

# Требования к управлению событиями безопасности

чек-лист

ТИПЫ СОБЫТИЙ

СОСТАВ СОБЫТИЯ

СРОКИ ХРАНЕНИЯ

## Типы событий

### Действия с аккаунтами, паролями, ключами и токенами, в том числе:

- создание
- чтение
- изменение
- блокировка и разблокировка
- удаление

### Действия с полномочиями, ролями и разрешениями для работы с файлами, системой в целом и отдельными функциям, в том числе сетевыми соединениями:

- создание и выдача, включая добавление в группы
- изменение
- удаление и отзыв, удаление из групп

### Действия с объектами на разных технологических уровнях — исполняемыми, конфигурационными и прочими файлами, журналами событий, базами данных, виртуальными машинами, кластерами и т.п.:

- создание
- чтение
- запись, в том числе обновление программного обеспечения, что предполагает изменение исполняемых и конфигурационных файлов
- запуск
- остановка
- удаление
- резервное копирование и восстановление из резервной копии
- подключение и отключение съемных носителей информации, а также их использование

### Действия, выполняемые с повышенными привилегиями — в дополнение к описанным выше действиям:

- повышение привилегий
- вводимые в терминале команды со всеми параметрами

### Вход в систему — попытки аутентификации сервисов и всех пользователей, даже служебных, — как успешные, так и неудачные.

### Сессии работы с системой:

- создание и открытие
- завершение и закрытие, включая автоматическое прерывание по таймауту или по требованию пользователя

### Запуск, остановка (штатная или аварийная)

а также изменение режимов работы программных модулей, механизмов защиты и специализированных средств безопасности, в том числе переключение или смену ролей узлов отказоустойчивого кластера.

### Действия, выполняемые средствами безопасности — активность антивирусов, межсетевых экранов, сканеров, инструментов контроля целостности и аналогичных средств:

- обновление контента, используемого для работы, — сигнатур, баз разрешающих и блокирующих правил и т.п.
- выполнение задач по расписанию — сканирования, резервного копирования конфигураций и других требуемых действий
- обнаружение и блокирование угроз — сетевых атак, вредоносного кода, нарушения целостности и подобных событий

## Состав события

Каждая запись в журнале событий должна содержать следующие основные атрибуты:

### Дата и время

точная хронологическая метка события с точностью до секунд

### Источник

Имя компонента системы, который зарегистрировал событие

### Субъект доступа

идентификатор пользователя или процесса, MAC или IP-адрес источника, а также другие инициаторы активности

### Действие

чтение, запись, блокировка, изменение контрольной суммы и прочие операции с объектом доступа

### Объект доступа

имя файла или виртуальной машины, конкретный элемент в базе данных, MAC или IP-адрес назначения и подобные целевые ресурсы

### Результат

успех или ошибка

**Внимание!** Если объектом доступа являются аутентификационные данные (пароли, ключи шифрования или токены), то в записи указывается только идентификатор объекта. Это может быть имя файла закрытого ключа или содержащая токен переменная, а также другая неконфиденциальная информация. Записывать в лог секретное содержимое категорически запрещено!

## Сроки хранения

Конкретная глубина архива зависит от применимых нормативных требований. В общем случае мы рекомендуем ориентироваться на следующие оптимальные значения:

- **не менее 3 месяцев** — для оперативного («горячего») доступа,
- **от 3 до 5 лет** — для архивного («холодного») хранения.

В контексте отдельных документов следует учитывать требования нормативов к срокам хранения событий безопасности:

- Приказы **ФСТЭК России №17** и **№21**: **сроки хранения оператор устанавливает самостоятельно** с учетом того, что они должны обеспечивать возможность обнаружения, идентификации и анализа инцидентов, возникших в системе;
- **ГОСТ Р 57580.1**:
  - хранение событий безопасности в течение **5 лет** – для систем 1-го уровня защиты информации;
  - хранение событий безопасности в течение **3 лет** – для систем 2-го и 3-го уровня защиты информации;
- **PCI DSS**: хранение событий безопасности в течение **1 года** с возможностью оперативного доступа к просмотру событий за ближайшие **3 месяца**.