|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Критерии (показатели) | Виды | Типы событий безопасности, подлежащих регистрации | Основные события безопасности | Опасное - /  неопасное+/  нейтральное+- |
| По виду ИС | Автономная: защищаемая информация не передается по каналам связи (обработка на одном узле) |  |  |  |
|  | события безопасности, связанные с обнаружением признаков компьютерных атак на узле | «Обнаружена аномальная сетевая активность на узле», | - |
|  |  | «Обнаружена компьютерная атака на узле», | - |
|  |  | «На узле заблокирован подозрительный трафик» | - |
|  | события безопасности, связанные с фильтрацией сетевого трафика на прикладном уровне | «Попытка эксплуатации уязвимости», | - |
|  |  | «Внедрение кода», | - |
|  |  | «Межсайтовое выполнение сценариев» | - |
| Локальная: защищаемая информация передается по каналам связи в пределах контролируемой зоны | события безопасности, связанные с обнаружением признаков компьютерных атак в сетевом трафике | «Обнаружена аномальная сетевая активность», | - |
|  |  | «Обнаружена компьютерная атака», | - |
|  |  | «Заблокирован подозрительный трафик» | +- |
|  | события безопасности, связанные с фильтрацией сетевого трафика на уровне логических границ сети и сегментов сети | «Обнаружен пакет», | + |
|  |  | «Пакет заблокирован», | - |
|  |  | «Обнаружен поток», | + |
|  |  | «Поток заблокирован», | - |
|  |  | «Соединение разрешено», | + |
|  |  | «Соединение запрещено», | - |
|  |  | «Соединение заблокировано» | +- |
|  | события безопасности, связанного  с управлением фильтрацией сетевого трафика | «Создание правила фильтрации», | + |
|  |  | «Изменение правила фильтрации», | +- |
|  |  | «Удаление правила фильтрации» | +- |
|  | события безопасности, связанные с изменениями в сетевой адресации | «Изменение IP-адреса», | +- |
|  |  | «Автоматическое назначение IP-адреса», | +- |
|  |  | «Изменение дополнительных параметров IP‑адресации» | +- |
|  | события безопасности, связанные с изменениями в аппаратной адресации | «Изменение аппаратного адреса» | +- |
|  | события безопасности, связанные с изменениями в статической маршрутизации | «Добавление маршрута в таблицу маршрутизации», | +- |
|  |  | «Удаление маршрута из таблицы маршрутизации», | + |
|  |  | «Назначение  маршрута по умолчанию» | +- |
|  | события безопасности, связанные с изменениями в таблице сопоставления аппаратных адресов и портов | «Добавление статической записи в САМ-таблицу», | +- |
|  |  | «Добавление MAC-адреса в таблицу» | +- |
| Распределенная: представляет собой сеть передачи данных, сфера действия которой простирается за пределы локальной сети. | события безопасности, связанные с фильтрацией сетевого трафика на уровне логических границ сети и сегментов сети | «Обнаружен пакет», | + |
|  |  | «Пакет заблокирован», | - |
|  |  | «Обнаружен поток», | + |
|  |  | «Поток заблокирован», | - |
|  |  | «Соединение разрешено», | + |
|  |  | «Соединение запрещено», | - |
|  |  | «Соединение заблокировано» | +- |
|  | события безопасности, связанные с изменениями в сетевой адресации | «Изменение IP-адреса», | +- |
|  |  | «Автоматическое назначение IP-адреса», | +- |
|  |  | «Изменение дополнительных параметров IP‑адресации» | +- |
|  | события безопасности, связанные с фильтрацией сетевого трафика на уровне узла | «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» | - |
|  |  | события безопасности, связанные с обнаружением и действиями по защите от атак, направленных на отказ в обслуживании | Срабатывание правила обнаружения атаки», | - |
|  |  |  | «Срабатывание правила оповещения» | - |
|  |  | события безопасности, связанные с использованием терминального сервера | «Вход/выход пользователя», | +- |
|  |  |  | «Неудачные попытки входа пользователя» | +- |
|  |  |  | «Проверка лицензирования сервера термина-  лов» | + |
| Используемые сетевые протоколы | DNS | события безопасности, связанные с использованием сервиса доменных имен | «Прямой запрос к серверу», | + |
| «Рекурсивный запрос к серверу», | +- |
| «Трансфер зоны», | +- |
| «Ошибка обработки запроса», | - |
| «Ошибка чтения конфигурации зоны», | - |
| «Превышен лимит количества запросов» | - |
| Динамическая настройка сети (DHCP) | события безопасности, связанные с использованием сервиса динамической настройки сети | «Ошибка предоставления IP-адреса для узла», | - |
| «Выделение IP-адреса узлу», | +- |
| «Превышен лимит запросов», | - |
| «Назначенный статический IP-адрес уже занят» | +- |
| Используемые серверы | Веб-сервер | события безопасности, связанные с использованием веб-сервера | «Предоставлен доступ к ресурсу на узле», | +- |
|  |  | «Заблокирован доступ к ресурсу на узле», | +- |
|  |  | «Ошибка доступа к ресурсу на узле», | - |
|  |  | «Некорректный сертификат» | - |
| Сервер электронной почты | события безопасности, связанные с использованием сервера электронной почты | «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» | + |
| Сервер службы каталога | события безопасности, связанные с использованием сервера службы каталога | «Создание контейнера», | + |
|  |  | «Изменение контейнера», | + |
|  |  | «Добавление объекта в контейнер», | + |
|  |  | «Изменение объекта в контейнере» | +- |
| Прокси-сервер | события безопасности, связанные с использованием прокси-сервера | «Соединение с сервером успешно установлено», | + |
|  |  | «Соединение с сервером не установлено», | +- |
|  |  | «Получен и обработан запрос на контент», | + |
|  |  | «Получен запрещенный запрос», | +- |
|  |  | «Ошибка отправки проксированного запроса на удаленный сервер», | - |
|  |  | «Локальная ошибка обработки запроса», | - |
|  |  | «Ошибка работы с кэш» | - |
|  |  |  |  |
| По применяемым технологиям | Используются технологии беспроводного доступа | события безопасности, связанные с использованием контроллера беспроводного доступа | «Регистрация устройства», | + |
|  |  |  | «Разрегистрация устройства», | - |
|  |  |  | «Регистрация пользователя», | + |
|  |  |  | «Разрегистрация пользователя», | - |
|  |  |  | «Конфигурация точки доступа изменена», | - |
|  |  |  | «Повышение уровня шума (смена профилей контроля шума)», | - |
|  |  |  | «Смена канала» | - |
|  |  | события безопасности, связанные с управлением контроллером беспроводного доступа | «Изменение конфигурации контроллера», | - |
|  |  |  | «Изменение состояния интерфейсов» | +- |
|  |  | события безопасности, связанные с обнаружением активности вредоносных программ в сетевом трафике; | «Проверка входящих и исходящих сетевых соединений на наличие вирусной активности», | + |
|  |  |  | «Проверка файлов, обнаруженных в сетевом трафике» | + |
|  |  | события безопасности, связанные с использованием маршрутизатора | «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» | - |
|  | Используются аппаратные идентификаторы | события безопасности, связанные с управлением аппаратными идентификаторами | «Создание идентификатора», | +- |
|  |  | «Изменение идентификатора», | +- |
|  |  | «Удаление идентификатора», | + |
|  |  | «Блокирование идентификатора» | - |
|  | события безопасности, связанные с управлением средствами аутентификации | «Пароль не соответствует параметрам безопасности», | +- |
|  |  |  | «Истекает срок действия сертификата», | - |
|  |  |  | «Истек срок действия сертификата» | - |
|  | Используются съемные машинные носители | события безопасности, связанные с обнаружением утечки информации через съемные машинные носители информации и сетевые устройства; | «Обнаружение утечки информации», | - |
|  |  | «Обнаружение теневого копирования», | - |
|  |  | «Обнаружение конфиденциальной информации на узле» | - |
|  | события безопасности, связанные с подключением/отключением съемного машинного носителя информации | «Подключен съемный машинный носитель информации», | +- |
|  |  | «Отключен съемный машинный носитель информации» | + |
|  | события безопасности, связанные с выполнением действий с файлами на съемных машинных носителях информации; | «Копирование файла на съемный машинный носитель информации», | - |
|  |  | «Создание файла на съемном машинном носителе информации» | +- |
|  | события безопасности, связанные с гарантированным уничтожением информации | «Файл гарантированно уничтожен», | + |
|  |  |  | «Полное затирание съемного машинного носителя информации произведено» | + |
|  | Используются виртуальные машины | события безопасности, связанные с выполнением действий по управлению виртуальными машинами | «Успешный запуск виртуальный машины», | + |
|  |  | «Виртуальная машина приостановлена» | + |
|  | события безопасности, связанные с изменением состояния виртуальных машин | «Виртуальная машина перезагружена», | + |
|  |  | «Виртуальная машина не отвечает» | +- |
|  | события безопасности, связанные с изменением конфигурации виртуальной машины | «В состав виртуальной машины добавлено новое устройство», | +- |
|  |  | «Сбой изменения конфигурации» | - |
|  | события безопасности, связанные с изменением конфигурации гипервизора | «Веб-интерфейс гипервизора отключен», | - |
|  |  | «Гипервизор перезагружен», | + |
|  |  | «Виртуальный коммутатор добавлен» | +- |
|  | события безопасности, связанные с перемещением (размещением) виртуальных машин | «Виртуальная машина перемещена на другой гипервизор», | +- |
|  |  | «Сбой перемещения виртуальной машины» | - |
|  | события безопасности, связанные с управлением контрольными точками виртуальной машины | «Контрольная точка создана», | + |
|  |  |  | «Сбой слияния контрольных точек» | +- |
| По используемым СЗИ | Используется СДЗ | события безопасности, связанные с прохождением процедуры доверенной загрузки операционной системы | «Загрузка пройдена успешно», | + |
|  |  |  | «Ошибка при прохождении загрузки», | - |
|  |  |  | «Отказ в загрузке» | - |
|  | СЗИ от НСД | события безопасности, связанные с доступом к защищаемой информации | «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» | +- |
|  |  | события безопасности, связанные с идентификацией и аутентификацией субъекта доступа | «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» | + |
|  |  | события безопасности, связанные с контролем использования интерфейсов ввода (вывода) информации | «Устройство подключено», | +- |
|  |  |  | «Доступ к устройству заблокирован» | - |
|  |  | события безопасности, связанные с контролем целостности | «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» | - |
|  |  | события безопасности, связанные с управлением атрибутами доступа | «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» | + |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  | Используется антивирус | события безопасности, связанные с управлением антивирусной защитой | «Запуск службы», | + |
|  |  |  | «Останов службы», | +- |
|  |  |  | «Включение сканера», | + |
|  |  |  | «Отключение сканера», | +- |
|  |  |  | «Лицензия просрочена», | - |
|  |  |  | «Лицензия не найдена», | - |
|  |  |  | «У лицензии окончен срок действия» | - |
|  |  | события безопасности, связанные с обнаружением файловой активности вредоносных программ | «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» | - |
|  |  | события безопасности, связанные с обнаружением активности вредоносных программ в почтовом трафике | «Централизованная проверка входящих и исходящих почтовых сообщений на наличие вирусов», | + |
|  |  |  | «Выборочная проверка входящих и исходящих почтовых сообщений на наличие вирусов» | + |
|  |  | события безопасности, связанные с обнаружением активности вредоносных программ в сетевом трафике | «Проверка входящих и исходящих сетевых соединений на наличие вирусной активности», | + |
|  |  |  | «Проверка файлов, обнаруженных в сетевом трафике» | + |
|  |  | события безопасности, связанные с обнаружением и действиями по защите от незапрашиваемых электронных сообщений (спама); | «Обнаружен спам», | - |
|  |  |  | «Отправитель заблокирован» | +- |
|  |  | события безопасности, связанные с управлением защитой от спама | «Запуск службы», | + |
|  |  |  | «Останов службы», | +- |
|  |  |  | «Включение сканера», | + |
|  |  |  | «Отключение сканера», | +- |
|  |  |  | «Лицензия просрочена», | - |
|  |  |  | «Лицензия не найдена», | - |
|  |  |  | «У лицензии окончен срок действия», | - |
|  |  |  | «Конфигурация изменена» | +- |
|  |  | события безопасности, связанные с проведением обновления базы данных признаков вредоносных компьютерных программ (вирусов) | «Успешное проведение обновления базы данных признаков вредоносных компьютерных программ (вирусов)», | + |
|  |  |  | «Ошибка при обновлении базы данных признаков вредоносных компьютерных программ (вирусов)» | - |
|  | Используется средство анализа защищенности | события безопасности, связанные с обнаружением уязвимостей программного обеспечения | «Обнаружена уязвимость», | +- |
|  |  |  | «Устранена уязвимость» | + |
|  |  | события безопасности, связанные с проведением обновления базы уязвимостей | «База уязвимостей обновлена успешно», | + |
|  |  |  | «Ошибка при обновлении базы уязвимостей» | +- |
|  |  | события безопасности, связанные с изменениями состава программного обеспечения | «Обнаружено изменение состава ПО», | +- |
|  |  |  | «Обнаружено запрещенное ПО» | - |
|  | Используется средство обнаружения вторжения | события безопасности, связанные с управлением средством обнаружения и блокирования компьютерных атак | «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» | +- |
|  |  | события безопасности, связанные с проведением обновления базы решающих правил | «База решающих правил обновлена успешно», | + |
|  |  |  | «Ошибка при обновлении базы решающих правил» | - |
|  | Используется DLP | события безопасности, связанные с обнаружением утечки информации через съемные машинные носители информации и сетевые устройства | «Обнаружение утечки информации», | - |
|  |  |  | «Обнаружение теневого копирования», | - |
|  |  |  | «Обнаружение конфиденциальной информации на узле» | - |
|  |  | события безопасности, связанные с обнаружением утечки информации через системы обмена мгновенными сообщениями | «Обнаружение утечки информации», | - |
|  |  |  | «Обнаружение конфиденциальной информации на узле» | +- |
|  |  | события безопасности, связанные с обнаружением утечки информации через электронную почту | «Обнаружение утечки информации», | - |
|  |  |  | «Обнаружение конфиденциальной информации на узле» | +- |
|  |  | события безопасности, связанные с выводом защищаемой информации на печать | «Обнаружение утечки информации через печать», | - |
|  |  |  | «Печать файла», | +- |
|  |  |  | «Печать файла запрещена» | + |
|  | Используется многофункциональный межсетевой экран уровня сети | события безопасности, связанные с фильтрацией сетевого трафика на уровне логических границ сети и  сегментов сети; | «Обнаружен пакет», | + |
|  |  |  | «Пакет заблокирован», | - |
|  |  |  | «Обнаружен поток», | + |
|  |  |  | «Поток заблокирован», | - |
|  |  |  | «Соединение разрешено», | + |
|  |  |  | «Соединение запрещено», | - |
|  |  |  | «Соединение заблокировано» | +- |
|  |  | события безопасности, связанные с управлением фильтрацией сетевого трафика | «Создание правила фильтрации», | + |
|  |  |  | «Изменение правила фильтрации», | +- |
|  |  |  | «Удаление правила фильтрации» | +- |
|  |  | события безопасности, связанные с обнаружением признаков вредоносного программного обеспечения в сетевом трафике; | «Проверка входящих и исходящих сетевых соединений на наличие вирусной активности», | + |
|  |  |  | «Проверка файлов, обнаруженных в сетевом трафике» | + |
|  |  | события безопасности, связанные с обнаружением признаков компьютерных атак в сетевом трафике; | «Обнаружена аномальная сетевая активность», | - |
|  |  |  | «Обнаружена компьютерная атака», | - |
|  |  |  | «Заблокирован подозрительный  трафик» | + |
| Технологии обработки | Резервное копирование | события безопасности, связанные с выполнением резервного копирования | «Начало резервного копирования», | + |
|  |  |  | «Останов резервного копирования», | +- |
|  |  |  | «Ошибка доступа к цели резервирования», | - |
|  |  |  | «Ошибка доступа к хранилищу» | - |
|  |  | события безопасности, связанные с управлением резервным копированием | «Изменение в составе целей/хранилищ», | - |
|  |  |  | «Изменение задачи резервного копирования» | +- |
|  |  | события безопасности, связанные с выполнением восстановления информации | «Успешное восстановление файла», | + |
|  |  |  | «Ошибка восстановления» | - |
|  | Обновление и изменение конфигурации ПО | события безопасности, связанные с изменениями состава программного обеспечения | «Обнаружено изменение состава ПО», | +- |
|  |  |  | «Обнаружено запрещенное ПО» | - |
|  |  | события безопасности, связанные с установкой, изменением системного времени | «Системное время установлено», | + |
|  |  |  | «Системное время изменено» | +- |
|  |  | события безопасности, связанные с изменением настроек общего программного обеспечения | «Конфигурация компонента программного обеспечения изменена», | +- |
|  |  |  | «Компонент программного обеспечения отключен» | +- |
|  |  | события безопасности, связанные с контролем наличия обязательных обновлений программного обеспечения | «Сбой в централизованном распространении  обновлений» | - |
|  |  | события безопасности, связанные с выполнением процедуры установки/удаления компонентов программного обеспечения | «Начата установка ПО», | +- |
|  |  |  | «ПО установлено», | +- |
|  |  |  | «Служба удалена» | + |
|  |  | события безопасности, связанные с управлением запуском/остановкой компонентов программного обеспечения | «Запуск программ и процессов (заданий, задач)», | +- |
|  |  |  | «Завершение программ и процессов (заданий, задач)», | + |
|  |  |  | «Запрет запуска программы», | - |
|  |  |  | «Запрет загрузки библиотеки» | - |
|  | Хранение | события безопасности, связанные с использованием файлового хранилища | «Заканчивается свободное место в хранилище», | - |
|  |  |  | «Запросы на чтение/запись/создание/удаление файлов и директорий» | +- |
|  |  | события безопасности, связанные с изменением конфигурации дискового хранилища | «Хранилище отформатировано», | + |
|  |  |  | «Заканчивается свободное место в хранилище» | - |
|  | Среда безопасного выполнения | события безопасности, связанные с анализом компонента программного обеспечения в среде безопасного выполнения компьютерных программ (песочнице); | «Создание новой песочницы», | + |
|  |  |  | «Запуск песочницы», | + |
|  |  |  | «Останов песочницы», | + |
|  |  |  | «Выполнение анализа начато» | + |
|  |  |  | «Выполнение анализа завершено» | + |
| Неисключаемые события | Контроль средств безопасности | события безопасности, связанные с контролем функционирования средств защиты информации | «Сбой функционирования компонента СЗИ», | - |
|  |  | «Ошибка запуска СЗИ» | - |
|  | события безопасности, связанные с прекращением функционирования (сбой, отказ) программного, технического или программно-технического средства защиты информации | «Прекращение функционирования средства защиты информации» | - |
|  | события безопасности, связанные с управлением (администрированием) функциями безопасности | «Конфигурация компонента СЗИ изменена», | - |
|  |  | «Компонент СЗИ отключен» | - |
|  | события безопасности, связанные с управлением журналами (записями) регистрации событий безопасности | «Журнал очищен», | +- |
|  |  | «Журналирование отключено», | - |
|  |  | «Журнал архивирован» | +- |
|  | события безопасности, связанные с изменениями параметров настроек средств защиты информации | «Конфигурация компонента СЗИ изменена», | - |
|  |  | «Компонент СЗИ отключен» | - |