации, полученные из различных источников.

6.4. В средстве обнаружения и реагирования на уровне узла должна быть реализована возможность определения полномочий для пользователей средства обнаружения и реагирования на уровне узла в пределах назначенных им ролей.

7. К идентификации и аутентификации пользователей средства обнаружения и реагирования на уровне узла предъявляются следующие требования:

7.1. Первичная идентификация пользователей средства обнаружения и реагирования на уровне узла 6 класса защиты должна осуществляться администратором средства обнаружения и реагирования на уровне узла.

В средстве обнаружения и реагирования на уровне узла должна отсутствовать возможность установления одинаковых идентификаторов для разных пользователей средства обнаружения и реагирования на уровне узла.

Идентификация и аутентификация пользователей средства обнаружения и реагирования на уровне узла осуществляется в соответствии с требованиями разделов 3—7 национального стандарта Российской Федерации ГОСТ Р 58833-2020 «Защита информации. Идентификация и аутентификация. Общие

положения», утвержденного и введенного в действие приказом Федерального агентства по техническому регулированию и метрологии от 10 апреля 2020 г. № 159-ст.

В случае неуспешной идентификации и аутентификации пользователя средства обнаружения и реагирования на уровне узла ему должно быть отказано в доступе в средство обнаружения и реагирования на уровне узла.

В средстве обнаружения и реагирования на уровне узла должна осуществляться идентификация и аутентификация пользователей средства обнаружения и реагирования на уровне узла при предъявлении идентификатора и пароля пользователя средства обнаружения и реагирования на уровне узла.

Пароль пользователя средства обнаружения и реагирования на уровне узла для первичной аутентификации должен назначаться администратором средства обнаружения и реагирования на уровне узла.

В средстве обнаружения и реагирования на уровне узла должна быть реализована возможность изменения пользователем средства обнаружения и реагирования на уровне узла установленного пароля после его первой аутентификации.

При попытке ввода неправильного значения идентификатора или пароля пользователя средства обнаружения и реагирования на уровне узла должно выводиться сообщение на экран средства вычислительной техники пользователя с приглашением ввести правильный идентификатор и пароль.

При исчерпании установленного максимального количества неуспешных попыток ввода неправильного пароля учетная запись пользователя средства обнаружения и реагирования на уровне узла должна быть заблокирована средством обнаружения и реагирования на уровне узла с возможностью ее разблокирования администратором средства обнаружения и реагирования на уровне узла или автоматически по истечении временного интервала, устанавливаемого администратором средства обнаружения и реагирования на уровне узла.

Защита пароля пользователя средства обнаружения и реагирования на уровне узла должна обеспечиваться при его вводе за счет исключения отображения символов вводимого пароля или за счет отображения вводимых символов условными знаками.

Пароль пользователя средства обнаружения и реагирования на уровне узла 6 класса защиты должен содержать не менее 6 символов при алфавите пароля не менее 60 символов. Максимальное количество попыток ввода неправильного пароля до блокировки – 10.

В средстве обнаружения и реагирования на уровне узла должна быть реализована возможность хранения аутентификационной информации

пользователя средства обнаружения и реагирования на уровне узла в защищенном от несанкционированного доступа виде.

В средстве обнаружения и реагирования на уровне узла должна быть реализована возможность использования результатов идентификации и аутентификации пользователей в информационной (автоматизированной) системе (в службе каталогов или в средстве централизованной идентификации и аутентификации).

7.2. Пароль пользователя средства обнаружения и реагирования на уровне узла 5 класса защиты наряду с требованиями, установленными в подпункте 7.1 пункта 7 настоящих Требований, дополнительно должен содержать не менее 6 символов при алфавите пароля не менее 70 символов. Максимальное количество попыток ввода неправильного пароля до блокировки – 8.

В средстве обнаружения и реагирования на уровне узла 5 класса защиты должна быть обеспечена взаимная идентификация и аутентификация пользователя средства обнаружения и реагирования на уровне узла и средства обнаружения и реагирования на уровне узла.

7.3. Пароль пользователя средства обнаружения и реагирования на уровне узла 4 класса защиты наряду с требованиями, установленными в подпунктах 7.1 и 7.2 пункта 7 настоящих Требований, дополнительно должен содержать не менее 8 символов при алфавите пароля не менее 70 символов. Максимальное количество попыток ввода неправильного пароля до блокировки – 4.

8. К получению данных мониторинга средством обнаружения и реагирования на уровне узла предъявляются следующие требования:

8.1. В средстве обнаружения и реагирования на уровне узла 6, 5 классов защиты должно осуществляться получение следующих данных мониторинга с узла:

информация об операционной системе узла (наименование, версия, архитектура);

информация о составе программного и аппаратного обеспечения узла;

идентификаторы узла (сетевой и аппаратный адрес, логическое имя);

сведения об операциях, связанных с идентификацией и аутентификацией объектов контроля в операционной системе;

сведения об операциях, связанных с созданием, изменением, блокированием, разблокированием, удалением учетных записей в операционной системе на узле, и результат их выполнения на узле;

сведения об операциях, связанных с файлами (в том числе создание, чтение, изменение, удаление), и результат их выполнения на узле;

сведения об операциях, связанных с процессами (в том числе запуск, приостановка, завершение), и результат их выполнения на узле;

сведения об операциях, связанных с задачами планировщика задач операционной системы (создание, изменение, удаление);

сведения об операциях, связанных со списком автозапуска программного обеспечения в операционной системе (добавление в список, удаление из списка);

сведения о выполненных командах в командной строке;

сведения об операциях, связанных с загрузкой программных библиотек (модулей) в адресное пространство процессов операционной системы, и результат их выполнения на узле;

сведения об операциях, связанных с системными процессами (установка, запуск, приостановка, завершение, удаление), и результат их выполнения на узле;

сведения об операциях, связанных с изменением параметров настройки системного программного обеспечения, и результат их выполнения на узле;

события безопасности, регистрируемые в журнале (журналах) событий безопасности операционной системы;

сведения об операциях, связанных с изменением аппаратной и программной конфигурации узла, и результат их выполнения на узле;

сведения о входящем и исходящем сетевом трафике узла;

сведения об обращении к сетевым ресурсам узла.

В средстве обнаружения и реагирования на уровне узла должно быть обеспечено сохранение следующих данных о входящем и исходящем сетевом трафике узла:

сетевые адреса источника и назначения;

используемые сетевые протоколы;

продолжительность передачи информационного потока (время начала и завершения передачи информационного потока);

наименование процесса или системного процесса, осуществляющего сетевое соединение;

статус сетевого соединения (активное, завершенное).

В средстве обнаружения и реагирования на уровне узла должны храниться полученные с узла данные мониторинга, а также результаты проведенных проверок данных мониторинга, в том числе если по результатам проверок не было выявлено вредоносных и (или) несанкционированных действий на узле, а также обеспечивать возможность ротации хранимых данных (запись новых данных мониторинга взамен старых). В средстве обнаружения и реагирования на уровне узла должна предоставляться возможность настройки ротации данных в зависимости от срока хранения данных мониторинга или от объемов занимаемой памяти.

В средстве обнаружения и реагирования на уровне узла должна

обеспечиваться возможность получения данных мониторинга посредством перехвата системных вызовов операционной системы средства вычислительной техники.

8.2. В средстве обнаружения и реагирования на уровне узла 4 класса защиты наряду с требованиями, установленными в подпункте 8.1 пункта 8 настоящих Требований, дополнительно должно осуществляться получение с узла сведений об операциях, связанных с метаданными (атрибутами) файлов, и результат их выполнения на узле.

К данным мониторинга, относящимся к операциям, связанным с метаданными (атрибутами) файлов, относятся данные о:

переименовании файла, в том числе об изменении расширения файла;

изменении прав доступа;

изменении даты и времени создания файла (если файловая система поддерживает и осуществляет хранение данной информации);

изменении даты и времени последнего изменения и чтения;

изменении сведений о владельце файла.

В составе данных мониторинга, относящихся к операциям, связанным с процессами (запуск, приостановка, завершение), дополнительно должны содержаться данные о:

родительском (основном) процессе, его идентификатор и параметры запуска;

дочерних (производных) процессах, их идентификаторы и параметры запуска.

9. К обнаружению признаков вредоносного программного обеспечения и компьютерных атак средством обнаружения и реагирования на уровне узла предъявляются следующие требования:

9.1. В средстве обнаружения и реагирования на уровне узла 6 класса защиты должны:

обнаруживаться признаки вредоносного программного обеспечения путем анализа полученных данных мониторинга с использованием индикаторов компрометации, представляющих собой известную информацию об объектах контроля и (или) операциях на узле, которая свидетельствует о том, что на узле реализованы вредоносные операции;

обнаруживаться признаки компьютерных атак путем анализа полученных данных мониторинга с использованием индикаторов компьютерных атак, представляющих собой известную информацию (или правила) о подозрительных операциях на узле, которая свидетельствует о том, что в отношении узла могла осуществляться компьютерная атака;

обнаруживаться признаки вредоносного программного обеспечения путем

анализа полученных данных мониторинга с использованием правил выявления признаков вредоносного программного обеспечения;

обнаруживаться признаки компьютерных атак путем анализа полученных данных мониторинга с использованием правил выявления признаков компьютерных атак.

В средстве обнаружения и реагирования на уровне узла должна обеспечиваться запись следующих данных о сетевом трафике узла, в котором были обнаружены признаки компьютерных атак:

сетевые адреса источника и назначения;

используемые сетевые протоколы;

продолжительность передачи информационного потока (время начала и завершения передачи информационного потока);

наименование процесса или системного процесса, осуществляющего сетевое соединение;

статус сетевого соединения (активное сетевое соединение, завершенное сетевое соединение).

В средстве обнаружения и реагирования на уровне узла должна обеспечиваться возможность использования следующих атрибутов при создании правил выявления признаков вредоносного программного обеспечения:

часть информации или последовательность байтов, содержащаяся в объекте контроля файловой системы или процессе операционной системы;

метаданные объекта файловой системы, включая имя, расширение имени и расположение этого объекта, версию сборки объекта, загружаемые объектом программные библиотеки, контрольную сумму объекта, размер объекта.

В средстве обнаружения и реагирования на уровне узла должны позволять создаваться правила выявления признаков вредоносного программного обеспечения на основе данных, указывающих на внедрение вредоносного программного обеспечения, в том числе данных из индикаторов компрометации, а также условий, выраженных с использованием переменных и логических выражений, содержащих логические операторы, реляционные операторы, побитовые операторы.

В средстве обнаружения и реагирования на уровне узла должны позволять создаваться правила выявления признаков компьютерных атак на основе данных, указывающих на реализацию компьютерных атак, в том числе данных из индикаторов компьютерных атак, а также условий, выраженных с использованием переменных и логических выражений, содержащих логические операторы, реляционные операторы, побитовые операторы.

В средстве обнаружения и реагирования на уровне узла должна быть предусмотрена возможность проверки узла на наличие признаков вредоносного

программного обеспечения и компьютерных атак следующими способами:

динамически (при изменениях данных мониторинга);

периодически (по расписанию) или по запросу (команде) администратора средства обнаружения и реагирования на уровне узла.

Механизмы обнаружения должны позволять обнаруживать признаки:

получения первоначального доступа к узлу;

внедрения и исполнения вредоносного программного обеспечения на узле;

закрепления (сохранения доступа) на узле с возможностью получения повторного доступа к нему;

управления вредоносным программным обеспечением и его компонентами;

повышения привилегий по доступу на узле;

сокрытия действий на узле;

получения доступа к другим узлам (распространение доступа);

сбора и вывода информации с узла;

несанкционированного доступа или воздействия.

В средстве обнаружения и реагирования на уровне узла должны обнаруживаться связи в последовательности операций (событий), выполняемых до и после обнаружения признака вредоносного программного обеспечения и компьютерных атак на узле.

В средстве обнаружения и реагирования на уровне узла должна осуществляться проверка синтаксиса созданных администратором средства обнаружения и реагирования на уровне узла правил выявления признаков вредоносного программного обеспечения и правил выявления признаков компьютерных атак.

9.2. В средстве обнаружения и реагирования на уровне узла 5, 4 классов защиты наряду с требованиями, установленными в подпункте 9.1 пункта 9 настоящих Требований, дополнительно должны:

предоставляться возможность применения правил выявления признаков компьютерных атак для проведения ретроспективного анализа (по историческим данным мониторинга, отражающим события предыдущих временных периодов);

сопоставляться (коррелироваться) между собой результаты работы разных механизмов обнаружения признаков вредоносного программного обеспечения и компьютерных атак на узле.

10. К реагированию средства обнаружения и реагирования на уровне узла предъявляются следующие требования:

10.1. В средстве обнаружения и реагирования на уровне узла 6 класса защиты должны обеспечиваться:

уведомление администратора безопасности информационной

(автоматизированной) системы и администратора средства обнаружения и реагирования на уровне узла об обнаруженном признаке вредоносного программного обеспечения и компьютерных атак на узле;

блокирование сетевой трафик узла.

10.2. В средстве обнаружения и реагирования на уровне узла 5 класса защиты наряду с требованиями, установленными в подпункте 10.1 пункта 10 настоящих Требований, дополнительно должны обеспечиваться:

блокирование сеанса доступа в операционной системе на узле;

блокирование учетной записи пользователя операционной системы на узле;

завершение процессов, а также блокирование их запуска;

завершение системных процессов, а также блокирование их запуска;

блокирование операций с объектом контроля;

получение копии объекта контроля администратором средства обнаружения и реагирования на уровне узла для дополнительного анализа;

отключение (изоляцию) узла от сети передачи данных информационной (автоматизированной) системы.

В эксплуатационной документации средства обнаружения и реагирования на уровне узла должны быть указаны типы объектов контроля, для которых обеспечивается получение копий объектов контроля администратором средства обнаружения и реагирования на уровне узла для дополнительного анализа.

Действия по реагированию должны выполняться по запросу (команде) администратора средства обнаружения и реагирования на уровне узла.

10.3. В средстве обнаружения и реагирования на уровне узла 4 класса защиты наряду с требованиями, установленными в подпунктах 10.1 и 10.2 пункта 10 настоящих Требований, дополнительно должны обеспечиваться:

логическая изоляция средства вычислительной техники узла от сети передачи данных информационной (автоматизированной) системы с сохранением возможности проведения администратором средства обнаружения и реагирования на уровне узла действий по реагированию на узле с использованием сети передачи данных информационной (автоматизированной) системы;

блокирование выполнения команд, определенных администратором средства обнаружения и реагирования на уровне узла, в командной строке на заданный промежуток времени;

копирование программного обеспечения или командного сценария на узел для реагирования на вредоносное программное обеспечение или компьютерные атаки;

запуск программного обеспечения или командного сценария на узле для

реагирования на вредоносное программное обеспечение или компьютерные атаки;

автоматическое блокирование сетевого трафика от источника, определенного администратором средства обнаружения и реагирования на уровне узла, на установленный промежуток времени;

получение данных об узле для проведения дополнительного анализа выявленного признака вредоносного программного обеспечения или компьютерных атак администратором средства обнаружения и реагирования на уровне узла по его запросу (команде);

завершение сеанса доступа в операционной системе на узле и выключение средства вычислительной техники.

В средстве обнаружения и реагирования на уровне узла должна обеспечиваться возможность получения следующих данных об узле для проведения дополнительного анализа выявленного признака вредоносного программного обеспечения и компьютерных атак администратором средства обнаружения и реагирования на уровне узла по его запросу (команде):

сведения о запущенных процессах операционной системы;

сведения об активных сетевых соединениях;

сведения об авторизованных учетных записях в операционной системе;

сведения о программном обеспечении, автозапуск которого осуществляется при загрузке операционной системы (точки автозапуска);

перечень объектов контроля в файловой системе;

дамп памяти процесса операционной системы;

дамп оперативной памяти.

При выполнении завершения сеанса доступа в операционной системе на узле или выключении средства вычислительной техники в средстве обнаружения и реагирования на уровне узла должна обеспечиваться возможность предупреждения пользователя информационной (автоматизированной) системы о предстоящем завершении сеанса доступа и предоставлять время для сохранения обрабатываемых данных. Средство обнаружения и реагирования на уровне узла должно предоставлять возможность настройки времени, которое дается пользователю для сохранения обрабатываемых данных.

В средстве обнаружения и реагирования на уровне узла должна предоставляться возможность администратору средства обнаружения и реагирования на уровне узла настраивать перечень действий по реагированию, а также обеспечивать возможность их автоматического выполнения или выполнения после подтверждения администратором средства обнаружения и реагирования на уровне узла.

11. К тестированию средства обнаружения и реагирования на уровне узла

предъявляются следующие требования.

В средстве обнаружения и реагирования на уровне узла 6, 5, 4 классов защиты должны:

обеспечиваться тестирование механизмов безопасности средства обнаружения и реагирования на уровне узла;

обеспечиваться информирование администратора средства обнаружения и реагирования на уровне узла о выявленных нарушениях функционирования средства обнаружения и реагирования на уровне узла.

12. К управлению установкой обновлений (актуализации) служебных баз данных средства обнаружения и реагирования на уровне узла предъявляются следующие требования:

12.1. В средстве обнаружения и реагирования на уровне узла 6, 5 классов защиты должно поддерживаться обновление служебных баз данных, включающих базы индикаторов компрометации и базы индикаторов компьютерных атак, по запросу администратора средства обнаружения и реагирования на уровне узла из следующих источников:

из информационного ресурса, определяемого ФСТЭК России (при наличии);

из информационного ресурса производителя (изготовителя) средства обнаружения и реагирования на уровне узла, расположенного на территории Российской Федерации;

со съемного машинного носителя информации или с сетевого источника информационной (автоматизированной) системы.

Правила, предоставляемые производителем (изготовителем) в составе базы индикаторов компрометации, базы индикаторов компьютерных атак и иных баз, необходимых для функционирования средства обнаружения и реагирования на уровне узла, должны содержать описание, позволяющее пользователю средства обнаружения и реагирования на уровне узла понять логику работы правила для определения необходимости применения правила в информационной (автоматизированной) системе.

Производитель (изготовитель) должен предоставлять комплект типовых правил выявления признаков вредоносного программного обеспечения и компьютерных атак, на основе которых администратор средства обнаружения и реагирования на уровне узла должен иметь возможность создавать собственные правила выявления признаков вредоносного программного обеспечения и компьютерных атак.

В эксплуатационной документации на средство обнаружения и реагирования на уровне узла должны содержаться инструкции по созданию администратором средства обнаружения и реагирования на уровне узла

собственных правил выявления признаков вредоносного программного обеспечения и компьютерных атак на основе предоставляемых производителем (изготовителем) типовых правил выявления признаков вредоносного программного обеспечения и компьютерных атак.

Производитель (изготовитель) должен размещать обновления базы индикаторов компрометации и базы индикаторов компьютерных атак, а также комплект типовых правил выявления признаков вредоносного программного обеспечения и компьютерных атак в информационном ресурсе служебных баз данных, поддерживаемом производителем (изготовителем), а также передавать их в информационный ресурс, определяемый ФСТЭК России (при наличии).

Защита информации в канале связи, используемом для получения обновлений индикаторов компрометации и индикаторов компьютерных атак, а также типовых правил выявления признаков вредоносного программного обеспечения и компьютерных атак, должна обеспечиваться посредством защиты каналов связи от несанкционированного физического доступа (подключения) к ним и (или) посредством применения в соответствии с законодательством Российской Федерации средств криптографической защиты информации.

12.2. В средстве обнаружения и реагирования на уровне узла 4 класса защиты наряду с требованиями, установленными в подпункте 12.1 пункта 12 настоящих Требований, дополнительно должно обеспечиваться получение индикаторов компрометации и индикаторов компьютерных атак в автоматизированном режиме по настроенному администратором средства обнаружения и реагирования на уровне узла расписанию.

13. К регистрации событий безопасности в средстве обнаружения и реагирования на уровне узла предъявляются следующие требования.

В средстве обнаружения и реагирования на уровне узла 6, 5, 4 классов защиты должны обеспечиваться:

регистрация выбранных администратором безопасности информационной (автоматизированной) системы событий безопасности в журнале (журналах) событий безопасности средства обнаружения и реагирования на уровне узла;

предоставление возможности просмотра всех событий безопасности в журнале (журналах) событий безопасности средства обнаружения и реагирования на уровне узла и выборочного просмотра событий безопасности (поиск, сортировка событий безопасности) в соответствии с ролью пользователя средства обнаружения и реагирования на уровне узла.

В средстве обнаружения и реагирования на уровне узла должна реализовываться возможность регистрации следующих типов событий безопасности в соответствии с разделами 3—6 национального стандарта Российской Федерации ГОСТ Р 59548-2022 «Защита информации. Регистрация

событий безопасности. Требования к регистрируемой информации», утвержденного и введенного в действие приказом Федерального агентства по техническому регулированию и метрологии от 13 января 2022 г. № 2-ст:

события безопасности, связанные с обнаружением признаков вредоносного программного обеспечения;

события безопасности, связанные с обнаружением признаков компьютерных атак;

события безопасности, связанные с получением индикаторов компрометации и индикаторов компьютерных атак;

события безопасности, связанные с идентификацией и аутентификацией пользователя средства обнаружения и реагирования на уровне узла;

события безопасности, связанные с управлением (администрированием) средства обнаружения и реагирования на уровне узла;

события безопасности, связанные с управлением журналом (журналами) событий безопасности;

события безопасности, связанные с выполнением действий по реагированию;

события безопасности, связанные со сбоями в работе средства обнаружения и реагирования на уровне узла.

В средстве обнаружения и реагирования на уровне узла должна реализовываться возможность хранения журнала (журналов) событий безопасности с возможностью ротации событий безопасности (запись новых событий безопасности взамен старых). В средстве обнаружения и реагирования на уровне узла должна предоставляться возможность управления журналом (журналами) событий безопасности в части настройки ротации событий в зависимости от срока хранения событий безопасности или от объемов занимаемой памяти.

В средстве обнаружения и реагирования на уровне узла при записи событий безопасности должно обеспечиваться получение информации о текущей дате, времени и часовом поясе от системных часов аппаратной платформы средства вычислительной техники, на котором оно установлено, или от операционной системы узла.

В средстве обнаружения и реагирования на уровне узла должно обеспечиваться оповещать пользователей средства обнаружения и реагирования на уровне узла о событиях безопасности в соответствии с ролями пользователей средства обнаружения и реагирования на уровне узла.

14. К взаимодействию с иными средствами защиты информации предъявляются следующие требования:

14.1. В средстве обнаружения и реагирования на уровне узла 6 класса

защиты должна обеспечиваться возможность передавать зарегистрированные им события безопасности в сертифицированную систему управления событиями безопасности информации.

14.2. В средстве обнаружения и реагирования на уровне узла 5 и 4 классов защиты наряду с требованиями, установленными в подпункте 14.1 пункта 14 настоящих Требований, дополнительно должно обеспечиваться взаимодействие с сертифицированной замкнутой системой (средой) предварительного выполнения программ. В рамках взаимодействия в средстве обнаружения и реагирования на уровне узла должна обеспечиваться возможность передачи копии объекта контроля и получения результатов его динамического анализа следующими способами:

автоматически, в случае идентификации средством обнаружения и реагирования на уровне узла потенциального вредоносного объекта контроля, потенциального вредоносного поведения объекта контроля;

по запросу (команде) администратора средства обнаружения и реагирования на уровне узла.

15. В состав средства обнаружения и реагирования на уровне узла 6, 5, 4 классов защиты должны входить компоненты, обеспечивающие возможность централизованного управления средствами обнаружения и реагирования на уровне узла, функционирующими в информационной (автоматизированной) системе, в соответствии с ролями пользователей средств обнаружения и реагирования на уровне узла.