



КОД
безопасности

Программный комплекс

Континент-СОА

Версия 4

Руководство администратора
Мониторинг и аудит



© Компания "Код Безопасности", 2021. Все права защищены.

Все авторские права на эксплуатационную документацию защищены.

Этот документ входит в комплект поставки изделия. На него распространяются все условия лицензионного соглашения. Без специального письменного разрешения компании "Код Безопасности" этот документ или его часть в печатном или электронном виде не могут быть подвергнуты копированию и передаче третьим лицам с коммерческой целью.

Информация, содержащаяся в этом документе, может быть изменена разработчиком без специального уведомления, что не является нарушением обязательств по отношению к пользователю со стороны компании "Код Безопасности".

Почтовый адрес: **115127, Россия, Москва, а/я 66**
ООО "Код Безопасности"

Телефон: **8 495 982-30-20**

E-mail: **info@securitycode.ru**

Web: **<https://www.securitycode.ru>**

Оглавление

Список сокращений	5
Введение	6
Общие сведения	7
Назначение и основные функции	7
Принципы функционирования	7
Объекты мониторинга	7
Типы и источники отображаемой информации	7
Правила и шаблоны	8
Статусы объектов	8
Запуск Менеджера конфигурации	9
Настройка подключения к системе	11
Настройка с помощью алгоритма ГОСТ Р 34.11-2012	11
Настройка с помощью RSA	12
Мониторинг	17
Вход в систему мониторинга и аудита	17
Главное окно	17
Раздел "Структура"	20
Настройка правил мониторинга	21
Узел безопасности	24
Группа узлов безопасности	29
Кластер	31
Раздел "Панель мониторинга"	33
Табличный виджет	34
Графический виджет	34
Структурный виджет	35
Настройка панели мониторинга	36
Раздел "Статистика"	39
Управление виджетами	39
Просмотр отчетов	40
Подготовка отчета к печати	41
Режимы мониторинга	42
Раздел "Настройки"	42
Аудит	43
Параметры журналирования	43
Уровень детализации журналов	44
Настройка хранения журналов на внешнем syslog-сервере	44
Настройка автоматической очистки журналов	46
Хранение журналов во внешней базе данных	47
Просмотр журналов с помощью веб-интерфейса	48
Системный журнал	50
Журнал сетевой безопасности	50
Журнал управления	53
Очистка журналов	53
Просмотр журналов с помощью локального меню	54
Системный журнал	55
Журнал сетевой безопасности	58
Журнал управления	61
Экспорт журналов	64
Очистка журналов	65
Передача сведений в ГосСОПКА	66
Настройка параметров клиента ГосСОПКА	66
Отправка сведений	66
Приложение	68
Установка CRL-сертификата	68

Документация 70

Список сокращений

БД	База данных
БРП	База решающих правил
ЛМ	Локальное меню
МК	Менеджер конфигурации
МЭ	Межсетевой экран
НСД	Несанкционированный доступ
ОЗУ	Оперативное запоминающее устройство
ПО	Программное обеспечение
ПК	Программный комплекс
СБ	Сетевая безопасность
СОВ	Система обнаружения вторжений (компьютерных атак)
УБ	Узел безопасности
ЦП	Центральный процессор
ЦУС	Центр управления сетью
CRL	Список отозванных сертификатов
RDP	Протокол удаленного рабочего стола
SWAP	Swapping — специальный раздел на диске, виртуальная память

Введение

Документ предназначен для администраторов изделия "Программный комплекс "Континент-СОА". Версия 4" RU.АМБС.58.29.12.008 (далее — комплекс "Континент", комплекс). В нем содержатся сведения, необходимые администраторам для управления системой мониторинга и аудита.

Приступая к изучению данного руководства, следует предварительно ознакомиться с [1] и [2].

Сайт в интернете. Информация о продуктах компании "Код Безопасности" представлена на сайте <https://www.securitycode.ru/>.

Служба технической поддержки. Связаться со службой технической поддержки можно по телефону 8 800 505-30-20 или по электронной почте support@securitycode.ru.

Учебные курсы. Освоить аппаратные и программные продукты компании "Код Безопасности" можно в авторизованных учебных центрах. Перечень учебных центров и условия обучения представлены на сайте компании <https://www.securitycode.ru/company/education/training-courses/>. Связаться с представителем компании по вопросам организации обучения можно по электронной почте education@securitycode.ru.

Глава 1

Общие сведения

Назначение и основные функции

Система мониторинга и аудита комплекса "Континент" (далее — система) представляет собой программное обеспечение, позволяющее проводить мониторинг различных параметров узлов безопасности, входящих в состав комплекса. Система выполняет следующие функции:

- регистрация и аудит событий безопасности, управления и системных событий;
- централизованный мониторинг состояния узлов безопасности.

Сведения о событиях, связанных с работой УБ, регистрируются в журналах на узлах безопасности, а затем передаются в ЦУС. В комплексе используются три типа журналов — системный, сетевой безопасности, управления (администрирования). В каждом журнале реализован механизм поиска и фильтрации сообщений. В системном журнале регистрируются события подсистем, в журнале сетевой безопасности — события СОВ, межсетевое экранирование и НСД, в журнале администрирования — действия администраторов и пользователей.

Аудит проводится администратором аудита. В задачи аудита входят:

- регулярный просмотр содержимого журналов;
- настройка параметров хранения журналов;
- управление содержимым журналов (записями о событиях).

Принципы функционирования

Объекты мониторинга

Объектами мониторинга комплекса "Континент" являются:

- кластер безопасности;
- узлы безопасности;
- группы узлов безопасности.

Изначально все узлы безопасности в системе отображаются как члены группы "Несортированное", входящей в корневую группу домена.

Примечание. Корневая группа домена содержит в себе все УБ и группы. Для нее доступно создание шаблонов, которые действуют на все УБ и группы в структуре. Корневая группа содержит набор правил мониторинга по умолчанию. При желании этот набор можно изменить (см. стр.21).

Пользователь, имеющий права доступа к странице "Управление группами", может создавать новые группы, помещать в них УБ из группы "Несортированное" и перемещать УБ между группами.

Типы и источники отображаемой информации

В системе мониторинга и аудита используются следующие типы информации:

- события;
- данные;
- состояние.

Тип и источник информации — это параметры, используемые для отображения сведений о состоянии объектов мониторинга в системе.

Источники для каждого из типов информации приведены в таблице ниже:

Тип информации	Источник
События	Система управления Система мониторинга и аудита Контроль целостности Контроль доступа Контроль приложений Межсетевой экран Прикладная фильтрация Защищенные коммуникации Система обнаружения вторжений Удаленный доступ Базовая платформа VPN
Данные	Сетевые интерфейсы Система мониторинга и аудита Срабатывание сигнатур
Состояние	Система мониторинга и аудита

Правила и шаблоны

Для отображения сведений о состоянии объекта в системе необходимо сформировать правило мониторинга для объекта.

В системе используются четыре типа правил мониторинга:

- правило кластера — распространяется на УБ, входящие в состав кластера;
- правило узла безопасности — распространяется на соответствующий УБ;
- групповое — распространяется на все УБ, входящие в группу и ее подгруппы любого уровня вложенности;
- общее — распространяется на все УБ и группы УБ.

Шаблон — это правило или группа правил, применяемых к УБ, группам УБ и задающих срабатывание датчиков событий в системе.

Приоритет срабатывания зависит от типа правила. Наивысшим приоритетом обладает правило кластера, затем следует правило УБ и групповое правило. Общее правило имеет наименьший приоритет.

Статусы объектов

При отображении объекта в системе указывается его статус. Статус может иметь одно из значений, перечисленных в таблице ниже:

Статус	Описание
Критический (Critical)	Статус присваивается объекту при наступлении события критического уровня. Для изменения статуса требуется присвоить событию статус "Закрывать", т. е. изменить состояние параметра, сгенерировавшего событие, в соответствии с политикой безопасности
Предупреждение (Warning)	Статус присваивается при наступлении события, имеющего соответствующий уровень опасности. Объект остается в этом статусе до тех пор, пока событию не будет присвоен статус "Закрывать" или статус объекта не изменится на "Критический"
Информация (Info)	Статус присваивается при наступлении события информационного уровня. Статус сохраняется до изменения состояния параметра

Примечание. Уровень критичности события определяется правилом мониторинга, создавшего это событие (см. стр. 21).

Для визуализации статуса объекта используются следующие цвета:

- красный — критический;
- оранжевый — предупреждение;
- синий — информация;
- зеленый — отсутствие событий, имеющих перечисленные выше статусы.

Запуск Менеджера конфигурации

Для запуска Менеджера конфигурации:

- активируйте в главном меню ОС Windows команду "Код Безопасности" | "Менеджер конфигурации" или на рабочем столе ОС Windows ярлык приложения "Менеджер конфигурации".

На экране появится окно "Менеджер конфигурации".

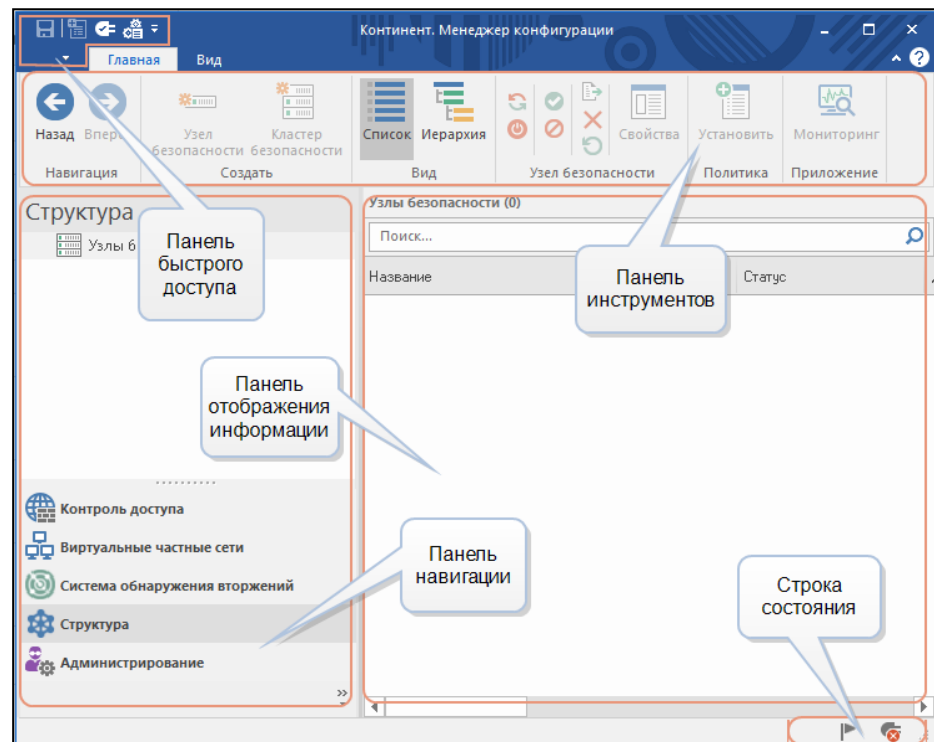





Рис.1 Окно "Менеджер конфигурации"

Окно "Менеджер конфигурации" содержит следующие основные элементы интерфейса:

Элемент интерфейса	Описание
Панель инструментов	<p>Содержит набор инструментов и две вкладки:</p> <ul style="list-style-type: none"> • "Главная" — отображает панель инструментов; • "Вид" — настраивает отображения элементов окна Менеджера конфигурации. <p>Инструменты — это функциональные кнопки, предназначенные для запуска часто используемых команд. Состав кнопок зависит от выбора подраздела на панели навигации, а их доступность определяется текущей ситуацией. При наведении курсора мыши на кнопку появляется всплывающая подсказка с дополнительной информацией</p>
Панель быстрого доступа	<p>Предназначена для быстрого доступа к часто используемым командам. Содержит настраиваемые кнопки:</p> <ul style="list-style-type: none"> •  — сохранение текущей конфигурации; •  — установка политики безопасности; •  — настройка подключений к ЦУС и панели быстрого доступа; •  — установка соединения с ЦУС; •  — настройка панели быстрого доступа; •  — вызов меню команд быстрого доступа
Панель навигации	<p>Содержит следующие разделы:</p> <ul style="list-style-type: none"> • "Контроль доступа" — предназначен для управления правилами фильтрации и трансляции трафика; • "Виртуальные частные сети" — предназначен для создания и настройки VPN, организации удаленного доступа; • "Система обнаружения вторжений" — предназначен для настройки параметров системы обнаружения и предупреждения вторжений; • "Структура" — предназначен для управления параметрами УБ комплекса; • "Администрирование" — предназначен для управления сервисными функциями (работа с сертификатами, резервными копиями, управление лицензиями, обновлением и др.)
Панель отображения информации	<p>Предназначена для отображения информации выбранного раздела панели навигации</p>
Строка состояния	<p>Содержит следующие данные:</p> <ul style="list-style-type: none"> • число выполняемых задач и кнопка вызова центра уведомлений , содержащего информацию о выполняемых задачах и ссылку на переход к общему списку задач; • пиктограмма состояния соединения с ЦУС (при установленном соединении — с именем учетной записи авторизованного администратора, к примеру )

Глава 2

Настройка подключения к системе

Перед началом работы с системой необходимо настроить безопасную передачу данных между МК и ЦУС. Защищенное соединение при подключении к системе осуществляется с помощью следующих алгоритмов шифрования:

- ГОСТ Р 34.11-2012.
Требует установки дополнительного ПО СКЗИ "Континент TLS VPN Клиент" 1.2 (далее — TLS-клиент).
- Комплект алгоритмов на основе RSA (далее — RSA).

Настройка с помощью алгоритма ГОСТ Р 34.11-2012

Для настройки подключения системы с помощью TLS-клиента выполните следующие процедуры:

- Экспорт и установка сертификатов безопасности и CRL (см. ниже).
- Установка TLS-клиента и настройка в соответствии с документом [3].

Внимание! При установке TLS-клиента учтите следующие особенности:

- В случае использования СКЗИ "Континент TLS VPN Клиент" 1.2 при создании нового подключения в конфигураторе укажите его по имени сертификата сервера, используемого при настройке ЦУС (далее — "адрес_мониторинга").
- Для соответствия имени сертификата сервера IP-адресу ЦУС требуется настроить DNS-сервер или дополнить файл hosts.

- Настройка конфигурационного файла МК (см. стр. 11).

В ходе процедуры выполняется запуск приложения по защищенному соединению при нажатии кнопки "Мониторинг" на панели инструментов.

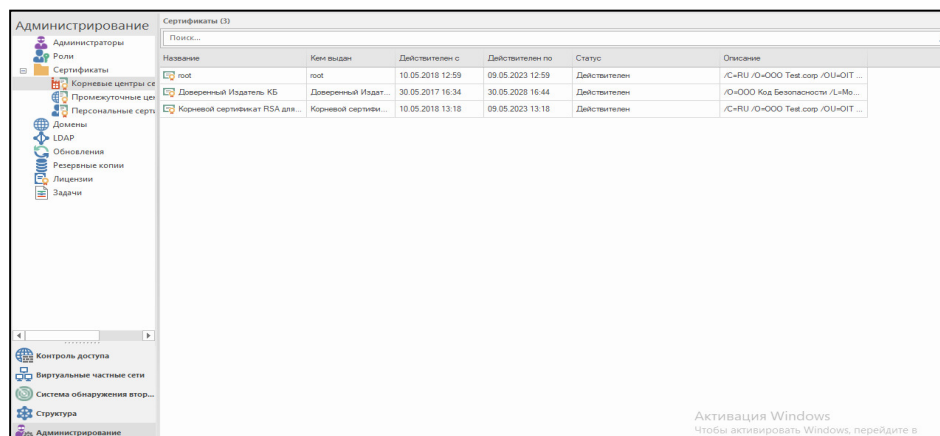
- Запуск системы (см. стр. 17).

Примечание. При ошибке подключения TLS-клиента настройте в ЦУС дополнительный сетевой интерфейс. В настройках профиля соединений TLS-клиента введите в поле "Адрес получения CRL" IP-адрес сетевого интерфейса. Например: http://192.168.80.70/cdc.crl

Для экспорта и установки сертификата и CRL:

1. Откройте МК и перейдите в раздел "Администрирование" (см. стр. 9).
2. В списке сертификатов выберите "Корневые центры сертификации".

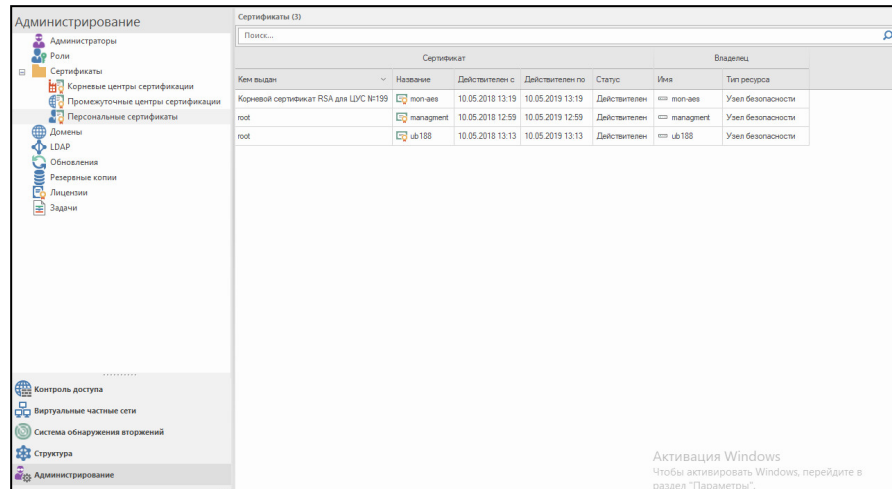
В правой части экрана появится список установленных корневых сертификатов.



3. Вызовите контекстное меню действующего корневого сертификата и выберите команду "Экспортировать".

На экране появится стандартное окно сохранения файла сертификата.

4. Выберите место для сохранения файла, укажите имя и тип файла и нажмите кнопку "Сохранить".
5. Выберите на панели навигации подраздел "Персональные сертификаты".
В правой части экрана появится список установленных персональных сертификатов.



6. Вызовите контекстное меню действующего сертификата ЦУС и выберите команду "Экспортировать".
На экране появится стандартное окно сохранения файла сертификата.
7. Выберите место для сохранения файла, укажите имя и тип файла и нажмите кнопку "Сохранить".
8. Откройте окно браузера и скачайте CRL-файл по адресу "http://адрес_мониторинга/cdc.crl". Если страница не откроется, замените "адрес_мониторинга" на основной или дополнительный IP-адрес ЦУС.

Примечание. Если скачивание CRL-файла средствами браузера не выполняется, то в локальном меню ЦУС перейдите в раздел "Сертификаты | Отозванные сертификаты | Экспортировать список отозванных сертификатов" и укажите корневой сертификат, выбранный в п.3.

9. Установите CRL-файл в хранилище сертификатов Windows, расположенное на локальном компьютере (см. стр.68).

Внимание! Срок действия CRL-файла — 1 месяц.

10. Выполните установку TLS-клиента и его настройку в соответствии с документом [3].

Для настройки конфигурационного файла Менеджера конфигурации:

1. С помощью приложения "Проводник" Windows откройте содержимое папки "C:\Users\%username%\AppData\Local\Continent\CCM", где %username% — папка учетной записи пользователя.
2. Откройте файл "CCM.config" с помощью приложения "Блокнот".
3. Найдите в начальной части файла строку (для поиска целесообразно использовать сочетание клавиш <Ctrl> + <F>) и впишите адрес_мониторинга:
monitoring_url="адрес_мониторинга"
4. В меню "Файл" приложения "Блокнот" выберите команды "Сохранить" и "Выход".

Настройка с помощью RSA

Для настройки подключения системы выполните следующие процедуры:

- Выпуск сертификатов веб-сервера мониторинга с помощью локального меню (см. стр.13) или с помощью МК (см. стр.14).

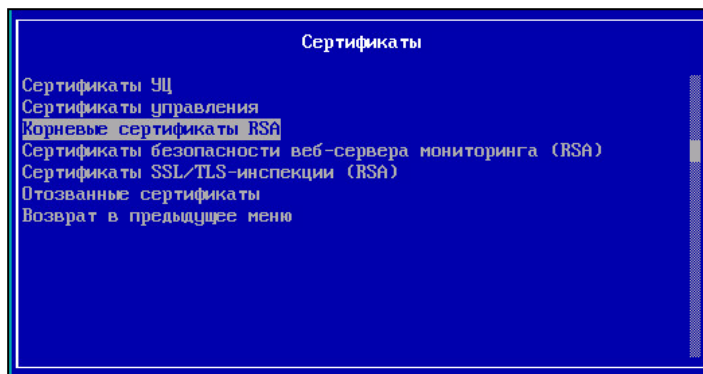
- Настройка конфигурационного файла МК (см. стр.12).
- Запуск системы (см. стр.17).

Внимание! Подключение системы с помощью RSA не защищено от доступа стороннего пользователя с правами доступа к рабочему месту по протоколу RDP.

Для выпуска сертификатов веб-сервера мониторинга с помощью локального меню:

1. В главном меню локального управления ЦУС выберите пункт "Сертификаты" и нажмите клавишу <Enter>.

На экране появится окно "Сертификаты".



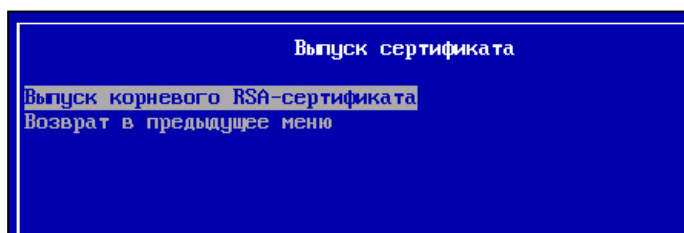
2. Выберите в меню "Сертификаты" пункт "Корневые сертификаты RSA" и нажмите клавишу <Enter>.

На экране появится окно "Корневые сертификаты RSA".

Корневые сертификаты RSA		
Кому выдан	Кем выдан	Тип
CA RSA	/C=RU/O=org/OU=dep/CN=CA RSA/role=carsa	carsa

3. Для создания корневого сертификата нажмите клавишу <F2>.

На экране появится окно "Выпуск сертификата".



4. Выберите пункт "Выпуск корневого RSA-сертификата" и нажмите клавишу <Enter>.

На экране появится окно "Сертификат".

Сертификат	
Страна	RU
Организация	
Отдел	
Название	Корневой сертификат RSA для ЦУС №199

5. Заполните поля "Организация", "Отдел" и "Название" и нажмите клавишу <Enter>.

Примечание. Для перемещения используйте стандартные клавиши: <↑>, <↓>, <Page Down>, <Page Up>, <Home>.

На экране появится сообщение об успешном завершении операции.

6. Нажмите клавишу <Enter>.

Осуществится возврат в окно "Выпуск сертификата".

7. Выполните возврат в меню "Сертификаты", выберите пункт "Сертификаты безопасности веб-сервера мониторинга (RSA)" и нажмите клавишу <Enter>. На экране появится окно "Сертификаты безопасности веб-сервера мониторинга (RSA)".

Сертификаты безопасности веб-сервера мониторинга (RSA)			
Кому выдан	Кем выдан	Тип	Действителен с
mon-aes	/C=RU/O=org/OU=dep/CN=CA RSA/role=carsa	monit	2017-09-08 12:41

8. Повторите пп. 3-5.

Внимание! Название RSA-сертификата для веб-сервера используется как "адрес_мониторинга". При этом требуется соответствующим образом настроить DNS-сервер или дополнить файл hosts на PM администратора.

На экране появится окно выбора корневого сертификата.

9. Выберите корневой сертификат и нажмите клавишу <Enter>. Осуществится выпуск сертификата управления и на экране появится сообщение об успешном завершении операции.
10. Нажмите клавишу <Enter>. На экране появится сообщение с URL-адресом, содержащим доменное имя веб-сервера системы для RSA-доступа.

URL Мониторинга для RSA-доступа: <https://mon-aes>
Нажмите Enter

11. Нажмите клавишу <Enter>. Осуществится возврат в окно "Выпуск сертификата".
12. Для применения сертификатов перейдите в меню настроек, выберите пункт "Применить локальную политику" и нажмите клавишу <Enter>. Дождитесь успешного завершения операции и появления соответствующего сообщения.
13. Нажмите клавишу <Enter>, выберите пункт "Возврат в главное меню".
14. Нажмите клавишу <Enter> и перейдите в меню "Инструменты".
15. Выберите пункт "Подтверждение изменений настроек УБ". Нажмите клавишу <Enter>. На экране появится окно "Неподтвержденные конфигурации".

Неподтвержденные конфигурации
[] Локальные изменения с node_11(11) (код 23)

16. Установите отметку клавишей <Пробел> и нажмите клавишу <Enter>. На экране появится сообщение о подтверждении конфигурации.

Подтверждено конфигураций :1
Нажмите Enter

17. Для возврата в меню "Инструменты" нажмите клавишу <Enter>.

Для выпуска сертификатов веб-сервера мониторинга с помощью МК:

1. В МК на панели навигации перейдите в раздел "Администрирование | Сертификаты".
2. На панели инструментов нажмите кнопку "Корневой сертификат".

Откроется окно "Корневой сертификат".

3. В появившемся окне заполните обязательные поля, выберите алгоритм подписи RSA (2048) и нажмите кнопку "Создать сертификат".

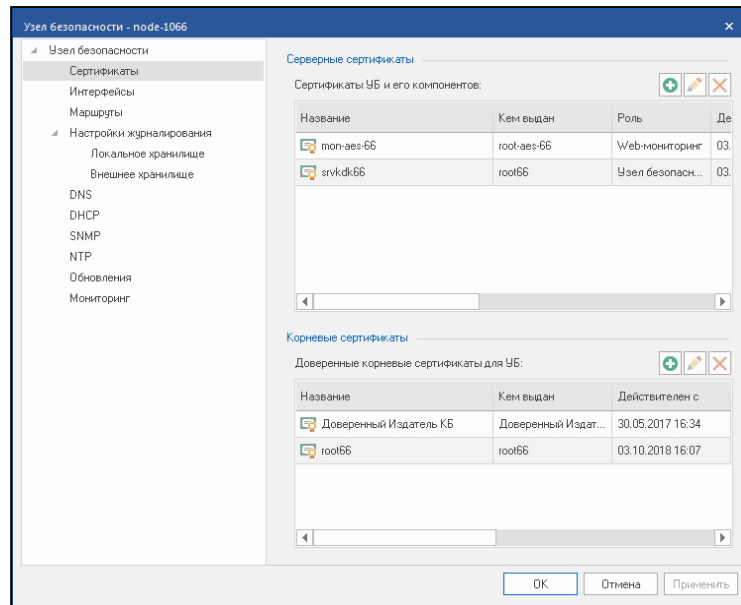
Примечание. Для избежания путаницы с сертификатами присваивайте корневым и серверным сертификатам легко идентифицируемые имена.


4. На панели навигации в раскрывающемся списке "Сертификаты" выберите пункт "Персональные сертификаты".
5. На панели инструментов нажмите кнопку "Сертификат".

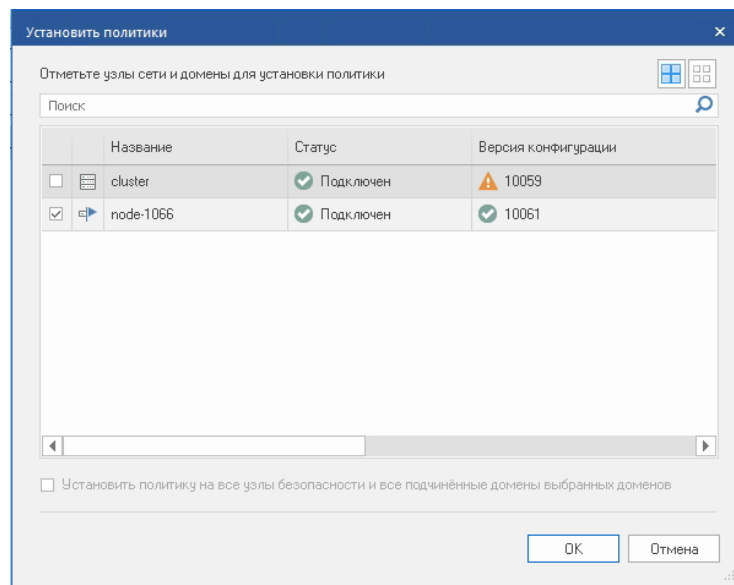
Откроется окно "Сертификат".

6. В появившемся окне выберите тип сертификата "Web-мониторинг", заполните обязательные поля и выберите корневой сертификат, созданный в п. 3.
7. На панели навигации перейдите в раздел "Структура".
8. На панели отображения информации выберите компонент ЦУС. На панели инструментов нажмите кнопку "Свойства".

Откроется окно "Узел безопасности".



9. В меню перейдите в "Узел безопасности | Сертификаты".
10. Добавьте серверный сертификат с помощью кнопки .
11. Нажмите кнопку "ОК".
12. На панели инструментов нажмите кнопку "Установить".
Откроется окно "Установить политики".



13. Отметьте узел безопасности ЦУС и нажмите кнопку "ОК". Изменения будут отправлены в ЦУС.

Важно! Для успешного подключения установите соответствие IP-адреса сетевого имени.

Глава 3

Мониторинг

Для настройки мониторинга необходимо выполнить следующие процедуры:

1. Вход в систему (см. ниже).
2. Настройка узлов безопасности, групп узлов безопасности и правил мониторинга в разделе "Структура" (см. стр.20).
3. Настройка информационной панели в разделе "Панель мониторинга" (см. стр.33).
4. Формирование отчета о работе системы в разделе "Статистика" (см. стр.39).
5. Настройка отправки почтовых уведомлений в разделе "Настройки" (см. стр.42).

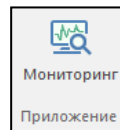
Вход в систему мониторинга и аудита

Вход в систему выполняется в Менеджере конфигурации или из интернет-браузера по ссылке https://адрес_сервера.

Внимание! Система корректно работает только при обращении по протоколу https.

Для входа в систему:

1. Откройте Менеджер конфигурации, перейдите в раздел "Структура" и в панели инструментов нажмите кнопку "Мониторинг".



На экране появится окно ввода имени и пароля администратора.

2. Введите имя и пароль администратора и нажмите кнопку "OK".
На экране появится главное окно системы.

Примечание. Для входа в систему по имени серверного сертификата настройте DNS-сервер.

Главное окно

Основные элементы главного окна системы:

1. Панель навигации.
2. Счетчики событий.
3. Кнопки вызова настроек сессии и сброса счетчиков.
4. Рабочая область.

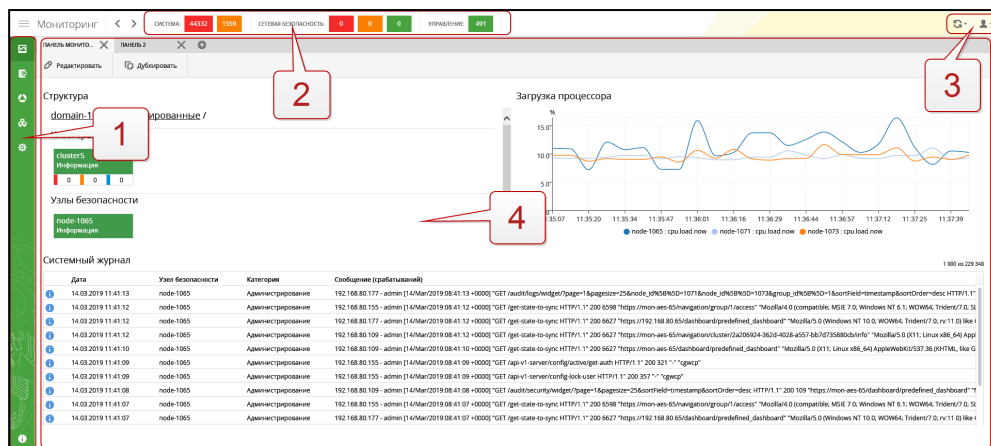


Рис.2 Главное окно системы

Панель навигации служит для перехода между разделами системы. Краткое описание разделов приводится в таблице ниже:

Раздел	Описание
Панель мониторинга (см. стр.33)	Набор настраиваемых виджетов для отображения информации о состоянии объектов мониторинга
Журналы (см.стр.48)	Просмотр сообщений журналов системы, собранных со всех УБ контролируемого домена
Статистика (см.стр.39)	Формирование и просмотр настраиваемых отчетов, предоставляющих в визуальной форме статистическую информацию за определенный период времени
Структура (см.стр.20)	Настройка шаблонов групп и узлов безопасности. Управление доступом администраторов комплекса к мониторингу его узлов безопасности. Просмотр активных событий на узлах безопасности. Просмотр сведений о состоянии программных и аппаратных компонентов и сетевых интерфейсов узлов. Просмотр сведений о лицах, ответственных за эксплуатацию групп и узлов безопасности
Настройки (см. стр.42)	Настройка сервера исходящих почтовых сообщений

Счетчик событий показывает количество событий, зарегистрированных на данный момент времени. В случае обнуления счетчиков верхняя панель будет отображать события, произошедшие с момента обнуления по настоящее время.

Примечание. Отображаются данные счетчиков только тех УБ, к которым у текущего пользователя системы имеется доступ.





- Левая часть — системные события. При нажатии на одну из плиток откроется системный журнал с установленным фильтром на события соответствующей важности.

Примечание. Плитка красного цвета отображает количество событий критической важности, оранжевого — событий-предупреждений.


- Средняя часть — события сетевой безопасности. При нажатии на одну из плиток откроется журнал сетевой безопасности с установленным фильтром на сообщения соответствующей важности.

Примечание. Плитка красного цвета отображает количество событий высокой важности, оранжевого — средней важности, зеленого — низкой важности.

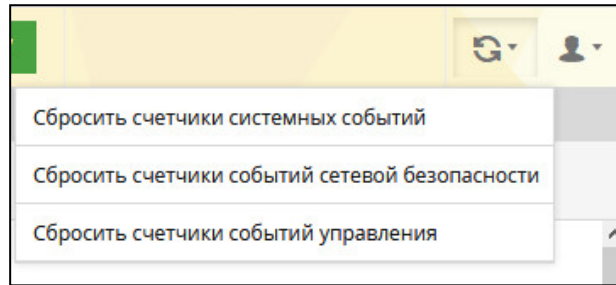
- Правая часть — события управления. При нажатии на плитку откроется журнал управления с установленным фильтром "Информация".


Кнопки сброса счетчиков  и вызова настроек параметров сессии  расположены в области (3).

Для сброса счетчиков:


1. Нажмите кнопку .

На экране появится следующее меню:

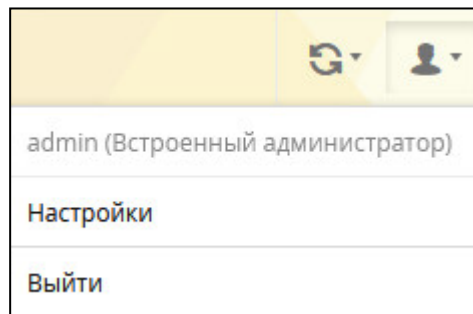


2. Выберите пункт меню.
3. Для закрытия меню нажмите кнопку .

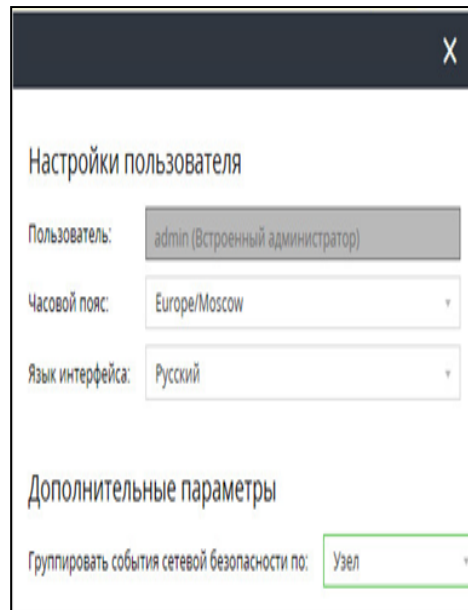
Для настройки параметров:

1. Нажмите кнопку .

На экране появится следующее окно:



2. Выберите пункт "Настройки".
На экране появится окно "Настройки пользователя".



3. В области "Настройки пользователя" выберите часовой пояс и язык интерфейса.

Примечание. В предлагаемом списке часовых поясов города России находятся в подкаталогах Asia и Europe. Также можно воспользоваться подкаталогом Etc с выбором часового пояса.

4. В поле "Группировать события сетевой безопасности по" выберите критерий группировки для счетчика событий.

Примечание. По умолчанию группировка событий безопасности выполняется по идентификатору сигнатуры.

5. Нажмите кнопку "Сохранить" в нижней части экрана.

Раздел "Структура"

Раздел предназначен для просмотра сведений о состоянии объектов мониторинга и настройки шаблонов.

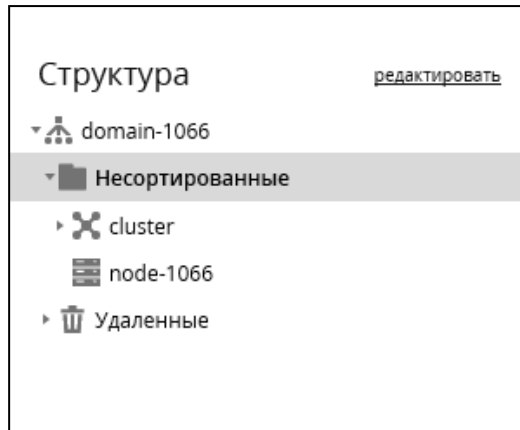
Поиск по структуре		шаблон	доступ
Поиск...		Редактировать	
Структура свернуть/развернуть			
<ul style="list-style-type: none"> domain-1065 <ul style="list-style-type: none"> Несортированные Удаленные 			
Свои правила			
Имя	Условие	Состояние	Причина
SMART ошибки SDA: критично	Для sda Если <code>filesystem.storage_devices.sda.smart.failures.count.critical > 0</code>	критический	Узел безопасности %host%. Кри
SMART ошибки SDA: предупреждение	Для sda Если <code>filesystem.storage_devices.sda.smart.failures.count.casual > 0</code>	предупреждение	Узел безопасности %host%. Сбо
SMART ошибки SDB: критично	Для sdb Если <code>filesystem.storage_devices.sdb.smart.failures.count.critical > 0</code>	критический	Узел безопасности %host%. Кри
SMART ошибки SDB: предупреждение	Для sdb Если <code>filesystem.storage_devices.sdb.smart.failures.count.casual > 0</code>	предупреждение	Узел безопасности %host%. Сбо

Для навигации используется дерево объектов, расположенное слева на рабочей области. В состав дерева объектов входят следующие элементы:

- кластер;
- узлы безопасности;
- группы узлов безопасности;
- домен.

Примечание. По умолчанию раздел "Структура" состоит из двух групп: "Несортированные", включающая все зарегистрированные УБ, и "Удаленные", включающая все УБ, удаленные посредством Менеджера конфигурации.

Для перехода на страницу настройки элемента выберите его в дереве объектов.



Примечание. Корневая группа домена содержит в себе все УБ и группы. Для нее доступно создание шаблонов, которые действуют на все УБ и группы в структуре. Корневая группа содержит набор правил по умолчанию.

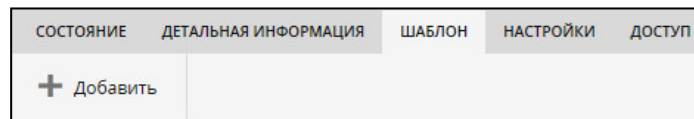
Настройка правил мониторинга

Настройка заключается в создании, редактировании и удалении правил.

Внимание! Перед выполнением операций нажмите кнопку "редактировать".

Для создания правила:

1. Выберите в дереве объектов группу или УБ.
В окне отобразится страница с параметрами выбранного объекта.
2. Выберите вкладку "Шаблон".



3. Для создания правила нажмите кнопку "Добавить".
На экране появится окно "Новое правило".

Правило - Новое правило

Имя:

Если: **Условие 1**

=

[добавить еще одно условие](#)

То:

Отправить письмо

Для:

Причина:

4. Укажите имя правила и условие его применения. Для этого:

- В поле "Имя" введите имя правила.

Примечание. Допускается использование следующих символов:

- прописные и строчные буквы латинского алфавита A–Z, a–z;
- прописные и строчные буквы кириллицы А–Я, а–я;
- цифры 0–9;
- символы:

() [] _ - * ? ! %

- В группе полей "Если" укажите параметр системы, логическое условие и порог срабатывания.

Примечание. Для ввода параметра системы используйте нижние поля группы для выбора элементов из раскрывающегося списка.

- Условий срабатывания правила может быть несколько. Для добавления дополнительного условия нажмите кнопку "Добавить".

Примечание. При добавлении еще одного условия появится новое поле "Условие". В раскрывающемся списке выберите вариант срабатывания правила — при выполнении всех или одного из условий.



5. Укажите значения параметров:

Параметр	Описание
То	Действие, выполняемое при срабатывании правила. Настраивается критичность события, генерируемого срабатыванием правила, а также рассылка оповещений
Для	Подсистема, на которую распространяется действие правила

Параметр	Описание
Причина	Сообщение, описывающее событие. Для более точной формулировки сообщения допускается использование макросов. Поддерживаются следующие макросы для каждого из условий: <ul style="list-style-type: none"> %host% — УБ, где произошло событие; %value% — текущее значение параметра; %condition% — текстовое значение условия (например, ">" — больше); %threshold% — порог срабатывания. В тексте сообщения допускается использование символов, приведенных в примечании п. 4

6. Нажмите кнопку "Сохранить".

Сохраненное правило появится в списке правил соответствующей группы или УБ.

Имя	Условие	Состояние	Причина	Действия
cpu	Для cpu Если cpu >= 90	● предупреждение	%host%	 

Примечание.

Пример правила мониторинга:

Для условия "Если средняя загрузка ЦП станет равной или превысит 90%, то регистрируется предупреждающее событие" настройка выглядит следующим образом:

Правило - CPU_critical

Имя:

Если: **Условие 1**

добавить еще одно условие

То:

Отправить письмо


Для:

Причина:



Узел %host%. Загрузка процессора %value (cpu.load.avg1)%

Пример сообщения в поле "Причина": "Если средняя загрузка ЦП станет равной или превысит %threshold (cpu/load/avg1)%, то регистрируется предупреждающее событие".

Для редактирования правила:

1. Выберите в дереве объектов группу или УБ.
В окне отобразится страница с параметрами выбранного объекта.
2. Выберите вкладку "Шаблон".
3. Выберите в таблице правило для редактирования и нажмите кнопку , расположенную в столбце "Действия".
4. Выполните пп. 3–6 процедуры, представленной на стр. 21.

Для удаления правила:

1. Выберите в дереве объектов группу или УБ.
В окне отобразится страница с параметрами выбранного объекта.
2. Выберите вкладку "Шаблон".
3. Выберите в таблице правило для редактирования и нажмите кнопку , расположенную в столбце "Действия".
4. Для восстановления правила в шаблоне в столбце "Действия" нажмите .

Для создания общих правил:

Примечание. Общее правило распространяется на все УБ и группы УБ и имеет наименьший приоритет.

1. Перейдите в раздел "Структура" и выделите в дереве объектов верхний уровень иерархии.

На экране появится список общих правил. По умолчанию в системе имеется набор предустановленных общих правил.

Имя	Условие	Состояние	Причина
SMART ошибки SDA: критично	Для sda Если fileSystem.storage_devices.sda.smart.failures.count.critical > 0	критический	Узел безопасности %host%
SMART ошибки SDA: предупреждение	Для sda Если fileSystem.storage_devices.sda.smart.failures.count.casual > 0	предупреждение	Узел безопасности %host%
SMART ошибки SDB: критично	Для sdb Если fileSystem.storage_devices.sdb.smart.failures.count.critical > 0	критический	Узел безопасности %host%
SMART ошибки SDB: предупреждение	Для sdb Если fileSystem.storage_devices.sdb.smart.failures.count.casual > 0	предупреждение	Узел безопасности %host%

2. Для добавления в список нового правила нажмите кнопку "Добавить".

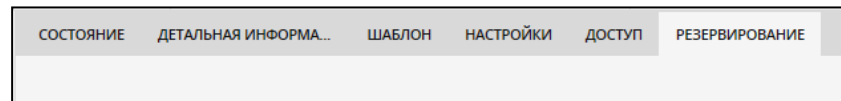
На экране появится окно настройки правила.

3. Выполните настройку правила (см. стр. 21) и сохраните его.

При необходимости добавьте в список новое правило.

Узел безопасности

Страница УБ содержит следующие вкладки:



Состояние

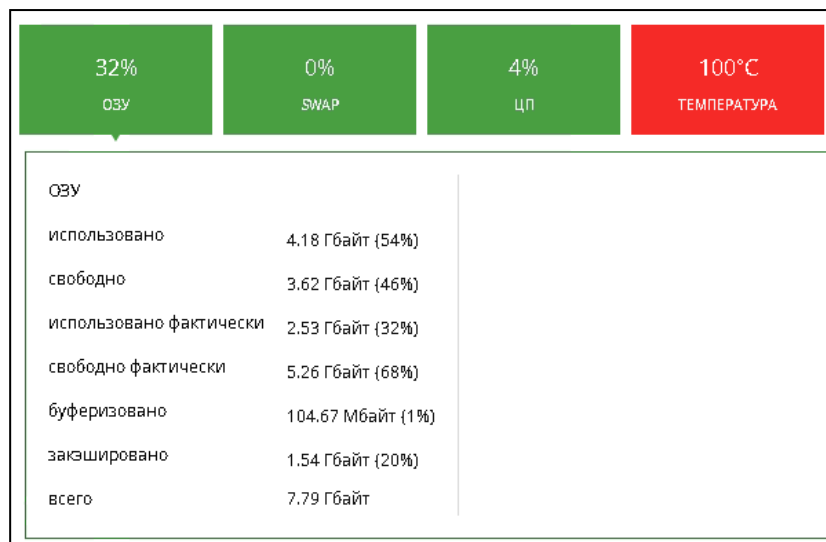
На вкладке в реальном времени отображаются данные, разделенные на следующие группы:

- Активные события — таблица со списком активных событий на УБ с указанием их важности, продолжительности и причины.

Важность	Продолжительность	Причина
критический	20:42:54	Узел безопасности node-1065. Температура процессора 100С

- ЦП и память — сведения о состоянии центрального процессора и оперативной памяти, представленные в виде подгрупп параметров:
 - загрузка ОЗУ;
 - использование SWAP;
 - загрузка ЦП;
 - температура ЦП, материнской платы и дисковой подсистемы.

Для просмотра значений параметров каждой группы выберите соответствующую плитку.

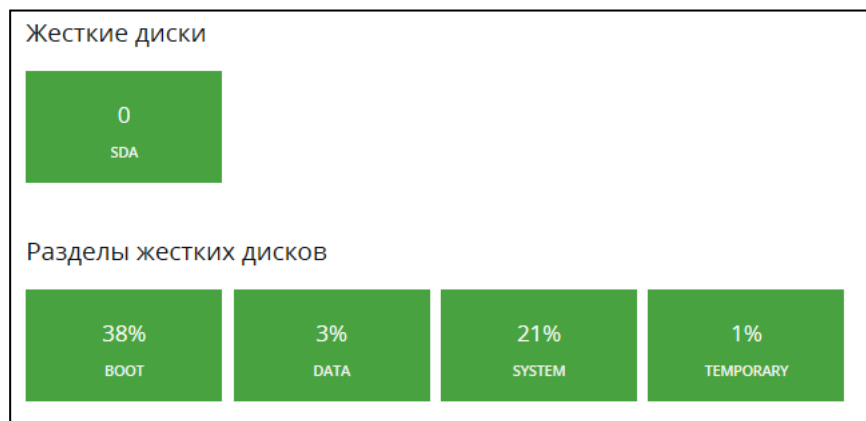


Для редактирования состава группы нажмите вкладку "Настройки" (см. стр.27).

- Подсистемы — сведения о состоянии COB, МЭ, системы журналирования, VPN, кластера.



- Жесткие диски — сведения о жестких дисках и состоянии их разделов.



- Сетевые интерфейсы — информация о статусе и статистике сетевых интерфейсов.

Интерфейс	IP адрес	MAC адрес	Состояние	Трафик		Ошибки		Отброшено	
				Получено	Передано	Вх.	Иск.	Вх.	Иск.
● ge-0-0	192.168.80.67/24 fe80::250:56ff:fe8c:2601/64	00:50:56:8c:26:01	Up	28.23 Мбайт	193.85 Мбайт	0	0	0	0
● ge-1-0	192.168.50.67/24 fe80::250:56ff:fe8c:3f76/64	00:50:56:8c:3f:76	Up	6.02 Мбайт	4.21 Мбайт	0	0	0	0
● ge-2-0	192.168.40.67/24 fe80::250:56ff:fe8c:5cd8/64	00:50:56:8c:5c:d8	Up	4.86 Мбайт	442.66 кбайт	0	0	0	0

- Активные сетевые соединения.

Отправитель			Получатель			Трафик				
Хост	IP адрес	Порт	Хост	IP адрес	Порт	Протокол	Дата начала	Продолжительность	Получено	Передано
node-1071.domain-108067	192.168.80.71	30624	cdc	192.168.80.67	6666	tcp	05.06.2019 15:08:23	00:47:46	7.51 Мбайт	9.85 Мбайт
	fc00:777:b380:e84c::42f	15142		fc00:777:b380:e84c::1a523	6432	tcp	05.06.2019 15:08:30	00:47:39	900.19 Кбайт	2.09 Мбайт
node-1071.domain-108067	192.168.80.71	46760		fc00:777:b380:e84c::1a523	5432	tcp	05.06.2019 15:08:31	00:47:38	1022.06 Кбайт	1.51 Мбайт
	192.168.80.71	60828	cdc	192.168.80.67	8888	tcp	05.06.2019 15:08:00	00:48:09	100.24 Кбайт	42.01 Кбайт

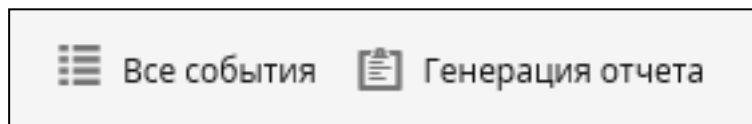
- Активные соединения VPN.

Канал	Входящий трафик				Исходящий трафик			Ошибки		
	Объем трафика	Скорость	Пакеты в секунду	Объем трафика	Скорость	Пакеты в секунду	Ошибки входящих пакетов	Ошибки исходящих пакетов	Ошибки инициализации	
108067	3.39 Мбайт	163 бит/с	10	48.35 Мбайт	2.63 Кбит/с	6	0	8698055	0	
108077	3.45 Мбайт	188 бит/с	11	48.34 Мбайт	2.63 Кбит/с	6	0	0	0	

В верхней части рабочей области в правом углу приводится время непрерывной работы УБ и время на УБ.

Время: 08.10.2018 08:28:40 (UTC+00:00)	Время непрерывной работы: 4 дн, 19:01:03
---	---

В верхней части рабочей области в левом углу приводятся кнопки для генерации отчета о работе УБ и просмотра всех событий мониторинга УБ.



Примечание. Генерация отчета занимает длительное время, по истечении которого будет предложено сохранить файл отчета на диск стандартными средствами веб-браузера.

Детальная информация

Вкладка предназначена для настройки и отображения сведений о лицах, ответственных за эксплуатацию УБ:

- ФИО контактного лица;
- номер рабочего телефона;
- номер мобильного телефона;
- учетная запись Skype;
- адрес электронной почты;

Примечание. Адрес электронной почты автоматически используется при создании нового профиля мониторинга в поле "Отправить письмо".

- адрес электронной почты для уведомлений;

Примечание. Адрес электронной почты используется при создании автоматического уведомления пользователя об отказе УБ.

- дополнительная информация.

Примечание. Содержимое поля выводится на плитке виджета типа "Структура" в разделе "Панель мониторинга".

Начальный вид вкладки "Детальная информация":

✎ Редактировать

Детальная информация

Контактное лицо:

Для изменения данных:




1. Нажмите кнопку "Редактировать".

Рабочая область примет вид:

Редактировать

Детальная информация

Контактное лицо +

2. Для добавления нового параметра нажмите кнопку "Добавить" . Внизу списка появится дополнительное поле для нового параметра.
3. Для изменения типа параметра нажмите кнопку  и выберите тип из раскрывшегося списка.
4. Введите/измените значение параметра в поле справа от его названия.
5. Для удаления параметра нажмите кнопку .
6. Нажмите кнопку "Сохранить".

Детальная информация

Контактное лицо	Иванов	X
Телефон	8435555524	X
E-mail для уведо...	aminemail@com	X

Шаблон

Вкладка предназначена для настройки правил мониторинга УБ. Процедура настройки параметров подробно рассматривается в разделе "Настройка правил мониторинга" (см. стр. 21).

Настройки

Вкладка предназначена для выбора интервала сбора статистики и параметров мониторинга.

Редактировать

Настройки узла безопасности

Мониторинг узла безопасности:

Интервал сбора статистики: 5 мин

Таймаут неактивности: Отключить

Список параметров мониторинга:

- as
- cpu
- filesystem
- firewall
- jrnl
- network
- raid
- ram
- swap
- syslog
- temperature
- vpn

Для отключения мониторинга нажмите кнопку "Редактировать" и снимите флажок "Мониторинг узла безопасности". По умолчанию мониторинг УБ включен.

Для настройки параметров мониторинга узла безопасности:

1. Выберите из раскрывающегося списка значение интервала сбора статистики.
2. Для выбора параметра поставьте отметку в поле рядом с его названием и нажмите кнопку "Сохранить".

Внимание! При отключении параметра будет прекращен сбор статистики и в том числе не будут работать виджеты и правила, связанные с отключенным параметром.

Параметр	Соответствующая подгруппа	Группа
cluster	КЛАСТЕР	Подсистемы
cpu	ЦП	ЦП и память
filesystem	SDA BOOT; DATA; SYSTEM; TEMPORARY	Жесткие диски Разделы жестких дисков
firewall	МЕЖСЕТЕВОЙ ЭКРАН	Подсистемы
ips	СОБ	Подсистемы
jrnl	ЖУРНАЛ	Подсистемы
network	Вся таблица	Сетевые интерфейсы
raid	RAID	Жесткие диски
ram	ОЗУ	ЦП и память
swap	SWAP	ЦП и память
syslog	SYSLOG	Подсистемы
temperature	ТЕМПЕРАТУРА	ЦП и память
vpn	VPN	VPN соединения

Примечание. При переходе на вкладку "Состояние" возможна небольшая задержка при обновлении данных в соответствии с выполненными настройками.

Доступ

Вкладка используется для настройки доступа администраторов системы к мониторингу УБ.

Учетная запись	Роль	Доступ
Все администраторы		<input checked="" type="checkbox"/>
test (test1)	Администратор аудита	<input checked="" type="checkbox"/>
user (user)	Администратор аудита	<input type="checkbox"/>

Для запрета доступа администратора снимите соответствующую отметку в таблице и нажмите кнопку "Сохранить".

Примечание! Настройка доступа возможна только для администратора с ограниченными правами.

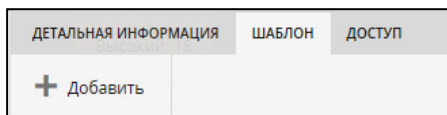
Резервирование

Вкладка предназначена для отображения сведений о статусе узла безопасности, присвоенной ему роли и статусе синхронизации. Для активного ЦУС отображается статус синхронизации резервных ЦУС, для резервных ЦУС отображается статус синхронизации активного ЦУС.

Узел безопасности	Роль	Статус синхронизации
1067	резервный	синхронизированный

Группа узлов безопасности

Страница содержит три вкладки: "Детальная информация", "Шаблон" и "Доступ".



Детальная информация

Вкладка "Детальная информация" используется для настройки данных о лицах, ответственных за эксплуатацию группы УБ:

- контактное лицо;
- мобильный телефон;
- телефон;
- учетная запись Skype;
- адрес электронной почты;

Примечание. Адрес электронной почты используется по умолчанию при создании нового правила в поле "Отправить письмо".

- адрес электронной почты для уведомлений;

Примечание. Адрес электронной почты используется при создании уведомления пользователя об отказе УБ.

- произвольная дополнительная информация.

Примечание. Содержимое поля выводится на плитке виджета типа "Структура" на панели мониторинга.

Процедура настройки параметров вкладки "Детальная информация" подробно рассматривается в разделе "Узел безопасности" (см. стр. 24).

Шаблон

Вкладка "Шаблон" предназначена для настройки правил мониторинга УБ. Процедура настройки параметров подробно рассматривается в разделе "Настройка правил мониторинга" (см. стр. 21).

Доступ

Вкладка предназначена для настройки доступа администраторов системы к мониторингу группы УБ и состоит из двух областей:

- верхняя область "Выберите узлы безопасности" отображает УБ, входящие в эту группу, с перечнем администраторов, которым разрешен доступ к ним;
- нижняя область "Выберите администраторов" содержит полный список администраторов системы, имеющих ограниченные права.

Редактировать

Объекты доступа
Выберите объекты, к которым будет разрешен доступ

Учитывать узлы в подгруппах

Объект доступа	Администраторы
<input type="checkbox"/> cluster5	admin2
<input type="checkbox"/> node-1065	admin2

Администраторы
Отметьте администраторов, которым будет разрешен доступ к выбранным объектам

Учетная запись	Роль	Доступ
Все администраторы		<input type="checkbox"/>
admin2 (admin2)	Администратор аудита	<input type="checkbox"/>

Выберите УБ в верхней области. Для выбора всех УБ поставьте отметку в поле "Объект доступа".

Внимание! По умолчанию в список УБ включены УБ, относящиеся к подгруппам выбранной группы. Для их отключения уберите отметку в поле "Учитывать узлы в подгруппах".

В нижней области появится список администраторов с правами доступа к выбранному УБ. Для настройки доступа определенного администратора к выделенным УБ отметьте поля в столбце "Доступ" и нажмите кнопку "Сохранить". Для управления доступом сразу всех администраторов системы воспользуйтесь отметкой "Все администраторы".

Внимание! Для доступа к группе у пользователя должны быть права доступа ко всем УБ, содержащимся в этой группе.

Создание группы

1. Для создания группы перейдите в родительскую папку в дереве объектов и нажмите кнопку "редактировать".
2. В рабочей области нажмите кнопку "+ Добавить". В дереве объектов появится папка с автоматически присвоенным именем "Группа N", где N — это порядковый номер группы.
3. Нажмите кнопку "Сохранить" в нижней части экрана.

Управление группами

Раздел "Редактор структуры" предназначен для настройки структуры групп и УБ, отличающейся от структуры, созданной средствами Менеджера конфигурации в ЦУС.

Поиск по структуре

Поиск...

Структура

- domain-1111111111
- Группа_3
 - Группа_4
 - Группа_5
 - Группа_6
- Несортированные
- Удаленные

Редактор структуры

Имя

- [-]
- Группа_4
- Группа_5
- Группа_6

В верхней части окна располагаются кнопки, с помощью которых выполняются следующие операции:

- перемещение группы и ее содержимого;
- удаление группы;
- переименование группы;
- восстановление исходной структуры корневого каталога.

В нижней части окна располагаются кнопки сохранения и отмены внесенных изменений.

Перед выполнением процедур выберите группу в дереве объектов.

Для переименования группы:

1. Нажмите кнопку "Переименовать".
Появится поле для ввода названия группы.
2. Замените название группы и нажмите кнопку "Сохранить".

Для удаления группы:

1. Нажмите в правой области кнопку "Удалить".
2. Нажмите кнопку "Сохранить".

Для перемещения группы:

1. Выберите группу для перемещения в правой области.
2. Нажмите кнопку "Вырезать".
3. Перейдите в родительскую группу в дереве объектов.
4. Нажмите кнопку "Вставить". Структура групп и УБ изменится.
5. Для сохранения изменений нажмите кнопку "Сохранить".

Для восстановления исходной структуры корневого каталога:

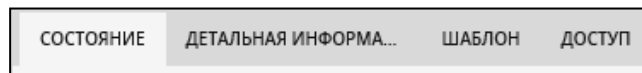
1. Для восстановления структуры, настроенной в ЦУС средствами Менеджера конфигурации, нажмите в правой области кнопку "Загрузить с ЦУС".
Появится окно подтверждения восстановления структуры системы.

Внимание! Восстановление структуры необратимо.

2. Нажмите кнопку "Да".
3. Нажмите кнопку "Сохранить".

Кластер

Страница УБ содержит следующие вкладки:

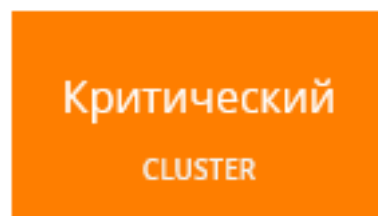


Состояние

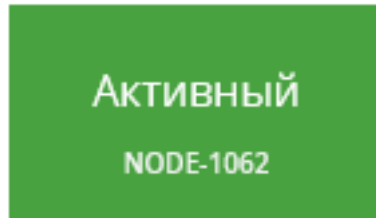
На вкладке в реальном времени отображаются данные, разделенные на следующие группы:

- Активные события — таблица со списком активных событий на УБ с указанием их важности, продолжительности и причины и плитка с названием кластера и его состоянием.

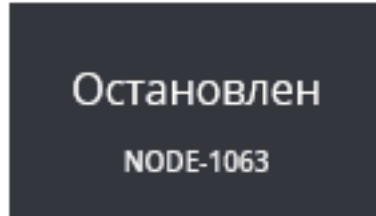
Важность	Продолжительность	Причина
● предупреждение	00:00:05	Кластер cluster в критическом состоянии



- Основной узел безопасности — имя основного УБ и его состояние.



- Резервный узел безопасности — имя резервного УБ и его состояние.



Детальная информация

Вкладка предназначена для настройки и отображения сведений о лицах, ответственных за эксплуатацию УБ:

- ФИО контактного лица;
- номер рабочего телефона;
- номер мобильного телефона;
- учетная запись Skype;
- адрес электронной почты;

Примечание. Адрес электронной почты автоматически используется при создании нового правила мониторинга в поле "Отправить письмо".

- адрес электронной почты для уведомлений;

Примечание. Адрес электронной почты используется при создании автоматического уведомления пользователя об отказе УБ.




- дополнительная информация.

Примечание. Содержимое поля выводится на плитке виджета типа "Структура" в разделе "Панель мониторинга".

Начальный вид вкладки "Детальная информация":

Для изменения данных:

1. Нажмите кнопку "Редактировать".
2. Рабочая область примет вид:

3. Для добавления нового параметра нажмите кнопку "Добавить" .
Внизу списка появится дополнительное поле для нового параметра.
4. Для изменения типа параметра нажмите кнопку  и выберите тип из раскрывшегося списка.
5. Введите/измените значение параметра в поле справа от его названия.
6. Для удаления параметра нажмите кнопку .
7. Нажмите кнопку "Сохранить".

Детальная информация

Контактное лицо ▾	Иванов	✕
Телефон ▾	8435555524	✕
E-mail для уведо... ▾	aminemail@com	✕

Шаблон

Вкладка предназначена для настройки правил мониторинга кластера. Процедура настройки параметров подробно рассматривается в разделе "Настройка правил мониторинга" (см. стр. [21](#)).

Доступ

Вкладка используется для настройки доступа администраторов системы к мониторингу УБ.

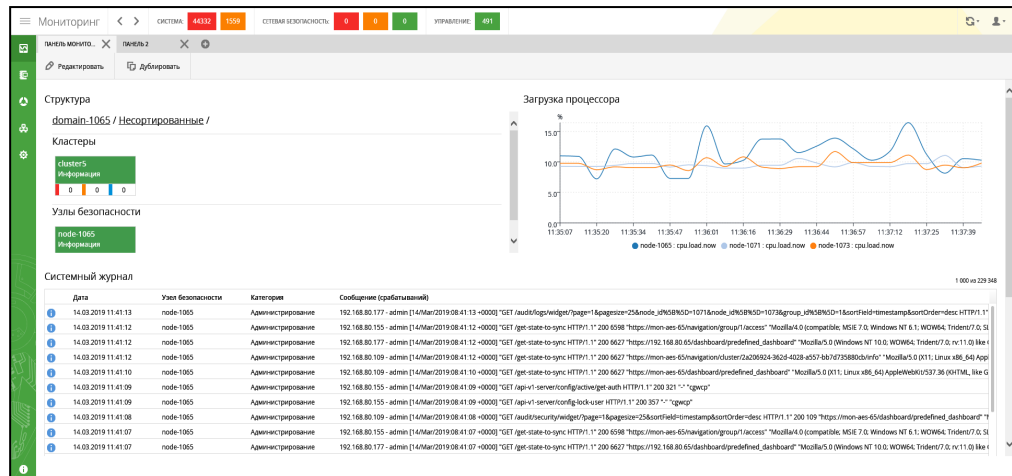
Учетная запись	Роль	Доступ
Все администраторы		<input checked="" type="checkbox"/>
test (test1)	Администратор аудита	<input checked="" type="checkbox"/>
user (user)	Администратор аудита	<input type="checkbox"/>

Для запрета доступа администратора снимите соответствующую отметку в таблице и нажмите кнопку "Сохранить".

Примечание! Настройка доступа возможна только для администратора с ограниченными правами.

Раздел "Панель мониторинга"

Панель мониторинга представляет собой набор виджетов. Виджет — конструктивный элемент панели, отвечающий за визуальный вывод части информации, собранной системой.



Максимально допустимое количество виджетов, используемых для отображения в панели мониторинга, — 12.

В системе используются виджеты следующих типов:

- табличный;
- графический;
- структурный.

Внимание! При некорректном отображении виджетов графического типа перезагрузите страницу в браузере.

Табличный виджет

Табличный виджет представляет собой таблицу с данными.

Дата	Узел безопасности	Категория	Сообщение (срабатываний)
14.03.2019 12:23:58	node-1065	Администрирование	192.168.80.109 - admin [14/Mar/2019:09:23:58 +0000] "GET /audit/security/widget/?page=1&pagesize=25&sortfield=timestamp&sortOrder=desc HTTP/1.1" 200 109 "https://mon-ae545/dashboard/cluster/2a206924-362d-4028-a557-b670735880b/info?Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Firefox/35.0"
14.03.2019 12:23:57	node-1065	Администрирование	192.168.80.155 - admin [14/Mar/2019:09:23:57 +0000] "GET /get-state-to-sync HTTP/1.1" 200 6705 "https://mon-ae545/dashboard/cluster/2a206924-362d-4028-a557-b670735880b/info?Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Firefox/35.0"
14.03.2019 12:23:57	node-1065	Администрирование	192.168.80.109 - admin [14/Mar/2019:09:23:57 +0000] "GET /get-state-to-sync HTTP/1.1" 200 6705 "https://mon-ae545/dashboard/cluster/2a206924-362d-4028-a557-b670735880b/info?Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Firefox/35.0"
14.03.2019 12:23:57	node-1065	Администрирование	192.168.80.155 - admin [14/Mar/2019:09:23:57 +0000] "GET /audit/logs/widget/?page=1&pagesize=25&node_id=9089501071&node_id=9089501073&group_id=9089501071&sortfield=timestamp&sortOrder=desc HTTP/1.1"
14.03.2019 12:23:56	node-1073	Управление	[cluster_monitoring] Канал синхронизации кластера в порядке
14.03.2019 12:23:56	node-1073	Управление	[cluster_monitoring] Канал синхронизации кластера в порядке
14.03.2019 12:23:56	node-1065	Управление	[monitoring_analyzer.cluster] Состояние кластера <cluster>- критический (основной: исправный, резервный: остановленный)
14.03.2019 12:23:56	node-1065	Управление	[monitoring_analyzer.cluster] Состояние кластера <cluster>- критический (основной: исправный, резервный: остановленный)
14.03.2019 12:23:56	node-1073	Управление	[cluster_monitoring] Состояние узла кластера: остановленный (статус в ожидании)
14.03.2019 12:23:56	node-1073	Управление	[cluster_monitoring] Канал синхронизации кластера неактивен
14.03.2019 12:23:56	node-1073	Управление	[cluster_monitoring] Канал синхронизации <192.168.80.71> недоступен
14.03.2019 12:23:55	node-1065	Администрирование	192.168.80.109 - admin [14/Mar/2019:09:23:55 +0000] "GET /get-state-to-sync HTTP/1.1" 200 6706 "https://mon-ae545/dashboard/cluster/2a206924-362d-4028-a557-b670735880b/info?Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Firefox/35.0"

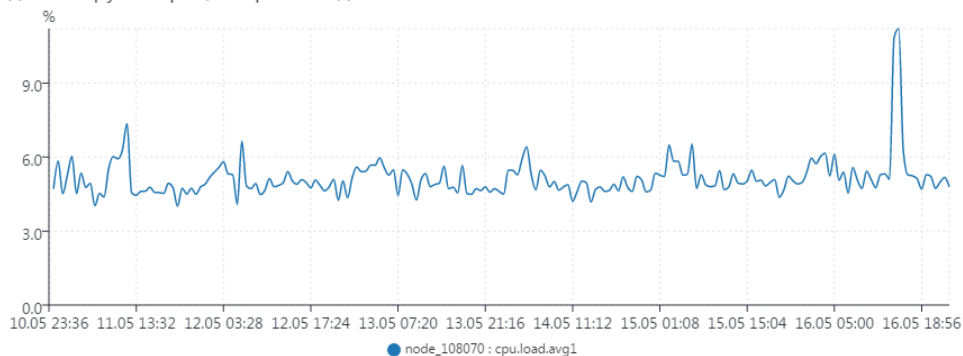
Тип информации виджета выбирается при его настройке и может быть событиями или данными. Источниками информации в системе являются:

- системный журнал;
- журнал сетевой безопасности;
- журнал управления;
- база данных мониторинга и аудита.

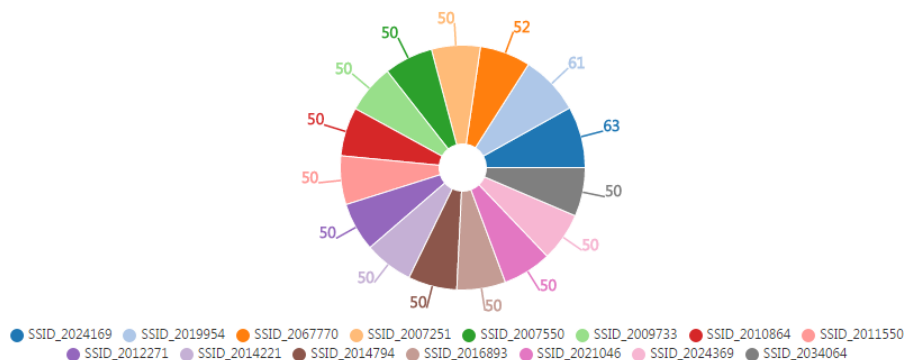
Графический виджет

Графический виджет представляет собой график или круговую диаграмму.

Средняя загрузка процессора за неделю



Топ 15 обнаруженных атак по сигнатурам



Источником информации для виджета являются данные системы мониторинга и аудита.

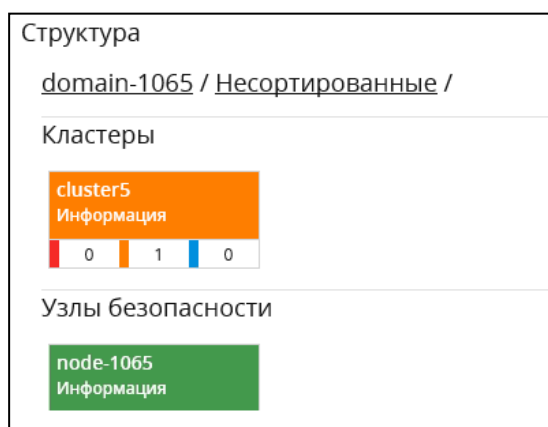
Структурный виджет

Виджет отображает структуру объектов мониторинга в виде трех разделов:

- кластеры — перечень сформированных кластеров в домене;
- группы — перечень всех сформированных групп в домене;
- узлы безопасности — перечень УБ выбранной группы.

Отображение того или иного раздела задается при настройке виджета.

В каждом разделе входящие в него объекты представлены в виде плитки с указанием имени объекта и количества зарегистрированных событий того или иного уровня критичности. Цвет плитки указывает на максимальный уровень критичности события, произошедшего на данном объекте или на одном из объектов группы.



Нажмите на плитку группы для просмотра вложенных групп и узлов. Для возврата на более высокие уровни структуры воспользуйтесь строкой навигации в верхней части виджета.

Для перехода на страницу УБ в разделе "Структура" нажмите на соответствующую плитку.

Настройка панели мониторинга

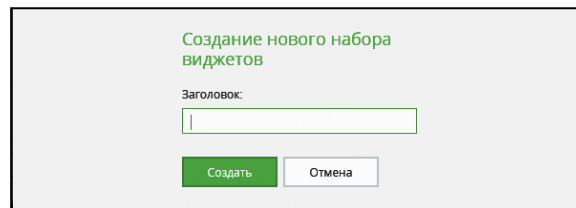
Настройка панели включает в себя:

- добавление новых виджетов на панель;
- удаление виджетов с панели;
- редактирование виджетов;
- перемещение виджета в пределах панели и изменение его размера.

Для создания нового набора виджетов:

1. На панели с вкладками нажмите .

На экране появится окно:

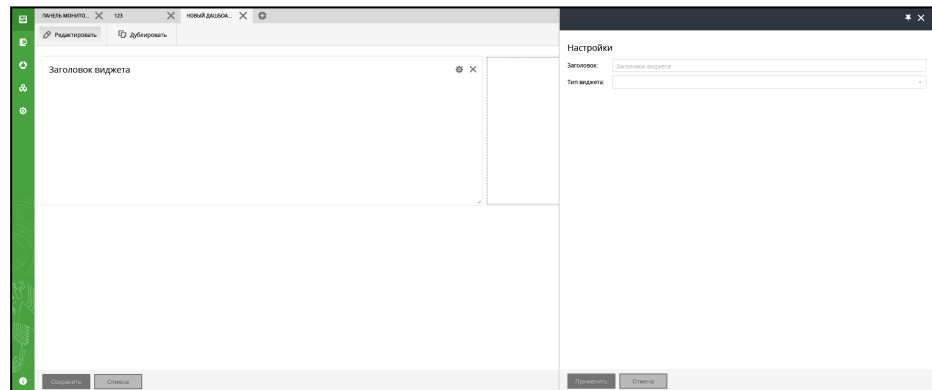


Создание нового набора виджетов

Заголовок:

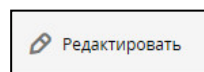
2. Введите название набора и нажмите "Создать".

Будет создана новая вкладка. Панель мониторинга автоматически перейдет в режим редактирования, новый виджет будет готов к настройке.



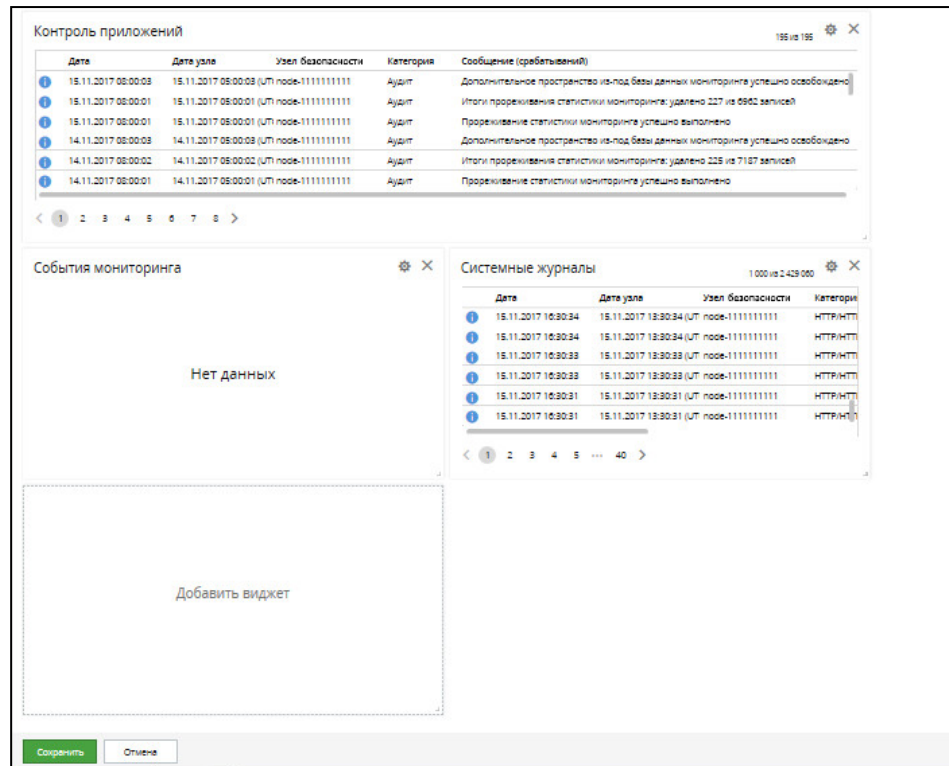
Для настройки виджета:


1. Нажмите кнопку "Редактировать" в рабочей области.



Панель мониторинга перейдет в режим редактирования.

2. Для добавления нового виджета нажмите плитку "Добавить виджет".
На панели появится шаблон виджета.



3. Для настройки виджета нажмите кнопку , расположенную в правом верхнем углу виджета.

В правой части главного окна появится панель настроек виджета.

Настройки

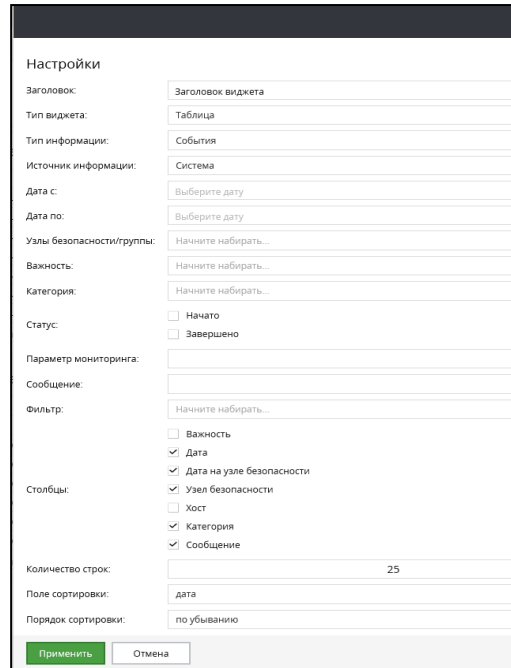
Заголовок:

Тип виджета:

4. Введите заголовок виджета и выберите его тип — таблица, график или структура.

В окне настроек добавится поле "Тип информации". Последующие поля и этапы настройки параметров зависят от выбранных типов виджета и информации.



Пример. На рисунке представлены поля настроек виджета при выборе следующих параметров: "Тип виджета" — Таблица, "Тип информации" — Событие, "Источник информации" — Система.



В настройках параметров могут использоваться фильтры по группам и УБ.

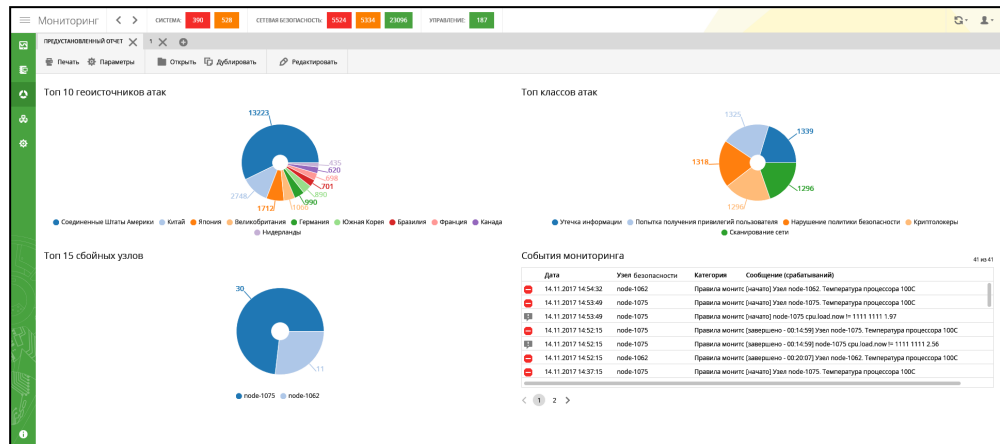
5. Настройте параметры виджета и нажмите кнопку "Применить", расположенную в нижней части панели настройки.

Виджет отобразит значения заданных параметров.

6. Для изменения размера виджета используйте указатель , расположенный в его правом нижнем углу.
7. Для добавления следующего виджета повторите пп. 3–6.
8. Для удаления виджета нажмите кнопку , расположенную в правом верхнем углу виджета.
9. Для перемещения виджета выделите его заголовок и перетащите на свободное место панели.
10. Для изменения параметров виджета нажмите кнопку редактирования, расположенную в его правом верхнем углу, и в открывающейся панели настроек укажите значения параметров (см. пп. 5, 6).
11. Для завершения настройки нажмите кнопку "Сохранить", расположенную в нижней части панели мониторинга.

Раздел "Статистика"

Раздел предназначен для формирования и просмотра настраиваемых отчетов, предоставляющих в визуальной форме статистическую информацию за определенный период времени.



Каждый отчет представляет собой набор виджетов табличного и/или графического типа.

При переходе в раздел "Статистика" в рабочей области главного окна отобразится последний выбранный отчет. Если отчеты не формировались, в главном окне отобразится отчет, настроенный по умолчанию.

Внимание! Виджеты, входящие в состав отчета, на экране отображаются в режиме предварительного просмотра. В связи с этим табличные виджеты событий содержат 1000 последних записей (распределенных на 40 страниц по 25 строк) с указанием их общего количества.

В верхней части окна расположены кнопки, с помощью которых выполняются следующие операции:

- вывод отчета на печать;
- настройка параметров печати;
- вывод на экран сохраненных отчетов;
- копирование наборов виджетов;
- редактирование виджетов.

Управление виджетами

Для редактирования виджетов:

1. Нажмите кнопку  Редактировать.

Рабочая область перейдет в режим редактирования.

2. Выполните пп. **3–12** процедуры, представленной на стр. **36**.

Для виджетов (поле "Тип информации"—"Данные", поле "Источник информации"—"Мониторинг") реализовано автоматическое прореживание накопленных данных в соответствии со следующей таблицей:

Время появления данных	Процент сохраненных данных, %
1 – 3 дня назад	80
3 – 7 дней назад	65
7 – 14 дней назад	50
14 дней – 1 месяц назад	35
1 – 6 месяцев назад	15

Время появления данных	Процент сохраненных данных, %
6 – 12 месяцев назад	5
Больше года назад	0

При этом в журнале аудита появляются сообщения следующего характера:

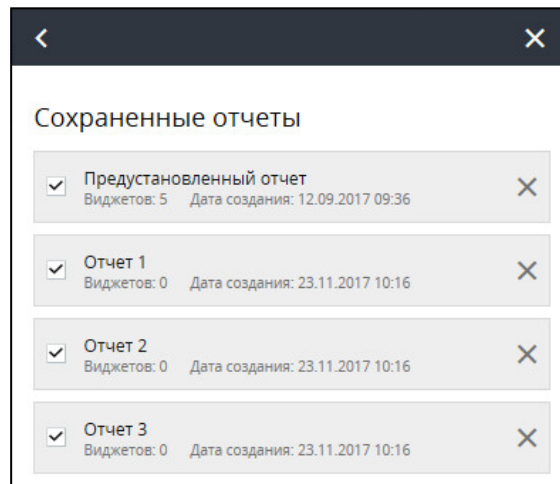
Категория	Сообщение (срабатываний)
Аудит и мониторинг	Дополнительное пространство из-под базы данных мониторинга успешно освобождено
Аудит и мониторинг	Итоги прореживания статистики мониторинга: удалено 67 из 771 записей
Аудит и мониторинг	Прореживание статистики мониторинга успешно выполнено

Просмотр отчетов

Для просмотра отчета:

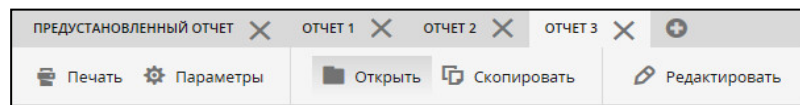
1. Нажмите кнопку "Открыть" в рабочей области.

В правой части главного окна появится список сформированных отчетов, упорядоченный по времени создания:



Примечание. Если отчеты не создавались, в списке будет сформирован один отчет по умолчанию.

Для просмотра отчета поставьте отметку в поле рядом с его названием. Все отмеченные отчеты выводятся в рабочую область. Для перемещения по ним используйте вкладки.



2. Для копирования отчета перейдите на его вкладку и нажмите кнопку "Скопировать" в рабочей области.
3. Для удаления отчета с рабочей области удалите отметку в поле рядом с его названием.
4. Для удаления отчета из системы нажмите значок .

Внимание! Список отчетов не может быть пустым. Если в списке только один отчет, его удалить нельзя.

Подготовка отчета к печати

Используйте настройки оформления внешнего вида отчета.

Для настройки оформления отчета:

1. Нажмите кнопку "Параметры" на рабочей области.

В правой части рабочего окна появится всплывающее окно "Параметры печати".

Параметры печати

Логотип:

Титульный лист:

Вывод листа: Добавить титульный лист

Название отчёта:

Вывод даты: Добавить дату генерации отчёта

Верхний колонтитул:

Вывод верхнего колонтитула: Добавить верхний колонтитул

Текст верхнего колонтитула: [Просмотреть список доступных макросов](#)

Нижний колонтитул:

Вывод нижнего колонтитула: Добавить нижний колонтитул

Текст нижнего колонтитула: [Просмотреть список доступных макросов](#)

Виджеты:

Вывод виджетов:

- Top 10 геоисточников атак (Топ геоисточников атак)
- Top 15 обнаруженных атак по сигнатурам (Топ сигнатур)
- Top 15 сбойных узлов (Топ сбойных узлов)
- Количество атак за неделю (Количество атак)

2. Для выбора логотипа отчета выполните щелчок мышью в поле "Логотип". На экране появится стандартное окно выбора файла. Укажите нужный файл. В поле "Логотип" появится имя файла.

Для просмотра изображения наведите курсор на ссылку "Показать логотип".

Для выбора другого файла или удаления выбранного логотипа из отчета удалите имя файла.

3. Задайте оставшиеся параметры оформления внешнего вида отчета.

Внимание! Колонтитулы можно добавить вручную или использовать макросы. Для просмотра доступных макросов нажмите ссылку "Просмотреть список доступных макросов".

4. При выборочной печати отчета снимите отметки у тех виджетов, которые не должны войти в отчет. У табличных виджетов доступно ограничение числа печатаемых строк.
5. После настройки внешнего вида отчета нажмите кнопку "Сохранить", расположенную в нижней части окна.

Для формирования отчета:

1. Нажмите кнопку "Печать" в рабочей области.

В нижней части рабочего окна появится сообщение о начале процедуры формирования отчета. Когда отчет будет готов, на активной странице появится сообщение с предложением скачивания файла в формате PDF.

Внимание! Время формирования отчета ограничено и составляет 30 минут. В случае его превышения рекомендуется сократить количество виджетов и повторить процедуру.

2. Сохраните PDF-файл и при необходимости распечатайте его.

Режимы мониторинга

В системе используются два режима визуализации данных: в реальном времени и за выбранный период.

Мониторинг за выбранный период предназначен для накопления и просмотра отчетности в разделе "Статистика" (см. стр. 39) при наличии настроек виджета:

- поле "Тип виджета" – "Таблица", поле "Тип информации" – "Данные", поле "Источник информации" – "Мониторинг";
- поле "Тип виджета" – "График", поле "Тип информации" – "Данные", поле "Источник информации" – "Мониторинг".

Режим реального времени доступен при переходе на страницу просмотра состояния УБ, а также в панели мониторинга при наличии соответствующих настроек виджета (см. стр. 38) и отражает значения параметров в настоящий момент времени.

Примечание. В реальном времени значения параметров обновляются с интервалом 5 секунд. Не рекомендуется переводить в режим реального времени более 20 узлов безопасности в системе, поскольку этот режим ресурсоемкий и его использование тормозит работу системы.

Раздел "Настройки"

Главное окно рабочей области раздела выглядит следующим образом:

Настройка email сервера (SMTP)

Включить отправку почтовых уведомлений

Сервер:

Порт:

Пользователь:

Пароль:

Отправитель:

Безопасность: Без шифрования
 Включить TLS
 Включить SSL

Раздел предназначен для настройки отправки сообщений в случае недоступности УБ.

Для настройки отправки сообщений:

1. Нажмите кнопку "Редактировать".
2. Поставьте отметку в поле "Включить отправку почтовых уведомлений".
3. Заполните остальные поля.
4. Выберите метод шифрования сообщения.
5. Нажмите кнопку "Сохранить" в нижней части экрана.

Глава 4

Аудит

Для проведения аудита необходимо выполнить следующие процедуры:

1. Настройка параметров сбора и хранения журналов (см. ниже).
2. Просмотр и анализ сообщений журналов одним из двух способов:
 - с помощью средств веб-интерфейса системы мониторинга и аудита (см. стр.48);
 - с помощью средств локального меню (см. стр.54).

Параметры журналирования

В системе выполняются следующие настройки журналирования:

- выбор уровня детализации журналов (см. ниже);
- настройка хранения журналов на внешнем syslog-сервере (см. стр.44);
- настройка автоматической очистки журналов (см. стр.46);
- хранение журналов во внешней базе данных (см. стр.47).

Для вызова настройки параметров журналирования:

1. Откройте Менеджер конфигурации и перейдите в раздел "Структура".
2. Выберите УБ из списка и нажмите кнопку "Свойства".
На экране появится окно "Узел безопасности".
3. Выберите в левой части окна в разделе "Узел безопасности" пункт "Настройки журналирования".

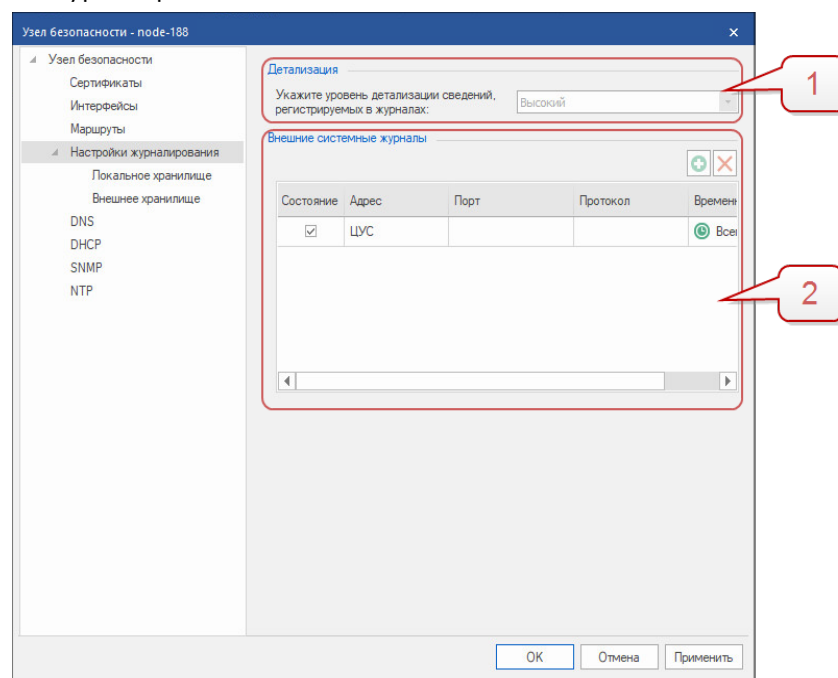


Рис.3 Окно "Свойства узла безопасности"

В правой части окна "Узел безопасности" появятся текущие настройки журналов УБ:

- область 1 — используется для выбора уровня детализации событий, регистрируемых в журналах;
- область 2 — используется для просмотра и настройки внешних системных журналов.

Уровень детализации журналов

Для выбора уровня детализации:

1. В области 1 (см. Рис.3 на стр.43) выберите требуемый уровень детализации журналов из раскрывающегося списка:

Уровень детализации журналов	Уровень важности события
Отладочный	Отладка (DEBUG)
Минимальный	Информация (INFO)
Низкий	Ошибка (ERR)
Средний	Критическая ошибка (CRIT)
Высокий	Тревога (ALERT)
Предустановленный	Предупреждение (Warning)


Внимание! При выборе уровня детализации в журналы будут записываться события, уровень важности которых соответствует или выше выбранного уровня детализации.



2. Нажмите кнопку "ОК" в окне "Узел безопасности".
3. Для применения настроек нажмите кнопку "Установить политику" на панели инструментов, отметьте УБ с измененными параметрами и нажмите кнопку "ОК" в окне "Установить политики".


Настройка хранения журналов на внешнем syslog-сервере

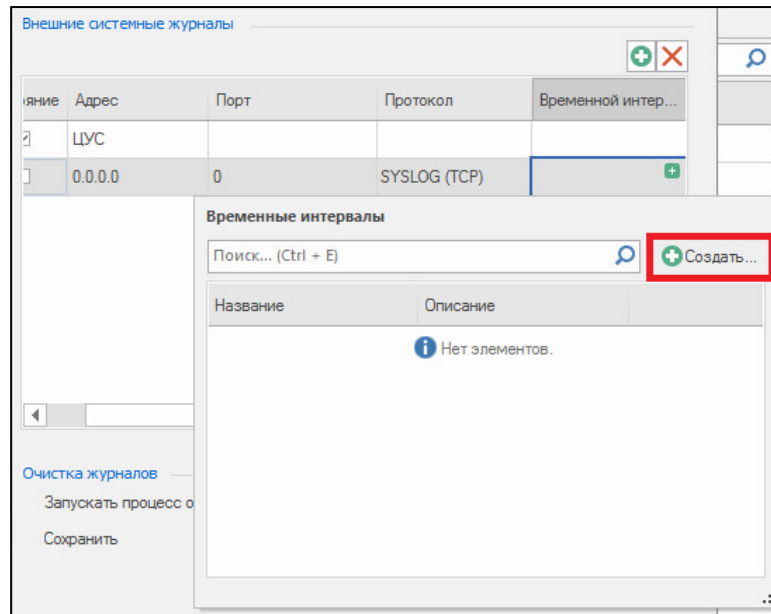
Внимание! Syslog-сервер должен поддерживать формат событий, описанный в RFC 5424.

Для добавления нового syslog-сервера:

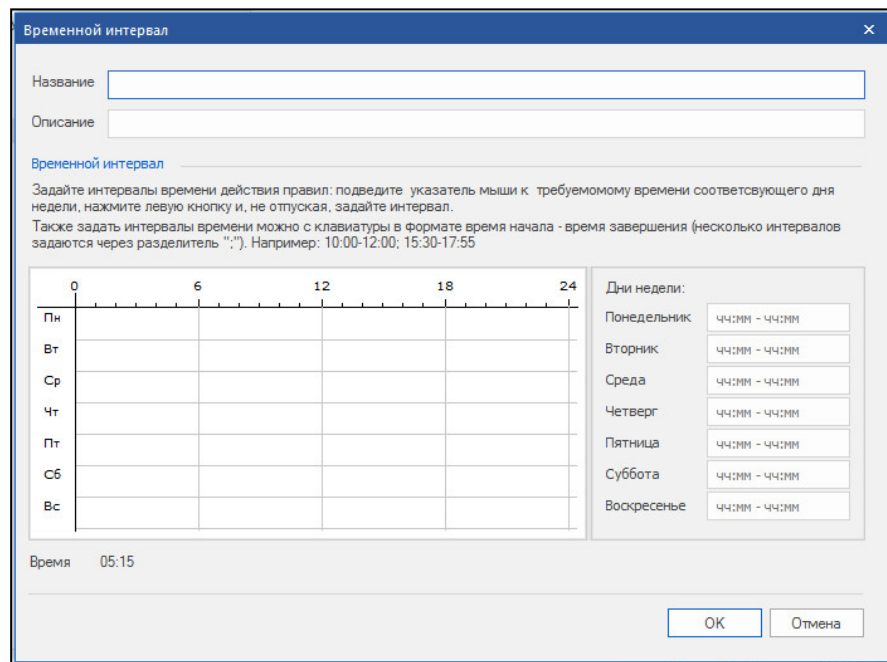
1. В области 2 (см. Рис.3 на стр.43) нажмите кнопку . На экране появится строка ввода параметров syslog-сервера.

Состояние	Адрес	Порт	Протокол	Временной интер...
<input checked="" type="checkbox"/>	ЦУС			 Всегда
<input checked="" type="checkbox"/>	110.220.101.10	100	SYSLOG (TCP)	 Всегда

2. Введите параметры syslog-сервера. Если доступ к syslog-серверу предоставляется только в определенное время, укажите временной интервал подключения в последней графе строки параметров. Для этого нажмите кнопку  в ячейке. Откроется окно "Временные интервалы".



3. В окне "Временные интервалы" нажмите кнопку "Создать". На экране появится новое окно.



4. Заполните поля согласно инструкции и нажмите кнопку "OK".
5. Нажмите кнопку "OK" в окне "Узел безопасности".
6. Для применения настроек нажмите кнопку "Установить политику" на панели инструментов, отметьте УБ с измененными параметрами и нажмите кнопку "OK" в окне "Установить политики".

Для изменения параметров syslog-сервера:

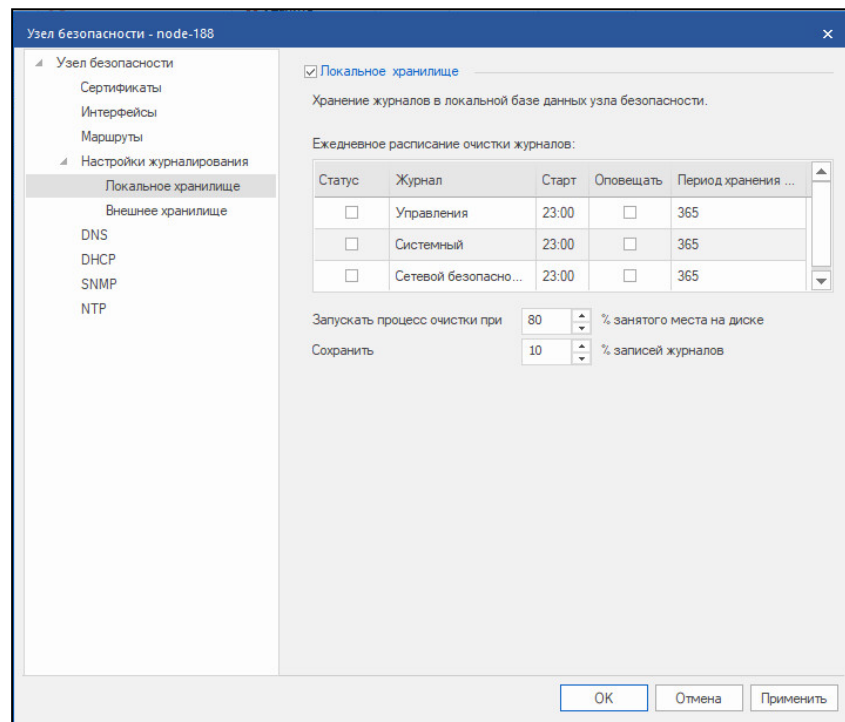
1. В области 2 (см. Рис.3 на стр.43) выберите нужную строку.
2. Измените параметры syslog-сервера. Выделите ячейку двойным щелчком мыши и внесите изменение.

Состояние	Адрес	Порт	Протокол	Временной интер...
<input checked="" type="checkbox"/>	ЦУС			Всегда
<input checked="" type="checkbox"/>	110.220.101.10	100	SYSLOG (TCP)	Всегда

- Для отмены хранения журналов на сервере снимите отметку состояния.
- Нажмите кнопку "ОК" в окне "Узел безопасности" (см. Рис.3 на стр.43).
- Для применения настроек нажмите кнопку "Установить политику" на панели инструментов, отметьте УБ с измененными параметрами и нажмите кнопку "ОК" в окне "Установить политики".

Настройка автоматической очистки журналов

В меню "Настройки журналирования" перейдите в раздел "Локальное хранилище":



Для очистки журналов по расписанию:

- Поставьте отметку в поле "Локальное хранилище". Настройки станут доступны для редактирования.

Примечание. Поле "Локальное хранилище" отсутствует на УБ с активированным ЦУС.

- Включите функцию очистки для каждого конкретного журнала, поставив отметку рядом с его названием в поле столбца "Статус" таблицы "Ежедневное расписание очистки журналов".
- Настройте время запуска очистки журналов. Для этого выделите двойным щелчком мыши ячейку столбца "Старт" и внесите изменения с помощью клавиатуры.
- Поставьте отметку в поле "Оповещать" для отправки почтовых уведомлений о выполнении операции очистки.
- Настройте количество дней хранения записей журналов. Для этого выделите двойным щелчком мыши ячейку столбца "Период хранения данных (дней)" и внесите изменения с помощью клавиатуры.
- Нажмите кнопку "ОК" в окне "Узел безопасности".

7. Для применения настроек нажмите кнопку "Установить политику" на панели инструментов, отметьте УБ с измененными параметрами и нажмите кнопку "ОК" в окне "Установить политики".

Ежедневное расписание очистки журналов				
Статус	Журнал	Старт	Оповещать	Период хранения ...
<input checked="" type="checkbox"/>	Администрирования	11:29	<input checked="" type="checkbox"/>	112
<input checked="" type="checkbox"/>	Системный	08:00	<input checked="" type="checkbox"/>	10
<input checked="" type="checkbox"/>	Сетевой безопасности	03:00	<input type="checkbox"/>	365

Автоматическая очистка записей журналов по сроку давности отключена по умолчанию. Процесс очистки будет автоматически запускаться в случае, когда объем заполненного диска будет равен указанному значению в процентном соотношении от общего объема дискового пространства (системное ограничение диапазона возможных значений от 50 до 80%). При этом процент сохраняемых записей журналов не может составлять менее 10% (системное ограничение диапазона возможных значений от 10 до 50%).

Для автоматической очистки журналов по количеству свободного места на диске:

1. Заполните поля "Запускать процесс очистки при" и "Сохранить".
2. Нажмите кнопку "ОК" в окне "Узел безопасности".
3. Для применения настроек нажмите кнопку "Установить политику" на панели инструментов, отметьте УБ с измененными параметрами и нажмите кнопку "ОК" в окне "Установить политики".

Хранение журналов во внешней базе данных

Внимание! Если система настроена на работу с внешней базой данных, то при потере соединения с базой данных веб-интерфейс системы будет недоступен.

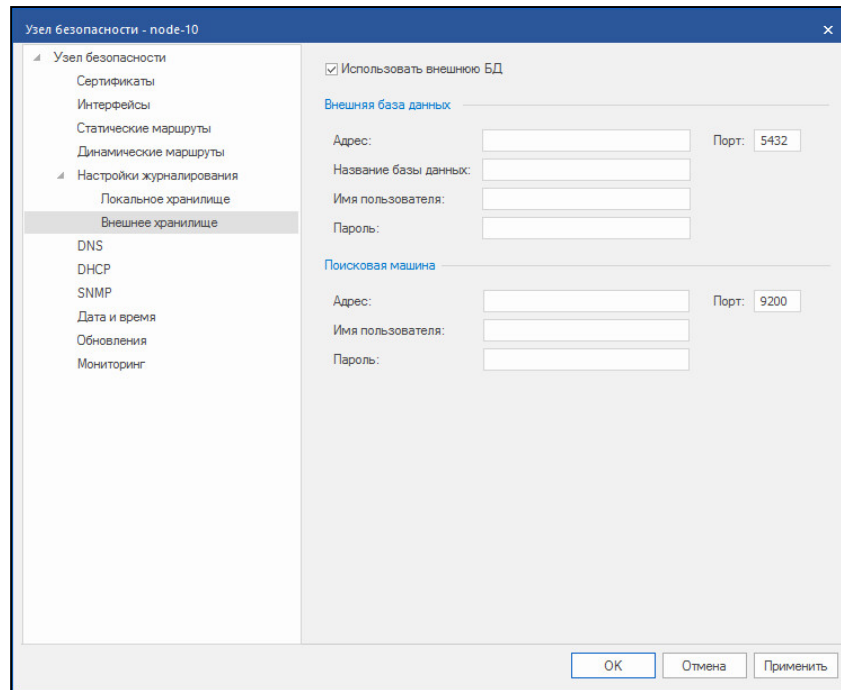
По умолчанию хранение журнала сетевой безопасности и системного журнала во внешней базе данных отключено.

Внимание! В качестве внешней базы данных может выступать только СУБД PostgreSQL версии 9.5.13.

Для настройки хранения журналов во внешней базе данных:

1. В окне "Узел безопасности" в разделе "Узел безопасности" выберите пункт "Настройки журналирования" и подпункт "Внешнее хранилище".

В правой части окна появятся текущие настройки хранения журналов во внешней базе данных.



- Установите отметку "Внешняя база данных".

На экране станут активными разделы для ввода параметров внешней базы данных и поисковой машины.

- Введите параметры настройки и нажмите кнопку "Применить".

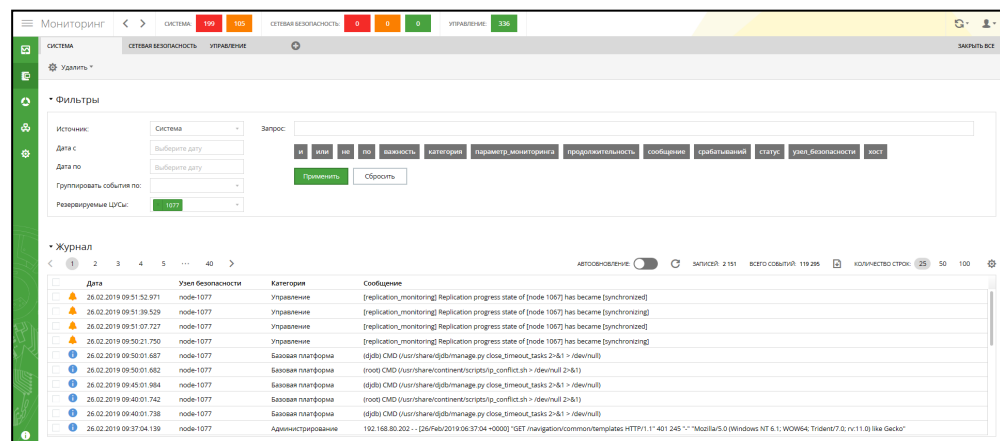
Внимание! Сервер внешней базы данных должен поддерживать формат событий, описанный в RFC 5424.

- Нажмите кнопку "OK" в окне "Узел безопасности".
- Для применения настроек нажмите кнопку "Установить политику" на панели инструментов, отметьте УБ с измененными параметрами и нажмите кнопку "OK" в окне "Установить политики".

Просмотр журналов с помощью веб-интерфейса

Для просмотра журналов в системе мониторинга и аудита перейдите в раздел "Журналы" на панели навигации.

Общий вид рабочей области раздела "Журналы" меняется в зависимости от выбора источника информации. На рисунке ниже представлен вид рабочей области журнала "Система":



Для фильтрации сообщений в журнале:

1. Выберите тип журнала в поле "Источник".
2. Уточните временной диапазон запроса в полях "Дата с" и "Дата по".
3. Выберите параметр для группировки событий в поле "Группировать события".
4. При настроенном резервировании ЦУС в фильтре выберите те ЦУС, журналы которых требуется отобразить. По умолчанию в строке выбран активный ЦУС.
5. Введите правило фильтрации, используя специализированные теги, расположенные ниже. Завершите ввод правила нажатием клавиши <Enter>.

Примечание. При создании правила фильтрации некоторые теги сопровождаются подтегом "точно". Для расширенной фильтрации уберите подтег и часть содержания тега.

6. Для добавления в фильтр дополнительного условия выберите логическую операцию в тегах запроса и повторите п.3.

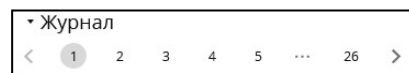
Примечание. Условия запроса без логических связей между собой будут интерпретироваться как теги с союзом ИЛИ.

7. Нажмите кнопку "Применить".

Пример фильтрации:


Сообщение	Текст запроса
Выборка по диапазону портов отправителя сообщения от 1000 до 60000	порт_отправителя: [1000 по 60000]
Выборка по стране получателя — Россия или категории потенциально опасного трафика	страна_получателя: "RU" категория.точно: "Потенциально опасный трафик"
Выборка по категориям событий, содержащим слово "трафик"	категория: "трафик"


Для навигации по результатам фильтрации используйте кнопки перехода по страницам:




Количество показываемых в окне записей определяется параметром "Кол-во строк" в правой части окна:



Для выбора отображаемых параметров событий в журнале нажмите кнопку  и отметьте требуемые опции.

При работе с несколькими вариантами фильтрации или разными журналами нажмите кнопку формирования нового запроса в верхней части экрана . Параметры запроса сохраняются после каждого нажатия кнопки "Применить". При авторизации администратора системы и переходе в раздел "Журналы" администратору будут показаны его последние запросы с сохраненными параметрами фильтрации.

Для удаления запроса нажмите кнопку .

При создании запроса появляется окно "Создать новый запрос". В пустом поле введите название запроса, а затем нажмите кнопку "Создать".

Системный журнал

В системном журнале содержится следующая информация:

- Важность сообщения — информация об уровне важности сообщения, показываемая соответствующим значком.

Важность сообщения			
Иконка	Уровень	Иконка	Уровень
	Авария		Тревога
	Критическая ошибка		Ошибка
	Предупреждение		Оповещение
	Информация		Отладка

- Дата — дата и время сообщения. Временная зона выбирается администратором системы мониторинга и аудита.
- Дата на узле безопасности — дата и время сообщения, представленные во временной зоне узла безопасности, на котором сгенерировано сообщение.
- Узел безопасности — узел безопасности, на котором сгенерировано сообщение.
- Класс — категория события.
- Сигнатура/правило — текст сообщения и количество срабатываний.

Для фильтрации записей используют следующие теги:



Тег	Пояснение
важность:[уровень]	Выборка сообщений определенного уровня важности
категория:[текст]	Выборка записей, содержащих в поле "Категория" определенный текст
сообщение:[текст]	Выборка записей, содержащих в поле "Сообщение" определенный текст
срабатываний:[число]	Выборка групп с определенным числом событий
узел:[имя узла]	Выборка сообщений с определенного УБ
хост:[имя хоста]	Выборка сообщений определенного хоста
параметр_мониторинга:[подсистема]	Выборка событий мониторинга определенных подсистем




Примечание. Имя хоста образуется из имен УБ и домена, разделенных ".".

Журнал сетевой безопасности

В журнале сетевой безопасности содержится следующая информация:

- Важность сообщения — информация об уровне важности сообщения, показываемая соответствующим значком.


Важность сообщения			
Иконка	Уровень	Иконка	Уровень
	Высокий		Предупреждение
	Средний		Оповещение

	Низкий		Информация
	Очень низкий		

- Дата — дата и время сообщения. Временная зона выбирается администратором системы мониторинга и аудита.
- Дата на узле безопасности — дата и время сообщения, представленные во временной зоне узла безопасности, на котором сгенерировано сообщение.
- Узел безопасности — узел безопасности, на котором сгенерировано сообщение.
- Класс — класс события.
- Компонент — подсистема, которая записала событие в журнал.
- Идентификатор сигнатуры — уникальный номер сигнатуры.
- Ревизия — версия сигнатуры.
- Действие — тип реакции на передаваемый трафик.
- Порты — сетевые порты отправителя и получателя.
- Протокол — протокол, по которому проводится атака.
- Домен получателя — домен, на который сгенерирована атака.
- Интерфейс — сетевой интерфейс детектора атак, на котором была обнаружена атака.
- Адрес отправителя — адрес, с которого сгенерирована атака.
- Адрес получателя — адрес, на который сгенерирована атака.
- Сигнатура/правило — текст сообщения и количество срабатываний.

При выборе события СБ открывается окно с полной информацией о событии. Полная информация содержит время первого и последнего события группы, представленное во временной зоне УБ, на котором сгенерировано сообщение, IP-адрес и порт источника атаки, порт и IP-адрес, на который проводилась атака.

Детальная информация о событии	
Дата последнего события:	07.02.2019 12:45:10.844
Дата на шлюзе безопасности:	07.02.2019 09:45:10.844 (UTC)
Важность:	Оповещение
Адрес отправителя:	192.168.10.2 : 49543
Действие:	блокировать
Узел безопасности (интерфейс):	node-1065
Компонент:	ПФ
Кол-во срабатываний:	1
Порт получателя:	443
Домен получателя:	site1.testers.com
Служба:	HTTP(S)
Детальная информация:	URL: https://site1.testers.com/favicon.ico HTTP method: GET MIME type: text/html

Для просмотра полного текста сообщения о событии в формате CSV нажмите кнопку  в главном окне журнала.

Для просмотра сообщений в журнале СБ используется механизм группировки по одному из параметров. В главном окне отображается последнее сообщение из каждой группы, описание сигнатуры, количество сообщений в группе.

Сортировка записей сгруппированных событий в главном окне журнала происходит по количеству срабатываний в сторону их убывания. В результате группировки событий выводится максимум 10000 записей.

Для фильтрации записей используют следующие теги:

Тег	Пояснение
адрес отправителя: [IP-адрес]	Выборка событий, сгенерированных атакой с определенного адреса
адрес получателя: [IP-адрес]	Выборка событий, сгенерированных атакой на определенный адрес
важность: [уровень]	Выборка событий определенного уровня важности
действие: [Оповестить/Разрешить/Блокировать/Обнаружить/Перенаправить]	Выборка событий с определенным типом реакции на передаваемый трафик
домен_получателя: [доменное имя]	Выборка событий, сгенерированных на определенный домен
идентификатор сигнатуры: [SID]	Выборка событий, сгенерированных срабатыванием сигнатуры с определенным идентификатором
интерфейс: [текст]	Выборка событий, сгенерированных атакой на определенный интерфейс
класс: [текст]	Выборка записей, содержащих в поле "Класс" определенный текст
компонент: [подсистема]	Выборка событий определенной подсистемы
порт отправителя: [номер порта]	Выборка событий, сгенерированных атакой с определенного порта
порт получателя: [номер порта]	Выборка событий, сгенерированных атакой на определенный порт
протокол: [TCP/UDP]	Выборка событий, сгенерированных атакой по определенному протоколу
ревизия: [текст]	Выборка событий, сгенерированных срабатыванием сигнатуры с определенной версией
сигнатура: [текст]	Выборка записей, содержащих в поле "Сигнатура" определенный текст
срабатываний: [число]	Выборка групп с определенным числом событий
страна отправителя: [код страны]	Выборка событий, сгенерированных атаками от IP-адресов определенной страны
страна получателя: [код страны]	Выборка событий, сгенерированных атаками на IP-адреса определенной страны
узел: [имя узла безопасности]	Выборка записей с определенного УБ

Пример правила фильтрации:

Требуется найти сообщения об атаках с УБ 1.1.1.1 на УБ 2.2.2.2 и интерфейс Ethernet0.

Для этого введите в строке запроса:

адрес отправителя:1.1.1.1 и адрес получателя:2.2.2.2 и интерфейс:eth0

и нажмите кнопку "Применить".

Журнал управления

Журнал содержит сообщения событий системы, собранные со всех УБ домена, контролируемого текущим ЦУС.

В журнале содержится следующая информация:

- Важность сообщения — информация об уровне важности сообщения, показываемая соответствующим значком.

Важность сообщения			
Иконка	Уровень	Иконка	Уровень
	Авария		Тревога
	Критическая ошибка		Ошибка
	Предупреждение		Оповещение
	Информация		Отладка

- Дата — дата и время сообщения. Временная зона выбирается администратором системы мониторинга и аудита.
- Дата на узле безопасности — дата и время сообщения, представленные во временной зоне узла безопасности, на котором сгенерировано сообщение.
- Узел безопасности — узел безопасности, на котором сгенерировано сообщение.
- Категория — категория события.
- Хост — имя узла безопасности.
- Субъект — администратор, который совершил действие.
- Сообщение (срабатываний) — текст сообщения и количество срабатываний.

Для поиска нужных событий используйте фильтр, который настраивается с помощью следующих параметров:

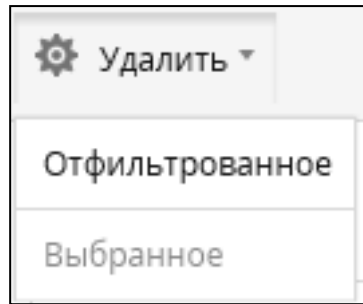
Тег	Пояснение
важность:[уровень]	Выборка сообщений определенного уровня важности
категория:[текст]	Выборка записей, содержащих в поле "Категория" определенный текст
сообщение:[текст]	Выборка записей, содержащих в поле "Сообщение" определенный текст
срабатываний:[]	Выборка групп с определенным числом событий
субъект:[]	Выборка событий, совершенных определенным администратором
хост:[имя хоста]	Выборка сообщений определенного хоста
категория:[тип]	События, относящиеся к указанному параметру узла безопасности
узел:[текст]	События, относящиеся только к указанному узлу безопасности

Очистка журналов

Для полной очистки журналов:

1. Перейдите в раздел "Журналы".
2. Выберите журнал для очистки.

3. Откройте выпадающее меню "Удалить" в верхней части рабочей области:



4. Нажмите кнопку "Отфильтрованное".

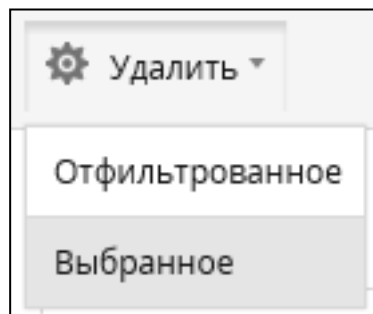
Если строка запроса в рабочей области пустая, то журнал выводит все записи. Таким образом, команда "Отфильтрованное" удаляет все записи журнала. Для очистки журнала от конкретных записей добавьте соответствующие фильтры в строку запроса.

Для удаления выбранных записей:

1. Выберите записи для удаления, проставив отметку в пустое поле таблицы.

<input type="checkbox"/>	Дата	Действие	Узел безопасности (интерфейс)	Компонент	Адрес отправителя
<input type="checkbox"/>	26.02.2019 10:22:35.493	Разрешить	node-1065	Межсетевой эк	93.191.9.124
<input type="checkbox"/>	26.02.2019 10:22:35.493	Оповещать	node-1065 (eth2)	СОВ	39.69.76.51
<input type="checkbox"/>	26.02.2019 10:22:35.492	Оповещать	node-1065	VPN	93.191.9.124
<input checked="" type="checkbox"/>	26.02.2019 10:22:35.492	Разрешить	node-1065 (eth3)	КП	77.104.1.22
<input checked="" type="checkbox"/>	26.02.2019 10:22:35.492	Блокировать	node-1065 (eth0)	СОВ	39.69.76.51
<input checked="" type="checkbox"/>	26.02.2019 10:22:35.492	Обнаружить	node-1065 (eth1)	КП	93.191.9.124
<input type="checkbox"/>	26.02.2019 10:22:35.492	Перенаправить	node-1065	VPN	77.104.1.22
<input type="checkbox"/>	26.02.2019 10:22:35.492	Оповещать	node-1065	VPN	39.69.76.51
<input type="checkbox"/>	26.02.2019 10:22:35.492	Разрешить	node-1065 (eth0)	КП	93.191.9.124

2. Откройте выпадающее меню "Удалить" в верхней части рабочей области. Кнопка "Выбранное" станет активной:



3. Нажмите кнопку "Выбранное". Отмеченные записи будут удалены.

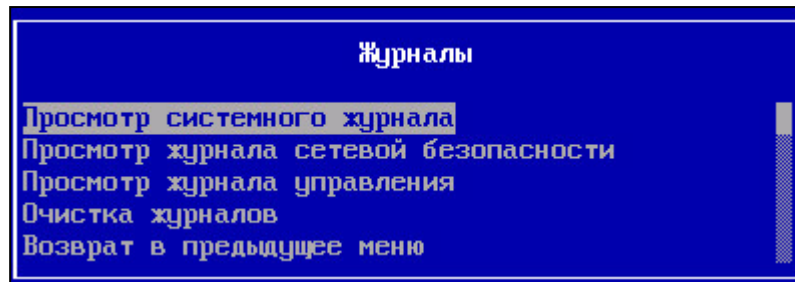
Примечание. Чтобы выделить все записи на текущей странице, отметьте пустое поле в заголовке таблицы.

Просмотр журналов с помощью локального меню

Для работы с журналами:

- Вызовите главное меню локального управления, выберите пункт "Журналы" и нажмите клавишу <Enter>.

На экране появится меню работы с журналами.

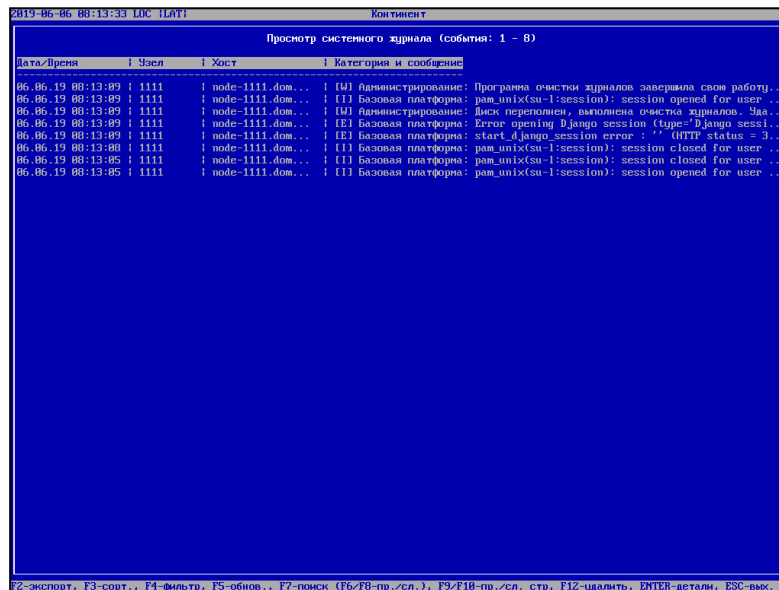


Системный журнал

Для просмотра журнала:

- Выберите в меню работы с журналами пункт "Просмотр системного журнала" и нажмите клавишу <Enter>.

На экране появится окно просмотра системного журнала.



Для каждого события приводится следующая информация:

- дата и время;
- хост;
- категория события;
- сообщение.

Для перемещения по списку используйте стандартные клавиши: <↑>, <↓>, <Page Down>, <Page Up>, <Home>.

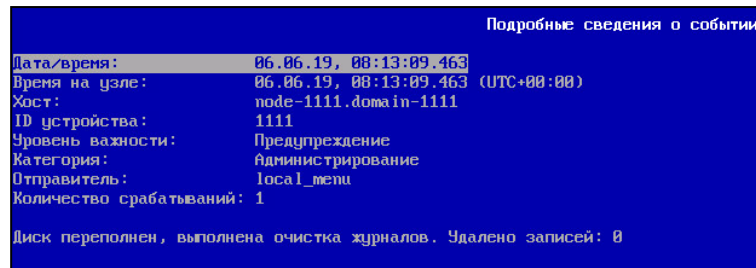
Для обновления журнала используйте клавишу <F5>.

Для возврата в меню работы с журналами нажмите клавишу <Esc>.

Для просмотра подробной информации о событии:

1. Выделите событие в списке и нажмите клавишу <Enter>.

На экране появится окно с подробными сведениями о выбранном событии.



Дополнительно приводятся следующие сведения:

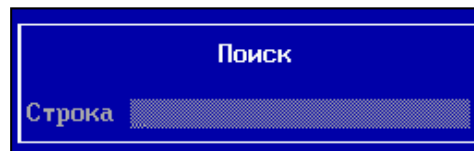
- номер УБ, на котором зафиксировано событие;
- уровень важности (полностью);
- источник;
- текст сообщения полностью.

2. Для возврата в окно просмотра журнала нажмите клавишу <Esc>.

Для поиска события по фрагменту текста сообщения:

1. Нажмите клавишу <F7>.

На экране появится окно для ввода фрагмента текста.



Введите фрагмент текста для поиска и нажмите клавишу <Enter>.

Начнется поиск события, содержащего в тексте сообщения введенный фрагмент. Поиск осуществляется вниз по списку от текущей выделенной записи.

Первое найденное событие будет выделено в списке.

2. Для продолжения поиска события с таким же фрагментом текста нажмите клавишу <F8>. При необходимости вернуться к предыдущему найденному событию нажмите клавишу <F6>.
3. Для изменения критерия поиска нажмите клавишу <F7>, введите новый фрагмент текста и нажмите клавишу <Enter>.

Начнется поиск вниз по списку от выделенной строки.

Для изменения направления поиска используйте клавишу <F8>.

Фильтр системного журнала

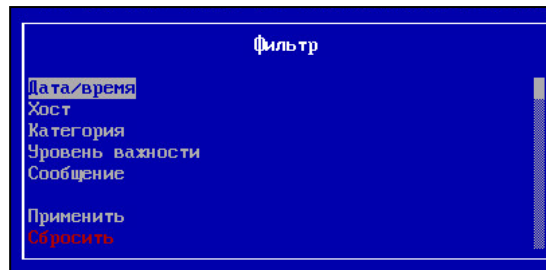
Для отображения определенных событий в окне просмотра системного журнала можно использовать фильтр, настраиваемый по следующим параметрам:

- дата и время;
- хост — источник события;
- категория сообщения;
- уровень важности;
- сообщение.

Для настройки фильтра:

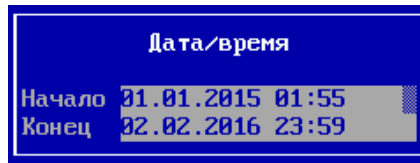
1. В окне просмотра системного журнала нажмите клавишу <F4>.

На экране появится меню настройки фильтра.



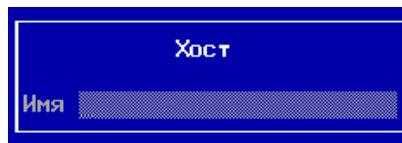
2. Выберите в меню параметр, нажмите клавишу <Enter> и задайте значение параметра.

- При настройке по дате и времени введите начало и конец периода в соответствии с приведенным ниже форматом.



Примечание. Для перемещения между вводимыми параметрами используйте стандартные клавиши: <↑>, <↓>.

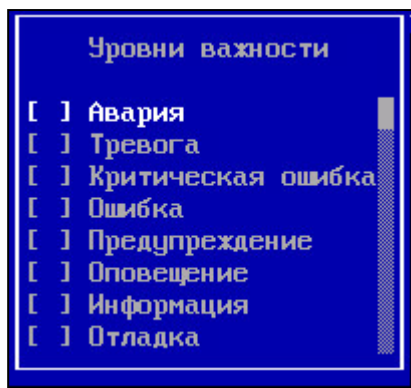
- При настройке по имени хоста введите имя или часть имени хоста. Данный фильтр удобно использовать для просмотра журналов в ЦУС, в котором отображаются события различных УБ сети.



- При настройке по категориям событий выделите клавишей <Пробел> категории, которые не должны отображаться в окне просмотра журнала.



- При настройке по уровню важности удалите клавишей <Пробел> ненужные уровни.



3. Нажмите клавишу <Enter>.

Будет выполнен возврат в меню настройки фильтра.

Примечание. После настройки по одному из параметров можно выполнить настройку по другому параметру (или параметрам). Для этого повторите выполнение пп. 2, 3.

4. Выберите пункт "Применить" и нажмите клавишу <Enter>.

В окне просмотра журнала отобразятся только те события, которые удовлетворяют настройкам фильтра.

5. Для обновления сведений нажмите клавишу <F5>.

Внимание! Для отмены действия фильтра выполните сброс его настроек.

Для сброса настроек фильтра:

1. В меню настройки фильтра выберите пункт "Сбросить".
2. Нажмите клавишу <Enter>.

Журнал сетевой безопасности

Для просмотра журнала:

- Выберите в меню работы с журналами пункт "Просмотр журнала сетевой безопасности" и нажмите клавишу <Enter>.

На экране появится окно просмотра журнала узла безопасности.

2018-05-16 12:58:02 UTC (ПЯТ)		Континент 4.0		Просмотр журнала сетевой безопасности (события: 1 - 1800)							
Дата/время	Чел	Компонент	Источник	Принимки	Протокол	Действие					
16.05.18 12:54:11	1806	Д	1117.222.32.135	1145.183.39.225	1	pkthdr	1	Заблокировано(6)			
16.05.18 12:54:11	1815	Д	188.197.189.59	1145.85.128.229	1	tcp-stream	1	Заблокировано(1)			
16.05.18 12:54:11	1806	Д	1182.24.180.78	1169.26.288.213	1	icmp6	1	Оповестить			
16.05.18 12:54:11	1815	Д	1117.38.52.145	1121.199.134.72	1	ip6	1	Заблокировано(5)			
16.05.18 12:54:11	1806	Д	1227.35.137.162	1282.118.198.2251	1	pkthdr	1	Оповестить(6)			
16.05.18 12:54:11	1815	Д	1146.194.28.145	1229.7.142.189	1	icmp6	1	Заблокировано(3)			
16.05.18 12:54:11	1815	Д	18.67.155.226	125.65.148.216	1	smtp	1	Заблокировано(1)			
16.05.18 12:54:11	1815	Д	1223.9.114.52	1119.112.113.1581	1	snmp	1	Оповестить(9)			
16.05.18 12:54:11	1806	Д	145.241.158.58	1152.55.198.117	1	tcp	1	Заблокировано(3)			
16.05.18 12:54:11	1807	Д	1162.234.237.98	115.59.27.168	1	tcp	1	Оповестить(6)			
16.05.18 12:54:11	1806	Д	176.211.59.28	136.183.43.2	1	tls	1	Оповестить(2)			
16.05.18 12:54:11	1818	Д	175.228.187.59	1122.288.127.1331	1	tls	1	Оповестить(18)			
16.05.18 12:54:11	1807	Д	176.98.229.123	1112.172.23.34	1	ftp	1	Заблокировано			
16.05.18 12:54:11	1818	Д	1124.244.158.1831121.167.234.1181		1	tcp-stream	1	Заблокировано(1)			
16.05.18 12:54:11	1818	Д	174.155.229.166	118.167.186.69	1	tcp-stream	1	Оповестить(5)			
16.05.18 12:54:11	1806	Д	1126.239.32.235	1181.255.193.36	1	snmp	1	Оповестить(2)			
16.05.18 12:54:11	1872	Д	176.111.45.179	1125.238.41.36	1	smtp	1	Оповестить(4)			
16.05.18 12:54:11	1807	Д	1253.188.65.188	1171.37.16.18	1	icmp4	1	Оповестить(3)			
16.05.18 12:54:11	1818	Д	1114.17.93.158	1182.232.43.183	1	http	1	Оповестить(18)			
16.05.18 12:54:11	1818	Д	1151.33.35.14	281.124.68.69	1	ip6	1	Оповестить			
16.05.18 12:54:11	1807	Д	148.138.33.192	1129.148.186.1461	1	snmp	1	Заблокировано(5)			
16.05.18 12:54:11	1806	Д	1214.28.282.235	1188.232.128.14	1	icmp4	1	Заблокировано			
16.05.18 12:54:11	1815	Д	1164.119.153.2281133.16.141.146		1	tcp-stream	1	Заблокировано(1)			
16.05.18 12:54:11	1818	Д	1184.181.197.116179.27.66.286		1	udp	1	Оповестить(6)			
16.05.18 12:54:11	1818	Д	1121.185.65.221	137.236.51.31	1	dccprrdnc	1	Оповестить(1)			
16.05.18 12:54:11	1807	Д	1214.61.43.167	195.182.96.181	1	ip	1	Заблокировано(6)			
16.05.18 12:54:11	1807	Д	1288.247.82.286	1134.15.3.1	1	dccprrdnc	1	Заблокировано(1)			
16.05.18 12:54:11	1815	Д	1239.81.36.12	1233.99.127.18	1	udp	1	Заблокировано(1)			
16.05.18 12:54:11	1807	Д	1184.53.138.7	132.153.199.165	1	pkthdr	1	Заблокировано(9)			
16.05.18 12:54:11	1872	Д	1173.44.48.118	1285.127.244.2531	1	ip6	1	Заблокировано(1)			
16.05.18 12:54:11	1818	Д	1138.43.148.185	1159.219.68.112	1	ip6	1	Заблокировано(9)			
16.05.18 12:54:11	1818	Д	1245.78.212.283	1189.243.122.1281	1	http	1	Заблокировано(6)			
16.05.18 12:54:11	1807	Д	1127.226.211.1851148.225.86.177		1	icmp4	1	Заблокировано(6)			
16.05.18 12:54:11	1807	Д	18.199.181.78	1188.41.222.238	1	dccprrdnc	1	Заблокировано(8)			
16.05.18 12:54:11	1818	Д	1138.43.148.185	1159.219.68.112	1	ip6	1	Заблокировано(8)			
16.05.18 12:54:11	1818	Д	1245.78.212.283	1189.243.122.1281	1	http	1	Оповестить(9)			
16.05.18 12:54:11	1815	Д	1142.116.121.69	176.139.48.12	1	pkthdr	1	Оповестить(6)			
16.05.18 12:54:11	1806	Д	1153.112.115.25	18.171.118.252	1	tls	1	Заблокировано(8)			
16.05.18 12:54:11	1818	Д	1186.169.145.1	116.98.48.15	1	ftp	1	Заблокировано(8)			
16.05.18 12:54:11	1806	Д	149.119.226.46	159.212.51.284	1	ssh	1	Заблокировано(5)			
16.05.18 12:54:11	1872	Д	1241.86.77.198	187.111.45.15	1	tcp-stream	1	Заблокировано(6)			

В окне просмотра отображается список всех хранящихся в журнале событий.

В заголовке журнала приводится количество событий, зарегистрированных за определенный интервал времени (по умолчанию — 10 секунд). Повторы

одного и того же события за этот интервал времени представлены в журнале одной записью.

Для каждого события приводится следующая информация:

- дата и время;
- узел безопасности;
- компонент;
- IP-адрес источника атаки;
- IP-адрес приемника атаки;
- тип протокола;
- действие.

Для перемещения по списку используйте стандартные клавиши: <↑>, <↓>, <Page Down>, <Page Up>, <Home>.

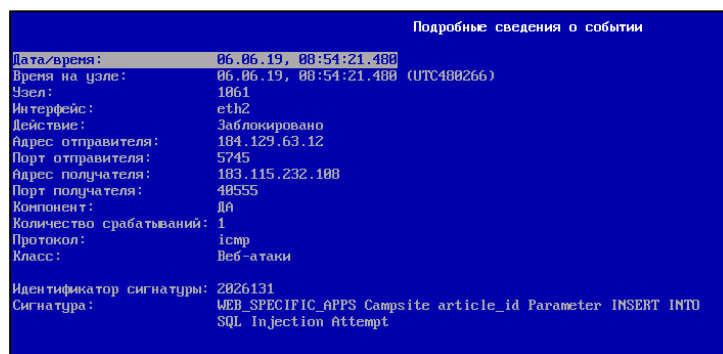
Для обновления журнала используйте клавишу <F5>.

Для возврата в меню работы с журналами нажмите клавишу <Esc>.

Для просмотра подробной информации о событии:

1. Выделите событие в списке и нажмите клавишу <Enter>.

На экране появится окно с подробными сведениями о выбранном событии.



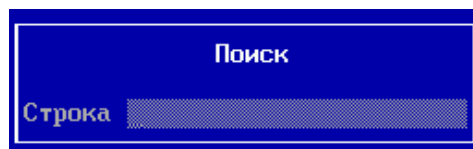
Дополнительно приводятся следующие сведения:

- порт источника;
 - порт приемника;
 - протокол;
 - категория;
 - полное описание сигнатуры.
2. Для возврата в окно просмотра журнала нажмите клавишу <Enter> или <Esc>.

Для поиска события по фрагменту описания сигнатуры:

1. Нажмите клавишу <F7>.

На экране появится окно для ввода фрагмента описания сигнатуры.



Введите фрагмент описания сигнатуры для поиска и нажмите клавишу <Enter>.

Начнется поиск события, содержащего в описании сигнатуры введенный фрагмент. Поиск осуществляется вниз по списку от текущей выделенной записи.

Первое найденное событие будет выделено в списке.

2. Для продолжения поиска события с таким же фрагментом описания сигнатуры нажмите клавишу <F8>. При необходимости вернуться к предыдущему найденному событию нажмите клавишу <F6>.
3. Для изменения критерия поиска нажмите клавишу <F7>, введите новый фрагмент текста и нажмите клавишу <Enter>. Начнется поиск вниз по списку от выделенной строки.
Для изменения направления поиска используйте клавишу <F8>.

Фильтр журнала сетевой безопасности

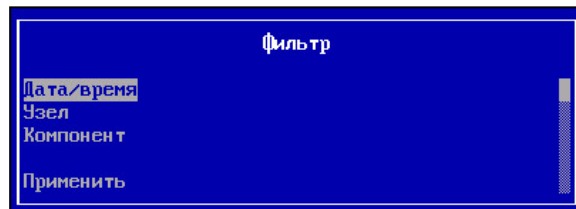
Для отображения определенных событий в окне просмотра журнала сетевой безопасности используйте фильтр, настраиваемый по следующим параметрам:

- дата и время;
- серийный номер узла безопасности;
- компонент.

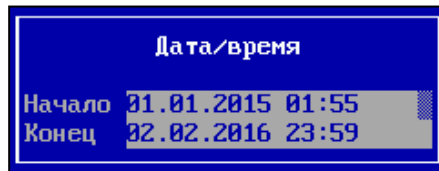
Примечание. Фильтр по серийному номеру узла безопасности рекомендуется использовать при просмотре журнала в ЦУС.

Для настройки фильтра:

1. В окне просмотра журнала сетевой безопасности нажмите клавишу <F4>. На экране появится меню настройки фильтра.



2. Выберите в меню параметр, нажмите клавишу <Enter> и задайте его значение.
 - При настройке по дате и времени введите начало и конец периода в соответствии с форматом, приведенным ниже:



Примечание. Для перемещения между вводимыми параметрами используйте стандартные клавиши: <↑>, <↓>.

- При настройке по серийному номеру узла безопасности введите номера или несколько номеров, используя запятую:



- При настройке по компонентам отбираются события по системам, которые зарегистрировали событие в журнале:



3. После настройки параметра нажмите клавишу <Enter>.

Будет выполнен возврат в меню настройки фильтра.

Примечание. После настройки по одному из параметров можно выполнить настройку по другому параметру. Для этого повторите выполнение пп. 2, 3.

4. Выберите пункт "Применить" и нажмите клавишу <Enter>.

В окне просмотра журнала отобразятся только те события, которые удовлетворяют настройкам фильтра.

5. Для обновления сведений нажмите клавишу <F5>.

Внимание! Для отмены действия фильтра выполните сброс его настроек.

Для сброса настроек фильтра:

1. В меню настройки фильтра выберите пункт "Сбросить".
2. Нажмите клавишу <Enter>.

Журнал управления

Для просмотра журнала:

- Выберите в меню работы с журналами пункт "Журнал управления" и нажмите клавишу <Enter>.

На экране появится окно просмотра журнала управления.

Дата/Время	Узел	Хост	Субъект	Категория и сообщение
06.06.19 08:56:36	1954	node-1954.doma...	superuser	[1] Администрирование: Просмотр журнала управления
06.06.19 08:55:29	1954	node-1954.doma...	superuser	[1] Администрирование: Просмотр журнала сетевой безо
06.06.19 08:55:21	1954	node-1954.doma...	admin	[1] Управление: Администратор выполнил Выход в блонд
06.06.19 08:55:19	1954	node-1954.doma...	admin	[1] Управление: Администратор выполнил вход. Резуль
06.06.19 08:55:19	1954	node-1954.doma...	admin	[1] Управление: Администратор выполнил вход. Резуль
06.06.19 08:55:17	1954	node-1954.doma...	admin	[1] Администрирование: Вход в систему
06.06.19 13:23:58	1954	node-1954.doma...	admin	[1] Управление: Администратор выполнил выход. Резуль
06.06.19 13:23:58	1954	node-1954.doma...	admin	[1] Управление: Администратор выполнил Снятие блонд
06.06.19 13:23:13	1954	node-1954.doma...	admin	[1] Управление: Администратор выполнил формирование
06.06.19 13:23:06	1954	node-1954.doma...	admin	[1] Управление: Администратор выполнил формирование
06.06.19 13:22:57	1954	node-1954.doma...	admin	[1] Управление: Администратор выполнил формирование
06.06.19 13:22:15	1887	node-1887.doma...	admin	[1] Управление: Администратор выполнил формирование
06.06.19 13:22:13	1954	node-1954.doma...	admin	[1] Управление: Администратор выполнил формирование
06.06.19 13:22:13	1954	node-1954.doma...	admin	[1] Управление: Администратор выполнил формирование
06.06.19 13:22:07	1954	node-1954.doma...	admin	[1] Управление: Администратор выполнил формирование
06.06.19 13:21:37	1955	node-1955.doma...	admin	[1] Управление: Администратор выполнил формирование
06.06.19 13:21:32	1954	node-1954.doma...	admin	[1] Управление: Администратор выполнил формирование
06.06.19 13:21:26	1886	node-1886.doma...	admin	[1] Управление: Администратор выполнил формирование
06.06.19 13:21:25	1954	node-1954.doma...	admin	[1] Управление: Администратор выполнил формирование
06.06.19 13:21:16	1954	node-1954.doma...	admin	[1] Управление: Администратор выполнил формирование
06.06.19 13:21:16	1954	node-1954.doma...	admin	[1] Управление: Администратор выполнил формирование
06.06.19 13:20:54	1954	node-1954.doma...	admin	[1] Управление: Администратор выполнил формирование
06.06.19 13:20:58	1861	node-1861.doma...	admin	[1] Управление: Администратор выполнил формирование
06.06.19 13:19:39	1954	node-1954.doma...	admin	[1] Управление: Администратор выполнил формирование
06.06.19 13:19:38	1954	node-1954.doma...	admin	[1] Управление: Администратор выполнил Сохранение ко
06.06.19 13:19:36	1954	node-1954.doma...	admin	[1] Управление: Администратор обновил объект типа Уз
06.06.19 13:16:47	1886	node-1886.doma...	admin	[1] Управление: Администратор выполнил формирование
06.06.19 13:16:43	1887	node-1887.doma...	admin	[1] Управление: Администратор выполнил формирование
06.06.19 13:12:44	1954	node-1954.doma...	admin	[1] Управление: Администратор выполнил Перегрузка
06.06.19 13:12:01	1887	node-1887.doma...	admin	[1] Администрирование: Вход в систему
06.06.19 13:09:53	1954	node-1954.doma...	admin	[1] Управление: Администратор выполнил формирование
06.06.19 13:09:42	1954	node-1954.doma...	admin	[1] Управление: Администратор выполнил формирование
06.06.19 13:09:42	1954	node-1954.doma...	admin	[1] Управление: Администратор выполнил формирование
06.06.19 13:09:40	1954	node-1954.doma...	admin	[1] Управление: Администратор выполнил формирование
06.06.19 13:08:52	1887	node-1887.doma...	admin	[1] Управление: Администратор выполнил формирование
06.06.19 13:08:48	1954	node-1954.doma...	admin	[1] Управление: Администратор выполнил формирование
06.06.19 13:08:42	1954	node-1954.doma...	admin	[1] Управление: Администратор выполнил формирование
06.06.19 13:07:51	1954	node-1954.doma...	admin	[1] Управление: Администратор выполнил формирование
06.06.19 13:07:51	1954	node-1954.doma...	admin	[1] Управление: Администратор выполнил формирование
06.06.19 13:07:58	1955	node-1955.doma...	admin	[1] Управление: Администратор выполнил формирование

В окне просмотра отображается список всех хранящихся в журнале событий. Для каждого события приводится следующая информация:

- дата и время;
- хост;
- субъект;
- категория и действие.

Для перемещения по списку используйте стандартные клавиши: <↑>, <↓>, <Page Down>, <Page Up>, <Home>.

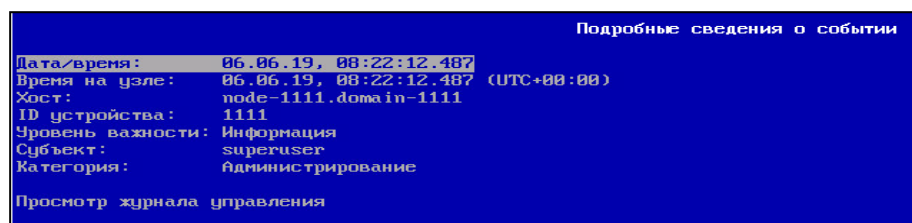
Для обновления журнала используйте клавишу <F5>.

Для возврата в меню работы с журналами нажмите клавишу <Esc>.

Для просмотра подробной информации о событии:

1. Выделите событие в списке и нажмите клавишу <Enter>.

На экране появится окно с подробными сведениями о выбранном событии.



Дополнительно приводятся следующие сведения:

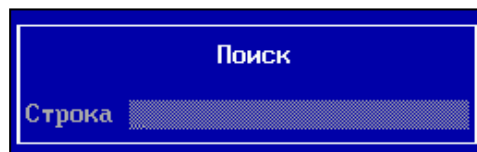
- номер УБ, на котором зафиксировано событие;
- уровень важности (полностью);
- текст сообщения полностью.

2. Для возврата в окно просмотра журнала нажмите клавишу <Esc>.

Для поиска события по фрагменту текста сообщения:

1. Нажмите клавишу <F7>.

На экране появится окно для ввода фрагмента текста.



Введите фрагмент текста для поиска и нажмите клавишу <Enter>.

Начнется поиск события, содержащего в тексте сообщения введенный фрагмент. Поиск осуществляется вниз по списку от текущей выделенной записи.

Первое найденное событие будет выделено в списке.

2. Для продолжения поиска события с таким же фрагментом текста нажмите клавишу <F8>. При необходимости вернуться к предыдущему найденному событию нажмите клавишу <F6>.
3. Для изменения критерия поиска нажмите клавишу <F7>, введите новый фрагмент текста и нажмите клавишу <Enter>.

Начнется поиск вниз по списку от выделенной строки.

Для изменения направления поиска используйте клавишу <F8>.

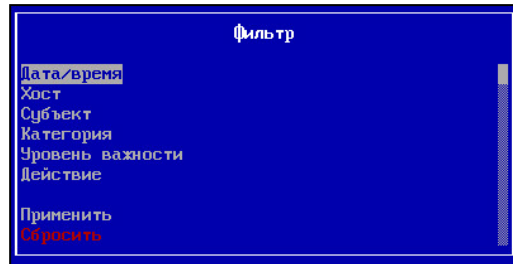
Фильтр журнала управления

Для отображения определенных событий в окне просмотра журнала управления можно использовать фильтр, настраиваемый по следующим параметрам:

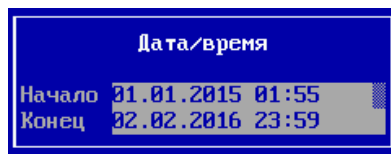
- дата и время;
- хост — источник события;
- субъект;
- категория сообщения;
- уровень важности;
- сообщение.

Для настройки фильтра:

1. В окне просмотра системного журнала нажмите клавишу <F4> .
На экране появится меню настройки фильтра.

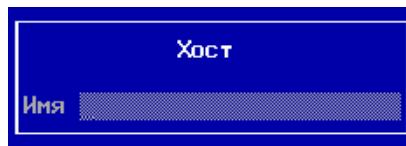


2. Выберите в меню параметр, нажмите клавишу <Enter> и задайте значение параметра.
 - При настройке по дате и времени введите начало и конец периода в соответствии с приведенным ниже форматом.

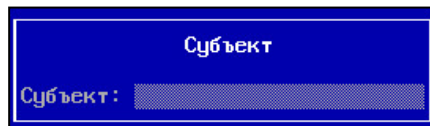


Примечание. Для перемещения между вводимыми параметрами используйте клавиши курсоров: <↑>, <↓>.

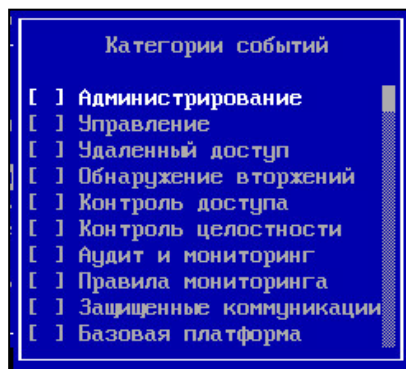
- При настройке по имени хоста введите имя или часть имени хоста. Данный фильтр удобно использовать для просмотра журналов в ЦУС, в котором отображаются события различных УБ сети.



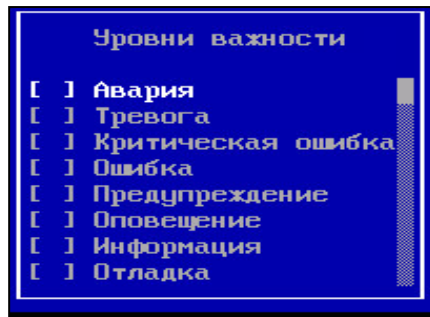
- При настройке по имени субъекта введите имя или часть имени субъекта.



- При настройке по категориям событий выделите клавишей <Пробел> категории, которые не должны отображаться в окне просмотра журнала.



- При настройке по уровню важности удалите клавишей <Пробел> уровни, не используемые при поиске событий.



3. Нажмите клавишу <Enter>.

Будет выполнен возврат в меню настройки фильтра.

Примечание. После настройки по одному из параметров можно выполнить настройку по другому параметру (или параметрам). Для этого повторите выполнение пп. 2, 3.

4. Выберите пункт "Применить" и нажмите клавишу <Enter>.

В окне просмотра журнала отобразятся только те события, которые удовлетворяют настройкам фильтра.
5. Для обновления сведений нажмите клавишу <F5>.

Внимание! Для отмены действия фильтра выполните сброс его настроек.

Для сброса настроек фильтра:

1. В меню настройки фильтра выберите пункт "Сбросить".
2. Нажмите клавишу <Enter>.

Экспорт журналов

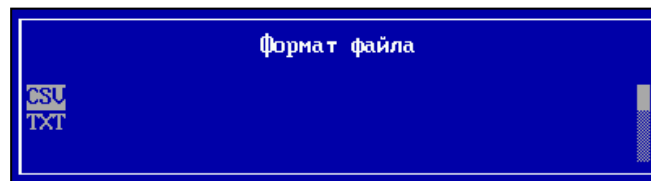
В системе предусмотрен экспорт журналов на внешний носитель с помощью локального меню.

В качестве внешнего носителя используется USB-флеш-накопитель, на котором журналы сохраняются в файлах формата TXT или CSV.

Для экспорта журнала:

1. Откройте окно просмотра журнала.
2. При необходимости настройте и примените фильтр.
3. Нажмите клавишу <F2>.

На экране появится окно выбора формата файла.



4. Выберите формат и нажмите клавишу <Enter>.

На экране появится сообщение о необходимости вставить внешний носитель.
5. Подключите USB-флеш-накопитель и нажмите клавишу <Enter>.

Начнется запись файла на внешний носитель. Дождитесь сообщения об успешном завершении операции.
6. Извлеките внешний носитель и нажмите клавишу <Enter>.

Будет выполнен возврат в окно просмотра журнала.

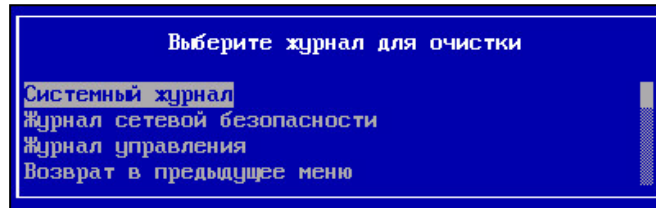
Очистка журналов

В системе предусмотрены несколько вариантов очистки журналов: автоматическая, по расписанию, полная и за указанный период. Автоматическая очистка и очистка журналов по расписанию настраиваются с помощью МК (см. стр. 46). Полная очистка журналов и очистка за указанный период настраиваются с помощью локального меню (см. ниже).

Для удаления записей журнала:

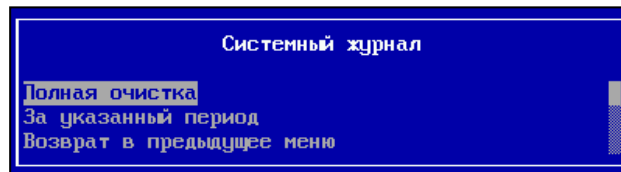
1. Откройте меню работы с журналами, выберите пункт "Очистка журналов" и нажмите клавишу <Enter>.

На экране появится меню выбора журнала для очистки.



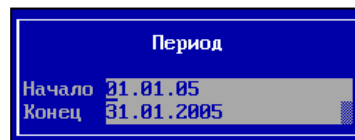
2. Выберите журнал и нажмите клавишу <Enter>.

На экране появится меню выбора варианта очистки.



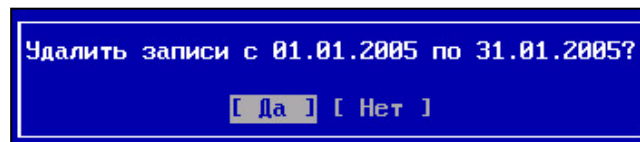
3. Выберите вариант и нажмите клавишу <Enter>.

- Если был выбран вариант "Полная очистка", на экране появится запрос на подтверждение удаления записей. Нажмите "Да".
- Начнется очистка журнала. Дождитесь сообщения "Журнал очищен".
- Если был выбран вариант "За указанный период", на экране появится окно для ввода начала и конца периода.



- Укажите начало и конец периода и нажмите клавишу <Enter>.

На экране появится запрос на подтверждение удаления записей за указанный период.



- Выберите "Да" и нажмите клавишу <Enter>.

Начнется удаление записей. Дождитесь сообщения "Журнал очищен".

4. Нажмите клавишу <Enter>.

Будет выполнен возврат в меню выбора варианта очистки журнала.

Примечание. Для удаления отфильтрованных записей откройте журнал, примените фильтр и нажмите клавишу <F12>.

Передача сведений в ГосСОПКА

Для передачи сведений в ГосСОПКА предварительно необходимо выполнить следующее:

1. Установить и настроить защищенный канал между локальными сетями АПКШ "Континент" и ГосСОПКА.

Для реализации защищенного канала используют решение "абонентский пункт — сервер доступа". Установку и настройку соединения абонентского пункта с сервером доступа выполняют в соответствии с описанием, приведенным в эксплуатационной документации на абонентский пункт. Для получения значений параметров настройки необходимо обратиться в службу технической поддержки ООО "Код Безопасности".

2. Настроить параметры работы Клиента (см. далее).

Настройка параметров клиента ГосСОПКА

Для настройки параметров:

1. Раскройте в иерархическом списке объектов узел "Детекторы атак", вызовите контекстное меню любого из детекторов атак и выберите пункт "Экспорт журналов на внешний сервер (ГосСОПКА)".

На экране появится диалог "Клиент ГосСОПКА".

2. Перейдите на вкладку "Настройки" и укажите нужные значения параметров.

Параметр	Описание
Адрес сервера	IP-адрес или DNS веб-сервера, расположенного в локальной сети ГосСОПКА
Порт	Используемый порт веб-сервера

3. Удалите отметку в поле "Использовать TLS-клиент".

Примечание. Поле используется в том случае, если в качестве защищаемого канала применяется решение "TLS-клиент — TLS-сервер". В текущей версии не поддерживается.

4. Если в качестве защищенного канала используется вариант TLS-клиент — TLS-сервер, установите отметку в поле "Использовать TLS-клиент" и укажите параметры:

Параметр	Описание
Адрес	IP-адрес компьютера с установленным TLS-клиентом
Порт TLS-клиента	Используемый порт TLS-клиента

5. Нажмите кнопку "Сохранить".

Примечание. Значения остальных параметров на вкладке "Настройки" заполняются автоматически.

Отправка сведений

Для отправки сведений:

1. В зависимости от используемого защищенного соединения установите соединение с сервером доступа или с TLS-сервером.

Примечание. При первом соединении с TLS-сервером необходимо указать сертификат, предъявить ключи и ввести пароль.

2. Вызовите контекстное меню узла "Детекторы атак" и выберите пункт "Экспорт журналов на внешний сервер (ГосСОПКА)".

На экране появится диалог "Клиент ГосСОПКА" с открытой вкладкой "Отчет".

По умолчанию временной интервал, за который будут отправлены сведения, составляет неделю.

3. Выберите из раскрывающегося списка детектор атак.

Начнется подсчет количества записей за указанный временной интервал и результат отобразится в нижней части диалога.

4. Если необходимо изменить временной интервал, введите новые значения.

Начнется пересчет количества записей.

Внимание! Пересчет количества записей происходит после каждого изменения значений в полях "Детектор атак" и "Временной диапазон".

5. Нажмите кнопку "Отправить".

Начнется передача сведений веб-серверу.

Дождитесь сообщения об успешной отправке сведений.

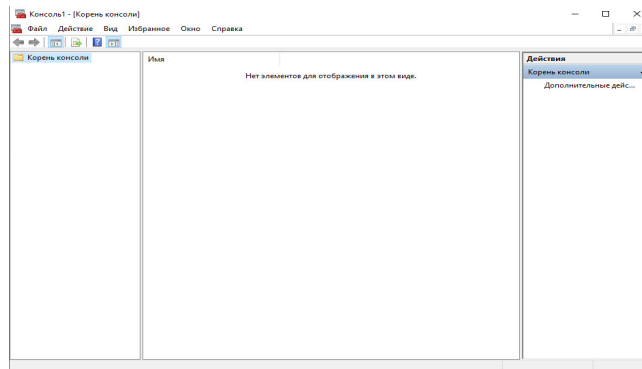
Приложение

Установка CRL-сертификата

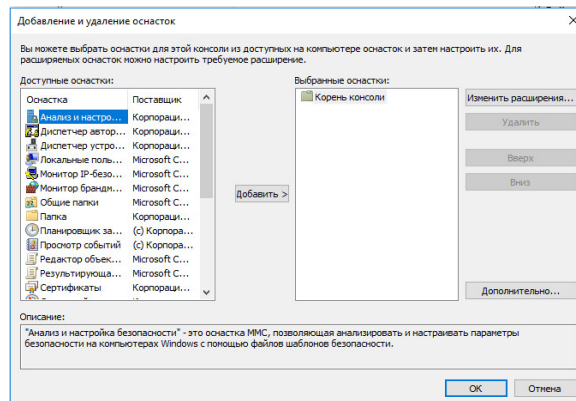
Для установки CRL-сертификата в хранилище сертификатов Windows на локальном компьютере добавьте соответствующую оснастку и осуществите импорт CRL-файла в доверенные корневые центры сертификации.

Для подключения оснастки "Сертификаты" в консоли MMC:

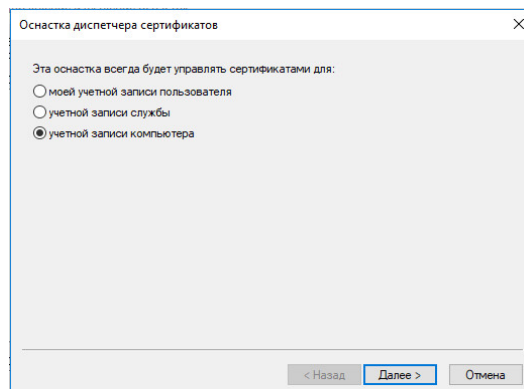
1. Откройте окно команды "Выполнить", нажав сочетание клавиш <Win> + <R>.
2. Введите "mmc" и нажмите клавишу <Enter>.



3. В меню "Файл" выберите команду "Добавить или удалить оснастку...".



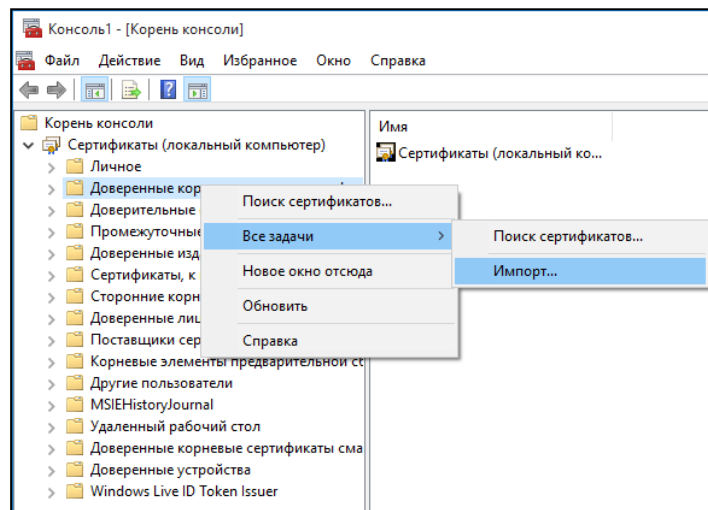
4. В открывшемся диалоговом окне "Добавление или удаление оснасток" в списке доступных оснасток выберите "Сертификаты". Нажмите кнопку "Добавить". Откроется окно "Оснастка диспетчера сертификатов".



5. В диалоговом окне "Оснастка диспетчера сертификатов" установите переключатель в положение учетной записи компьютера и нажмите кнопку "Далее".
6. В диалоговом окне "Выбор компьютера" нажмите кнопку "Готово".
7. В диалоговом окне "Добавление или удаление оснасток" нажмите кнопку "ОК".
8. В корне консоли откройте узел "Сертификаты (локальный компьютер)", чтобы просмотреть хранилища сертификатов для данного компьютера.
9. В меню "Файл" выберите команду "Сохранить как...", укажите место сохранения командной консоли для последующих импортов CRL-файлов и нажмите кнопку "Сохранить".

Для импорта CRL-файла:

1. Откройте командную консоль и разверните дерево сертификатов локального компьютера.
2. Выберите пункт "Доверенные корневые центры сертификации" и вызовите его контекстное меню.



3. Выберите команду "Все задачи | Импорт".
На экране появится окно мастера импорта сертификатов.
4. Нажмите кнопку "Далее" и в диалоговом окне импортируемого файла нажмите кнопку "Обзор...".
5. В открывшемся диалоге выбора файла укажите тип открываемого сертификата и путь к CRL-файлу.
6. Выберите нужный файл и нажмите кнопку "Открыть".
7. В диалоговом окне импортируемого файла нажмите кнопку "Далее".
8. В диалоговом окне выбора хранилища сертификатов выберите пункт "Доверенные корневые центры сертификации" и нажмите кнопку "Далее".
9. В окне мастера импорта сертификатов нажмите кнопку "Готово".

Документация

1. Программный комплекс "Континент-COA". Версия 4. Руководство администратора. Обнаружение вторжений.
2. Программный комплекс "Континент-COA". Версия 4. Руководство администратора. Ввод в эксплуатацию.
3. Средство криптографической защиты информации "Континент TLS VPN Клиент". Версия 1.2. Руководство по эксплуатации.