1. Кандидату на основании своей экспертизы предлагается выделить (определить) список из 15 информационных систем (желательно с практическими примерами), события с которых нужно собирать первоочередно. Информационные системы нужно расположить в порядке приоритета, то есть в какой последовательности происходил бы сбор, если кандидат сам подключал их на практике.

При определении перечня информационных систем, подключаемых к SIEM (далее объектов защиты ОЗ), необходимо в первую очередь опираться на нормативно-правовые акты (как акты регуляторов, так и внутренние регламенты организации), в которых определены требования по защите информации в информационных системах, в зависимости от категории обрабатываемой информации.

Как пример таких НПА в рамках требований федеральных законов 98-ФЗ, 187-ФЗ и 152-ФЗ можно привести:

- Приказ ФСТЭК № 239, который определяет требование АУД.4 «Регистрация событий безопасности»
- приказ ФСТЭК № 17, который определяет требование РСБ.1 «Регистрация событий безопасности»
- РД ГТК "Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации». В данном документе приведены требования по регистрации событий в ИС различных категорий.

Также важным источником информации для определения объектов защиты могу выступать стандарты по информационной безопасности, как международные, так и национальные. В качестве международных могу привести CIS Critical Security Controls, NIST Cybersecurity Framework. В качестве отечественных ГОСТ Р 59547 и 59548.

Для определения перечня объектов защиты можно обратиться к стандарту ГОСТ Р 59547-2021 «МОНИТОРИНГ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ». Данный ГОСТ в качестве объектов мониторинга определяет:

- автоматизированные рабочие места;
- серверное оборудование;
- телекоммуникационное оборудование;
- технологическое и (или) производственное оборудование (исполнительные устройства);
- средства защиты информации.

Конкретный перечень объектов защиты, а также перечень событий безопасности, регистрация которых должна осуществляется на этих ОЗ, определяется эксплуатирующей организацией исходя из возможностей реализации угроз безопасности и фиксируется в организационно-распорядительных документах, например в модели угроз.

Предположим типовую коммерческую организацию в которой есть ЛВС с ИС расположенными в различных сегментах сети и обрабатывающие информацию различной категории. Условимся, что организация может иметь филиальную структуру, часть сотрудников компании может работать удаленно. Компания имеет распределенную ИТ-инфраструктуру. Основные сервисы с чувствительной информацией расположены он-прем, сервисы, доступные клиентам извне - расположены у облачного провайдера.

Для указанного примера в такой организации могли бы быть следующие ИС:

| # | Наименование информационной системы | Перечень объектов защиты, входящих в ИС | Приоритет подключения к SIEM |
|---|---|---|---|
| 1 | **ИС Инфраструктурных сервисов** | DNS (Bind);<br>dhcp;<br>NTP;<br>DC (MS AD/FreeIPA/ ALDPro/SambaDC);<br>терминальные серверы;<br>Система управления PKI (Microsoft CA, Alladin ECA) | Высокий |
| 2 | **ИС Управления учетными данными пользователей (IDM, IAM)** | WSO2IS или Keycloak | Высокий |
| 3 | **ИС Периметральная система защиты информации** | NGFW, включающий модули: FW+URLfilter+IPS/ IDS+VPN+AV+AS.<br>Checkpoint SecurityCenter + SecurityGateway (Gaia R80) | Высокий |
| 4 | **ИС Веб-приложение** | Веб-сайт в открытом доступе (Apache);<br>Балансировщик нагрузки;<br>WAF (PT AF);<br>Сервер приложений (Apache Tomcat);<br>СУБД MongoDB;<br>СУБД PostgreSQL;<br>Серверная ОС семейства Linux | Высокий |
| 5 | **ИС Система виртуализации серверов** | VMWare ESXi или решение на базе oVirt;<br>VeAmBackup; | Высокий |
| 6 | **ИС Антивирусной защиты** | Kaspersky Security Center | Высокий |
| 7 | **СЗИ EDR/XDR** | Checkpoint Endpoint Security и Kaspersky Endpoint Security (В том числе для BYOD утройств) | Высокий |
| 8 | **ИС Мониторинга инфраструктуры** | Prometheus и Zabbix 6.0 | Высокий |

| # | Наименование информационной системы | Перечень объектов защиты, входящих в ИС | Приоритет подключения к SIEM |
|---|---|---|---|
| 9 | **ИС Телекомуникационного оборудования** | Cisco router (ISR 1000);<br>Cisco switch (Catalyst 35xx, Catalyst 25xx);<br>Eltex router (MES 51xx, MES 52xx);<br>Eltex switch (MES 23xx, MES 24xx);<br>средства централизованной аутентификации (RADIUS, TACACS+); | Средний |
| 10 | **ИС Корпоративный портал для сотрудников (в том числе доступ удаленных сотрудников)** | Серверная ОС семейства Windows<br>MS SharePoint;<br>1С Битрикс;<br>СУБД PostgreSQL; | Средний |
| 12 | **ИС Защиты от утечек (DLP)** | Infowatch TrafficMonitro, DeviceMonitor | Средний |
| 13 | **ИС ERP** | 1С Enterprise и/или SAP ERP | Средний |
| 14 | **ИС Клиентские АРМ** | ОС MS Windows 7,10,11;<br>ОС Astra Linux;<br>ОС Linux Ubuntu;<br>ОС MacOS; | Средний |
| 11 | **ИС Система электронного документооборота** | Серверная ОС семейства Linux;<br>ППО Directum RX, программный комплекс включает различные компоненты (сервер приложений, толстый клиент, тонкий клиент, СУБД), но имеет единую подсистему регистрации событий. | Низкий |
| 15 | **Система контроля и управления доступом (СКУД)** | Серверная ОС семейства Linux;<br>СКУД Бастион;<br>+ АРМ Операторов с Windows 7 | Низкий |

2. Каждая информационная система может содержать свои типы событий безопасности. Для указанных выше 15 информационных система кандидату предлагается определить типы событий, которые возможны (существуют) в информационных системах, и каких из них требуется собирать - некоторые "базовый" список.

НПА и стандарты по информационной безопасности регламентирует функции которые должна выполнять SIEM-система. Одной из таких функций SIEM-системы является организация единого места хранения событий безопасности (в установленный период хранения), таким образом нужно собирать и хранить в SIEM-системе все значимые события для выполнения требований НПА и рекомендаций стандартов.

Еще одной важной функцией SIEM является корреляция событий для выявлений признаков реализации угроз ИБ. Для детализации перечня событий, которые стоило бы собирать в SIEM необходимо обратиться к модели угроз организации, для определения актуальных угроз. Также данную модель угроз можно наложить на классификатор угроз, например на фреймворк MITRE ATTACK Enterprise или БДУ ФСТЭК. Таким образом удастся определить «базовый» перечень необходимых событий.

Необходимо отметить, что с ОЗ необходимо собирать: события внутреннего аудита, функциональные события (события связанные с функциональным назначением источника), события ИБ, к которым в том числе относятся ошибки и сбои функционирования источника.

Для удобства представления информации я сгруппировал некоторые источники (например условимся, что DNS, dhcp и ntp размещены на одном сервере и мы их рассматриваем как один ОЗ)

Базовый перечень событий для вышеперечисленных ИС привожу в таблице:

| № | Наименование ИС (ОЗ) | Базовый перечень типов регистрируемых событий |
|---|---|---|
| **1** | **ИС Инфраструктурных сервисов (DNS, dhcp, ntp)** | Общие события системы (внутренний аудит):<br>• Создание, удаление, изменение пользователя, блокировка/разблокировка пользователя, изменение пароля пользователя,.<br>• Создание, удаление, изменение группы пользователей, блокировка/разблокировка группы пользователей,<br>• Добавление/ удаление пользователя в группу<br>• Изменение привилегий пользователя/группы пользователей<br>• Вход в систему, выход из системы, неуспешный вход в систему<br>• Успешный переход из УЗ в УЗ/Неуспешный переход из УЗ в УЗ<br>• Попытка аутентификации под несуществующей учетной записью<br>• Запуск, остановка, изменение параметров логирования<br>• Чтение, очистка, изменение журналов событий (логов)<br>• Изменение конфигурации источника<br>• События с уровнем Ошибка/Предупреждение/Тревога<br>• Выключение/перезапуск источника<br><br>**DNS**: Прямой запрос к серверу, Рекурсивный запрос к серверу, События связанные с трансфером зоны, Ошибка обработки запроса, Ошибка чтения конфигурации зоны, Превышен лимит количества запросов<br>**Dhcp**: Ошибка предоставления IP-адреса для узла, Выделение IP-адреса узлу, Превышен лимит запросов, Назначенный статический IP-адрес уже занят<br>**NTP**: Системное время установлено, Системное время изменено<br>**DC**: Создание контейнера, Изменение контейнера, Добавление объекта в контейнер, Изменение объекта в контейнере, события репликаци/синхронизации нод<br>**Система управления PKI**: Обновление/создание сертификата, Ошибки при работе с сертификатами, Запрос на сертификат, Ошибка импорта CRL, События создания или обновления CRL, Работа с CRL, Компрометация ключей PKI, Работа с ключами, Ошибки при работе с ключами, События создания или обновления ключей |

| № | Наименование ИС (ОЗ) | Базовый перечень типов регистрируемых событий |
|---|---|---|
| **2** | **ИС Управления учетными данными пользователей (IDM, IAM)** | Общие события системы (внутренний аудит):<br>• Создание, удаление, изменение пользователя, блокировка/ разблокировка пользователя, изменение пароля пользователя,.<br>• Создание, удаление, изменение группы пользователей, блокировка/разблокировка группы пользователей,<br>• Добавление/ удаление пользователя в группу<br>• Изменение привилегий пользователя/группы пользователей<br>• Вход в систему, выход из системы, неуспешный вход в систему<br>• Успешный переход из УЗ в УЗ/Неуспешный переход из УЗ в УЗ<br>• Попытка аутентификации под несуществующей учетной записью<br>• Запуск, остановка, изменение параметров логирования<br>• Чтение, очистка, изменение журналов событий (логов)<br>• Изменение конфигурации источника<br>• События с уровнем Ошибка/Предупреждение/Тревога<br>• Выключение/перезапуск источника<br><br>Так как данные система относится к СрЗИ дополнительно предлагаю регистрировать следующие типы событий:<br>• Сбой функционирования компонента СЗИ<br>• Ошибка запуска СЗИ<br>• Прекращение функционирования средства защиты информации<br>• Конфигурация компонента СЗИ изменена<br>• Компонент СЗИ отключен<br>• События активации/деактивации лицензии, а также окончания срока действия лицензии<br><br>Функциональные события:<br>• Создание/изменение/удаление субъекта доступа<br>• Блокирование/разблокирование субъекта доступа<br>• Создание/изменение/удаление типа доступа<br>• Создание/изменение/удаление группы пользователей<br>• Занесение/удаление учетной записи в группу пользователей<br>• Создание/изменение/удаление параметров ресурса (объекта доступа)<br>• Получение/изменение/ удаление доступа субъекта к объекту<br>• Ошибка получения доступа<br>• Поступление запроса на предоставление доступа<br>• Ошибка обработки запроса на предоставление доступа<br>• Получен доступ к ресурсу<br>• Отказ в доступе<br>• Доступ прекращен |

| № | Наименование ИС (ОЗ) | Базовый перечень типов регистрируемых событий |
|---|---|---|
| 3 | **ИС Периметральная система защиты информации**<br><br>*Так как данный источник включает в себя несколько модулей привожу основные типы регистрируемых событий с данных модулей. Также отмечу что перечень модулей не исчерпывающий.*<br><br>*Также такая ПСЗИ может выполнять функции роутера между подсетями, dhcp релея. Для упрощения такие типы событий здесь не привожу. Данные типы событий указаны в ИС Телекомуникационного оборудования.* | Общие события системы (внутренний аудит):<br>• Создание, удаление, изменение пользователя, блокировка/разблокировка пользователя, изменение пароля пользователя,.<br>• Создание, удаление, изменение группы пользователей, блокировка/разблокировка группы пользователей,<br>• Добавление/ удаление пользователя в группу<br>• Изменение привилегий пользователя/группы пользователей<br>• Вход в систему, выход из системы, неуспешный вход в систему<br>• Успешный переход из УЗ в УЗ/Неуспешный переход из УЗ в УЗ<br>• Попытка аутентификации под несуществующей учетной записью<br>• Запуск, остановка, изменение параметров логирования<br>• Чтение, очистка, изменение журналов событий (логов)<br>• Изменение конфигурации источника<br>• События с уровнем Ошибка/Предупреждение/Тревога<br>• Выключение/перезапуск источника<br><br>Так как данные система относится к СрЗИ дополнительно предлагаю регистрировать следующие типы событий:<br>• Сбой функционирования компонента СЗИ<br>• Ошибка запуска СЗИ<br>• Прекращение функционирования средства защиты информации<br>• Конфигурация компонента СЗИ изменена<br>• Компонент СЗИ отключен<br>• События активации/деактивации лицензии, а также окончания срока действия лицензии<br>• Управление объектами и субъектами доступа.<br><br>Функциональные события:<br>**FW**: Обнаружен пакет, Пакет заблокирован, Обнаружен поток, Поток заблокирован, Соединение разрешено, Соединение запрещено, Соединение заблокировано.<br>**URL filtering**: Разрешение/запрет доступа к URL, Изменение правила фильтрации, Создание правила фильтрации, Удаление правила фильтрации, Включение/отключение правил фильтрации<br>**IPS/IDS**: Обнаружена аномальная сетевая активность, Обнаружена компьютерная атака, Заблокирован подозрительный трафик, Обнаружена аномальная сетевая активность на узле, Обнаружена компьютерная атака на узле, На узле заблокирован подозрительный трафик, Действия с базами решающих правил (создание/изменение/удаление) Включение/отключение отдельных правил, Срабатывание правила обнаружения атаки, Срабатывание правила оповещения.<br>**VPN**: Создание/изменение/удаление VPN конфигурации, Создание VPN сессии, Успешное/не успешное соединение между VPN серверами, Успешная/не успешная авторизация на VPN сервер, Отключение VPN-соединения, Дублирующая VPN сессия.<br>**AV/AS**: обнаружением активности вредоносных программ в почтовом трафике, активности вредоносных программ в сетевом трафике, проведением обновления базы данных признаков вредоносных компьютерных программ (вирусов). |

| № | Наименование ИС (ОЗ) | Базовый перечень типов регистрируемых событий |
|---|---|---|
| **4** | **ИС Веб-приложение** | Общие события системы (внутренний аудит):<br>• Создание, удаление, изменение пользователя, блокировка/ разблокировка пользователя, изменение пароля пользователя,.<br>• Создание, удаление, изменение группы пользователей, блокировка/разблокировка группы пользователей,<br>• Добавление/ удаление пользователя в группу<br>• Изменение привилегий пользователя/группы пользователей<br>• Вход в систему, выход из системы, неуспешный вход в систему<br>• Успешный переход из УЗ в УЗ/Неуспешный переход из УЗ в УЗ<br>• Попытка аутентификации под несуществующей учетной записью<br>• Запуск, остановка, изменение параметров логирования<br>• Чтение, очистка, изменение журналов событий (логов)<br>• Изменение конфигурации источника<br>• События с уровнем Ошибка/Предупреждение/Тревога<br>• Выключение/перезапуск источника<br><br>Функциональные события от **веб-сервера и балансировщика**: Предоставлен/заблокирован доступ к ресурсу на узле, Ошибка доступа к ресурсу на узле, Некорректный сертификат, 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»<br><br>События от **WAF**: Срабатывание правила фильтрации запросов, Срабатывание правила, Попытка эксплуатации уязвимости, Внедрение кода, Межсайтовое выполнение сценариев, Создание правила фильтрации, Изменение правила фильтрации, Удаление правила фильтрации.<br><br>События от **сервера приложений**: Получение запроса, выполнение/ошибка выполнения запросов, события взаимодействие с компонентами системы, Запуск/останов компонентов, изменение конфигурации компонентов, установка/сбой установки обновлений, доступ/отказ доступа к компонентам.<br><br>События от **СУБД**: Создание/удаление БД, Подключение/ отключение к БД, Запуск/остановка сервиса, Создание/ изменение/удаление схемы/таблицы/табличного пространства/ представлениея/тригера/процедуры, Создание/изменение/ удаление кластера БД, Обработка CRUD запросов к БД, Импорт/экспорт БД<br><br>События от **серверной ОС**: Загрузка пройдена успешно, Ошибка при прохождении загрузки, Изменения сетевого/ аппаратного адреса, Запуск (завершение) программ и процессов (заданий, задач), Предоставление/отказ в предоставлении доступа к ресурсам. |

| № | Наименование ИС (ОЗ) | Базовый перечень типов регистрируемых событий |
|---|---|---|
| **5** | **ИС Система виртуализации серверов** | Общие события системы (внутренний аудит):<br>• Создание, удаление, изменение пользователя, блокировка/ разблокировка пользователя, изменение пароля пользователя,.<br>• Создание, удаление, изменение группы пользователей, блокировка/разблокировка группы пользователей,<br>• Добавление/ удаление пользователя в группу<br>• Изменение привилегий пользователя/группы пользователей<br>• Вход в систему, выход из системы, неуспешный вход в систему<br>• Успешный переход из УЗ в УЗ/Неуспешный переход из УЗ в УЗ<br>• Попытка аутентификации под несуществующей учетной записью<br>• Запуск, остановка, изменение параметров логирования<br>• Чтение, очистка, изменение журналов событий (логов)<br>• Изменение конфигурации источника<br>• События с уровнем Ошибка/Предупреждение/Тревога<br>• Выключение/перезапуск источника<br><br>Функциональные события **гипервизора**: Создание ВМ, Удаление ВМ, Изменение конфигурации ВМ, Запуск/ возобновление ВМ, Ошибка запуска/возобновления ВМ, Выключение/приостановка ВМ, Перезагрузка ВМ, Миграция ВМ, Ошибка миграции ВМ, Виртуальный коммутатор добавлен, Виртуальная сеть виртуального коммутатора изменена, К виртуальному коммутатору подключена виртуальная машина, Ошибки конфигурации ВМ, ВМ не отвечает, Импорт/ восстановление ВМ из снапшота, Ошибка импорта/ восстановления ВМ из снапшота, Экспорт/создание снапшота ВМ, Удаление снапшота ВМ, Подключение/отключение сетевого интерфейса к ВМ.<br><br>Функциональные события **средства резервного копирования ВМ**: Создание резервной копии, Удаление резервной копии, Создание задания резервного копирования, Удаление задания резервного копирования, Изменение задания резервного копирования, Восстановление конфигурации из резервной копии, Восстановление файлов из резервной копии |

| № | Наименование ИС (ОЗ) | Базовый перечень типов регистрируемых событий |
|---|---|---|
| **6** | **ИС Антивирусной защиты** | Общие события системы (внутренний аудит):<br>• Создание, удаление, изменение пользователя, блокировка/ разблокировка пользователя, изменение пароля пользователя,.<br>• Создание, удаление, изменение группы пользователей, блокировка/разблокировка группы пользователей,<br>• Добавление/ удаление пользователя в группу<br>• Изменение привилегий пользователя/группы пользователей<br>• Вход в систему, выход из системы, неуспешный вход в систему<br>• Успешный переход из УЗ в УЗ/Неуспешный переход из УЗ в УЗ<br>• Попытка аутентификации под несуществующей учетной записью<br>• Запуск, остановка, изменение параметров логирования<br>• Чтение, очистка, изменение журналов событий (логов)<br>• Изменение конфигурации источника<br>• События с уровнем Ошибка/Предупреждение/Тревога<br>• Выключение/перезапуск источника<br><br>Так как данные система относится к СрЗИ дополнительно предлагаю регистрировать следующие типы событий:<br>• Сбой функционирования компонента СЗИ<br>• Ошибка запуска СЗИ<br>• Прекращение функционирования средства защиты информации<br>• Конфигурация компонента СЗИ изменена<br>• Компонент СЗИ отключен<br>• События активации/деактивации лицензии, а также окончания срока действия лицензии<br>• Управление объектами и субъектами доступа.<br><br>Функциональные события **AB**: Включение сканера, Отключение сканера, Обнаружено вредоносное ПО, Зараженный файл удален/вылечен, Зараженный файл оставлен без изменений, Зараженный файл помещен в карантин, Зараженный файл помещен в резервное хранилище, Объект восстановлен из карантина, Невозможно восстановить объект из карантина, Базы устарели, Ошибка обновления баз, Базы обновлены, Блокировка запуска потенциально опасного файла, Программа признана опасной (добавление в черный список), Программа добавлена в белый список.<br><br>Функциональные события компонента **песочница**: Создание новой песочницы, Запуск песочницы, Останов песочницы, Выполнение анализа начато, Выполнение анализа завершено |

| № | Наименование ИС (ОЗ) | Базовый перечень типов регистрируемых событий |
|---|---|---|
| 7 | **СЗИ EDR/XDR** | Здесь типы событий будут схожи с функциональными событиями от периметральной системы защиты информации и системы антивирусной защиты + песочницы. Отличие в том, что события от EDR/XDR системы будут фиксироваться на конечных узлах.<br>Дополнительно отмечу, что общепринятым подходом является реализация сбора событий от конечных устройств на сервер управления (например Checkpoint SecurityManagementServer, Kaspersky SC). Сбор событий в SIEM также реализуется централизованно с серверов управления. |
| 8 | **ИС Мониторинга инфраструктуры** | Общие события системы (внутренний аудит):<br>• Создание, удаление, изменение пользователя, блокировка/разблокировка пользователя, изменение пароля пользователя,.<br>• Создание, удаление, изменение группы пользователей, блокировка/разблокировка группы пользователей,<br>• Добавление/ удаление пользователя в группу<br>• Изменение привилегий пользователя/группы пользователей<br>• Вход в систему, выход из системы, неуспешный вход в систему<br>• Успешный переход из УЗ в УЗ/Неуспешный переход из УЗ в УЗ<br>• Попытка аутентификации под несуществующей учетной записью<br>• Запуск, остановка, изменение параметров логирования<br>• Чтение, очистка, изменение журналов событий (логов)<br>• Изменение конфигурации источника<br>• События с уровнем Ошибка/Предупреждение/Тревога<br>• Выключение/перезапуск источника<br><br>Функциональные события:<br>Различные события мониторинга серверов, виртуальных серверов, контейнеров, подов и прочих сущностей в современных информационных системах, в том числе: Создание/изменение/удаление сущностей, превышение пороговых значений загрузки ЦП/памяти/сетевой нагрузки устройств, Высокая загрузка swap, Проверка сетевой доступности, Доступность хоста по определенным протоколам, Пограничное состояние ресурса/Исчерпание ресурса, количество запросов/обращений. |

| № | Наименование ИС (ОЗ) | Базовый перечень типов регистрируемых событий |
|---|---|---|
| **9** | **ИС Телекомуникационного оборудования** | Общие события системы (внутренний аудит):<br>• Создание, удаление, изменение пользователя, блокировка/разблокировка пользователя, изменение пароля пользователя,.<br>• Создание, удаление, изменение группы пользователей, блокировка/разблокировка группы пользователей,<br>• Добавление/ удаление пользователя в группу<br>• Изменение привилегий пользователя/группы пользователей<br>• Вход в систему, выход из системы, неуспешный вход в систему<br>• Успешный переход из УЗ в УЗ/Неуспешный переход из УЗ в УЗ<br>• Попытка аутентификации под несуществующей учетной записью<br>• Запуск, остановка, изменение параметров логирования<br>• Чтение, очистка, изменение журналов событий (логов)<br>• Изменение конфигурации источника<br>• События с уровнем Ошибка/Предупреждение/Тревога<br>• Выключение/перезапуск источника<br><br>События **коммутаторов**: Системное время установлено/изменено, Добавление статической записи в CAM-таблицу, Добавление MAC-адреса в таблицу, Выполнение команды пользователем, Коллизия MAC-адресов, Переполнение таблицы MAC-адресов, Широковещательный шторм, Ошибка контрольной суммы на интерфейсе, Соединение заблокировано, Ошибка функционирования коммутатора, Факт стирания (очистки) журнала регистрации событий коммутатора, Факт срабатывания правила фильтрации коммутатора, Изменение конфигурации коммутатора, Изменение состояния интерфейса (подключение/отключение интерфейсного кабеля), Изменение версии программного обеспечения коммутатора, Сбой функционирования компонента защитных механизмов, Запуск/останов/конфигурирование защитных механизмов, Ошибка запуска защитных механизмов, Конфигурация протоколов, Установка/изменение ip-адреса.<br><br>События **маршрутизаторов**: все типы событий, которые перечислены для коммутатора + Изменение маршрутной информации, включение/отключение/конфигурирование различных протоколов маршрутизации, Ошибка функционирования маршрутизатора, Добавление/удаление маршрутов в таблицу маршрутизации, Назначение маршрута по умолчанию<br><br>События **беспроводных точек доступа**: Регистрация/разрегистрация устройства, Регистрация/разрегистрация пользователя, Конфигурация точки доступа изменена, Повышение уровня шума (смена профилей контроля шума), Смена канала, Изменение конфигурации контроллера, Изменение состояния интерфейсов, Изменение IP-адреса. |

| № | Наименование ИС (ОЗ) | Базовый перечень типов регистрируемых событий |
|---|---|---|
| **10** | **ИС Корпоративный портал для сотрудников (в том числе доступ удаленных сотрудников)** | Общие события системы (внутренний аудит):<br>• Создание, удаление, изменение пользователя, блокировка/ разблокировка пользователя, изменение пароля пользователя,.<br>• Создание, удаление, изменение группы пользователей, блокировка/разблокировка группы пользователей,<br>• Добавление/ удаление пользователя в группу<br>• Изменение привилегий пользователя/группы пользователей<br>• Вход в систему, выход из системы, неуспешный вход в систему<br>• Успешный переход из УЗ в УЗ/Неуспешный переход из УЗ в УЗ<br>• Попытка аутентификации под несуществующей учетной записью<br>• Запуск, остановка, изменение параметров логирования<br>• Чтение, очистка, изменение журналов событий (логов)<br>• Изменение конфигурации источника<br>• События с уровнем Ошибка/Предупреждение/Тревога<br>• Выключение/перезапуск источника<br><br>Функциональные события от **веб-сервера**:<br>Предоставлен/заблокирован доступ к ресурсу на узле, Ошибка доступа к ресурсу на узле, Некорректный сертификат, 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 |

| № | Наименование ИС (ОЗ) | Базовый перечень типов регистрируемых событий |
|---|---|---|
| **11** | **ИС Защиты от утечек (DLP)** | Общие события системы (внутренний аудит):<br>• Создание, удаление, изменение пользователя, блокировка/ разблокировка пользователя, изменение пароля пользователя,.<br>• Создание, удаление, изменение группы пользователей, блокировка/разблокировка группы пользователей,<br>• Добавление/ удаление пользователя в группу<br>• Изменение привилегий пользователя/группы пользователей<br>• Вход в систему, выход из системы, неуспешный вход в систему<br>• Успешный переход из УЗ в УЗ/Неуспешный переход из УЗ в УЗ<br>• Попытка аутентификации под несуществующей учетной записью<br>• Запуск, остановка, изменение параметров логирования<br>• Чтение, очистка, изменение журналов событий (логов)<br>• Изменение конфигурации источника<br>• События с уровнем Ошибка/Предупреждение/Тревога<br>• Выключение/перезапуск источника<br><br>Так как данные система относится к СрЗИ дополнительно предлагаю регистрировать следующие типы событий:<br>• Сбой функционирования компонента СЗИ<br>• Ошибка запуска СЗИ<br>• Прекращение функционирования средства защиты информации<br>• Конфигурация компонента СЗИ изменена<br>• Компонент СЗИ отключен<br>• События активации/деактивации лицензии, а также окончания срока действия лицензии<br><br>Функциональные события: Получение/прекращение доступа к ресурсу, Ошибка получения доступа, Отказ в доступе, Создание/изменение/удаление ресурса, Обнаружение утечки информации по различным каналам, Обнаружение теневого копирования, Обнаружение конфиденциальной информации на узле, Подключен/отключен съемный машинный носитель информации, Копирование файла на съемный машинный носитель информации, Создание файла на съемном машинном носителе информации, Обнаружение утечки информации через печать, Печать/запрет печати файла |

| № | Наименование ИС (ОЗ) | Базовый перечень типов регистрируемых событий |
|---|---|---|
| **12** | **ИС ERP** | Общие события системы (внутренний аудит):<br>• Создание, удаление, изменение пользователя, блокировка/ разблокировка пользователя, изменение пароля пользователя,.<br>• Создание, удаление, изменение группы пользователей, блокировка/разблокировка группы пользователей,<br>• Добавление/ удаление пользователя в группу<br>• Изменение привилегий пользователя/группы пользователей<br>• Вход в систему, выход из системы, неуспешный вход в систему<br>• Успешный переход из УЗ в УЗ/Неуспешный переход из УЗ в УЗ<br>• Попытка аутентификации под несуществующей учетной записью<br>• Запуск, остановка, изменение параметров логирования<br>• Чтение, очистка, изменение журналов событий (логов)<br>• Изменение конфигурации источника<br>• События с уровнем Ошибка/Предупреждение/Тревога<br>• Выключение/перезапуск источника<br><br>Функциональные события от **веб-сервера**:<br>Предоставлен/заблокирован доступ к ресурсу на узле, Ошибка доступа к ресурсу на узле, Некорректный сертификат, 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» |

| № | Наименование ИС (ОЗ) | Базовый перечень типов регистрируемых событий |
|---|---|---|
| **13** | **ИС Клиентские АРМ** | • Создание, удаление, изменение пользователя<br>• блокировка/разблокировка пользователя, изменение пароля пользователя,.<br>• Создание, удаление, изменение группы пользователей<br>• блокировка/разблокировка группы пользователей,<br>• Добавление/ удаление пользователя в группу<br>• Изменение привилегий пользователя/группы пользователей<br>• Вход в систему, выход из системы, неуспешный вход в систему<br>• Успешный переход из УЗ в УЗ/Неуспешный переход из УЗ в УЗ<br>• Попытка аутентификации под несуществующей учетной записью<br>• Запуск, остановка, изменение параметров логирования<br>• Чтение, очистка, изменение журналов событий (логов)<br>• Изменение конфигурации источника<br>• События с уровнем Ошибка/Предупреждение/Тревога<br>• Выключение/перезапуск источника<br>• Загрузка пройдена успешно<br>• Ошибка при прохождении загрузки<br>• Отказ в загрузке<br>• Изменение сетевой или аппаратной адресации<br>• Установка/удаление ПО/службы<br>• Запуск/останов служб<br>• Запуск (завершение) программ и процессов (заданий, задач)<br>• Аварийное завершение программ и процессов<br>• Запрет запуска программы<br>• Запрет загрузки библиотеки<br>• Системное время установлено/изменено<br>• Процесс создал/закрыл/получил доступ к сокету<br>• Syscall |
| **14** | **ИС Система электронного документооборота** | Общие события системы (внутренний аудит):<br>• Создание, удаление, изменение пользователя, блокировка/разблокировка пользователя, изменение пароля пользователя,.<br>• Создание, удаление, изменение группы пользователей, блокировка/разблокировка группы пользователей,<br>• Добавление/ удаление пользователя в группу<br>• Изменение привилегий пользователя/группы пользователей<br>• Вход в систему, выход из системы, неуспешный вход в систему<br>• Успешный переход из УЗ в УЗ/Неуспешный переход из УЗ в УЗ<br>• Попытка аутентификации под несуществующей учетной записью<br>• Запуск, остановка, изменение параметров логирования<br>• Чтение, очистка, изменение журналов событий (логов)<br>• Изменение конфигурации источника<br>• События с уровнем Ошибка/Предупреждение/Тревога<br>• Выключение/перезапуск источника<br><br>Доступ УЗ/групп к объектам доступа. События CRUD документов/ПЗ/отчетов, отправка/отзыв согласования. |

| № | Наименование ИС (ОЗ) | Базовый перечень типов регистрируемых событий |
|---|---|---|
| **15** | **Система контроля и управления доступом (СКУД)** | Общие события системы (внутренний аудит):<br>• Создание, удаление, изменение пользователя, блокировка/разблокировка пользователя, изменение пароля пользователя,.<br>• Создание, удаление, изменение группы пользователей, блокировка/разблокировка группы пользователей,<br>• Добавление/ удаление пользователя в группу<br>• Изменение привилегий пользователя/группы пользователей<br>• Вход в систему, выход из системы, неуспешный вход в систему<br>• Успешный переход из УЗ в УЗ/Неуспешный переход из УЗ в УЗ<br>• Попытка аутентификации под несуществующей учетной записью<br>• Запуск, остановка, изменение параметров логирования<br>• Чтение, очистка, изменение журналов событий (логов)<br>• Изменение конфигурации источника<br>• События с уровнем Ошибка/Предупреждение/Тревога<br>• Выключение/перезапуск источника<br><br>Функциональные события **СКУД**: выдачи/отзывы карт для субъектов, добавление/изменение/удаление объектов доступа, настройка правил доступа, тревоги, предъявление карты, открытие/закрытие дверей/ворот/турникетов, запирание/отпирание дверей/ворот/турникетов. Постановка/снятие зон с охраны, вход/выход сотрудника в зону, нарушение правил нахождение в зоне.<br><br>События от **СУБД**: Создание/удаление БД, Подключение/отключение к БД, Запуск/остановка сервиса, Создание/изменение/удаление схемы/таблицы/табличного пространства/представлениея/тригера/процедуры, Создание/изменение/удаление кластера БД, Обработка CRUD запросов к БД, Импорт/экспорт БД |