ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 59548— 2022

Защита информации

РЕГИСТРАЦИЯ СОБЫТИЙ БЕЗОПАСНОСТИ

Требования к регистрируемой информации

Издание официальное

Москва
Российский институт стандартизации
2022

gost.e-ecolog.ru

Предисловие

1 РАЗРАБОТАН Федеральной службой по техническому и экспортному контролю (ФСТЭК России), Обществом с ограниченной ответственностью «Центр безопасности информации» (ООО «ЦБИ»)

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 362 «Защита информации»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 13 января 2022 г. № 2-ст

4 ВВЕДЕН ВПЕРВЫЕ

*Правила применения настоящего стандарта установлены в статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (*gost.e-ecolog.ru

© Оформление. ФГБУ «РСТ», 2022

Настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Федерального агентства по техническому регулированию и метрологии

Содержание

1 Область применения 1
2 Нормативные ссылки 1
3 Термины и определения 2
4 Сокращения 2
5 Общие положения 2
6 Требования к составу и содержанию регистрируемой информации 3
Приложение А (справочное) Типы событий безопасности, подлежащих регистрации средствами защиты информации 58
Приложение Б (справочное) Типы событий безопасности, подлежащих регистрации средствами обеспечения безопасности информационных технологий и иными программно-техническими средствами (а также программным обеспечением), применяемыми в информационных (автоматизированных) системах 63
Библиография 66

Введение

Настоящий стандарт предназначен для изготовителей средств защиты информации, средств обеспечения безопасности информационных технологий, иных программно-технических средств (а также программного обеспечения), применяемых в информационных (автоматизированных) системах, в том числе в интересах мониторинга информационной безопасности, контроля (анализа) защищенности, выявления инцидентов информационной безопасности в информационных (автоматизированных) системах, а также контроля функционирования элементов и в целом таких систем.

Настоящий стандарт содержит требования к составу и содержанию информации, которая подлежит регистрации указанными средствами, по отношению к событиям безопасности, регистрируемым в информационных (автоматизированных) системах.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Защита информации

РЕГИСТРАЦИЯ СОБЫТИЙ БЕЗОПАСНОСТИ

Требования к регистрируемой информации

Information protection. Security event logging. Requirements for registered information

Дата введения — 2022—02—01

1 Область применения

Настоящий стандарт устанавливает требования к составу и содержанию информации, которая подлежит регистрации средствами защиты информации, в том числе встроенными в программное обеспечение и (или) программно-технические средства, средствами обеспечения безопасности информационных технологий, иными программно-техническими средствами (а также программным обеспечением), применяемыми в информационных (автоматизированных) системах.

Настоящий стандарт не устанавливает требования к технической реализации и формату хранения событий безопасности. Для соответствия требованиям настоящего стандарта достаточно, чтобы средства, осуществляющие регистрацию событий безопасности, предоставляли возможность получения информации о событиях безопасности для реализации мониторинга информационной безопасности в информационных (автоматизированных) системах, контроля (анализа) защищенности, выявления инцидентов информационной безопасности в информационных (автоматизированных) системах, а также контроля функционирования элементов и в целом таких систем. При этом допускается расширение состава предоставляемой информации о событиях безопасности по сравнению с требованиями настоящего стандарта.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ Р 7.0.64 Система стандартов по информации, библиотечному и издательскому делу. Представление дат и времени. Общие требования

ГОСТ Р 50922 Защита информации. Основные термины и определения

ГОСТ Р 59547 Защита информации. Мониторинг информационной безопасности. Общие положения

Примечание — При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодному информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по выпускам ежемесячного информационного указателя «Национальные стандарты» за текущий год. Если заменен ссылочный стандарт, на который дана недатированная ссылка, то рекомендуется использовать действующую версию этого стандарта с учетом всех внесенных в данную версию изменений. Если заменен ссылочный стандарт, на который дана датированная ссылка, то рекомендуется использовать версию этого стандарта с указанным выше годом утверждения (принятия). Если после утверждения настоящего стандарта в ссылочный стандарт, на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение рекомендуется применять без учета данного изменения. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, рекомендуется применять в части, не затрагивающей эту ссылку.

Издание официальное

3 Термины и определения

В настоящем стандарте применены термины по ГОСТ Р 50922, ГОСТ 59547, а также следующие термины с соответствующими определениями:

3.1 **регистрация события безопасности:** Процесс автоматического (автоматизированного) занесения в электронный журнал регистрации событий безопасности записи о событии безопасности.

3.2 **регистрируемая информация (о событии безопасности):** Сведения о событии безопасности, подлежащие регистрации в электронном журнале регистрации событий безопасности.

3.3 **событие безопасности:** Зафиксированное в обрабатываемом виде состояние информационной (автоматизированной) системы, сетевого, телекоммуникационного, коммуникационного, иного прикладного сервиса или информационно-телекоммуникационной сети, указывающее на возможное нарушение целостности, доступности и (или) конфиденциальности информации, а также на сбой в работе средства защиты/обработки информации или иную ситуацию, которая может быть значимой для безопасности информации.

3.4 **электронный журнал регистрации событий безопасности:** Объект (файл в электроном виде) или их совокупность в информационной (автоматизированной) системе, предназначенный (предназначенные) для хранения записей о событиях безопасности.

4 Сокращения

В настоящем стандарте применены следующие сокращения:

БРП — база решающих правил;

ОС — операционная система;

СЗИ — средство защиты информации;

ПО — программное обеспечение.

5 Общие положения

5.1 События безопасности могут быть зарегистрированы следующими составными частями информационной (автоматизированной) системы:

- средствами защиты информации;
- средствами обеспечения безопасности информационных технологий;
- иными программно-техническими средствами (а также программным обеспечением), применяемыми в информационных (автоматизированных) системах.

5.2 Средства защиты информации регистрируют события безопасности, связанные с реализованными в них функциями безопасности.

Типы событий безопасности, подлежащих регистрации средствами защиты информации в зависимости от реализуемых ими функций безопасности, приведены в приложении А.

5.3 Средства обеспечения безопасности информационных технологий и иные программно-технические средства (а также программное обеспечение), применяемые в информационных (автоматизированных) системах, регистрируют события безопасности, связанные с выполняемыми ими мерами защиты.

Типы событий безопасности, подлежащих регистрации средствами обеспечения безопасности информационных технологий и иными программно-техническими средствами (а также программным обеспечением), применяемыми в информационных (автоматизированных) системах, в зависимости от выполняемых ими мер защиты, представлены в приложении Б.

5.4 При необходимости зарегистрированная информация о событиях безопасности может быть передана в средства автоматизации мониторинга информационной безопасности. Для этого средства, осуществляющие регистрацию событий безопасности, должны обеспечивать предоставление доступа к информации о зарегистрированных событиях безопасности и (или) передавать сведения о событиях безопасности в средства автоматизации мониторинга информационной безопасности.

6 Требования к составу и содержанию регистрируемой информации

6.1 Общие требования

6.1.1 Элементы регистрационной записи о событии безопасности должны соответствовать типам данных (форматам), указанным в таблице 1.

Таблица 1 — Требования к типам данных регистрируемой информации

Наименование типа данных	Описание типа данных
«Дата/время»	Дату и время указывают в соответствии с ГОСТ Р 7.0.64 в формате: YYYY-MM-DDThh:mm:ss[.sss]±hh:mm, где YYYY-MM-DD обозначает «год»-«месяц»-«день»; - T — определитель времени, указывающий на начало обозначения элемента времени дня; - hh:mm:ss[.sss] обозначает элементы времени «час»-«минута»-«секунда»-«миллисекунда», при этом указание миллисекунд не является обязательным; - «-» и «:» разделители используют в обозначениях даты и времени дня соответственно; - «±» символ обозначает разность между местным временем и Всемирным координированным временем дня. Пример описания: 2019-05-20T18:30:15.587+04:00
«Продолжительность»	Продолжительность указывают в соответствии с ГОСТ Р 7.0.64. Продолжительность является неотрицательной величиной, приписываемой периоду времени, значение которой равно разности между метками времени конечного момента и начального момента периода времени (если метки времени являются числовыми). Продолжительность соответствует целочисленному типу данных. Принимаемые значения: секунда/минута/час/день
«Целое число»	Соответствует целочисленному типу данных
«Текст»	Любая последовательность символов
«Набор значений»	Указывают одно значение из фиксированного набора принимаемых значений (набор значений определяют исходя из особенностей регистрируемой информации)
«Сетевой адрес»	Сетевой адрес — уникальный сетевой идентификатор, присваивающийся каждому участнику сетевого взаимодействия в вычислительной сети. Сетевой адрес, как правило, представлен двумя версиями: 4-й (IPv4) и 6-й (IPv6). IP-адрес (IPv4) представляет собой 32-битовое число. Формой записи IP-адреса (IPv4) является запись в виде четырех десятичных чисел значением от 0 до 255, разделенных точками (например, 192.168.0.1). IP-адрес (IPv6) представляет собой 128-битовое число. Внутри адреса разделителем служит двоеточие (например, 2001:0db8:85a3:0000:0000:8a2e:0370:7334). Ведущие нули допускается в записи опускать. Нулевые группы, идущие подряд, могут быть опущены, вместо них ставят двойное двоеточие (например, fe80:0:0:0:0:0:0:1 можно записать как fe80::1). Более одного такого пропуска в адресе не допускается
«Аппаратный адрес»	Аппаратный адрес — уникальный идентификатор, присваиваемый каждой единице активного оборудования или некоторым их интерфейсам в вычислительных сетях. Аппаратный адрес, как правило, представляет собой MAC-адрес и определяется 6 октетами, между которыми ставят разделитель «:». Пример описания: AA:BB:CC:DD:EE:FF
«Версия ПО»	Указывают полную версию ПО в текстовом виде. Рекомендовано представить в виде A.B.C.D, где: A — мажорная версия (изменение номера мажорной версии ПО происходит при глобальном изменении функциональности); - B — минорная версия (изменение номера минорной версии ПО происходит при введении новой функциональности, ведущей к программной несовместимости со старой версией);

Окончание таблицы 1

Наименование типа данных	Описание типа данных
«Версия ПО»	- C — номер релиза (изменение номера релиза ПО происходит при каждом публичном выпуске обновления ПО, не обозначенном в A и B. Как правило, номерами релизов обозначают выходы исправлений ошибок); - D — номер сборки (изменение номера сборки ПО происходит при любой новой сборке ПО). - «.» — разделитель. Пример описания: 1.3.7.248
«Адрес электронной почты»	Указывают адрес электронной почты, состоящий из двух частей, разделенных символом «@». Левая часть указывает имя почтового ящика. Правая часть адреса указывает доменное имя того сервера, на котором расположен почтовый ящик. Адрес электронной почты определен в соответствии с разделом 3.4 международной спецификации [1]. Пример описания: gost.e-ecolog.ru

6.1.2 Для каждого типа события безопасности как минимум должна быть зарегистрирована информация, состав и содержание которой представлены в таблице 2.

Таблица 2 — Состав и содержание регистрируемой информации

Состав регистрируемой информации	Содержание регистрируемой информации
Дата и время	Включает информацию о дате и времени, в которое было зарегистрировано соответствующее событие безопасности. Формат «Дата/время»
Идентификатор	Представляет собой уникальный идентификатор события безопасности, который должен позволять однозначно идентифицировать событие безопасности в электронном журнале регистрации событий безопасности соответствующего средства, осуществляющего регистрацию событий безопасности, и связанный с ним ожидаемый набор параметров регистрируемой информации. Формат «Текст». Указывают уникальную (для соответствующего средства) последовательность чисел, обозначающую числовой код события безопасности
Наименование	Позволяет определить действие в информационной (автоматизированной) системе, которое привело к его регистрации. Формат «Текст». Указывают краткое наименование события безопасности. Примеры наименования событий безопасности приведены в примечаниях к типам событий безопасности, указанных в приложениях А и Б
Субъект доступа	Представляет собой имя учетной записи пользователя или иные идентификационные данные, позволяющие сопоставить субъект доступа с событием безопасности. В случае невозможности определения субъекта доступа (например, при компьютерных атаках, направленных на отказ в обслуживании) данное поле следует оставить пустым. Формат «Текст»
Тип	Указывают в соответствии с приложениями А и Б. Формат «Текст»
Уровень важности	Влияет на приоритетность обработки события безопасности. Формат «Набор значений». Принимаемые значения: аварийный/фатальный/критический/высокий/средний/низкий/отладочный

6.1.3 Для каждого типа события безопасности дополнительно может быть зарегистрирована информация, состав и содержание которой представлены в таблице 3.

Таблица 3 — Состав и содержание дополнительной регистрируемой информации

Состав регистрируемой информации	Содержание регистрируемой информации
Идентификационная информация средства, осуществляющего регистрацию	Представляет собой уникальный идентификатор средства, осуществляющего регистрацию событий безопасности, который должен позволять идентифицировать события безопасности, зарегистрированные конкретным средством. Формат «Текст». Указывают наименование средства или идентификатор средства
Порядковый номер	Номер, указывающий место конкретной регистрационной записи в последовательности регистрационных записей соответствующего средства, осуществляющего регистрацию событий безопасности (если возможно). Формат «Целое число». Указывают уникальный числовой номер события
Объект доступа	Представляет собой идентификатор (сетевое имя, сетевой адрес, идентификатор процесса и т.п.), позволяющий связать субъект доступа с объектом доступа в части события безопасности (если возможно). Формат «Текст»

6.2 Требования к составу и содержанию регистрируемой информации для типов событий безопасности

6.2.1 Состав и содержание регистрируемой информации для типа события безопасности, связанного с идентификацией и аутентификацией субъекта доступа, представлены в таблице 4.

Таблица 4 — Состав и содержание регистрируемой информации для типа события безопасности, связанного с идентификацией и аутентификацией субъекта доступа

Состав регистрируемой информации	Содержание регистрируемой информации
Идентификатор учетной записи	Формат «Текст». Указывают имя учетной записи пользователя
Результат операции	Формат «Набор значений». Принимаемые значения: успешный/неуспешный
Наличие прав администратора	Формат «Набор значений». Принимаемые значения: да/нет
Сетевой адрес источника входа	Формат «Сетевой адрес»

Дополнительно (если применимо) может быть зарегистрирована информация, представленная в таблице 5.

Таблица 5 — Дополнительно регистрируемая информация для типа события безопасности, связанного с идентификацией и аутентификацией субъекта доступа

Состав регистрируемой информации	Содержание регистрируемой информации
Идентификатор сеанса	Формат «Целое число». Указывают числовое значение номера сеанса пользователя
Идентификатор процесса	Формат «Текст». Указывают номер процесса ОС, при помощи которого выполняется идентификация и аутентификация субъекта доступа
Наименование процесса (полный путь)	Формат «Текст». Указывают полный путь к исполняемому файлу процесса ОС, при помощи которого выполняется идентификации и аутентификации субъекта доступа
Порт источника входа	Формат «Целое число». Число от 0 до 65535, указанное в заголовках протоколов транспортного уровня
Тип входа	Формат «Текст». Указывают способ, при помощи которого выполняется идентификация и аутентификация субъекта доступа: интерактивны/сетевой/удаленный/иные

6.2.2 Состав и содержание регистрируемой информации для типа события безопасности, связанного с осуществлением идентификации объекта доступа, представлены в таблице 6.

Таблица 6 — Состав и содержание регистрируемой информации для типа события безопасности, связанного с осуществлением идентификации объекта доступа

Состав регистрируемой информации	Содержание регистрируемой информации
Идентификатор объекта доступа (или устройства)	Формат «Текст». Указывают уникальный признак объекта, позволяющий отличать его от других объектов
Статус идентификации	Формат «Текст». Указывают причину неуспешной идентификации

Дополнительно (если применимо) может быть зарегистрирована информация, представленная в таблице 7.

Таблица 7 — Дополнительно регистрируемая информация для типа события безопасности, связанного с осуществлением идентификации объекта доступа

Состав регистрируемой информации	Содержание регистрируемой информации
Идентификатор сеанса	Формат «Целое число». Указывают числовое значение номера сеанса пользователя
Идентификатор процесса	Формат «Текст». Указывают номер процесса ОС, при помощи которого выполняется идентификация объекта доступа
Наименование процесса (полный путь)	Формат «Текст». Указывают полный путь к исполняемому файлу процесса ОС, при помощи которого выполняется идентификация объекта доступа
Идентификатор связанной учетной записи	Формат «Текст». Указывают имя учетной записи пользователя, используемое при идентификации устройства (например, токена)
Серийный номер устройства	Формат «Текст». Указывают уникальный заводской номер устройства

6.2.3 Состав и содержание регистрируемой информации для типа события безопасности, связанного с осуществлением аутентификации объекта доступа, представлены в таблице 8.

Таблица 8 — Состав и содержание регистрируемой информации для типа события безопасности, связанного с осуществлением аутентификации объекта доступа

Состав регистрируемой информации	Содержание регистрируемой информации
Идентификатор объекта доступа (или устройства)	Формат «Текст». Указывают уникальный признак объекта, позволяющий отличать его от других объектов
Статус аутентификации	Формат «Текст». Указывают причину неуспешной авторизации

Дополнительно (если применимо) может быть зарегистрирована информация, представленная в таблице 9.

Таблица 9 — Дополнительно регистрируемая информация для типа события безопасности, связанного с осуществлением аутентификации объекта доступа

Состав регистрируемой информации	Содержание регистрируемой информации
Идентификатор связанной учетной записи	Формат «Текст». Указывают имя учетной записи пользователя
Идентификатор сеанса	Формат «Целое число». Указывают числовое значение номера сеанса пользователя
Идентификатор процесса	Формат «Целое число». Указывают числовой уникальный номер процесса ОС, при помощи которого выполняется аутентификация объекта доступа
Наименование процесса (полный путь)	Формат «Текст». Указывают полный путь к исполняемому файлу процесса ОС, при помощи которого выполняется аутентификация объекта доступа
Серийный номер устройства	Формат «Текст». Указывают уникальный заводской номер устройства

6.2.4 Состав и содержание регистрируемой информации для типа события безопасности, связанного с управлением учетными записями пользователей, представлены в таблице 10.

Таблица 10 — Состав и содержание регистрируемой информации для типа события безопасности, связанного с управлением учетными записями пользователей

Состав регистрируемой информации	Содержание регистрируемой информации
Дата и время последнего входа	Формат «Дата/время». Указывают дату и время последней авторизации учетной записи
Идентификатор учетной записи	Формат «Текст». Указывают имя учетной записи пользователя
Параметры проверки пароля	Формат «Набор значений». Принимаемые значения: требуется/не требуется/необходимо сменить
Срок действия учетной записи	Формат «Дата/время». Указывают дату и время окончания срока действия учетной записи. Если срок действия учетной записи не ограничен, указывают значение, определяемое изготовителем средства
Статус учетной записи	Формат «Набор значений». Принимаемые значения: включена/отключена/заблокирована
Тип действия	Формат «Набор значений». Принимаемые значения: создание/изменение/удаление
Тип учетной записи	Формат «Текст». Значения типов учетных записей принимаются в зависимости от ролей, реализованных в СЗИ (например, администратор/пользователь)

Дополнительно (если применимо) может быть зарегистрирована информация, представленная в таблице 11.

Таблица 11 — Дополнительно регистрируемая информация для типа события безопасности, связанного с управлением учетными записями пользователей

Состав регистрируемой информации	Содержание регистрируемой информации
Дата и время последней установки пароля	Формат «Дата/время»
Квалификационная метка	Формат «Текст». Указывают значение метки конфиденциальности
Основной идентификатор группы	Формат «Текст». Указывают идентификатор основной группы учетной записи
Путь к домашнему каталогу	Формат «Текст». Указывают набор символов, определяющий расположение каталога пользователя в файловой системе
Членство в группах	Формат «Набор значений». Указывают перечень идентификаторов или наименований групп, в которых состоит учетная запись
Наименование учетной записи	Формат «Текст». Указываются сведения о владельце учетной записи (например, фамилия, имя, отчество)
Разрешенное время входа	Формат «Дата/время». Указывают время, в течение которого пользователю разрешено использовать учетную запись
Связанный идентификатор устройства идентификации	Формат «Текст». Указывают уникальный признак устройства идентификации, позволяющий отличать его от других устройств идентификации
Результат изменения	Формат «Набор значений». Принимаемые значения: успешный/неуспешный

6.2.5 Состав и содержание регистрируемой информации для типа события безопасности, связанного с управлением аппаратными идентификаторами, представлены в таблице 12.

Таблица 12 — Состав и содержание регистрируемой информации для типа события безопасности, связанного с управлением аппаратными идентификаторами

Состав регистрируемой информации	Содержание регистрируемой информации
Идентификатор связанной учетной записи	Формат «Текст». Указывают имя учетной записи пользователя
Наименование идентификатора	Формат «Текст». Указывают наименование устройства
Серийный номер устройства	Формат «Текст». Указывают уникальный заводской номер устройства
Тип действия	Формат «Набор значений». Принимаемые значения: добавление/изменение/удаление

Дополнительно (если применимо) может быть зарегистрирована информация, представленная в таблице 13.

Таблица 13 — Дополнительно регистрируемая информация для типа события безопасности, связанного с управлением аппаратными идентификаторами

Состав регистрируемой информации	Содержание регистрируемой информации
Срок действия идентификатора	Формат «Дата/время». Указывают дату и время окончания срока действия идентификатора
Результат изменения	Формат «Набор значений». Принимаемые значения: успешный/неуспешный

6.2.6 Состав и содержание регистрируемой информации для типа события безопасности, связанного с управлением средствами аутентификации, представлены в таблице 14.

Таблица 14 — Состав и содержание регистрируемой информации для типа события безопасности, связанного с управлением средствами аутентификации

Состав регистрируемой информации	Содержание регистрируемой информации
Длительность блокировки	Формат «Продолжительность». Указывают количество минут
Количество неуспешных попыток ввода	Формат «Целое число»
Максимальное время действия пароля	Формат «Продолжительность». Указывают количество дней
Минимальная длина пароля	Формат «Целое число»
Сложность пароля	Формат «Набор значений». Указывают сложность пароля. Принимаемые значения: легкий/средний/надежный
Способ аутентификации	Формат «Текст». Указывают допустимые способы прохождения аутентификации
Тип действия	Формат «Набор значений». Принимаемые значения: создание/изменение/удаление

Дополнительно (если применимо) может быть зарегистрирована информация, представленная в таблице 15.

Таблица 15 — Дополнительно регистрируемая информация для типа события безопасности, связанного с управлением средствами аутентификации

Состав регистрируемой информации	Содержание регистрируемой информации
Минимальное время действия пароля	Формат «Продолжительность». Указывают количество дней
Способ хранения пароля	Формат «Набор значений». Принимаемые значения: обратимое шифрование/шифрование/хеш-функция/без преобразования/иное

Окончание таблицы 15

Состав регистрируемой информации	Содержание регистрируемой информации
Результат изменения	Формат «Набор значений». Принимаемые значения: успешный/неуспешный
Количество хранимых предыдущих паролей	Формат «Целое число»

6.2.7 Состав и содержание регистрируемой информации для типа события безопасности, связанного с управлением атрибутами доступа, представлены в таблице 16.

Таблица 16 — Состав и содержание регистрируемой информации для типа события безопасности, связанного с управлением атрибутами доступа

Состав регистрируемой информации	Содержание регистрируемой информации
Идентификатор объекта доступа	Формат «Текст». Указывают уникальный признак объекта, позволяющий отличать его от других объектов
Права владельца объекта	Формат «Текст». Указывают значения прав, разделенные символом «;»
Тип действия	Формат «Набор значений». Принимаемые значения: создание/изменение/удаление
Результат операции	Формат «Набор значений». Принимаемые значения: успешный/неуспешный (если результат операции не определяется идентификатором события безопасности)

Дополнительно (если применимо) может быть зарегистрирована информация, представленная в таблице 17.

Таблица 17 — Дополнительно регистрируемая информация для типа события безопасности, связанного с управлением атрибутами доступа

Состав регистрируемой информации	Содержание регистрируемой информации
Права группы объектов	Формат «Текст». Указывают значения прав, разделенные символом «;»
Квалификационная метка	Формат «Текст». Указывают значение метки конфиденциальности

6.2.8 Состав и содержание регистрируемой информации для типа события безопасности, связанного с доступом к защищаемой информации, представлены в таблице 18.

Таблица 18 — Состав и содержание регистрируемой информации для типа события безопасности, связанного с доступом к защищаемой информации

Состав регистрируемой информации	Содержание регистрируемой информации
Идентификатор объекта доступа	Формат «Текст». Указывают уникальный признак объекта, позволяющий отличать его от других объектов
Тип действия	Формат «Набор значений». Пример принимаемых значений: чтение/запись/исполнение
Результат операции	Формат «Набор значений». Принимаемые значения: успешный/неуспешный (если результат операции не определяется идентификатором события безопасности)

Дополнительно (если применимо) может быть зарегистрирована информация, представленная в таблице 19.

Таблица 19 — Дополнительно регистрируемая информация для типа события безопасности, связанного с доступом к защищаемой информации

Состав регистрируемой информации	Содержание регистрируемой информации
Идентификатор процесса	Формат «Целое число». Указывают числовой уникальный номер процесса ОС
Идентификатор сеанса пользователя	Формат «Целое число». Указывают числовое значение номера сеанса пользователя
Имя процесса (полный путь)	Формат «Текст». Указывают полный путь к исполняемому файлу процесса ОС
Квалификационная метка	Формат «Текст». Указывают значение метки конфиденциальности

6.2.9 Состав и содержание регистрируемой информации для типа события безопасности, связанного с прохождением процедуры доверенной загрузки операционной системы, представлены в таблице 20.

Таблица 20 — Состав и содержание регистрируемой информации для типа события безопасности, связанного с прохождением процедуры доверенной загрузки операционной системы

Состав регистрируемой информации	Содержание регистрируемой информации
Серийный номер носителя	Формат «Текст». Указывают уникальный заводской номер устройства
Результат загрузки	Формат «Набор значений». Принимаемые значения: успешный/неуспешный
Тип действия	Формат «Текст». Указывают этап процедуры прохождения доверенной загрузки
Тип носителя	Формат «Текст». Указывают интерфейс подключения носителя

Дополнительно (если применимо) может быть зарегистрирована информация, представленная в таблице 21.

Таблица 21 — Дополнительно регистрируемая информация для типа события безопасности, связанного с прохождением процедуры доверенной загрузки операционной системы

Состав регистрируемой информации	Содержание регистрируемой информации
Версия средства доверенной загрузки	Формат «Версия ПО»
Наименование носителя	Формат «Текст». Указывают полное официальное наименование носителя
Описание события	Формат «Текст». Указывают расширенную информацию о данном событии безопасности
Состояние сторожевого таймера	Формат «Набор значений». Принимаемые значения: включен/отключен
Состояние тестирования датчика случайных чисел	Формат «Набор значений». Принимаемые значения: успешно/ошибка
Состояние датчика вскрытия корпуса	Формат «Набор значений». Принимаемые значения: вскрыто/не вскрыто
Версия операционной системы	Формат «Версия ПО»
Версия процессора	Формат «Версия ПО»
Версия базовой системы ввода-вывода	Формат «Версия ПО»

6.2.10 Состав и содержание регистрируемой информации для типа события безопасности, связанного с обнаружением файловой активности вредоносных программ, представлены в таблице 22.

Таблица 22 — Состав и содержание регистрируемой информации для типа события безопасности, связанного с обнаружением файловой активности вредоносных программ

Состав регистрируемой информации	Содержание регистрируемой информации
Версия антивирусной программы	Формат «Версия ПО»
Контрольная сумма объекта	Формат «Текст». Указывают значение однонаправленной хеш-функции
Алгоритм контрольной суммы	Формат «Текст». Указывают алгоритм контрольной суммы (например, md5, sha1, sha256 и др.)
Имя вируса	Формат «Текст». Указывают наименование, принятое производителем антивирусной программы
Полный путь к объекту	Формат «Текст». Указывают набор символов, определяющий расположение файла в файловой системе
Тип действия	Формат «Набор значений». Принимаемые значения: вылечен/удален/перемещен на карантин/блокирован/не вылечен/пропущен

Дополнительно (если применимо) может быть зарегистрирована информация, представленная в таблице 23.

Таблица 23 — Дополнительно регистрируемая информация для типа события безопасности, связанного с обнаружением файловой активности вредоносных программ

Состав регистрируемой информации	Содержание регистрируемой информации
Версия базы вирусов	Формат «Дата/время». Указывают дату и время формирования
Наименование зараженного объекта (по возможности)	Формат «Текст». Указывают имя файла
Тип зараженного объекта	Формат «Набор значений». Принимаемые значения: вирус/троянская программа/вредоносная программа/червь/эксплоит/фишинг/вредоносная программа/вредоносная ссылка/потенциальная опасность/поведенческий вирус/иное
Размер зараженного объекта	Формат «Целое число». Указывают размер в байтах
Технология, при помощи которой обнаружен объект	Формат «Набор значений». Принимаемые значения: файловый антивирус/почтовый антивирус/веб-антивирус/антивирус мессенджера/система обнаружения вторжений уровня узла/межсетевой экран/обнаружение подозрительной активности/предотвращение эксплоита/задача сканирования по требованию/иное
Формат зараженного объекта	Формат «Текст». Указывают расширение файла (если применимо)

6.2.11 Состав и содержание регистрируемой информации для типа события безопасности, связанного с обнаружением активности вредоносных программ в почтовом трафике, представлены в таблице 24.

Таблица 24 — Состав и содержание регистрируемой информации для типа события безопасности, связанного с обнаружением активности вредоносных программ в почтовом трафике

Состав регистрируемой информации	Содержание регистрируемой информации
Адрес электронной почты отправителя	Формат «Адрес электронной почты»
Адрес электронной почты получателя	Формат «Адрес электронной почты»
Версия антивирусной программы	Формат «Версия ПО»
Контрольная сумма объекта	Формат «Текст». Указывают значение однонаправленной хеш-функции вложения

Окончание таблицы 24

Состав регистрируемой информации	Содержание регистрируемой информации
Алгоритм контрольной суммы	Формат «Текст». Указывают алгоритм контрольной суммы (например, md5, sha1, sha256 и др.)
Идентификатор сообщения электронной почты	Формат «Текст». Примером описания является уникальный идентификатор сообщения, состоящий из адреса узла-отправителя и номера (уникального в пределах узла)
Имя вируса	Формат «Текст». Указывают наименование, принятое производителем антивирусной программы
Наименование зараженного объекта	Формат «Текст». Указывают имя файла
Сетевой адрес отправителя	Формат «Сетевой адрес»
Тема сообщения	Формат «Текст»
Тип действия	Формат «Набор значений». Принимаемые значения: вылечен/удален/перемещен на карантин/блокирован/не вылечен/пропущен

Дополнительно (если применимо) может быть зарегистрирована информация, представленная в таблице 25.

Таблица 25 — Дополнительно регистрируемая информация для типа события безопасности, связанного с обнаружением активности вредоносных программ в почтовом трафике

Состав регистрируемой информации	Содержание регистрируемой информации
Версия базы вирусов	Формат «Дата/время». Указывают дату и время формирования
Контрольная сумма каждого из вложений	Формат «Текст». Указывают значение однонаправленной хеш-функции
Алгоритм контрольной суммы	Формат «Текст». Указывают алгоритм контрольной суммы (например, md5, sha1, sha256 и др.)
Наименования вложений	Формат «Текст». Указывают имя файла вложения
Размер зараженного объекта	Формат «Целое число». Указывают размер в байтах
Текст сообщения	Формат «Текст»
Технология, при помощи которой обнаружен объект	Формат «Набор значений». Принимаемые значения: файловый антивирус/почтовый антивирус/веб-антивирус/антивирус мессенджера/система обнаружения вторжений уровня узла/межсетевой экран/обнаружение подозрительной активности/предотвращение эксплоита/задача сканирования по требованию/иное
Тип зараженного объекта	Формат «Набор значений». Принимаемые значения: вирус/троянская программа/вредоносная программа/червь/эксплоит/фишинг/вредоносная программа/вредоносная ссылка/потенциальная опасность/поведенческий вирус/иное

6.2.12 Состав и содержание регистрируемой информации для типа события безопасности, связанного с обнаружением активности вредоносных программ в сетевом трафике, представлены в таблице 26.

Таблица 26 — Состав и содержание регистрируемой информации для типа события безопасности, связанного с обнаружением активности вредоносных программ в сетевом трафике

Состав регистрируемой информации	Содержание регистрируемой информации
Версия антивирусной программы	Формат «Версия ПО»
Контрольная сумма объекта	Формат «Текст». Указывают значение однонаправленной хеш-функции

Окончание таблицы 26

Состав регистрируемой информации	Содержание регистрируемой информации
Алгоритм контрольной суммы	Формат «Текст». Указывают алгоритм контрольной суммы (например, md5, sha1, sha256 и др.)
Имя вируса	Формат «Текст». Указывают наименование, принятое производителем антивирусной программы
Порт источника	Формат «Целое число». Число от 0 до 65535, указанное в заголовках протоколов транспортного уровня
Порт назначения	Формат «Целое число». Число от 0 до 65535, указанное в заголовках протоколов транспортного уровня
Сетевой адрес источника	Формат «Сетевой адрес»
Сетевой адрес назначения	Формат «Сетевой адрес»
Протокол	Формат «Текст». Указывают сокращение наименования сетевого протокола. Пример описания: IP/TCP/HTTP
Тип действия	Формат «Набор значений». Принимаемые значения: вылечен/удален/перемещен на карантин/блокирован/не вылечен/пропущен

Дополнительно (если применимо) может быть зарегистрирована информация, представленная в таблице 27.

Таблица 27 — Дополнительно регистрируемая информация для типа события безопасности, связанного с обнаружением активности вредоносных программ в сетевом трафике

Состав регистрируемой информации	Содержание регистрируемой информации
Версия базы вирусов	Формат «Дата/время». Указывают дату и время формирования
Размер зараженного объекта	Формат «Целое число». Указывают размер в байтах
Технология, при помощи которой обнаружен объект	Формат «Набор значений». Принимаемые значения: файловый антивирус/почтовый антивирус/веб-антивирус/антивирус мессенджера/система обнаружения вторжений уровня узла/межсетевой экран/обнаружение подозрительной активности/предотвращение эксплоита/задача сканирования по требованию/иное
Наименование зараженного объекта	Формат «Текст». Указывают имя файла
Тип зараженного объекта	Формат «Набор значений». Принимаемые значения: вирус/троянская программа/вредоносная программа/червь/эксплоит/фишинг/вредоносная программа/вредоносная ссылка/потенциальная опасность/поведенческий вирус/иное
Фрагмент сетевого трафика, содержащий активность вредоносной программы	Формат «Текст»

6.2.13 Состав и содержание регистрируемой информации для типа события безопасности, связанного с проведением обновления базы данных признаков вредоносных компьютерных программ (вирусов), представлены в таблице 28.

Таблица 28 — Состав и содержание регистрируемой информации для типа события безопасности, связанного с проведением обновления базы данных признаков вредоносных компьютерных программ (вирусов)

Состав регистрируемой информации	Содержание регистрируемой информации
Версия антивирусной программы	Формат «Версия ПО»
Версия базы вирусов	Формат «Дата/время». Указывают дату и время формирования
Результат операции	Формат «Набор значений». Принимаемые значения: успешный/неуспешный (если результат операции не определяется идентификатором события безопасности)

Дополнительно (если применимо) может быть зарегистрирована информация, представленная в таблице 29.

Таблица 29 — Дополнительно регистрируемая информация для типа события безопасности, связанного с проведением обновления базы данных признаков вредоносных компьютерных программ (вирусов)

Состав регистрируемой информации	Содержание регистрируемой информации
Количество записей в базе вирусов	Формат «Целое число»
Причина ошибки	Формат «Текст»

6.2.14 Состав и содержание регистрируемой информации для типа события безопасности, связанного с управлением антивирусной защитой, представлены в таблице 30.

Таблица 30 — Состав и содержание регистрируемой информации для типа события безопасности, связанного с управлением антивирусной защитой

Состав регистрируемой информации	Содержание регистрируемой информации
Версия антивирусной программы	Формат «Версия ПО»
Компонент антивирусной программы	Формат «Текст». Указывают краткое наименование
Тип действия	Формат «Текст». Указывают краткое наименование выполняемых действий
Результат операции	Формат «Набор значений». Принимаемые значения: успешный/неуспешный (если результат операции не определяется идентификатором события безопасности)

Дополнительно (если применимо) может быть зарегистрирована информация, представленная в таблице 31.

Таблица 31 — Дополнительно регистрируемая информация для типа события безопасности, связанного с управлением антивирусной защитой

Состав регистрируемой информации	Содержание регистрируемой информации
Значения параметров конфигурации	Формат «Текст». Указывают в следующем виде: «параметр: значение;». Если параметров несколько, то они отделяются при помощи разделителя «;»
Новые (измененные) значения параметров конфигурации	Формат «Текст». Указывают в следующем виде: «параметр: старое значение => новое значение;». Если параметров несколько, то они отделяются при помощи разделителя «;»
Сетевой адрес источника входа	Формат «Сетевой адрес»
Версия базы вирусов	Формат «Дата/время». Указывают дату и время формирования базы вирусов
Время окончания лицензии	Формат «Дата/время»
Номер лицензии	Формат «Текст»
Статус лицензии	Формат «Набор значений». Принимаемые значения: активная/неактивная

6.2.15 Состав и содержание регистрируемой информации для типа события безопасности, связанного с анализом компонента программного обеспечения в среде безопасного выполнения компьютерных программ (песочнице), представлены в таблице 32.

Таблица 32 — Состав и содержание регистрируемой информации для типа события безопасности, связанного с анализом компонента программного обеспечения в среде безопасного выполнения компьютерных программ (песочнице)

Состав регистрируемой информации	Содержание регистрируемой информации
Версия ПО песочницы	Формат «Версия ПО»

Окончание таблицы 32

Состав регистрируемой информации	Содержание регистрируемой информации
Контрольная сумма файла	Формат «Текст». Указывают значение однонаправленной хеш-функции
Алгоритм контрольной суммы	Формат «Текст». Указывают алгоритм контрольной суммы (например, md5, sha1, sha256 и др.)
Наименование файла	Формат «Текст». Указывают наименование файла вместе с расширением (если применимо)
ОС песочницы	Формат «Текст». Указывают полное официальное наименование ОС
Результат анализа	Формат «Текст»
Статус анализа	Формат «Текст». Указывают этап выполнения анализа
Тип действия	Формат «Текст». Указывают краткое наименование выполняемых действий

Дополнительно (если применимо) может быть зарегистрирована информация, представленная в таблице 33.

Таблица 33 — Дополнительно регистрируемая информация для типа события безопасности, связанного с анализом компонента программного обеспечения в среде безопасного выполнения компьютерных программ (песочнице)

Состав регистрируемой информации	Содержание регистрируемой информации
Затраченное время на анализ	Формат «Продолжительность». Указывают количество минут
Расширенный результат анализа	Формат «Текст»
Разрядность ОС песочницы	Формат «Целое число»
Архитектура ПО песочницы	Формат «Текст»

6.2.16 Состав и содержание регистрируемой информации для типа события безопасности, связанного с обнаружением и действиями по защите от незапрашиваемых электронных сообщений (спама), представлены в таблице 34.

Таблица 34 — Состав и содержание регистрируемой информации для типа события безопасности, связанного с обнаружением и действиями по защите от незапрашиваемых электронных сообщений (спама)

Состав регистрируемой информации	Содержание регистрируемой информации
Версия баз антиспама	Формат «Дата/время». Указывают дату и время формирования
Версия программы	Формат «Версия ПО»
Идентификатор сообщения электронной почты	Формат «Текст». Указывают уникальный идентификатор сообщения, состоящий из адреса узла-отправителя и номера
Сетевой адрес отправителя	Формат «Сетевой адрес»
Статус письма	Формат «Текст». Указывают статус отправки/получения письма
Тема сообщения	Формат «Текст»
Тип действия	Формат «Текст». Указывают краткое наименование выполняемых действий
Адрес электронной почты отправителя	Формат «Адрес электронной почты»
Адрес электронной почты получателя	Формат «Адрес электронной почты»

Дополнительно (если применимо) может быть зарегистрирована информация, представленная в таблице 35.

Таблица 35 — Дополнительно регистрируемая информация для типа события безопасности, связанного с обнаружением и действиями по защите от незапрашиваемых электронных сообщений (спама)

Состав регистрируемой информации	Содержание регистрируемой информации
Размер объекта	Формат «Целое число». Указывают размер в байтах
Содержимое служебных заголовков сообщения	Формат «Текст». Указывают служебные заголовки, разделенные символом «;»
Текст сообщения	Формат «Текст»

6.2.17 Состав и содержание регистрируемой информации для типа события безопасности, связанного с управлением защитой от спама, представлены в таблице 36.

Таблица 36 — Состав и содержание регистрируемой информации для типа события безопасности, связанного с управлением защитой от спама

Состав регистрируемой информации	Содержание регистрируемой информации
Тип действия	Формат «Текст». Указывают краткое наименование выполняемых действий

Дополнительно (если применимо) может быть зарегистрирована информация, представленная в таблице 37.

Таблица 37 — Дополнительно регистрируемая информация для типа события безопасности, связанного с управлением защитой от спама

Состав регистрируемой информации	Содержание регистрируемой информации
Значения параметров конфигурации	Формат «Текст». Указывают в следующем виде: «параметр: значение;». Если параметров несколько, то они отделяются при помощи разделителя «;»
Новые (измененные) значения параметров конфигурации	Формат «Текст». Указывают в следующем виде: «параметр: старое значение => новое значение;». Если параметров несколько, то они отделяются при помощи разделителя «;»
Сетевой адрес администратора	Формат «Сетевой адрес»

6.2.18 Состав и содержание регистрируемой информации для типа события безопасности, связанного с обнаружением признаков компьютерных атак в сетевом трафике, представлены в таблице 38.

Таблица 38 — Состав и содержание регистрируемой информации для типа события безопасности, связанного с обнаружением признаков компьютерных атак в сетевом трафике

Состав регистрируемой информации	Содержание регистрируемой информации
Идентификатор сенсора	Формат «Текст». Указывают уникальный (в рамках одного производителя) идентификатор устройства
Класс атаки	Формат «Текст»
Наименование сигнатуры атаки	Формат «Текст»
Сетевой адрес источника	Формат «Сетевой адрес»
Сетевой адрес назначения	Формат «Сетевой адрес»
Протокол	Формат «Текст». Указывают сокращение наименования сетевого протокола. Пример описания: IP/TCP/HTTP
Тип действия	Формат «Текст». Указывают краткое наименование выполняемых действий

Дополнительно (если применимо) может быть зарегистрирована информация, представленная в таблице 39.

Таблица 39 — Дополнительно регистрируемая информация для типа события безопасности, связанного с обнаружением признаков компьютерных атак в сетевом трафике

Состав регистрируемой информации	Содержание регистрируемой информации
Аппаратный адрес источника (если применимо)	Формат «Аппаратный адрес»
Аппаратный адрес назначения (если применимо)	Формат «Аппаратный адрес»
Время жизни пакета	Формат «Целое число». Указывают максимальное число переходов между маршрутизаторами
Идентификатор уязвимости	Формат «Текст»
Используемый метод запроса протокола передачи гипертекста	Формат «Набор значений». Принимаемые значения: GET/POST/PUT/DELETE/HEAD/OPTIONS/PATCH/TRACE/CONNECT
Количество пакетов	Формат «Целое число»
Флаг заголовка пакета	Формат «Набор значений». Принимаемые значения: URG/ACK/PSH/RST/SYN/FIN
Наименование сетевого интерфейса	Формат «Текст». Указывают наименование/порядковый номер интерфейса
Описание сигнатуры атаки	Формат «Текст»
Размер пакета	Формат «Целое число». Указывают размер в байтах
Содержимое пакета	Формат «Текст»

6.2.19 Состав и содержание регистрируемой информации для типа события, связанного с обнаружением признаков компьютерных атак на узле, представлены в таблице 40.

Таблица 40 — Состав и содержание регистрируемой информации для типа события, связанного с обнаружением признаков компьютерных атак на узле

Состав регистрируемой информации	Содержание регистрируемой информации
Класс атаки	Формат «Текст»
Наименование выполняемой службы/ПО/процесса	Формат «Текст». Указывают наименование выполняемой службы/ПО или имя файла
Наименование сигнатуры атаки	Формат «Текст»
Порт источника	Формат «Целое число». Число от 0 до 65535, указанное в заголовках протоколов транспортного уровня
Порт назначения	Формат «Целое число». Число от 0 до 65535, указанное в заголовках протоколов транспортного уровня
Сетевой адрес источника	Формат «Сетевой адрес»
Сетевой адрес назначения	Формат «Сетевой адрес»
Протокол	Формат «Текст». Указывают сокращение наименования сетевого протокола. Пример описания: IP/TCP/HTTP
Тип действия	Формат «Текст». Указывают краткое наименование выполняемых действий
Унифицированный идентификатор ресурса	Формат «Текст»

Дополнительно (если применимо) может быть зарегистрирована информация, представленная в таблице 41.

Таблица 41 — Дополнительно регистрируемая информация для типа события, связанного с обнаружением признаков компьютерных атак на узле

Состав регистрируемой информации	Содержание регистрируемой информации
Аппаратный адрес источника (если применимо)	Формат «Аппаратный адрес»
Аппаратный адрес назначения (если применимо)	Формат «Аппаратный адрес»
Время жизни пакета	Формат «Целое число». Указывают максимальное число переходов между маршрутизаторами
Идентификатор сенсора	Формат «Текст». Указывают уникальный (в рамках одного производителя) идентификатор устройства
Идентификатор уязвимости	Формат «Текст»
Используемый метод запроса протокола передачи гипертекста	Формат «Набор значений». Принимаемые значения: GET/POST/PUT/DELETE/HEAD/OPTIONS/PATCH/TRACE/CONNECT
Количество пакетов	Формат «Целое число»
Флаг заголовка пакета	Формат «Набор значений». Принимаемые значения: URG/ACK/PSH/RST/SYN/FIN
Наименование сетевого интерфейса	Формат «Текст». Указывают наименование/порядковый номер интерфейса
Описание сигнатуры атаки	Формат «Текст»
Размер пакета	Формат «Целое число». Указывают размер в байтах
Содержимое пакета	Формат «Текст»

6.2.20 Состав и содержание регистрируемой информации для типа события безопасности, связанного с проведением обновления базы решающих правил, представлены в таблице 42.

Таблица 42 — Состав и содержание регистрируемой информации для типа события безопасности, связанного с проведением обновления базы решающих правил

Состав регистрируемой информации	Содержание регистрируемой информации
Версия базы решающих правил	Формат «Дата/время». Указывают дату и время формирования
Версия программы	Формат «Версия ПО»
Результат операции	Формат «Набор значений». Принимаемые значения: успешный/неуспешный (если результат операции не определяется идентификатором события безопасности)

Дополнительно (если применимо) может быть зарегистрирована информация, представленная в таблице 43.

Таблица 43 — Дополнительно регистрируемая информация для типа события безопасности, связанного с проведением обновления базы решающих правил

Состав регистрируемой информации	Содержание регистрируемой информации
Количество записей в базе решающих правил	Формат «Целое число»

6.2.21 Состав и содержание регистрируемой информации для типа события безопасности, связанного с управлением средством обнаружения и блокирования компьютерных атак, представлены в таблице 44.

Таблица 44 — Состав и содержание регистрируемой информации для типа события безопасности, связанного с управлением средством обнаружения и блокирования компьютерных атак

Состав регистрируемой информации	Содержание регистрируемой информации
Версия базы решающих правил	Формат «Дата/время». Указывают дату и время формирования
Версия программы	Формат «Версия ПО»
Тип действия	Формат «Текст». Указывают краткое наименование выполняемых действий
Результат операции	Формат «Набор значений». Принимаемые значения: успешный/неуспешный (если результат операции не определяется идентификатором события безопасности)

Дополнительно (если применимо) может быть зарегистрирована информация, представленная в таблице 45.

Таблица 45 — Дополнительно регистрируемая информация для типа события безопасности, связанного с управлением средством обнаружения и блокирования компьютерных атак

Состав регистрируемой информации	Содержание регистрируемой информации
Значения параметров конфигурации	Формат «Текст». Указывают в следующем виде: «параметр: значение;». Если параметров несколько, то они отделяются при помощи разделителя «;»
Новые (измененные) значения параметров конфигурации	Формат «Текст». Указывают в следующем виде: «параметр: старое значение => новое значение;». Если параметров несколько, то они отделяются при помощи разделителя «;»
Сетевой адрес администратора	Формат «Сетевой адрес»
Время окончания лицензии	Формат «Дата/время»
Номер лицензии	Формат «Текст»
Статус лицензии	Формат «Набор значений». Принимаемые значения: подключена/отключена

6.2.22 Состав и содержание регистрируемой информации для типа события безопасности, связанного с фильтрацией сетевого трафика на уровне логических границ сети и сегментов сети, представлены в таблице 46.

Таблица 46 — Состав и содержание регистрируемой информации для типа события безопасности, связанного с фильтрацией сетевого трафика на уровне логических границ сети и сегментов сети

Состав регистрируемой информации	Содержание регистрируемой информации
Наименование правила фильтрации	Формат «Текст»
Номер правила фильтрации	Формат «Целое число»
Порт источника	Формат «Целое число». Число от 0 до 65535, указанное в заголовках протоколов транспортного уровня
Порт назначения	Формат «Целое число». Число от 0 до 65535, указанное в заголовках протоколов транспортного уровня
Сетевой адрес источника	Формат «Сетевой адрес»
Сетевой адрес назначения	Формат «Сетевой адрес»
Сетевой интерфейс	Формат «Текст». Указывают наименование/порядковый номер интерфейса
Протокол	Формат «Текст». Указывают сокращение наименования сетевого протокола. Пример описания: IP/TCP/HTTP
Тип действия	Формат «Текст». Указывают краткое наименование выполняемых действий

Дополнительно (если применимо) может быть зарегистрирована информация, представленная в таблице 47.

Таблица 47 — Дополнительно регистрируемая информация для типа события безопасности, связанного с фильтрацией сетевого трафика на уровне логических границ сети и сегментов сети

Состав регистрируемой информации	Содержание регистрируемой информации
Аппаратный адрес источника (если применимо)	Формат «Аппаратный адрес»
Аппаратный адрес назначения (если применимо)	Формат «Аппаратный адрес»
Время жизни пакета	Формат «Целое число». Указывают максимальное число переходов между маршрутизаторами
Квалификационная метка пакета	Формат «Текст». Указывают значение метки конфиденциальности
Метод запроса протокола передачи гипертекста	Формат «Набор значений». Принимаемые значения: GET/POST/PUT/DELETE/HEAD/OPTIONS/PATCH/TRACE/CONNECT
Размер пакета	Формат «Целое число». Указывают размер в байтах
Унифицированный идентификатор ресурса	Формат «Текст»

6.2.23 Состав и содержание регистрируемой информации для типа события безопасности, связанного с фильтрацией сетевого трафика на уровне узла, представлены в таблице 48.

Таблица 48 — Состав и содержание регистрируемой информации для типа события безопасности, связанного с фильтрацией сетевого трафика на уровне узла

Состав регистрируемой информации	Содержание регистрируемой информации
Наименование правила фильтрации	Формат «Текст»
Направление потока	Формат «Набор значений». Принимаемые значения: входящий/исходящий
Номер правила фильтрации	Формат «Целое число»
Порт источника	Формат «Целое число». Число от 0 до 65535, указанное в заголовках протоколов транспортного уровня
Порт назначения	Формат «Целое число». Число от 0 до 65535, указанное в заголовках протоколов транспортного уровня
Сетевой адрес источника	Формат «Сетевой адрес»
Сетевой адрес назначения	Формат «Сетевой адрес»
Сетевой интерфейс	Формат «Текст». Указывают наименование/порядковый номер интерфейса
Протокол	Формат «Текст». Указывают сокращение наименования сетевого протокола. Пример описания: IP/TCP/HTTP
Тип действия	Формат «Текст». Указывают краткое наименование выполняемых действий

Дополнительно (если применимо) может быть зарегистрирована информация, представленная в таблице 49.

Таблица 49 — Дополнительно регистрируемая информация для типа события безопасности, связанного с фильтрацией сетевого трафика на уровне узла

Состав регистрируемой информации	Содержание регистрируемой информации
Аппаратный адрес источника	Формат «Аппаратный адрес»
Аппаратный адрес назначения	Формат «Аппаратный адрес»

Окончание таблицы 49

Состав регистрируемой информации	Содержание регистрируемой информации
Время жизни пакета	Формат «Целое число». Указывают максимальное число переходов между маршрутизаторами
Квалификационная метка пакета	Формат «Текст». Указывают значение метки конфиденциальности
Размер пакета	Формат «Целое число». Указывают размер в байтах
Метод запроса протокола передачи гипертекста	Формат «Набор значений». Принимаемые значения: GET/POST/PUT/DELETE/HEAD/OPTIONS/PATCH/TRACE/CONNECT
Унифицированный идентификатор ресурса	Формат «Текст»

6.2.24 Состав и содержание регистрируемой информации для типа события безопасности, связанного с фильтрацией сетевого трафика на прикладном уровне, представлены в таблице 50.

Таблица 50 — Состав и содержание регистрируемой информации для типа события безопасности, связанного с фильтрацией сетевого трафика на прикладном уровне при обработке протокола передачи гипертекста

Состав регистрируемой информации	Содержание регистрируемой информации
Версия веб-сервера	Формат «Версия ПО»
Версия ПО межсетевого экрана	Формат «Версия ПО»
Версия протокола передачи гипертекста	Формат «Текст»
Доменное имя	Формат «Текст»
Идентификатор сессии	Формат «Текст»
Идентификатор сигнатуры	Формат «Целое число». Указывают номер правила фильтрации
Код ответа	Формат «Целое число»
Метод запроса	Формат «Набор значений». Принимаемые значения: GET/POST/PUT/DELETE/HEAD/OPTIONS/PATCH/TRACE/CONNECT
Наименование веб-сервера	Формат «Текст». Указывают полное официальное наименование ПО
Пользовательское приложение	Формат «Текст». Указывают полное официальное наименование ПО
Порт назначения	Формат «Целое число». Число от 0 до 65535, указанное в заголовках протоколов транспортного уровня
Порт прокси-сервера	Формат «Целое число». Число от 0 до 65535, указанное в заголовках протоколов транспортного уровня
Порт источника	Формат «Целое число». Число от 0 до 65535, указанное в заголовках протоколов транспортного уровня
Сетевой адрес источника запроса	Формат «Сетевой адрес»
Сетевой адрес прокси-сервера	Формат «Сетевой адрес»
Тип атаки	Формат «Текст»
Тип действия	Формат «Текст». Указывают краткое наименование выполняемых действий
Унифицированный идентификатор источника запроса ресурса	Формат «Текст»
Унифицированный идентификатор ресурса	Формат «Текст»

Дополнительно (если применимо) может быть зарегистрирована информация, представленная в таблице 51.

Таблица 51 — Дополнительно регистрируемая информация для типа события безопасности, связанного с фильтрацией сетевого трафика на прикладном уровне

Состав регистрируемой информации	Содержание регистрируемой информации
Байт передано	Формат «Целое число»
Байт получено	Формат «Целое число»
Геоданные	Формат «Текст». Указывают страна и город
Идентификатор уязвимости	Формат «Текст»
Маркер взаимодействия	Формат «Текст». Указывают в следующем виде: «маркер: значение;»
Результат изменения	Формат «Набор значений». Принимаемые значения: успешный/неуспешный

6.2.25 Состав и содержание регистрируемой информации для типа события безопасности, связанного с управлением фильтрацией сетевого трафика, представлены в таблице 52.

Таблица 52 — Состав и содержание регистрируемой информации для типа события безопасности, связанного с управлением фильтрацией сетевого трафика

Состав регистрируемой информации	Содержание регистрируемой информации
Версия ПО межсетевого экрана	Формат «Версия ПО»
Компонент межсетевого экрана	Формат «Текст». Указывают краткое наименование
Тип действия	Формат «Текст». Указывают краткое наименование выполняемых действий
Результат операции	Формат «Набор значений». Принимаемые значения: успешный/неуспешный (если результат операции не определяется идентификатором события безопасности)

Дополнительно (если применимо) может быть зарегистрирована информация, представленная в таблице 53.

Таблица 53 — Дополнительно регистрируемая информация для типа события безопасности, связанного с управлением фильтрацией сетевого трафика

Состав регистрируемой информации	Содержание регистрируемой информации
Сетевой адрес администратора	Формат «Сетевой адрес»
Статус необходимости перезагрузки межсетевого экрана	Формат «Набор значений». Принимаемые значения: да/нет
Значения параметров конфигурации	Формат «Текст». Указывают в следующем виде: «параметр: значение;». Если параметров несколько, то они отделяются при помощи разделителя «;»
Новые (измененные) значения параметров конфигурации	Формат «Текст». Указывают в следующем виде: «параметр: старое значение => новое значение;». Если параметров несколько, то они отделяются при помощи разделителя «;»

6.2.26 Состав и содержание регистрируемой информации для типа события безопасности, связанного с изменениями в сетевой адресации, представлены в таблице 54.

Таблица 54 — Состав и содержание регистрируемой информации для типа события безопасности, связанного с изменениями в сетевой адресации

Состав регистрируемой информации	Содержание регистрируемой информации
Значение нового сетевого адреса	Формат «Сетевой адрес»
Значение старого сетевой адреса	Формат «Сетевой адрес»
Тип действия	Формат «Текст». Указывают краткое наименование выполняемых действий
Результат операции	Формат «Набор значений». Принимаемые значения: успешный/неуспешный (если результат операции не определяется идентификатором события безопасности)

Дополнительно (если применимо) может быть зарегистрирована информация, представленная в таблице 55.

Таблица 55 — Дополнительно регистрируемая информация для типа события безопасности, связанного с изменениями в сетевой адресации

Состав регистрируемой информации	Содержание регистрируемой информации
Значения маски подсети, шлюза, DNS и DHCP-серверов (при наличии), которые были актуальны для старого сетевого адреса	Формат «Текст». Указывают в следующем виде: «параметр: значение;». Если параметров несколько, то они отделяются при помощи разделителя «;»
Значения маски подсети, шлюза, DNS и DHCP-серверов (при наличии), которые актуальны для нового сетевого адреса	Формат «Текст». Указывают в следующем виде: «параметр: значение;». Если параметров несколько, то они отделяются при помощи разделителя «;»

6.2.27 Состав и содержание регистрируемой информации для типа события безопасности, связанного с изменениями в аппаратной адресации, представлены в таблице 56.

Таблица 56 — Состав и содержание регистрируемой информации для типа события безопасности, связанного с изменениями в аппаратной адресации

Состав регистрируемой информации	Содержание регистрируемой информации
Новый аппаратный адрес	Формат «Аппаратный адрес»
Старый аппаратный адрес	Формат «Аппаратный адрес»
Тип действия	Формат «Текст». Указывают краткое наименование выполняемых действий
Результат операции	Формат «Набор значений». Принимаемые значения: успешный/неуспешный (если результат операции не определяется идентификатором события безопасности)

Дополнительно (если применимо) может быть зарегистрирована информация, представленная в таблице 57.

Таблица 57 — Дополнительно регистрируемая информация для типа события безопасности, связанного с изменениями в аппаратной адресации

Состав регистрируемой информации	Содержание регистрируемой информации
Производитель, которому принадлежит аппаратный адрес	Формат «Текст». Указывают полное официальное наименование компании-производителя

6.2.28 Состав и содержание регистрируемой информации для типа события безопасности, связанного с изменениями в статической маршрутизации, представлены в таблице 58.

Таблица 58 — Состав и содержание регистрируемой информации для типа события безопасности, связанного с изменениями в статической маршрутизации

Состав регистрируемой информации	Содержание регистрируемой информации
Тип действия	Формат «Текст». Указывают краткое наименование выполняемых действий
Тип маршрута	Формат «Текст». Пример описания: к узлу/к сети/по умолчанию/циклический/оповещение
Результат операции	Формат «Набор значений». Принимаемые значения: успешный/неуспешный (если результат операции не определяется идентификатором события безопасности)

Дополнительно (если применимо) может быть зарегистрирована информация, представленная в таблице 59.

Таблица 59 — Дополнительно регистрируемая информация для типа события безопасности, связанного с изменениями в статической маршрутизации

Состав регистрируемой информации	Содержание регистрируемой информации
Интерфейс, через который доступен шлюз	Формат «Текст». Указывают наименование/порядковый номер интерфейса
Значение метрики маршрута	Формат «Целое число»
Значения сетевого адреса назначения, маски подсети, сетевого адреса шлюза, через который доступен сетевой адрес назначения, для старого маршрута	Формат «Текст». Указывают в следующем виде: «параметр: значение;». Если параметров несколько, то они отделяются при помощи разделителя «;»
Значения сетевого адреса назначения, маски подсети, сетевого адреса шлюза, через который доступен сетевой адрес назначения, для нового маршрута	Формат «Текст». Указывают в следующем виде: «параметр: значение;». Если параметров несколько, то они отделяются при помощи разделителя «;»

6.2.29 Состав и содержание регистрируемой информации для типа события безопасности, связанного с изменениями в таблице сопоставления аппаратных адресов и портов, представлены в таблице 60.

Таблица 60 — Состав и содержание регистрируемой информации для типа события безопасности, связанного с изменениями в таблице сопоставления аппаратных адресов и портов

Состав регистрируемой информации	Содержание регистрируемой информации
Аппаратный адрес	Формат «Аппаратный адрес»
Идентификатор виртуальной сети	Формат «Целое число»
Номер порта коммутатора	Формат «Целое число». Указывают порядковый номер порта коммутатора
Тип действия	Формат «Текст». Указывают краткое наименование выполняемых действий
Тип записи	Формат «Набор значений». Принимаемые значения: статическая/динамическая
Результат операции	Формат «Набор значений». Принимаемые значения: успешный/неуспешный (если результат операции не определяется идентификатором события безопасности)

Дополнительно (если применимо) может быть зарегистрирована информация, представленная в таблице 61.

Таблица 61 — Дополнительно регистрируемая информация для типа события безопасности, связанного с изменениями в таблице сопоставления аппаратных адресов и портов

Состав регистрируемой информации	Содержание регистрируемой информации
Количество аппаратных адресов на интерфейсе	Формат «Целое число»
Наименование виртуальной сети	Формат «Текст»
Описание интерфейса	Формат «Текст»

6.2.30 Состав и содержание регистрируемой информации для типа события безопасности, связанного с обнаружением и действиями по защите от атак, направленных на отказ в обслуживании, представлены в таблице 62.

Таблица 62 — Состав и содержание регистрируемой информации для типа события безопасности, связанного с обнаружением и действиями по защите от атак, направленных на отказ в обслуживании

Состав регистрируемой информации	Содержание регистрируемой информации
Источник атаки	Формат «Сетевой адрес»
Код атаки	Формат «Целое число»
Наименование атаки	Формат «Текст»
Порт источника	Формат «Целое число». Число от 0 до 65535, указанное в заголовках протоколов транспортного уровня
Порт назначения	Формат «Целое число». Число от 0 до 65535, указанное в заголовках протоколов транспортного уровня
Процент загрузки канала связи	Формат «Целое число»
Протокол	Формат «Текст». Указывают сокращение наименования сетевого протокола. Пример описания: IP/TCP/HTTP
Скорость проведения атаки	Формат «Целое число». Указывают в Мбит/с
Тип действия	Формат «Текст». Указывают краткое наименование выполняемых действий
Число пакетов	Формат «Целое число»

Дополнительно (если применимо) может быть зарегистрирована информация, представленная в таблице 63.

Таблица 63 — Дополнительно регистрируемая информация для типа события безопасности, связанного с обнаружением и действиями по защите от атак, направленных на отказ в обслуживании

Состав регистрируемой информации	Содержание регистрируемой информации
Время жизни пакета	Формат «Целое число». Указывают максимальное число переходов между маршрутизаторами
Дата и время начала атаки	Формат «Дата/время». Указывают дату и время начала атаки
Длительность атаки	Формат «Продолжительность». Указывают количество минут
Категория атаки	Формат «Текст»
Размер пакета	Формат «Целое число». Указывают размер в байтах

6.2.31 Состав и содержание регистрируемой информации для типа события безопасности, связанного с обнаружением уязвимостей программного обеспечения, представлены в таблице 64.

Таблица 64 — Состав и содержание регистрируемой информации для типа события безопасности, связанного с обнаружением уязвимостей программного обеспечения

Состав регистрируемой информации	Содержание регистрируемой информации
Версия ПО	Формат «Версия ПО»
Идентификатор	Формат «Текст»
Класс уязвимости	Формат «Набор значений». Принимаемые значения: уязвимость кода/уязвимость архитектуры/уязвимость многофакторная
Наименование операционной системы	Формат «Текст»
Наименование ПО	Формат «Текст». Указывают полное официальное наименование ПО
Наименование уязвимости	Формат «Текст»
Тип аппаратной платформы	Формат «Текст». Указывают аппаратную платформу, при установке на которую ПО содержит уязвимость
Тип действия	Формат «Текст». Указывают краткое наименование выполняемых действий
Тип ошибки	Формат «Текст». Указывают идентификатор, установленный в соответствии с общим перечнем ошибок CWE[1)]
Тип программного обеспечения	Формат «Текст»
Уровень опасности уязвимости	Формат «Набор значений». Принимаемые значения: высокий/средний/низкий

Дополнительно (если применимо) может быть зарегистрирована информация, представленная в таблице 65.

Таблица 65 — Дополнительно регистрируемая информация для типа события безопасности, связанного с обнаружением уязвимостей программного обеспечения

Состав регистрируемой информации	Содержание регистрируемой информации
Базовый вектор уязвимости	Формат «Текст». Указывают базовый вектор общей системы оценки уязвимости CVSS[2)]
Дата и время выявления	Формат «Дата/время»
Наличие эксплоита	Формат «Набор значений». Принимаемые значения: да/нет
Описание ошибки	Формат «Текст»
Описание уязвимости	Формат «Текст»
Рекомендации по устранению уязвимости	Формат «Текст»
Производитель ПО	Формат «Текст». Указывают полное официальное наименование
Ссылки на источники	Формат «Текст». Указывают унифицированный идентификатор источника запроса ресурса

6.2.32 Состав и содержание регистрируемой информации для типа события безопасности, связанного с проведением обновления базы уязвимостей, представлены в таблице 66.

[1)] Common Weakness Enumeration (CWE) — общий перечень недостатков (ошибок) опубликован на официальном сайте MITRE по адресу URL: gost.e-ecolog.ru

[2)] Common Vulnerability Scoring System (CVSS) — общая система оценки уязвимости опубликована на официальном сайте сообщества FIRST по адресу URL: gost.e-ecolog.ru

Таблица 66 — Состав и содержание регистрируемой информации для типа события безопасности, связанного с проведением обновления базы уязвимостей

Состав регистрируемой информации	Содержание регистрируемой информации
Версия базы уязвимостей	Формат «Дата/время». Указывают дату и время формирования
Версия программы	Формат «Версия ПО»
Наименование программы	Формат «Текст». Указывают полное официальное наименование ПО
Тип действия	Формат «Текст». Указывают краткое наименование выполняемых действий
Результат операции	Формат «Набор значений». Принимаемые значения: успешный/неуспешный (если результат операции не определяется идентификатором события безопасности)

Дополнительно (если применимо) может быть зарегистрирована информация, представленная в таблице 67.

Таблица 67 — Дополнительно регистрируемая информация для типа события безопасности, связанного с проведением обновления базы уязвимостей

Состав регистрируемой информации	Содержание регистрируемой информации
Количество записей в базе уязвимостей	Формат «Целое число»

6.2.33 Состав и содержание регистрируемой информации для типа события безопасности, связанного с изменениями состава программного обеспечения, представлены в таблице 68.

Таблица 68 — Состав и содержание регистрируемой информации для типа события безопасности, связанного с изменениями состава программного обеспечения

Состав регистрируемой информации	Содержание регистрируемой информации
Версия компонента	Формат «Версия ПО»
Разработчик компонента	Формат «Текст». Указывают полное официальное наименование компании
Тип компонента	Формат «Текст»
Наименование ПО	Формат «Текст». Указывают полное официальное наименование ПО
Полный путь к месту установки	Формат «Текст». Указывают набор символов, определяющий расположение каталога в файловой системе
Тип изменения	Формат «Текст»

Дополнительно (если применимо) может быть зарегистрирована информация, представленная в таблице 69.

Таблица 69 — Дополнительно регистрируемая информация для типа события безопасности, связанного с изменениями состава программного обеспечения

Состав регистрируемой информации	Содержание регистрируемой информации
Перечень пользователей, для которых установлен компонент	Формат «Текст». Указывают идентификаторы учетных записей, разделенные «;», или значение «Для всех»
Размер	Формат «Целое число». Указывают размер в байтах
Разрядность	Формат «Целое число»

6.2.34 Состав и содержание регистрируемой информации для типа события безопасности, связанного с изменениями параметров настроек средств защиты информации, представлены в таблице 70.

Таблица 70 — Состав и содержание регистрируемой информации для типа события безопасности, связанного с изменениями параметров настроек средств защиты информации

Состав регистрируемой информации	Содержание регистрируемой информации
Версия СЗИ	Формат «Версия ПО»
Компонент СЗИ	Формат «Текст». Указывают краткое наименование
Результат операции	Формат «Набор значений». Принимаемые значения: успешный/неуспешный (если результат операции не определяется идентификатором события безопасности)

Дополнительно (если применимо) может быть зарегистрирована информация, представленная в таблице 71.

Таблица 71 — Дополнительно регистрируемая информация для типа события безопасности, связанного с изменениями параметров настроек средств защиты информации

Состав регистрируемой информации	Содержание регистрируемой информации
Значения параметров конфигурации	Формат «Текст». Указывают в следующем виде: «параметр: значение;». Если параметров несколько, то они отделяются при помощи разделителя «;»
Новые (измененные) значения параметров конфигурации	Формат «Текст». Указывают в следующем виде: «параметр: старое значение => новое значение;». Если параметров несколько, то они отделяются при помощи разделителя «;»

6.2.35 Состав и содержание регистрируемой информации для типа события безопасности, связанного с установкой, изменением системного времени, представлены в таблице 72.

Таблица 72 — Состав и содержание регистрируемой информации для типа события безопасности, связанного с установкой, изменением системного времени

Состав регистрируемой информации	Содержание регистрируемой информации
Идентификатор процесса, вызвавшего изменение системного времени	Формат «Целое число». Указывают числовой уникальный номер процесса ОС
Новое значение системного времени	Формат «Дата/время»
Предыдущее значение системного времени	Формат «Дата/время»
Тип действия	Формат «Текст». Указывают краткое наименование выполняемых действий
Результат операции	Формат «Набор значений». Принимаемые значения: успешный/неуспешный (если результат операции не определяется идентификатором события безопасности)

Дополнительно (если применимо) может быть зарегистрирована информация, представленная в таблице 73.

Таблица 73 — Дополнительно регистрируемая информация для типа события безопасности, связанного с установкой, изменением системного времени

Состав регистрируемой информации	Содержание регистрируемой информации
Сетевой адрес сервера точного времени	Формат «Сетевой адрес»

6.2.36 Состав и содержание регистрируемой информации для типа события безопасности, связанного с изменением настроек общего программного обеспечения, представлены в таблице 74.

Таблица 74 — Состав и содержание регистрируемой информации для типа события безопасности, связанного с изменением настроек общего программного обеспечения

Состав регистрируемой информации	Содержание регистрируемой информации
Версия ПО	Формат «Версия ПО»
Наименование компонента ПО	Формат «Текст». Указывают краткое наименование ПО
Результат операции	Формат «Набор значений». Принимаемые значения: успешный/неуспешный (если результат операции не определяется идентификатором события безопасности)

Дополнительно (если применимо) может быть зарегистрирована информация, представленная в таблице 75.

Таблица 75 — Дополнительно регистрируемая информация для типа события безопасности, связанного с изменением настроек общего программного обеспечения

Состав регистрируемой информации	Содержание регистрируемой информации
Новые (измененные) значения параметров конфигурации	Формат «Текст». Указывают в следующем виде: «параметр: старое значение => новое значение;». Если параметров несколько, то они отделяются при помощи разделителя «;»
Значения параметров конфигурации	Формат «Текст». Указывают в следующем виде: «параметр: значение;». Если параметров несколько, то они отделяются при помощи разделителя «;»

6.2.37 Состав и содержание регистрируемой информации для типа события безопасности, связанного с контролем наличия обязательных обновлений программного обеспечения, представлены в таблице 76.

Таблица 76 — Состав и содержание регистрируемой информации для типа события безопасности, связанного с контролем наличия обязательных обновлений программного обеспечения

Состав регистрируемой информации	Содержание регистрируемой информации
Версия ПО	Формат «Версия ПО»
Идентификатор обновления	Формат «Текст»
Источник обновлений	Формат «Текст»
Контрольная сумма обновления	Формат «Текст». Указывают значение однонаправленной хеш-функции
Алгоритм контрольной суммы	Формат «Текст». Указывают алгоритм контрольной суммы (например, md5, sha1, sha256 и др.)
Наименование ПО	Формат «Текст». Указывают полное официальное наименование ПО
Результат операции	Формат «Набор значений». Принимаемые значения: успешный/неуспешный (если результат операции не определяется идентификатором события безопасности)

Дополнительно (если применимо) может быть зарегистрирована информация, представленная в таблице 77.

Таблица 77 — Дополнительно регистрируемая информация для типа события безопасности, связанного с контролем наличия обязательных обновлений программного обеспечения

Состав регистрируемой информации	Содержание регистрируемой информации
Ссылка на описание обновления	Формат «Текст». Указывают унифицированный идентификатор источника запроса ресурса
Размер файла обновлений	Формат «Целое число». Указывают размер в байтах

Окончание таблицы 77

Состав регистрируемой информации	Содержание регистрируемой информации
Список обновляемых файлов	Формат «Текст». Указывают перечень наименований файлов, разделенных символом «;»
Перечень закрываемых уязвимостей	Формат «Текст». Указывают перечень закрываемых уязвимостей, разделенных символом «;»
Производитель	Формат «Текст». Указывают полное официальное наименование производителя

6.2.38 Состав и содержание регистрируемой информации для типа события безопасности, связанного с выполнением процедуры установки/удаления компонентов программного обеспечения, представлены в таблице 78.

Таблица 78 — Состав и содержание регистрируемой информации для типа события безопасности, связанного с выполнением процедуры установки/удаления компонентов программного обеспечения

Состав регистрируемой информации	Содержание регистрируемой информации
Наименование компонента ПО	Формат «Текст». Указывают полное официальное наименование ПО
Версия компонента ПО	Формат «Версия ПО»
Полный путь к месту установки компонента	Формат «Текст». Указывают набор символов, определяющий расположение каталога в файловой системе
Производитель компонента	Формат «Текст». Указывают полное официальное наименование производителя
Тип действия	Формат «Набор значений». Принимаемые значения: установка/удаление
Результат операции	Формат «Набор значений». Принимаемые значения: успешный/неуспешный (если результат операции не определяется идентификатором события безопасности)

Дополнительно (если применимо) может быть зарегистрирована информация, представленная в таблице 79.

Таблица 79 — Дополнительно регистрируемая информация для типа события безопасности, связанного с выполнением процедуры установки/удаления компонентов программного обеспечения

Состав регистрируемой информации	Содержание регистрируемой информации
Размер	Формат «Целое число». Указывают размер в байтах
Разрядность	Формат «Целое число»
Перечень пользователей, для которых установлен компонент	Формат «Текст». Указываются идентификаторы учетных записей, разделенные «;», или значение «Для всех»

6.2.39 Состав и содержание регистрируемой информации для типа события безопасности, связанного с управлением запуском/остановкой компонентов программного обеспечения, представлены в таблице 80.

Таблица 80 — Состав и содержание регистрируемой информации для типа события безопасности, связанного с управлением запуском/остановкой компонентов программного обеспечения

Состав регистрируемой информации	Содержание регистрируемой информации
Идентификатор процесса	Формат «Целое число». Указывают числовой уникальный номер процесса ОС

Окончание таблицы 80

Состав регистрируемой информации	Содержание регистрируемой информации
Полный путь к файлу процесса	Формат «Текст». Указывают полный путь к исполняемому файлу процесса ОС
Имя родительского процесса	Формат «Текст». Указывают имя файла
Идентификатор родительского процесса	Формат «Целое число». Указывают числовой уникальный номер процесса ОС
Тип действия	Формат «Набор значений». Принимаемые значения: остановка/запуск

Дополнительно (если применимо) может быть зарегистрирована информация, представленная в таблице 81.

Таблица 81 — Дополнительно регистрируемая информация для типа события безопасности, связанного с управлением запуском/остановкой компонентов программного обеспечения

Состав регистрируемой информации	Содержание регистрируемой информации
Время работы процесса в режиме ядра	Формат «Продолжительность». Указывают количество секунд по завершению работы процесса
Время работы процесса в режиме пользователя	Формат «Продолжительность». Указывают количество секунд по завершению работы процесса
Версия исполняемого файла	Формат «Версия ПО»
Контрольная сумма исполняемого файла	Формат «Текст». Указывают значение однонаправленной хеш-функции
Алгоритм контрольной суммы	Формат «Текст». Указывают алгоритм контрольной суммы (например, md5, sha1, sha256 и др.)
Разработчик (производитель) исполняемого файла	Формат «Текст». Указывают полное официальное наименование производителя
Квалификационная метка процесса	Формат «Текст». Указывают значение метки конфиденциальности

6.2.40 Состав и содержание регистрируемой информации для типа события безопасности, связанного с обнаружением утечки информации через съемные машинные носители информации и сетевые устройства, представлены в таблице 82.

Таблица 82 — Состав и содержание регистрируемой информации для типа события безопасности, связанного с обнаружением утечки информации через съемные машинные носители информации и сетевые устройства

Состав регистрируемой информации	Содержание регистрируемой информации
Имя устройства	Формат «Текст»
Имя рабочей станции	Формат «Текст»
Имя файла	Формат «Текст»
Путь к файлу (если применимо)	Формат «Текст». Указывают набор символов, определяющий расположение файла в файловой системе

Дополнительно (если применимо) может быть зарегистрирована информация, представленная в таблице 83.

Таблица 83 — Дополнительно регистрируемая информация для типа события безопасности, связанного с обнаружением утечки информации через съемные машинные носители информации и сетевые устройства

Состав регистрируемой информации	Содержание регистрируемой информации
Объект защиты	Формат «Текст»
Категория объекта	Формат «Текст»
Наименование политики	Формат «Текст»
Размер файла	Формат «Целое число». Указывают размер в байтах
Квалификационная метка файла	Формат «Текст». Указывают значение метки конфиденциальности
Квалификационная метка съемного машинного носителя информации (сетевого устройства)	Формат «Текст». Указывают значение метки конфиденциальности
Тип действия	Формат «Текст». Указывают краткое наименование выполняемых действий
Результат операции	Формат «Текст». Пример описания: успешно/неуспешно

6.2.41 Состав и содержание регистрируемой информации для типа события безопасности, связанного с обнаружением утечки информации через системы обмена мгновенными сообщениями, представлены в таблице 84.

Таблица 84 — Состав и содержание регистрируемой информации для типа события безопасности, связанного с обнаружением утечки информации через системы обмена мгновенными сообщениями

Состав регистрируемой информации	Содержание регистрируемой информации
Сетевой адрес сервера перехвата	Формат «Сетевой адрес»
Имя устройства	Формат «Текст»
Имя рабочей станции	Формат «Текст»
Путь к файлу (если применимо)	Формат «Текст». Указывают набор символов, определяющий расположение файла в файловой системе
Тип действия	Формат «Текст». Указывают краткое наименование выполняемых действий

Дополнительно (если применимо) может быть зарегистрирована информация, представленная в таблице 85.

Таблица 85 — Дополнительно регистрируемая информация для типа события безопасности, связанного с обнаружением утечки информации через системы обмена мгновенными сообщениями

Состав регистрируемой информации	Содержание регистрируемой информации
Объект защиты	Формат «Текст»
Категория объекта	Формат «Текст»
Наименование политики	Формат «Текст»
Размер файла	Формат «Целое число». Указывают размер в байтах
Результат операции	Формат «Текст». Пример описания: успешно/неуспешно

6.2.42 Состав и содержание регистрируемой информации для типа события безопасности, связанного с обнаружением утечки информации через электронную почту, представлены в таблице 86.

Таблица 86 — Состав и содержание регистрируемой информации для типа события безопасности, связанного с обнаружением утечки информации через электронную почту

Состав регистрируемой информации	Содержание регистрируемой информации
Тип действия	Формат «Текст». Указывают краткое наименование выполняемых действий
Дата и время отправки	Формат «Дата/время»
Дата и время перехвата	Формат «Дата/время»
Состояние доставки	Формат «Текст»
Адрес электронной почты отправителя	Формат «Адрес электронной почты»
Адрес электронной почты получателя	Формат «Адрес электронной почты»
Наличие вложений	Формат «Текст». Указывают наличие вложений: есть/нет

Дополнительно (если применимо) может быть зарегистрирована информация, представленная в таблице 87.

Таблица 87 — Дополнительно регистрируемая информация для типа события безопасности, связанного с обнаружением утечки информации через электронную почту

Состав регистрируемой информации	Содержание регистрируемой информации
Объект защиты	Формат «Текст»
Категория объекта	Формат «Текст»
Наименование политики	Формат «Текст». Указывают наименование политики контроля утечки информации (для идентификации правил контроля утечки)
Размер файла	Формат «Целое число». Указывают размер в байтах
Тип файла	Формат «Текст»
Результат операции	Формат «Текст». Пример описания: успешно/неуспешно

6.2.43 Состав и содержание регистрируемой информации для типа события безопасности, связанного с выводом защищаемой информации на печать, представлены в таблице 88.

Таблица 88 — Состав и содержание регистрируемой информации для типа события безопасности, связанного с выводом защищаемой информации на печать

Состав регистрируемой информации	Содержание регистрируемой информации
Тип действия	Формат «Текст». Указывают краткое наименование выполняемых действий
Порт принтера	Формат «Текст»
Наименование принтера	Формат «Текст». Указывают наименование производителя и модель
Сетевой адрес клиента	Формат «Сетевой адрес»
Наименование файла	Формат «Текст». Указывают набор символов, определяющий расположение файла в файловой системе
Число страниц в файле	Формат «Целое число»
Число страниц распечатано	Формат «Целое число»
Тип печати	Формат «Набор значений». Принимаемые значения: в файл/на принтер
Сетевой адрес принтера	Формат «Сетевой адрес»
Результат операции	Формат «Набор значений». Принимаемые значения: успешный/неуспешный (если результат операции не определяется идентификатором события безопасности)

Дополнительно (если применимо) может быть зарегистрирована информация, представленная в таблице 89.

Таблица 89 — Дополнительно регистрируемая информация для типа события безопасности, связанного с выводом защищаемой информации на печать

Состав регистрируемой информации	Содержание регистрируемой информации
Номер задания	Формат «Целое число». Указывают номер задания печати
Причина отказа печати	Формат «Текст»
Формат листа	Формат «Текст». Пример описания: A4
Квалификационная метка документа	Формат «Текст». Указывают значение метки конфиденциальности

6.2.44 Состав и содержание регистрируемой информации для типа события безопасности, связанного с подключением/отключением съемного машинного носителя информации, представлены в таблице 90. В случае, если съемный машинный носитель содержит несколько логических томов, подключение каждого логического тома подлежит собственной регистрации.

Таблица 90 — Состав и содержание регистрируемой информации для типа события безопасности, связанного с подключением/отключением съемного машинного носителя информации

Состав регистрируемой информации	Содержание регистрируемой информации
Тип действия	Формат «Набор значений». Принимаемые значения: подключение/отключение
Серийный номер устройства или иные уникальные аппаратные идентификационные признаки съемного машинного носителя информации	Формат «Текст». Указывают уникальный заводской номер устройства
Класс устройства	Формат «Текст»
Наименование устройства	Формат «Текст»
Имя тома	Формат «Текст»
Результат операции	Формат «Набор значений». Принимаемые значения: успешный/неуспешный (если результат операции не определяется идентификатором события безопасности)
Размер тома	Формат «Целое число». Указывают размер в байтах
Файловая система	Формат «Текст». Указывают сокращенное наименование файловой системы. Пример описания: NTFS

Дополнительно (если применимо) может быть зарегистрирована информация, представленная в таблице 91.

Таблица 91 — Дополнительно регистрируемая информация для типа события безопасности, связанного с подключением/отключением съемного машинного носителя информации

Состав регистрируемой информации	Содержание регистрируемой информации
Доступное пространство	Формат «Целое число». Указывают значение в байтах
Причина блокировки	Формат «Текст»
Квалификационная метка	Формат «Текст». Указывают значение метки конфиденциальности
Код устройства	Формат «Текст». Указывают шестнадцатеричный код
Код изготовителя	Формат «Текст». Указывают шестнадцатеричный код

6.2.45 Состав и содержание регистрируемой информации для типа события безопасности, связанного с выполнением действий с файлами на съемных машинных носителях информации, представлены в таблице 92.

Таблица 92 — Состав и содержание регистрируемой информации для типа события безопасности, связанного с выполнением действий с файлами на съемных машинных носителях информации

Состав регистрируемой информации	Содержание регистрируемой информации
Серийный номер устройства	Формат «Текст». Указывают уникальный заводской номер устройства
Полный путь к файлу	Формат «Текст». Указывают набор символов, определяющий расположение файла в файловой системе
Тип доступа к файлу	Формат «Набор значений». Принимаемые значения: чтение/запись/исполнение
Идентификатор процесса	Формат «Целое число». Указывают числовой уникальный номер процесса ОС
Имя тома	Формат «Текст»
Результат операции	Формат «Набор значений». Принимаемые значения: успешный/неуспешный (если результат операции не определяется идентификатором события безопасности)

Дополнительно (если применимо) может быть зарегистрирована информация, представленная в таблице 93.

Таблица 93 — Дополнительно регистрируемая информация для типа события безопасности, связанного с выполнением действий с файлами на съемных машинных носителях информации

Состав регистрируемой информации	Содержание регистрируемой информации
Наименование файла	Формат «Текст». Указывают наименование файла вместе с расширением (если применимо)
Размер файла	Формат «Целое число». Указывают размер в байтах
Контрольная сумма файла	Формат «Текст». Указывают значение однонаправленной хеш-функции
Алгоритм контрольной суммы	Формат «Текст». Указывают алгоритм контрольной суммы (например, md5, sha1, sha256 и др.)
Квалификационная метка файла	Формат «Текст». Указывают значение метки конфиденциальности
Расширение файла (если применимо)	Формат «Текст». Указывают расширение файла без символа «.»

6.2.46 Состав и содержание регистрируемой информации для типа события безопасности, связанного с выполнением резервного копирования, представлены в таблице 94.

Таблица 94 — Состав и содержание регистрируемой информации для типа события безопасности, связанного с выполнением резервного копирования

Состав регистрируемой информации	Содержание регистрируемой информации
Идентификатор задания на резервирование	Формат «Целое число». Указывают номер задания
Тип действия	Формат «Текст». Указывают краткое наименование выполняемых действий
Тип резервного копирования	Формат «Текст». Пример описания: Полное
Затраченное время	Формат «Продолжительность». Указывают количество минут
Путь резервного копирования	Формат «Текст». Указывают набор символов, определяющий расположение каталога или файла в файловой системе
Идентификатор хранилища	Формат «Текст»

Окончание таблицы 94

Состав регистрируемой информации	Содержание регистрируемой информации
Количество исходных файлов	Формат «Целое число»
Контрольная сумма резервной копии	Формат «Текст». Указывают значение однонаправленной хеш-функции
Алгоритм контрольной суммы	Формат «Текст». Указывают алгоритм контрольной суммы (например, md5, sha1, sha256 и др.)
Сетевой адрес источника данных для резервирования	Формат «Сетевой адрес»
Результат операции	Формат «Текст». Пример описания: успешно/неуспешно (с ошибкой) (если результат операции не определяется идентификатором события безопасности)

Дополнительно (если применимо) может быть зарегистрирована информация, представленная в таблице 95.

Таблица 95 — Дополнительно регистрируемая информация для типа события безопасности, связанного с выполнением резервного копирования

Состав регистрируемой информации	Содержание регистрируемой информации
Тип файла	Формат «Текст»
Наименование файла	Формат «Текст». Указывают наименование файла вместе с расширением (если применимо)
Размер исходного файла (архивируемого)	Формат «Целое число». Указывают размер в байтах
Размер полученного файла	Формат «Целое число». Указывают размер в байтах
Свободное пространство	Формат «Целое число». Указывают в байтах
Скорость передачи данных	Формат «Целое число». Указывают среднюю скорость передачи данных в Мбит/с
Наименование ПО для резервного копирования	Формат «Текст». Указывают полное официальное наименование ПО
Версия ПО для резервного копирования	Формат «Версия ПО»
Сетевой адрес хранилища	Формат «Сетевой адрес»

6.2.47 Состав и содержание регистрируемой информации для типа события безопасности, связанного с управлением резервным копированием, представлены в таблице 96.

Таблица 96 — Состав и содержание регистрируемой информации для типа события безопасности, связанного с управлением резервным копированием

Состав регистрируемой информации	Содержание регистрируемой информации
Свободное пространство	Формат «Целое число». Указывают размер в байтах
Идентификатор хранилища	Формат «Текст»
Сетевой адрес хранилища	Формат «Сетевой адрес»
Путь резервного копирования	Формат «Текст». Указывают набор символов, определяющий расположение каталога или файла в файловой системе
Идентификатор задания на резервирование	Формат «Целое число». Указывают номер задания
Наименование задания на резервирование	Формат «Текст»

Окончание таблицы 96

Состав регистрируемой информации	Содержание регистрируемой информации
Тип действия	Формат «Текст». Указывают краткое наименование выполняемых действий
Тип резервного копирования	Формат «Текст». Пример описания: Полное
Результат операции	Формат «Текст». Пример описания: успешно/неуспешно (с ошибкой) (если результат операции не определяется идентификатором события безопасности)

Дополнительно (если применимо) может быть зарегистрирована информация, представленная в таблице 97.

Таблица 97 — Дополнительно регистрируемая информация для типа события безопасности, связанного с управлением резервным копированием

Состав регистрируемой информации	Содержание регистрируемой информации
Периодичность запуска задания	Формат «Продолжительность». Указывают количество минут
Дата и время следующего запуска задания	Формат «Дата/время». Указывают дату и время следующего запуска задания
Наименование ПО для резервного копирования	Формат «Текст». Указывают полное официальное наименование ПО
Версия ПО для резервного копирования	Формат «Версия ПО»

6.2.48 Состав и содержание регистрируемой информации для типа события безопасности, связанного с выполнением восстановления информации, представлены в таблице 98.

Таблица 98 — Состав и содержание регистрируемой информации для типа события безопасности, связанного с выполнением восстановления информации

Состав регистрируемой информации	Содержание регистрируемой информации
Идентификатор задания на восстановление	Формат «Целое число». Указывают номер задания
Тип действия	Формат «Текст». Указывают краткое наименование выполняемых действий
Тип восстанавливаемого файла	Формат «Текст»
Имя восстанавливаемого файла	Формат «Текст»
Размер полученного файла	Формат «Целое число». Указывают размер в байтах
Путь файла восстановления	Формат «Текст». Указывают набор символов, определяющий расположение каталога или файла в файловой системе
Контрольная сумма полученного файла	Формат «Текст». Указывают значение однонаправленной хеш-функции
Алгоритм контрольной суммы	Формат «Текст». Указывают алгоритм контрольной суммы (например, md5, sha1, sha256 и др.)
Результат операции	Формат «Текст». Пример описания: успешно/неуспешно (с ошибкой)

Дополнительно (если применимо) может быть зарегистрирована информация, представленная в таблице 99.

Таблица 99 — Дополнительно регистрируемая информация для типа события безопасности, связанного с выполнением восстановления информации

Состав регистрируемой информации	Содержание регистрируемой информации
Размер исходного файла	Формат «Целое число». Указывают размер в байтах
Затраченное время восстановления	Формат «Продолжительность». Указывают количество минут
Контрольная сумма файла до восстановления	Формат «Текст». Указывают значение однонаправленной хеш-функции
Алгоритм контрольной суммы	Формат «Текст». Указывают алгоритм контрольной суммы (например, md5, sha1, sha256 и др.)
Идентификатор хранилища	Формат «Текст»
Сетевой адрес хранилища	Формат «Сетевой адрес»

6.2.49 Состав и содержание регистрируемой информации для типа события безопасности, связанного с контролем использования интерфейсов ввода (вывода) информации, представлены в таблице 100.

Таблица 100 — Состав и содержание регистрируемой информации для типа события безопасности, связанного с контролем использования интерфейсов ввода (вывода) информации

Состав регистрируемой информации	Содержание регистрируемой информации
Тип шины	Формат «Текст». Указывают тип шины подключения устройства. Пример описания: USB
Серийный номер устройства	Формат «Текст». Указывают уникальный заводской номер устройства
Наименование устройства	Формат «Текст»
Код устройства	Формат «Текст». Указывают шестнадцатеричный код
Тип действия	Формат «Текст». Указывают краткое наименование выполняемых действий
Класс устройства	Формат «Текст»

Дополнительно (если применимо) может быть зарегистрирована информация, представленная в таблице 101.

Таблица 101 — Дополнительно регистрируемая информация для типа события безопасности, связанного с контролем использования интерфейсов ввода (вывода) информации

Состав регистрируемой информации	Содержание регистрируемой информации
Изготовитель устройства	Формат «Текст». Указывают полное официальное наименование компании
Код изготовителя устройства	Формат «Текст». Указывают шестнадцатеричный код
Идентификатор порта ввода (вывода)	Формат «Текст»

6.2.50 Состав и содержание регистрируемой информации для типа события безопасности, связанного с контролем целостности, представлены в таблице 102.

Таблица 102 — Состав и содержание регистрируемой информации для типа события безопасности, связанного с контролем целостности

Состав регистрируемой информации	Содержание регистрируемой информации
Тип объекта	Формат «Текст»
Имя ресурса	Формат «Текст»

Окончание таблицы 102

Состав регистрируемой информации	Содержание регистрируемой информации
Метод контроля	Формат «Текст»
Тип реакции	Формат «Текст»
Наименование алгоритма расчета контрольных сумм	Формат «Текст». Указывают сокращеное наименование алгоритма расчета контрольных сумм. Пример описания: MD5
Эталонное значение контрольной суммы	Формат «Текст». Указывают значение однонаправленной хеш-функции
Текущее значение контрольной суммы	Формат «Текст». Указывают значение однонаправленной хеш-функции

Дополнительно (если применимо) может быть зарегистрирована информация, представленная в таблице 103.

Таблица 103 — Дополнительно регистрируемая информация для типа события безопасности, связанного с контролем целостности

Состав регистрируемой информации	Содержание регистрируемой информации
Описание события	Формат «Текст». Указывают информацию о данном событии безопасности
Номер задания контроля целостности	Формат «Целое число»
Наименование задания контроля целостности	Формат «Текст»
Наименование СЗИ контроля целостности	Формат «Текст». Указывают полное официальное наименование ПО
Версия СЗИ контроля целостности	Формат «Версия ПО»
Дата и время создания эталонного значения	Формат «Дата/время»

6.2.51 Состав и содержание регистрируемой информации для типа события безопасности, связанного с гарантированным уничтожением информации, представлены в таблице 104.

Таблица 104 — Состав и содержание регистрируемой информации для типа события безопасности, связанного с гарантированным уничтожением информации

Состав регистрируемой информации	Содержание регистрируемой информации
Имя объекта	Формат «Текст»
Полный путь к объекту	Формат «Текст». Указывают набор символов, определяющий расположение файла в файловой системе
Количество циклов затирания	Формат «Целое число»
Идентификатор процесса	Формат «Целое число». Указывают числовой уникальный номер процесса ОС
Размер объекта	Формат «Целое число». Указывают размер в байтах

Дополнительно (если применимо) может быть зарегистрирована информация, представленная в таблице 105.

Таблица 105 — Дополнительно регистрируемая информация для типа события безопасности, связанного с гарантированным уничтожением информации

Состав регистрируемой информации	Содержание регистрируемой информации
Серийный номер устройства	Формат «Текст». Указывают уникальный заводской номер устройства

Окончание таблицы 105

Состав регистрируемой информации	Содержание регистрируемой информации
Расширение файла (если применимо)	Формат «Текст». Указывают расширение файла без символа «.»
Наименование СЗИ для уничтожения	Формат «Текст». Указывают полное официальное наименование ПО
Версия СЗИ для уничтожения	Формат «Версия ПО»
Квалификационная метка файла	Формат «Текст». Указывают значение метки конфиденциальности
Контрольная сумма объекта	Формат «Текст». Указывают значение однонаправленной хеш-функции
Алгоритм контрольной суммы	Формат «Текст». Указывают алгоритм контрольной суммы (например, md5, sha1, sha256 и др.)

6.2.52 Состав и содержание регистрируемой информации для типа события безопасности, связанного с контролем функционирования средств защиты информации, представлены в таблице 106.

Таблица 106 — Состав и содержание регистрируемой информации для типа события безопасности, связанного с контролем функционирования средств защиты информации

Состав регистрируемой информации	Содержание регистрируемой информации
Компонент СЗИ	Формат «Текст». Указывают краткое наименование
Наименование СЗИ	Формат «Текст». Указывают полное официальное наименование СЗИ
Версия СЗИ	Формат «Версия ПО»
Результат контроля	Формат «Текст». Пример описания: успешно/неуспешно

Дополнительно (если применимо) может быть зарегистрирована информация, представленная в таблице 107.

Таблица 107 — Дополнительно регистрируемая информация для типа события безопасности, связанного с контролем функционирования средств защиты информации

Состав регистрируемой информации	Содержание регистрируемой информации
Описание события	Формат «Текст». Указывают расширенную информацию о данном событии безопасности
Причина прекращения функционирования	Формат «Текст»
Длительность прекращения функционирования	Формат «Продолжительность». Указывают количество минут

6.2.53 Состав и содержание регистрируемой информации для типа события безопасности, связанного с прекращением функционирования (сбой, отказ) программного, технического или программно-технического средства защиты информации, представлены в таблице 108.

Таблица 108 — Состав и содержание регистрируемой информации для типа события безопасности, связанного с прекращением функционирования (сбой, отказ) программного, технического или программно-технического средства защиты информации

Состав регистрируемой информации	Содержание регистрируемой информации
Наименование СЗИ	Формат «Текст». Указывают полное официальное наименование СЗИ
Версия СЗИ	Формат «Версия ПО»
Причина прекращения функционирования	Формат «Текст»

Дополнительно (если применимо) может быть зарегистрирована информация, представленная в таблице 109.

Таблица 109 — Дополнительно регистрируемая информация для типа события безопасности, связанного с прекращением функционирования (сбой, отказ) программного, технического или программно-технического средства защиты информации

Состав регистрируемой информации	Содержание регистрируемой информации
Описание события	Формат «Текст». Указывают информацию о данном событии безопасности
Длительность прекращения функционирования	Формат «Продолжительность». Указывают количество минут

6.2.54 Состав и содержание регистрируемой информации для типа события безопасности, связанного с управлением (администрированием) функциями безопасности, представлены в таблице 110.

Таблица 110 — Состав и содержание регистрируемой информации для типа события безопасности, связанного с управлением (администрированием) функциями безопасности

Состав регистрируемой информации	Содержание регистрируемой информации
Компонент СЗИ	Формат «Текст». Указывают краткое наименование
Наименование СЗИ	Формат «Текст». Указывают полное официальное наименование ПО
Версия СЗИ	Формат «Версия ПО»
Тип действия	Формат «Текст». Указывают краткое наименование выполняемых действий
Результат операции	Формат «Набор значений». Принимаемые значения: успешный/неуспешный (если результат операции не определяется идентификатором события безопасности)

Дополнительно (если применимо) может быть зарегистрирована информация, представленная в таблице 111.

Таблица 111 — Дополнительно регистрируемая информация для типа события безопасности, связанного с управлением (администрированием) функциями безопасности

Состав регистрируемой информации	Содержание регистрируемой информации
Значения параметров конфигурации	Формат «Текст». Указывают в следующем виде: «параметр: значение;». Если параметров несколько, то они отделяются при помощи разделителя «;»
Новые (измененные) значения параметров конфигурации	Формат «Текст». Указывают в следующем виде: «параметр: старое значение => новое значение;». Если параметров несколько, то они отделяются при помощи разделителя «;»
Сетевой адрес администратора	Формат «Сетевой адрес»

6.2.55 Состав и содержание регистрируемой информации для типа события безопасности, связанного с управлением журналами (записями) регистрации событий безопасности, представлены в таблице 112.

Таблица 112 — Состав и содержание регистрируемой информации для типа события безопасности, связанного с управлением журналами (записями) регистрации событий безопасности

Состав регистрируемой информации	Содержание регистрируемой информации
Тип действия	Формат «Текст». Указывают краткое наименование выполняемых действий
Тип журнала	Формат «Текст». Указывают наименование журнала
Результат операции	Формат «Набор значений». Принимаемые значения: успешный/неуспешный (если результат операции не определяется идентификатором события безопасности)

Дополнительно (если применимо) может быть зарегистрирована информация, представленная в таблице 113.

Таблица 113 — Дополнительно регистрируемая информация для типа события безопасности, связанного с управлением журналами (записями) регистрации событий безопасности

Состав регистрируемой информации	Содержание регистрируемой информации
Значения параметров конфигурации	Формат «Текст». Указывают в следующем виде: «параметр: значение;». Если параметров несколько, то они отделяются при помощи разделителя «;»
Новые (измененные) значения параметров конфигурации	Формат «Текст». Указывают в следующем виде: «параметр: старое значение => новое значение;» Если параметров несколько, то они отделяются при помощи разделителя «;»
Сетевой адрес администратора	Формат «Сетевой адрес»

6.2.56 Состав и содержание регистрируемой информации для типов событий безопасности, связанных с применением методов криптографической защиты информации, определяются в соответствии с законодательством Российской Федерации.

6.2.57 Состав и содержание регистрируемой информации для типа события безопасности, связанного с выполнением действий по управлению виртуальными машинами, представлены в таблице 114.

Таблица 114 — Состав и содержание регистрируемой информации для типа события безопасности, связанного с выполнением действий по управлению виртуальными машинами

Состав регистрируемой информации	Содержание регистрируемой информации
Тип действия	Формат «Текст». Указывают краткое наименование выполняемых действий
Сетевой адрес гипервизора	Формат «Сетевой адрес»
Идентификатор виртуальной машины	Формат «Текст»
ОС виртуальной машины	Формат «Текст». Указывают полное официальное наименование ОС
Идентификатор хранилища данных	Формат «Текст»
Версия ПО гипервизора	Формат «Версия ПО»
Результат операции	Формат «Набор значений». Принимаемые значения: успешный/неуспешный (если результат операции не определяется идентификатором события безопасности)

Дополнительно (если применимо) может быть зарегистрирована информация, представленная в таблице 115.

Таблица 115 — Дополнительно регистрируемая информация для типа события безопасности, связанного с выполнением действий по управлению виртуальными машинами

Состав регистрируемой информации	Содержание регистрируемой информации
Идентификатор виртуальной сети	Формат «Целое число»
Идентификатор виртуального коммутатора	Формат «Текст»
Аппаратный адрес	Формат «Аппаратный адрес»

6.2.58 Состав и содержание регистрируемой информации для типа события безопасности, связанного с изменением состояния виртуальных машин, представлены в таблице 116.

Таблица 116 — Состав и содержание регистрируемой информации для типа события безопасности, связанного с изменением состояния виртуальных машин

Состав регистрируемой информации	Содержание регистрируемой информации
Тип действия	Формат «Текст». Указывают краткое наименование выполняемых действий
Сетевой адрес гипервизора	Формат «Сетевой адрес»
Идентификатор виртуальной машины	Формат «Текст»
ОС виртуальной машины	Формат «Текст». Указывают полное официальное наименование ОС
Идентификатор хранилища данных	Формат «Текст»
Версия ПО гипервизора	Формат «Версия ПО»
Результат операции	Формат «Набор значений». Принимаемые значения: успешный/неуспешный (если результат операции не определяется идентификатором события безопасности)

Дополнительно (если применимо) может быть зарегистрирована информация, представленная в таблице 117.

Таблица 117 — Дополнительно регистрируемая информация для типа события безопасности, связанного с изменением состояния виртуальных машин

Состав регистрируемой информации	Содержание регистрируемой информации
Идентификатор виртуальной сети	Формат «Целое число»
Идентификатор виртуального коммутатора	Формат «Текст»
Аппаратный адрес	Формат «Аппаратный адрес»

6.2.59 Состав и содержание регистрируемой информации для типа события безопасности, связанного с изменением конфигурации виртуальной машины, представлены в таблице 118.

Таблица 118 — Состав и содержание регистрируемой информации для типа события безопасности, связанного с изменением конфигурации виртуальной машины

Состав регистрируемой информации	Содержание регистрируемой информации
Сетевой адрес гипервизора	Формат «Сетевой адрес»
Идентификатор виртуальной машины	Формат «Текст»
ОС виртуальной машины	Формат «Текст». Указывают полное официальное наименование ОС
Идентификатор хранилища данных	Формат «Текст»
Идентификатор виртуальной сети	Формат «Целое число»
Аппаратный адрес	Формат «Аппаратный адрес»
Тип действия	Формат «Текст». Указывают краткое наименование выполняемых действий
Версия ПО гипервизора	Формат «Версия ПО»
Результат операции	Формат «Набор значений». Принимаемые значения: успешный/неуспешный (если результат операции не определяется идентификатором события безопасности)

Дополнительно (если применимо) может быть зарегистрирована информация, представленная в таблице 119.

Таблица 119 — Дополнительно регистрируемая информация для типа события безопасности, связанного с изменением конфигурации виртуальной машины

Состав регистрируемой информации	Содержание регистрируемой информации
Идентификатор виртуального коммутатора	Формат «Текст»
Значения параметров конфигурации	Формат «Текст». Указывают в следующем виде: «параметр: значение;». Если параметров несколько, то они отделяются при помощи разделителя «;»
Новые (измененные) значения параметров конфигурации	Формат «Текст». Указывают в следующем виде: «параметр: старое значение => новое значение;». Если параметров несколько, то они отделяются при помощи разделителя «;»

6.2.60 Состав и содержание регистрируемой информации для типа события безопасности, связанного с изменением конфигурации гипервизора, представлены в таблице 120.

Таблица 120 — Состав и содержание регистрируемой информации для типа события безопасности, связанного с изменением конфигурации гипервизора

Состав регистрируемой информации	Содержание регистрируемой информации
Компонент гипервизора	Формат «Текст». Указывают краткое наименование
Сетевой адрес гипервизора	Формат «Сетевой адрес»
Версия системы виртуализации	Формат «Версия ПО»
Наименование системы виртуализации	Формат «Текст». Указывают полное официальное наименование ПО
Версия ПО гипервизора	Формат «Версия ПО»
Тип действия	Формат «Текст». Указывают краткое наименование выполняемых действий
Результат операции	Формат «Набор значений». Принимаемые значения: успешный/неуспешный (если результат операции не определяется идентификатором события безопасности)

Дополнительно (если применимо) может быть зарегистрирована информация, представленная в таблице 121.

Таблица 121 — Дополнительно регистрируемая информация для типа события безопасности, связанного с изменением конфигурации гипервизора

Состав регистрируемой информации	Содержание регистрируемой информации
Значения параметров конфигурации	Формат «Текст». Указывают в следующем виде: «параметр: значение;». Если параметров несколько, то они отделяются при помощи разделителя «;»
Новые (измененные) значения параметров конфигурации	Формат «Текст». Указывают в следующем виде: «параметр: старое значение => новое значение;». Если параметров несколько, то они отделяются при помощи разделителя «;»

6.2.61 Состав и содержание регистрируемой информации для типа события безопасности, связанного с изменением конфигурации виртуального коммутатора, представлены в таблице 122.

Таблица 122 — Состав и содержание регистрируемой информации для типа события безопасности, связанного с изменением конфигурации виртуального коммутатора

Состав регистрируемой информации	Содержание регистрируемой информации
Сетевой адрес гипервизора	Формат «Сетевой адрес»
Идентификатор виртуального коммутатора	Формат «Текст»

Окончание таблицы 122

Состав регистрируемой информации	Содержание регистрируемой информации
Аппаратный адрес физического сетевого интерфейса гипервизора	Формат «Аппаратный адрес»
Идентификатор виртуальной сети	Формат «Целое число»
Версия ПО гипервизора	Формат «Версия ПО»
Тип действия	Формат «Текст». Указывают краткое наименование выполняемых действий
Результат операции	Формат «Набор значений». Принимаемые значения: успешный/неуспешный (если результат операции не определяется идентификатором события безопасности)

Дополнительно (если применимо) может быть зарегистрирована информация, представленная в таблице 123.

Таблица 123 — Дополнительно регистрируемая информация для типа события безопасности, связанного с изменением конфигурации виртуального коммутатора

Состав регистрируемой информации	Содержание регистрируемой информации
Значения параметров конфигурации	Формат «Текст». Указывают в следующем виде: «параметр: значение;». Если параметров несколько, то они отделяются при помощи разделителя «;»
Новые (измененные) значения параметров конфигурации	Формат «Текст». Указывают в следующем виде: «параметр: старое значение => новое значение;». Если параметров несколько, то они отделяются при помощи разделителя «;»

6.2.62 Состав и содержание регистрируемой информации для типа события безопасности, связанного с изменением конфигурации дискового хранилища, представлены в таблице 124.

Таблица 124 — Состав и содержание регистрируемой информации для типа события безопасности, связанного с изменением конфигурации дискового хранилища

Состав регистрируемой информации	Содержание регистрируемой информации
Сетевой адрес гипервизора	Формат «Сетевой адрес»
Идентификатор хранилища данных	Формат «Текст»
Тип хранилища	Формат «Текст»
Расположение хранилища	Формат «Текст»
Тип действия	Формат «Текст». Указывают краткое наименование выполняемых действий
Версия ПО гипервизора	Формат «Версия ПО»
Тип действия	Формат «Текст». Указывают краткое наименование выполняемых действий
Результат операции	Формат «Набор значений». Принимаемые значения: успешный/неуспешный (если результат операции не определяется идентификатором события безопасности)

Дополнительно (если применимо) может быть зарегистрирована информация, представленная в таблице 125.

Таблица 125 — Дополнительно регистрируемая информация для типа события безопасности, связанного с изменением конфигурации дискового хранилища

Состав регистрируемой информации	Содержание регистрируемой информации
Значения параметров конфигурации	Формат «Текст». Указывают в следующем виде: «параметр: значение;». Если параметров несколько, то они отделяются при помощи разделителя «;»
Новые (измененные) значения параметров конфигурации	Формат «Текст». Указывают в следующем виде: «параметр: старое значение => новое значение;». Если параметров несколько, то они отделяются при помощи разделителя «;»

6.2.63 Состав и содержание регистрируемой информации для типа события безопасности, связанного с перемещением (размещением) виртуальных машин, представлены в таблице 126.

Таблица 126 — Состав и содержание регистрируемой информации для типа события безопасности, связанного с перемещением (размещением) виртуальных машин

Состав регистрируемой информации	Содержание регистрируемой информации
Текущий сетевой адрес гипервизора	Формат «Сетевой адрес»
Предыдущий сетевой адрес гипервизора	Формат «Сетевой адрес»
Идентификатор виртуальной машины	Формат «Текст»
ОС виртуальной машины	Формат «Текст». Указывают полное официальное наименование ОС
Идентификатор хранилища данных	Формат «Текст»
Тип действия	Формат «Текст». Указывают краткое наименование выполняемых действий
Версия ПО гипервизора	Формат «Версия ПО»
Результат операции	Формат «Набор значений». Принимаемые значения: успешный/неуспешный (если результат операции не определяется идентификатором события безопасности)

Дополнительно (если применимо) может быть зарегистрирована информация, представленная в таблице 127.

Таблица 127 — Дополнительно регистрируемая информация для типа события безопасности, связанного с перемещением (размещением) виртуальных машин

Состав регистрируемой информации	Содержание регистрируемой информации
Идентификатор виртуальной сети	Формат «Целое число»
Идентификатор виртуального коммутатора	Формат «Текст»

6.2.64 Состав и содержание регистрируемой информации для типа события безопасности, связанного с управлением контрольными точками виртуальной машины, представлены в таблице 128.

Таблица 128 — Состав и содержание регистрируемой информации для типа события безопасности, связанного с управлением контрольными точками виртуальной машины

Состав регистрируемой информации	Содержание регистрируемой информации
Сетевой адрес гипервизора	Формат «Сетевой адрес»
Идентификатор виртуальной машины	Формат «Текст»
ОС виртуальной машины	Формат «Текст». Указывают полное официальное наименование ОС
Идентификатор хранилища данных	Формат «Текст»

Окончание таблицы 128

Состав регистрируемой информации	Содержание регистрируемой информации
Тип действия	Формат «Текст». Указывают краткое наименование выполняемых действий
Дата и время создания контрольной точки	Формат «Дата/время»
Версия ПО гипервизора	Формат «Версия ПО»
Результат операции	Формат «Набор значений». Принимаемые значения: успешный/неуспешный (если результат операции не определяется идентификатором события безопасности)

Дополнительно (если применимо) может быть зарегистрирована информация, представленная в таблице 129.

Таблица 129 — Дополнительно регистрируемая информация для типа события безопасности, связанного с управлением контрольными точками виртуальной машины

Состав регистрируемой информации	Содержание регистрируемой информации
Идентификатор виртуальной сети	Формат «Целое число»
Идентификатор виртуального коммутатора	Формат «Текст»
Аппаратный адрес	Формат «Аппаратный адрес»
Описание события	Формат «Текст». Указывают расширенную информацию о данном событии безопасности

6.2.65 Состав и содержание регистрируемой информации для типа события безопасности, связанного с использованием сервиса доменных имен, представлены в таблице 130.

Таблица 130 — Состав и содержание регистрируемой информации для типа события безопасности, связанного с использованием сервиса доменных имен

Состав регистрируемой информации	Содержание регистрируемой информации
Тип действия	Формат «Текст». Указывают краткое наименование выполняемых действий
Тип записи	Формат «Текст». Указывают тип ресурсной записи. Пример описания: MX
Доменное имя	Формат «Текст»
Сетевой адрес	Формат «Сетевой адрес»
Версия IP-протокола	Формат «Целое число»
Тип ответа	Формат «Текст»
Тип запроса	Формат «Текст»
Поле данных	Формат «Текст»
Протокол	Формат «Текст». Указывают сокращение наименования сетевого протокола. Пример описания: IP/TCP/HTTP
Сетевой адрес клиента	Формат «Сетевой адрес»
Порт сервера	Формат «Целое число». Число от 0 до 65535, указанное в заголовках протоколов транспортного уровня
Порт клиента	Формат «Целое число». Число от 0 до 65535, указанное в заголовках протоколов транспортного уровня

Дополнительно (если применимо) может быть зарегистрирована информация, представленная в таблице 131.

Таблица 131 — Дополнительно регистрируемая информация для типа события безопасности, связанного с использованием сервиса доменных имен

Состав регистрируемой информации	Содержание регистрируемой информации
Наименование ПО сервера доменных имен	Формат «Текст». Указывают полное официальное наименование ПО
Версия ПО сервера доменных имен	Формат «Версия ПО»

6.2.66 Состав и содержание регистрируемой информации для типа события безопасности, связанного с использованием сервиса динамической настройки сети, представлены в таблице 132.

Таблица 132 — Состав и содержание регистрируемой информации для типа события безопасности, связанного с использованием сервиса динамической настройки сети

Состав регистрируемой информации	Содержание регистрируемой информации
Сетевой адрес клиента	Формат «Сетевой адрес»
Тип действия	Формат «Текст». Указывают краткое наименование выполняемых действий
Аппаратный адрес клиента	Формат «Аппаратный адрес»
Длительность аренды	Формат «Продолжительность». Указывают количество минут
Дата и время окончания аренды	Формат «Дата/время»
Маска подсети	Формат «Целое число». Указывают количество единичных бит в маске

Дополнительно (если применимо) может быть зарегистрирована информация, представленная в таблице 133.

Таблица 133 — Дополнительно регистрируемая информация для типа события безопасности, связанного с использованием сервиса динамической настройки сети

Состав регистрируемой информации	Содержание регистрируемой информации
Сетевой адрес маршрутизатора	Формат «Сетевой адрес»
Адрес сервера доменных имен	Формат «Сетевой адрес»
Версия IP-протокола	Формат «Целое число»

6.2.67 Состав и содержание регистрируемой информации для типа события безопасности, связанного с использованием сервиса передачи файлов, представлены в таблице 134.

Таблица 134 — Состав и содержание регистрируемой информации для типа события безопасности, связанного с использованием сервиса передачи файлов

Состав регистрируемой информации	Содержание регистрируемой информации
Наименование файла	Формат «Текст». Указывают наименование файла вместе с расширением (если применимо)
Полный путь к файлу	Формат «Текст». Указывают набор символов, определяющий расположение файла в файловой системе
Размер файла	Формат «Целое число». Указывают размер в байтах
Сетевой адрес клиента	Формат «Сетевой адрес»
Порт клиента	Формат «Целое число». Число от 0 до 65535, указанное в заголовках протоколов транспортного уровня
Порт сервера	Формат «Целое число». Число от 0 до 65535, указанное в заголовках протоколов транспортного уровня

Окончание таблицы 134

Состав регистрируемой информации	Содержание регистрируемой информации
Метод запроса	Формат «Набор значений». Принимаемые значения: GET/POST/PUT/DELETE/HEAD/OPTIONS/PATCH/TRACE/CONNECT
Тип действия	Формат «Текст». Указывают краткое наименование выполняемых действий
Результат операции	Формат «Набор значений». Принимаемые значения: успешный/неуспешный (если результат операции не определяется идентификатором события безопасности)

Дополнительно (если применимо) может быть зарегистрирована информация, представленная в таблице 135.

Таблица 135 — Дополнительно регистрируемая информация для типа события безопасности, связанного с использованием сервиса передачи файлов

Состав регистрируемой информации	Содержание регистрируемой информации
Расширение файла (если применимо)	Формат «Текст». Указывают расширение файла без символа «.»
Скорость передачи	Формат «Целое число». Указывают в Мбит/с
Затраченное время	Формат «Продолжительность». Указывают количество минут

6.2.68 Состав и содержание регистрируемой информации для типа события безопасности, связанного с использованием веб-сервера, представлены в таблице 136.

Таблица 136 — Состав и содержание регистрируемой информации для типа события безопасности, связанного с использованием веб-сервера

Состав регистрируемой информации	Содержание регистрируемой информации
Сетевой адрес источника запроса	Формат «Сетевой адрес»
Версия протокола передачи гипертекста	Формат «Текст»
Порт источника	Формат «Целое число». Число от 0 до 65535, указанное в заголовках протоколов транспортного уровня
Порт назначения	Формат «Целое число». Число от 0 до 65535, указанное в заголовках протоколов транспортного уровня
Метод запроса	Формат «Набор значений». Принимаемые значения: GET/POST/PUT/DELETE/HEAD/OPTIONS/PATCH/TRACE/CONNECT
Пользовательское приложение	Формат «Текст»
Унифицированный идентификатор ресурса	Формат «Текст»
Код ответа	Формат «Целое число»
Унифицированный идентификатор источника запроса ресурса	Формат «Текст»
Доменное имя	Формат «Текст»
Идентификатор сессии	Формат «Текст»
Сетевой адрес прокси-сервера	Формат «Сетевой адрес»
Порт прокси-сервера	Формат «Целое число». Число от 0 до 65535, указанное в заголовках протоколов транспортного уровня

Дополнительно (если применимо) может быть зарегистрирована информация, представленная в таблице 137.

Таблица 137 — Дополнительно регистрируемая информация для типа события безопасности, связанного с использованием веб-сервера

Состав регистрируемой информации	Содержание регистрируемой информации
Наименование веб-сервера	Формат «Текст». Указывают полное официальное наименование ПО
Версия веб сервера	Формат «Версия ПО»
Геоданные клиента	Формат «Текст». Указывают страну и город
Байт передано	Формат «Целое число»
Байт получено	Формат «Целое число»

6.2.69 Состав и содержание регистрируемой информации для типа события безопасности, связанного с использованием прокси-сервера, представлены в таблице 138.

Таблица 138 — Состав и содержание регистрируемой информации для типа события безопасности, связанного с использованием прокси-сервера

Состав регистрируемой информации	Содержание регистрируемой информации
Сетевой адрес клиента	Формат «Сетевой адрес»
Порт клиента	Формат «Целое число». Число от 0 до 65535, указанное в заголовках протоколов транспортного уровня
Метод запроса	Формат «Набор значений». Принимаемые значения: GET/POST/PUT/DELETE/HEAD/OPTIONS/PATCH/TRACE/CONNECT
Унифицированный идентификатор ресурса	Формат «Текст»
Код ответа протокола передачи гипертекста	Формат «Целое число»
Клиентское приложение	Формат «Текст»
Сетевой адрес клиента	Формат «Сетевой адрес»
Ответ прокси-сервера на запрос	Формат «Текст»
Унифицированный идентификатор источника запроса ресурса	Формат «Текст»

Дополнительно (если применимо) может быть зарегистрирована информация, представленная в таблице 139.

Таблица 139 — Дополнительно регистрируемая информация для типа события безопасности, связанного с использованием прокси-сервера

Состав регистрируемой информации	Содержание регистрируемой информации
Порт прокси-сервера	Формат «Целое число». Число от 0 до 65535, указанное в заголовках протоколов транспортного уровня
Версия протокола запроса	Формат «Текст»
Время ответа в миллисекундах	Формат «Целое число»
Размер запроса	Формат «Целое число». Указывают размер в байтах
Размер ответа	Формат «Целое число». Указывают размер в байтах
Уровень прокси-сервера в иерархии нескольких прокси-серверов	Формат «Текст»

6.2.70 Состав и содержание регистрируемой информации для типа события безопасности, связанного с использованием сервера электронной почты, представлены в таблице 140.

Таблица 140 — Состав и содержание регистрируемой информации для типа события безопасности, связанного с использованием сервера электронной почты

Состав регистрируемой информации	Содержание регистрируемой информации
Идентификатор сообщения электронной почты	Формат «Текст». Указывают уникальный идентификатор сообщения, состоящий из адреса узла-отправителя и номера (уникального в пределах узла)
Статус письма	Формат «Текст». Указывают статус отправки/получения письма
Наименование ПО почтового сервера	Формат «Текст». Указывают полное официальное наименование ПО
Версия ПО почтового сервера	Формат «Версия ПО»
Сетевой адрес отправителя	Формат «Сетевой адрес»
Тема сообщения	Формат «Текст»
Текст сообщения	Формат «Текст»
Адрес электронной почты получателя	Формат «Адрес электронной почты»
Наличие вложений	Формат «Текст». Указывают наличие вложений: есть/нет
Тип действия	Формат «Текст». Указывают краткое наименование выполняемых действий
Результат операции	Формат «Набор значений». Принимаемые значения: успешный/неуспешный (если результат операции не определяется идентификатором события безопасности)

Дополнительно (если применимо) может быть зарегистрирована информация, представленная в таблице 141.

Таблица 141 — Дополнительно регистрируемая информация для типа события безопасности, связанного с использованием сервера электронной почты

Состав регистрируемой информации	Содержание регистрируемой информации
Адрес электронной почты отправителя	Формат «Адрес электронной почты»
Содержимое служебных заголовков сообщения	Формат «Текст». Указываются служебные заголовки, разделенные символом «;»

6.2.71 Состав и содержание регистрируемой информации для типа события безопасности, связанного с использованием сервера службы каталога, представлены в таблице 142.

Таблица 142 — Состав и содержание регистрируемой информации для типа события безопасности, связанного с использованием сервера службы каталога

Состав регистрируемой информации	Содержание регистрируемой информации
Наименование объекта	Формат «Текст». Указывают полное официальное наименование ПО
Идентификатор объекта	Формат «Текст». Указывают уникальный признак объекта, позволяющий отличать его от других объектов
Категория объекта	Формат «Текст»
Класс объекта	Формат «Текст»
Тип действия	Формат «Текст». Указывают краткое наименование выполняемых действий
Результат операции	Формат «Набор значений». Принимаемые значения: успешный/неуспешный (если результат операции не определяется идентификатором события безопасности)

Дополнительно (если применимо) может быть зарегистрирована информация, представленная в таблице 143.

Таблица 143 — Дополнительно регистрируемая информация для типа события безопасности, связанного с использованием сервера службы каталога

Состав регистрируемой информации	Содержание регистрируемой информации
Наименование измененного параметра	Формат «Текст»
Значение измененного параметра	Формат «Текст»

6.2.72 Состав и содержание регистрируемой информации для типа события безопасности, связанного с использованием терминального сервера, представлены в таблице 144.

Таблица 144 — Состав и содержание регистрируемой информации для типа события безопасности, связанного с использованием терминального сервера

Состав регистрируемой информации	Содержание регистрируемой информации
Идентификатор сессии	Формат «Целое число». Указывают порядковый номер сеанса
Длительность сессии	Формат «Продолжительность». Указывают количество минут
Сетевой адрес источника	Формат «Сетевой адрес»
Порт источника	Формат «Целое число». Число от 0 до 65535, указанное в заголовках протоколов транспортного уровня
Порт назначения	Формат «Целое число». Число от 0 до 65535, указанное в заголовках протоколов транспортного уровня
Протокол	Формат «Текст». Указывают сокращение наименования сетевого протокола. Пример описания: IP/TCP/HTTP
Тип действия	Формат «Текст». Указывают краткое наименование выполняемых действий
Результат операции	Формат «Набор значений». Принимаемые значения: успешный/неуспешный (если результат операции не определяется идентификатором события безопасности)

Дополнительно (если применимо) может быть зарегистрирована информация, представленная в таблице 145.

Таблица 145 — Дополнительно регистрируемая информация для типа события безопасности, связанного с использованием терминального сервера

Состав регистрируемой информации	Содержание регистрируемой информации
Наименование ПО терминального сервера	Формат «Текст». Указывают полное официальное наименование ПО
Версия ПО терминального сервера	Формат «Версия ПО»

6.2.73 Состав и содержание регистрируемой информации для типа события безопасности, связанного с использованием файлового хранилища, представлены в таблице 146.

Таблица 146 — Состав и содержание регистрируемой информации для типа события безопасности, связанного с использованием файлового хранилища

Состав регистрируемой информации	Содержание регистрируемой информации
Наименование файла	Формат «Текст». Указывают наименование файла вместе с расширением (если применимо)
Полный путь к файлу	Формат «Текст». Указывают набор символов, определяющий расположение файла в файловой системе

Окончание таблицы 146

Состав регистрируемой информации	Содержание регистрируемой информации
Размер файла	Формат «Целое число». Указывают размер в байтах
Тип действия над файлом	Формат «Текст». Указывают краткое наименование выполняемых действий
Результат операции	Формат «Набор значений». Принимаемые значения: успешный/неуспешный (если результат операции не определяется идентификатором события безопасности)

Дополнительно (если применимо) может быть зарегистрирована информация, представленная в таблице 147.

Таблица 147 — Дополнительно регистрируемая информация для типа события безопасности, связанного с использованием файлового хранилища

Состав регистрируемой информации	Содержание регистрируемой информации
Контрольная сумма файла	Формат «Текст». Указывают значение однонаправленной хеш-функции
Алгоритм контрольной суммы	Формат «Текст». Указывают алгоритм контрольной суммы (например, md5, sha1, sha256 и др.)
Расширение файла (если применимо)	Формат «Текст». Указывают расширение файла без символа «.»

6.2.74 Состав и содержание регистрируемой информации для типа события безопасности, связанного с использованием маршрутизатора, представлены в таблице 148.

Таблица 148 — Состав и содержание регистрируемой информации для типа события безопасности, связанного с использованием маршрутизатора

Состав регистрируемой информации	Содержание регистрируемой информации
Сетевой адрес источника	Формат «Сетевой адрес»
Порт источника	Формат «Целое число». Число от 0 до 65535, указанное в заголовках протоколов транспортного уровня
Аппаратный адрес источника (если применимо)	Формат «Аппаратный адрес»
Сетевой адрес назначения	Формат «Сетевой адрес»
Порт назначения	Формат «Целое число». Число от 0 до 65535, указанное в заголовках протоколов транспортного уровня
Аппаратный адрес назначения (если применимо)	Формат «Аппаратный адрес»
Протокол	Формат «Текст». Указывают сокращение наименования сетевого протокола. Пример описания: IP/TCP/HTTP
Тип действия	Формат «Текст». Указывают краткое наименование выполняемых действий
Номер правила фильтрации	Формат «Целое число»

Дополнительно (если применимо) может быть зарегистрирована информация, представленная в таблице 149.

Таблица 149 — Дополнительно регистрируемая информация для типа события безопасности, связанного с использованием маршрутизатора

Состав регистрируемой информации	Содержание регистрируемой информации
Сетевой интерфейс	Формат «Текст». Указывают наименование/порядковый номер интерфейса
Скорость интерфейса	Формат «Целое число». Указывают в Мбит/с

Окончание таблицы 149

Состав регистрируемой информации	Содержание регистрируемой информации
Идентификатор виртуальной сети	Формат «Целое число»
Время жизни пакета	Формат «Целое число». Указывают максимальное число переходов между маршрутизаторами

6.2.75 Состав и содержание регистрируемой информации для типа события безопасности, связанного с управлением маршрутизатором, представлены в таблице 150.

Таблица 150 — Состав и содержание регистрируемой информации для типа события безопасности, связанного с управлением маршрутизатором

Состав регистрируемой информации	Содержание регистрируемой информации
Тип действия	Формат «Текст». Указывают краткое наименование выполняемых действий
Результат операции	Формат «Набор значений». Принимаемые значения: успешный/неуспешный (если результат операции не определяется идентификатором события безопасности)

Дополнительно (если применимо) может быть зарегистрирована информация, представленная в таблице 151.

Таблица 151 — Дополнительно регистрируемая информация для типа события безопасности, связанного с управлением маршрутизатором

Состав регистрируемой информации	Содержание регистрируемой информации
Значения параметров конфигурации маршрутизатора	Формат «Текст». Указывают в следующем виде: «параметр: значение;». Если параметров несколько, то они отделяются при помощи разделителя «;»
Новые значения параметров конфигурации маршрутизатора	Формат «Текст». Указывают в следующем виде: «параметр: значение;». Если параметров несколько, то они отделяются при помощи разделителя «;»
Сетевой адрес администратора	Формат «Сетевой адрес»
Модель маршрутизатора	Формат «Текст». Указывают полное официальное наименование ПО
Версия ПО маршрутизатора	Формат «Версия ПО»

6.2.76 Состав и содержание регистрируемой информации для типа события безопасности, связанного с использованием коммутатора, представлены в таблице 152.

Таблица 152 — Состав и содержание регистрируемой информации для типа события безопасности, связанного с использованием коммутатора

Состав регистрируемой информации	Содержание регистрируемой информации
Аппаратный адрес источника	Формат «Аппаратный адрес»
Аппаратный адрес назначения	Формат «Аппаратный адрес»
Тип действия	Формат «Текст». Указывают краткое наименование выполняемых действий
Сетевой интерфейс	Формат «Текст». Указывают наименование/порядковый номер интерфейса

Дополнительно (если применимо) может быть зарегистрирована информация, представленная в таблице 153.

Таблица 153 — Дополнительно регистрируемая информация для типа события безопасности, связанного с использованием коммутатора

Состав регистрируемой информации	Содержание регистрируемой информации
Сетевой адрес источника	Формат «Сетевой адрес»
Порт источника	Формат «Целое число». Число от 0 до 65535, указанное в заголовках протоколов транспортного уровня
Сетевой адрес назначения	Формат «Сетевой адрес»
Порт назначения	Формат «Целое число». Число от 0 до 65535, указанное в заголовках протоколов транспортного уровня
Протокол	Формат «Текст». Указывают сокращеное наименование сетевого протокола. Пример описания: IP/TCP/HTTP
Скорость интерфейса	Формат «Целое число». Указывают в Мбит/с
Состояние интерфейса	Формат «Набор значений». Принимаемые значения: включен/отключен
Время жизни пакета	Формат «Целое число». Указывают максимальное число переходов между коммутаторами
Идентификатор виртуальной сети	Формат «Целое число»
Номер правила фильтрации	Формат «Целое число»

6.2.77 Состав и содержание регистрируемой информации для типа события безопасности, связанного с управлением коммутатором, представлены в таблице 154.

Таблица 154 — Состав и содержание регистрируемой информации для типа события безопасности, связанного с управлением коммутатором

Состав регистрируемой информации	Содержание регистрируемой информации
Тип действия	Формат «Текст». Указывают краткое наименование выполняемых действий
Результат операции	Формат «Набор значений». Принимаемые значения: успешный/неуспешный (если результат операции не определяется идентификатором события безопасности)

Дополнительно (если применимо) может быть зарегистрирована информация, представленная в таблице 155.

Таблица 155 — Дополнительно регистрируемая информация для типа события безопасности, связанного с управлением коммутатором

Состав регистрируемой информации	Содержание регистрируемой информации
Наименование и модель коммутатора	Формат «Текст». Указывают полное официальное наименование ПО
Значения параметров конфигурации	Формат «Текст». Указывают в следующем виде: «параметр: значение;». Если параметров несколько, то они отделяются при помощи разделителя «;»
Новые (измененные) значения параметров конфигурации	Формат «Текст». Указывают в следующем виде: «параметр: старое значение => новое значение;». Если параметров несколько, то они отделяются при помощи разделителя «;»
Сетевой адрес администратора	Формат «Сетевой адрес»
Версия ПО коммутатора	Формат «Версия ПО»

6.2.78 Состав и содержание регистрируемой информации для типа события безопасности, связанного с использованием контроллера беспроводного доступа, представлены в таблице 156.

Таблица 156 — Состав и содержание регистрируемой информации для типа события безопасности, связанного с использованием контроллера беспроводного доступа

Состав регистрируемой информации	Содержание регистрируемой информации
Идентификатор беспроводной сети	Формат «Текст». Указывают название сети (SSID)
Аппаратный адрес источника	Формат «Аппаратный адрес»
Аппаратный адрес назначения	Формат «Аппаратный адрес»
Диапазон частот	Формат «Текст»
Канал	Формат «Целое число». Указывают номер канала
Стандарт беспроводной связи	Формат «Текст». Пример описания: 802.11a
Тип действия	Формат «Текст». Указывают краткое наименование выполняемых действий

Дополнительно (если применимо) может быть зарегистрирована информация, представленная в таблице 157.

Таблица 157 — Дополнительно регистрируемая информация для типа события безопасности, связанного с использованием контроллера беспроводного доступа

Состав регистрируемой информации	Содержание регистрируемой информации
Наименование и модель контроллера беспроводного доступа	Формат «Текст». Указывают полное официальное наименование ПО
Версия ПО контроллера беспроводного доступа	Формат «Версия ПО»

6.2.79 Состав и содержание регистрируемой информации для типа события безопасности, связанного с управлением контроллером беспроводного доступа, представлены в таблице 158.

Таблица 158 — Состав и содержание регистрируемой информации для типа события безопасности, связанного с управлением контроллером беспроводного доступа

Состав регистрируемой информации	Содержание регистрируемой информации
Тип действия	Формат «Текст». Указывают краткое наименование выполняемых действий
Результат операции	Формат «Набор значений». Принимаемые значения: успешный/неуспешный (если результат операции не определяется идентификатором события безопасности)

Дополнительно (если применимо) может быть зарегистрирована информация, представленная в таблице 159.

Таблица 159 — Дополнительно регистрируемая информация для типа события безопасности, связанного с управлением контроллером беспроводного доступа

Состав регистрируемой информации	Содержание регистрируемой информации
Значения параметров конфигурации контроллера беспроводного доступа	Формат «Текст». Указывают в следующем виде: «параметр: значение;». Если параметров несколько, то они отделяются при помощи разделителя «;»
Новые значения параметров конфигурации контроллера беспроводного доступа	Формат «Текст». Указывают в следующем виде: «параметр: старое значение => новое значение;». Если параметров несколько, то они отделяются при помощи разделителя «;»
Сетевой адрес администратора	Формат «Сетевой адрес»
Наименование и модель контроллера беспроводного доступа	Формат «Текст». Указывают полное официальное наименование ПО
Версия ПО контроллера	Формат «Версия ПО»

6.2.80 Состав и содержание регистрируемой информации для типа события безопасности, связанного с использованием ответвителя сетевого трафика, представлены в таблице 160.

Таблица 160 — Состав и содержание регистрируемой информации для типа события безопасности, связанного с использованием ответвителя сетевого трафика

Состав регистрируемой информации	Содержание регистрируемой информации
Количество полученной информации	Формат «Целое число». Указывают размер в байтах
Количество переданной информации	Формат «Целое число». Указывают размер в байтах
Процент потерь	Формат «Целое число»
Скорость передаваемой информации	Формат «Целое число». Указывают в Мбит/с

Дополнительно (если применимо) может быть зарегистрирована информация, представленная в таблице 161.

Таблица 161 — Дополнительно регистрируемая информация для типа события безопасности, связанного с использованием ответвителя сетевого трафика

Состав регистрируемой информации	Содержание регистрируемой информации
Описание события	Формат «Текст». Указывают информацию о данном событии безопасности
Источник трафика	Формат «Текст»
Получатель трафика	Формат «Текст»

6.2.81 Состав и содержание регистрируемой информации для иных типов событий безопасности (в дополнение к требованию 6.1.2) определяют изготовители средств защиты информации, средств обеспечения безопасности информационных технологий, иных программно-технических средств (а также программного обеспечения), применяемыми в информационных (автоматизированных) системах.

Приложение А
(справочное)

Типы событий безопасности, подлежащих регистрации средствами защиты информации

Изготовитель средства защиты информации определяет типы событий безопасности на основании выполняемых средством защиты функций безопасности.

Выделяют следующие основные типы событий безопасности, подлежащих регистрации средствами защиты информации:

- события безопасности, связанные с идентификацией и аутентификацией субъекта доступа;

Примечание — Основными событиями безопасности, относящимися к данному типу, являются: «Отказ во входе в связи с тем, что идентификатор не зарегистрирован», «Отказ во входе в связи с тем, что идентификатор заблокирован», «Отказ во входе в связи с неправильным паролем», «Отказ во входе в связи с тем, что превышен лимит попыток ввода пароля», «Отказ во входе в связи с тем, что закончен срок действия пароля», «Успешный вход в систему», «Выход из системы» и другие события безопасности.

- события безопасности, связанные с осуществлением идентификации объекта доступа;

Примечание — Основными событиями безопасности, относящимися к данному типу, являются: «Успешная идентификация», «Ошибка прохождения идентификации» и другие события безопасности.

- события безопасности, связанные с осуществлением аутентификации объекта доступа;

Примечание — Основными событиями безопасности, относящимися к данному типу, являются: «Успешная аутентификация», «Ошибка прохождения аутентификации» и другие события безопасности.

- события безопасности, связанные с управлением учетными записями пользователей;

Примечание — Основными событиями безопасности, относящимися к данному типу, являются: «Создание учетной записи», «Изменение наименования учетной записи», «Изменение пароля учетной записи», «Удаление учетной записи», «Блокирование учетной записи», «Активация учетной записи» и другие события безопасности.

- события безопасности, связанные с управлением аппаратными идентификаторами;

Примечание — Основными событиями безопасности, относящимися к данному типу, являются: «Создание идентификатора», «Изменение идентификатора», «Удаление идентификатора», «Блокирование идентификатора» и другие события безопасности.

- события безопасности, связанные с управлением средствами аутентификации;

Примечание — Основными событиями безопасности, относящимися к данному типу, являются: «Пароль не соответствует параметрам безопасности», «Истекает срок действия сертификата», «Истек срок действия сертификата» и другие события безопасности.

- события безопасности, связанные с управлением атрибутами доступа;

Примечание — Основными событиями безопасности, относящимися к данному типу, являются: «Создание типа доступа», «Изменение типа доступа», «Удаление типа доступа», «Создание группы пользователей», «Изменение группы пользователей», «Удаление группы пользователей», «Занесение учетной записи в группу пользователей», «Удаление учетной записи из группы пользователей», «Изменение прав доступа», «Изменение параметров конфиденциального ресурса», «Запрет изменения параметров конфиденциального ресурса» и другие события безопасности.

- события безопасности, связанные с доступом к защищаемой информации;

Примечание — Основными событиями безопасности, относящимися к данному типу, являются: «Получение доступа», «Ошибка получения доступа», «Поступление запроса на предоставление доступа», «Ошибка обработки запроса на предоставление доступа», «Отказ в доступе», «Доступ прекращен», «Получен доступ к конфиденциальному ресурсу», «Запрет доступа к конфиденциальному ресурсу», «Создание конфиденциального ресурса», «Изменение конфиденциального ресурса», «Удаление конфиденциального ресурса» и другие события безопасности.

- события безопасности, связанные с прохождением процедуры доверенной загрузки операционной системы;

Примечание — Основными событиями безопасности, относящимися к данному типу, являются: «Загрузка пройдена успешно», «Ошибка при прохождении загрузки», «Отказ в загрузке» и другие события безопасности.

- события безопасности, связанные с обнаружением файловой активности вредоносных программ;

Примечание — Основными событиями безопасности, относящимися к данному типу, являются: «Обнаружен вирус, зараженный файл оставлен без изменений», «Обнаружен вирус, зараженный файл удален», «Обнаружен вирус, зараженный файл перемещен в карантин», «Ошибка при перемещении зараженного файла в карантин», «Сканирование завершено, вирусы не обнаружены», «Сканирование завершено, обнаружены вирусы», «Успешно восстановлен файл из карантина» и другие события безопасности.

- события безопасности, связанные с обнаружением активности вредоносных программ в почтовом трафике;

Примечание — Основными событиями безопасности, относящимися к данному типу, являются: «Централизованная проверка входящих и исходящих почтовых сообщений на наличие вирусов», «Выборочная проверка входящих и исходящих почтовых сообщений на наличие вирусов» и другие события безопасности.

- события безопасности, связанные с обнаружением активности вредоносных программ в сетевом трафике;

Примечание — Основными событиями безопасности, относящимися к данному типу, являются: «Проверка входящих и исходящих сетевых соединений на наличие вирусной активности», «Проверка файлов, обнаруженных в сетевом трафике» и другие события безопасности.

- события безопасности, связанные с проведением обновления базы данных признаков вредоносных компьютерных программ (вирусов);

Примечание — Основными событиями безопасности, относящимися к данному типу, являются: «Успешное проведение обновления базы данных признаков вредоносных компьютерных программ (вирусов)», «Ошибка при обновлении базы данных признаков вредоносных компьютерных программ (вирусов)» и другие события безопасности.

- события безопасности, связанные с управлением антивирусной защитой;

Примечание — Основными событиями безопасности, относящимися к данному типу, являются: «Запуск службы», «Останов службы», «Включение сканера», «Отключение сканера», «Лицензия просрочена», «Лицензия не найдена», «У лицензии окончен срок действия» и другие события безопасности.

- события безопасности, связанные с анализом компонента программного обеспечения в среде безопасного выполнения компьютерных программ (песочнице);

Примечание — Основными событиями безопасности, относящимися к данному типу, являются: «Создание новой песочницы», «Запуск песочницы», «Останов песочницы», «Выполнение анализа начато», «Выполнение анализа завершено» и другие события безопасности.

- события безопасности, связанные с обнаружением и действиями по защите от незапрашиваемых электронных сообщений (спама);

Примечание — Основными событиями безопасности, относящимися к данному типу, являются: «Обнаружен спам», «Отправитель заблокирован» и другие события безопасности.

- события безопасности, связанные с управлением защитой от спама;

Примечание — Основными событиями безопасности, относящимися к данному типу, являются: «Запуск службы», «Останов службы», «Включение сканера», «Отключение сканера», «Лицензия просрочена», «Лицензия не найдена», «У лицензии окончен срок действия», «Конфигурация изменена» и другие события безопасности.

- события безопасности, связанные с обнаружением признаков компьютерных атак в сетевом трафике;

Примечание — Основными событиями безопасности, относящимися к данному типу, являются: «Обнаружена аномальная сетевая активность», «Обнаружена компьютерная атака», «Заблокирован подозрительный трафик» и другие события безопасности.

- события безопасности, связанные с обнаружением признаков компьютерных атак на узле;

Примечание — Основными событиями безопасности, относящимися к данному типу, являются: «Обнаружена аномальная сетевая активность на узле», «Обнаружена компьютерная атака на узле», «На узле заблокирован подозрительный трафик» и другие события безопасности.

- события безопасности, связанные с проведением обновления базы решающих правил;

Примечание — Основными событиями безопасности, относящимися к данному типу, являются: «БРП обновлена успешно», «Ошибка при обновлении БРП» и другие события безопасности.

- события безопасности, связанные с управлением средством обнаружения и блокирования компьютерных атак;

Примечание — Основными событиями безопасности, относящимися к данному типу, являются: «Запуск службы», «Останов службы», «Лицензия просрочена», «Лицензия не найдена», «У лицензии окончен срок действия», «Включение отдельных правил», «Отключение отдельных правил», «Добавление правил», «Изменение правил», «Удаление правил» и другие события безопасности.

- события безопасности, связанные с фильтрацией сетевого трафика на уровне логических границ сети и сегментов сети;

Примечание — Основными событиями безопасности, относящимися к данному типу, являются: «Обнаружен пакет», «Пакет заблокирован», «Обнаружен поток», «Поток заблокирован», «Соединение разрешено», «Соединение запрещено», «Соединение заблокировано» и другие события безопасности.

- события безопасности, связанные с фильтрацией сетевого трафика на уровне узла;

Примечание — Основными событиями безопасности, относящимися к данному типу, являются: «На узле обнаружен пакет», «На узле заблокирован пакет», «На узле обнаружен поток», «На узле заблокирован поток», «На узле разрешено соединение», «На узле запрещено соединение», «На узле заблокировано соединение», «Срабатывание правила фильтрации запросов», «Срабатывание правила» и другие события безопасности.

- события безопасности, связанные с фильтрацией сетевого трафика на прикладном уровне;

Примечание — Основными событиями безопасности, относящимися к данному типу, являются: «Попытка эксплуатации уязвимости», «Внедрение кода», «Межсайтовое выполнение сценариев» и другие события безопасности.

- события безопасности, связанные с управлением фильтрацией сетевого трафика;

Примечание — Основными событиями безопасности, относящимися к данному типу, являются: «Создание правила фильтрации», «Изменение правила фильтрации», «Удаление правила фильтрации» и другие события безопасности.

- события безопасности, связанные с изменениями в сетевой адресации;

Примечание — Основными событиями безопасности, относящимися к данному типу, являются: «Изменение IP-адреса», «Автоматическое назначение IP-адреса», «Изменение дополнительных параметров IP-адресации» и другие события безопасности.

- события безопасности, связанные с изменениями в аппаратной адресации;

Примечание — Основными событиями безопасности, относящимися к данному типу, являются: «Изменение аппаратного адреса» и другие события безопасности.

- события безопасности, связанные с изменениями в статической маршрутизации;

Примечание — Основными событиями безопасности, относящимися к данному типу, являются: «Добавление маршрута в таблицу маршрутизации», «Удаление маршрута из таблицы маршрутизации», «Назначение маршрута по умолчанию» и другие события безопасности.

- события безопасности, связанные с изменениями в таблице сопоставления аппаратных адресов и портов;

Примечание — Основными событиями безопасности, относящимися к данному типу, являются: «Добавление статической записи в CAM-таблицу», «Добавление MAC-адреса в таблицу» и другие события безопасности.

- события безопасности, связанные с обнаружением и действиями по защите от атак, направленных на отказ в обслуживании;

Примечание — Основными событиями безопасности, относящимися к данному типу, являются: «Срабатывание правила обнаружения атаки», «Срабатывание правила оповещения» и другие события безопасности.

- события безопасности, связанные с обнаружением уязвимостей программного обеспечения;

Примечание — Основными событиями безопасности, относящимися к данному типу, являются: «Обнаружена уязвимость», «Устранена уязвимость» и другие события безопасности.

- события безопасности, связанные с проведением обновления базы уязвимостей;

Примечание — Основными событиями безопасности, относящимися к данному типу, являются: «База уязвимостей обновлена успешно», «Ошибка при обновлении базы уязвимостей» и другие события безопасности.

- события безопасности, связанные с изменениями состава программного обеспечения;

Примечание — Основными событиями безопасности, относящимися к данному типу, являются: «Обнаружено изменение состава ПО», «Обнаружено запрещенное ПО» и другие события безопасности.

- события безопасности, связанные с изменениями параметров настроек средств защиты информации;

Примечание — Основными событиями безопасности, относящимися к данному типу, являются: «Конфигурация компонента СЗИ изменена», «Компонент СЗИ отключен» и другие события безопасности.

- события безопасности, связанные с установкой, изменением системного времени;

Примечание — Основным событиями безопасности, относящимися к данному типу, являются: «Системное время установлено», «Системное время изменено» и другие события безопасности.

- события безопасности, связанные с изменением настроек общего программного обеспечения;

Примечание — Основными событиями безопасности, относящимися к данному типу, являются: «Конфигурация компонента программного обеспечения изменена», «Компонент программного обеспечения отключен» и другие события безопасности.

- события безопасности, связанные с контролем наличия обязательных обновлений программного обеспечения;

Примечание — Основными событиями безопасности, относящимися к данному типу, являются: «Обновления установлены», «Начат поиск установленных обновлений», «Сбой в централизованном распространении обновлений» и другие события безопасности.

- события безопасности, связанные с выполнением процедуры установки/удаления компонентов программного обеспечения;

Примечание — Основными событиями безопасности, относящимися к данному типу, являются: «Начата установка ПО», «ПО установлено», «Служба удалена» и другие события безопасности.

- события безопасности, связанные с управлением запуском/остановкой компонентов программного обеспечения;

Примечание — Основными событиями безопасности, относящимися к данному типу, являются: «Запуск (завершение) программ и процессов (заданий, задач)», «Запрет запуска программы», «Запрет загрузки библиотеки» и другие события безопасности.

- события безопасности, связанные с обнаружением утечки информации через съемные машинные носители информации и сетевые устройства;

Примечание — Основными событиями безопасности, относящимися к данному типу, являются: «Обнаружение утечки информации», «Обнаружение теневого копирования», «Обнаружение конфиденциальной информации на узле» и другие события безопасности.

- события безопасности, связанные с обнаружением утечки информации через системы обмена мгновенными сообщениями;

Примечание — Основными событиями безопасности, относящимися к данному типу, являются: «Обнаружение утечки информации», «Обнаружение конфиденциальной информации на узле» и другие события безопасности.

- события безопасности, связанные с обнаружением утечки информации через электронную почту;

Примечание — Основными событиями безопасности, относящимися к данному типу, являются: «Обнаружение утечки информации», «Обнаружение конфиденциальной информации на узле» и другие события безопасности.

- события безопасности, связанные с выводом защищаемой информации на печать;

Примечание — Основными событиями безопасности, относящимися к данному типу, являются: «Обнаружение утечки информации через печать», «Печать файла», «Печать файла запрещена» и другие события безопасности.

- события безопасности, связанные с подключением/отключением съемного машинного носителя информации;

Примечание — Основными событиями безопасности, относящимися к данному типу, являются: «Подключен съемный машинный носитель информации», «Отключен съемный машинный носитель информации» и другие события безопасности.

- события безопасности, связанные с выполнением действий с файлами на съемных машинных носителях информации;

Примечание — Основными событиями безопасности, относящимися к данному типу, являются: «Копирование файла на съемный машинный носитель информации», «Создание файла на съемном машинном носителе информации» и другие события безопасности.

- события безопасности, связанные с выполнением резервного копирования;

Примечание — Основными событиями безопасности, относящимися к данному типу, являются: «Начало резервного копирования», «Останов резервного копирования», «Ошибка доступа к цели резервирования», «Ошибка доступа к хранилищу» и другие события безопасности.

- события безопасности, связанные с управлением резервным копированием;

Примечание — Основными событиями безопасности, относящимися к данному типу, являются: «Изменение в составе целей/хранилищ», «Изменение задачи резервного копирования» и другие события безопасности.

- события безопасности, связанные с выполнением восстановления информации;

Примечание — Основными событиями безопасности, относящимися к данному типу, являются: «Успешное восстановление файла», «Ошибка восстановления» и другие события безопасности.

- события безопасности, связанные с контролем использования интерфейсов ввода (вывода) информации;

Примечание — Основными событиями безопасности, относящимися к данному типу, являются: «Устройство подключено», «Доступ к устройству заблокирован» и другие события безопасности.

- события безопасности, связанные с контролем целостности;

Примечание — Основными событиями безопасности, относящимися к данному типу, являются: «Добавлен новый объект контроля», «Удален объект контроля», «Запущен процесс выполнения контроля целостности для объекта», «Остановлен процесс выполнения контроля целостности для объекта», «Целостность объекта подтверждена», «Целостность объекта нарушена», «Ошибка при выполнении контроля целостности для объекта» и другие события безопасности.

- события безопасности, связанные с гарантированным уничтожением информации;

Примечание — Основными событиями безопасности, относящимися к данному типу, являются: «Файл гарантированно уничтожен», «Полное затирание съемного машинного носителя информации произведено» и другие события безопасности.

- события безопасности, связанные с контролем функционирования средств защиты информации;

Примечание — Основными событиями безопасности, относящимися к данному типу, являются: «Сбой функционирования компонента СЗИ», «Ошибка запуска СЗИ» и другие события безопасности.

- события безопасности, связанные с прекращением функционирования (сбой, отказ) программного, технического или программно-технического средства защиты информации;

Примечание — Основным событием безопасности, относящимся к данному типу, является «Прекращение функционирования средства защиты информации», а также другие события безопасности.

- события безопасности, связанные с управлением (администрированием) функциями безопасности;

Примечание — Основными событиями безопасности, относящимися к данному типу, являются: «Конфигурация компонента СЗИ изменена», «Компонент СЗИ отключен» и другие события безопасности.

- события безопасности, связанные с управлением журналами (записями) регистрации событий безопасности;

Примечание — Основными событиями безопасности, относящимися к данному типу, являются: «Журнал очищен», «Журналирование отключено», «Журнал архивирован» и другие события безопасности.

- события безопасности, связанные с применением методов криптографической защиты информации в соответствии с законодательством Российской Федерации;
- иные события безопасности.

Приложение Б
(справочное)

Типы событий безопасности, подлежащих регистрации средствами обеспечения безопасности информационных технологий и иными программно-техническими средствами (а также программным обеспечением), применяемыми в информационных (автоматизированных) системах

Изготовитель средства обеспечения безопасности информационных технологий, иных программно-технических средств и программного обеспечения определяет типы событий безопасности на основании выполняемых средствами и (или) программным обеспечением функций безопасности.

Выделяют следующие основные типы событий безопасности, подлежащих регистрации средствами обеспечения безопасности информационных технологий и иными программно-техническими средствами (а также программным обеспечением), применяемыми в информационных (автоматизированных) системах:

- события безопасности, связанные с выполнением действий по управлению виртуальными машинами;

Примечание — Основными событиями безопасности, относящимися к данному типу, являются: «Успешный запуск виртуальный машины», «Виртуальная машина приостановлена» и другие события безопасности.

- события безопасности, связанные с изменением состояния виртуальных машин;

Примечание — Основными событиями безопасности, относящимися к данному типу, являются: «Виртуальная машина перезагружена», «Виртуальная машина не отвечает» и другие события безопасности.

- события безопасности, связанные с изменением конфигурации виртуальной машины;

Примечание — Основными событиями безопасности, относящимися к данному типу, являются: «В состав виртуальной машины добавлено новое устройство», «Сбой изменения конфигурации» и другие события безопасности.

- события безопасности, связанные с изменением конфигурации гипервизора;

Примечание — Основными событиями безопасности, относящимися к данному типу, являются: «Веб-интерфейс гипервизора отключен», «Гипервизор перезагружен», «Виртуальный коммутатор добавлен» и другие события безопасности.

- события безопасности, связанные с изменением конфигурации виртуального коммутатора;

Примечание — Основными событиями безопасности, относящимися к данному типу, являются: «Виртуальная сеть виртуального коммутатора изменена», «К виртуальному коммутатору подключена виртуальная машина» и другие события безопасности.

- события безопасности, связанные с изменением конфигурации дискового хранилища;

Примечание — Основными событиями безопасности, относящимися к данному типу, являются: «Хранилище отформатировано», «Заканчивается свободное место в хранилище» и другие события безопасности.

- события безопасности, связанные с перемещением (размещением) виртуальных машин;

Примечание — Основными событиями безопасности, относящимися к данному типу, являются: «Виртуальная машина перемещена на другой гипервизор», «Сбой перемещения виртуальной машины» и другие события безопасности.

- события безопасности, связанные с управлением контрольными точками виртуальной машины;

Примечание — Основными событиями безопасности, относящимися к данному типу, являются: «Контрольная точка создана», «Сбой слияния контрольных точек» и другие события безопасности.

- события безопасности, связанные с использованием сервиса доменных имен;

Примечание — Основными событиями безопасности, относящимися к данному типу, являются: «Прямой запрос к серверу», «Рекурсивный запрос к серверу», «Трансфер зоны», «Ошибка обработки запроса», «Ошибка чтения конфигурации зоны», «Превышен лимит количества запросов» и другие события безопасности.

- события безопасности, связанные с использованием сервиса динамической настройки сети;

Примечание — Основными событиями безопасности, относящимися к данному типу, являются: «Ошибка предоставления IP-адреса для узла», «Выделение IP-адреса узлу», «Превышен лимит запросов», «Назначенный статический IP-адрес уже занят» и другие события безопасности.

- события безопасности, связанные с использованием сервиса передачи файлов;

Примечание — Основными событиями безопасности, относящимися к данному типу, являются: «Попытка подключения к серверу (анонимное/обычное, удачное/неудачное)», «Выполнение команды на сервере», «Ошибка доступа к файлу/каталогу», «Срабатывание правил фильтрации загружаемой информации» и другие события безопасности.

- события безопасности, связанные с использованием веб-сервера;

Примечание — Основными событиями безопасности, относящимися к данному типу, являются: «Предоставлен/заблокирован доступ к ресурсу на узле», «Ошибка доступа к ресурсу на узле», «Некорректный сертификат» и другие события безопасности.

- события безопасности, связанные с использованием прокси-сервера;

Примечание — Основными событиями безопасности, относящимися к данному типу, являются: «Соединение с сервером (открытие/закрытие, успешно/неуспешно)», «Получен и обработан запрос на контент», «Получен запрещенный запрос», «Ошибка отправки проксированного запроса на удаленный сервер», «Локальная ошибка обработки запроса», «Ошибка работы с кэш» и другие события безопасности.

- события безопасности, связанные с использованием сервера электронной почты;

Примечание — Основными событиями безопасности, относящимися к данному типу, являются: «Получение/передача сообщения», «Пересылка сообщения», «Подключение пользователя», «Блокировка передачи сообщения», «Отказ от приема сообщения», «Приближение к превышению квоты почтового ящика/превышение квоты», «Удаление почтового ящика» и другие события безопасности.

- события безопасности, связанные с использованием сервера службы каталога;

Примечание — Основными событиями безопасности, относящимися к данному типу, являются: «Создание контейнера», «Изменение контейнера», «Добавление объекта в контейнер», «Изменение объекта в контейнере» и другие события безопасности.

- события безопасности, связанные с использованием терминального сервера;

Примечание — Основными событиями безопасности, относящимися к данному типу, являются: «Вход/выход пользователя», «Неудачные попытки входа пользователя», «Проверка лицензирования сервера терминалов» и другие события безопасности.

- события безопасности, связанные с использованием файлового хранилища;

Примечание — Основными событиями безопасности, относящимися к данному типу, являются: «Заканчивается свободное место в хранилище», «Запросы на чтение/запись/создание/удаление файлов и директорий» и другие события безопасности.

- события безопасности, связанные с использованием маршрутизатора;

Примечание — Основными событиями безопасности, относящимися к данному типу, являются: «Высокая загруженность центрального процессора», «Изменение маршрутной информации», «Коллизия MAC-адресов», «Переполнение таблицы MAC-адресов», «Широковещательный шторм», «Ошибка контрольной суммы на интерфейсе», «Попытка несанкционированного доступа к маршрутизатору», «Ошибка функционирования маршрутизатора», «Факт стирания (очистки) журнала регистрации событий маршрутизатора», «Факт срабатывания правила фильтрации маршрутизатора», «Соединение заблокировано» и другие события безопасности.

- события безопасности, связанные с управлением маршрутизатором;

Примечание — Основными событиями безопасности, относящимися к данному типу, являются: «Изменение конфигурации», «Список запущенных сервисов/изменение статуса запущенных сервисов», «Изменение состояния интерфейса (подключение/отключение сетевого кабеля)», «Неудачная попытка доступа к управлению маршрутизатором», «Изменение версии программного обеспечения маршрутизатора», «Изменение состава учетных записей администраторов», «Изменение прав (полномочий) учетных записей администраторов» и другие события безопасности.

- события безопасности, связанные с использованием коммутатора;

Примечание — Основными событиями безопасности, относящимися к данному типу, являются: «Выполнение команды пользователем», «Коллизия MAC-адресов», «Переполнение таблицы MAC-адресов», «Широковещательный шторм», «Ошибка контрольной суммы на интерфейсе», «Соединение заблокировано», «Попытка несанкционированного доступа к коммутатору», «Ошибка функционирования коммутатора», «Факт стирания (очистки) журнала регистрации событий коммутатора», «Факт срабатывания правила фильтрации коммутатора» и другие события безопасности.

- события безопасности, связанные с управлением коммутатором;

Примечание — Основными событиями безопасности, относящимися к данному типу, являются: «Изменение конфигурации коммутатора», «Изменение состояния интерфейса (подключение/отключение интерфейсного кабеля)», «Неудачная попытка доступа к управлению коммутатором», «Изменение версии программного обеспечения коммутатора», «Изменение состава учетных записей администраторов», «Изменение прав (полномочий) учетных записей администраторов» и другие события безопасности.

- события безопасности, связанные с использованием контроллера беспроводного доступа;

Примечание — Основными событиями безопасности, относящимися к данному типу, являются: «Регистрация/разрегистрация устройства», «Регистрация/разрегистрация пользователя», «Конфигурация точки доступа изменена», «Повышение уровня шума (смена профилей контроля шума)», «Смена канала» и другие события безопасности.

- события безопасности, связанные с управлением контроллером беспроводного доступа;

Примечание — Основными событиями безопасности, относящимися к данному типу, являются: «Изменение конфигурации контроллера», «Изменение состояния интерфейсов» и другие события безопасности.

- события безопасности, связанные с использованием ответвителя сетевого трафика;
- иные события безопасности.

Библиография

[1] RFC 2822. Формат сообщений интернет [April 2001] доступен на gost.e-ecolog.ru

УДК 004.622:006.354 ОКС 35.020

Ключевые слова: защита информации, регистрация, событие безопасности, регистрируемая информация

Редактор *Т.Н. Магала*
Технический редактор *И.Е. Черепкова*
Корректор *И.А. Королева*
Компьютерная верстка *Л.А. Круговой*

Сдано в набор 14.01.2022. Подписано в печать 28.01.2022. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 7,90. Уч.-изд. л. 7,11.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении в ФГБУ «РСТ»
для комплектования Федерального информационного фонда стандартов,
117418 Москва, Нахимовский пр-т, д. 31, к. 2.

gost.e-ecolog.ru gost.e-ecolog.ru

gost.e-ecolog.ru