

Программный комплекс Континент-СОА Версия 4

Руководство администратора Мониторинг и аудит

RU.AMEC.58.29.12.008 90 3



© 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
Введен	ие	. 6
060040	сродония	7
оощие		. 7
	Пазначение и основные функции	/
	Принципы функционирования	/
	Объекты мониторинта	/
	Типы и источники отооражаемой информации	. /
	Правила и шаолоны Статусы объектов	ט פ
	Запуск Менелжера конфигурации	0 g
Hactro		
пастро		11.
	Настройка с помощью алгоритмат ОСТР 54.11-2012	11
	пастройка с помощью КЗА	. 12
Монито	оринг	.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
	Настроика панели мониторинга	. 30
	Раздел Статистика	39
	Управление виджетами	39 40
	Просмотр отчетов	40 //1
	Режимы мониторинга	42
	Разлел "Настройки"	42
•		
Аудит		.43
	Параметры журналирования	.43
	уровень детализации журналов	44
	Настроика хранения журналов на внешнем syslog-сервере	. 44
	Пастроика автоматической очистки журналов	.40 //7
	Просмотр журналов во внешней базе данных	.47 //Q
	Просмотр журналов с помощью вео-интерфейса	50
	Журнал сетевой безопасности	
	Журнал селевой осволаености	
	Очистка журналов	53
	Просмотр журналов с помошью локального меню	.54
	Системный журнал	55
	Журнал сетевой безопасности	
	Журнал управления	61
	Экспорт журналов	.64
	Очистка журналов	.65
	Передача сведений в ГосСОПКА	.66
	Настройка параметров клиента ГосСОПКА	. 66
	Отправка сведений	66
Придо		60
прило		.00
	установка СКС-сертификата	. 08

Документация	۹	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
COB	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-COA". Версия 4" RU.AMБС.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 <u>https://www.securitycode.ru</u>/.

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 <u>https://www.securitycode.ru/company/education/training-courses/</u>. 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, межсетевого экранирования 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.

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

Источники для каждого из типов информации приведены в таблице ниже:

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 "Закрыто", 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 "Закрыто" 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" I "Менеджер конфигурации" или на рабочем столе ОС Windows ярлык приложения "Менеджер конфигурации".

На экране появится окно "Менеджер конфигурации".

Контроль доступа Виртуальные частные сети Структура Система обнаружения вторжений Структура Система обнаружения вторжений Структура Система обнаружения вторжений Структура Система обнаружения вторжений Структура Система обнаружения вторжений Система обнаружения вторжений	Гавная Вид	Континент. Менеджер конфигу	грации	× ^ ?
Структура Узлы 6 Панепь быстрого доступа Панель отображения информации Контроль доступа Виртуальные частные сети Осистема обнаружения вторжений Статус Панель инструментов Статус Панель отображения инструментов Статус Строка состояния Строка	Создать Назад Впер Узел Кластер безопасности безопасности Создать	Список Иерархия	Свойства С О Свойства Уста	новить Мониторинг
быстрого доступа Панель отображения информации Статус Панель отображения информации Контроль доступа Виртуальные частные сети Осистема обнаружения вторжений Структура Администрирование У	Структура	Узлы безопасности (0) Поиск		٩
Панепь отображения информации Виртуальные частные сети Система обнаружения вторжений Сруктура Администрирование »	быстрого доступа	Название	Панель инструментов	Статус ,
	Панепь отображения информации Контроль доступа Виртуальные частные сети ОСистема обнаружения вторжений Структура Администрирование	Панепь навигации		Строка состояния

Рис.1 Окно "Менеджер конфигурации"

	0							
элемент интерфеиса	Описание							
Панель инструментов	 "Главная" — отображает панель инструментов; "Вид" — настраивает отображения элементов окна Менеджера конфигурации. 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 							
Панель быстрого доступа	Предназначена для быстрого доступа к часто используемым командам. Содержит настраиваемые кнопки: — 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	 Содержит следующие разделы: "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	Предназначена для отображения информации выбранного раздела панели навигации							
Строка состояния	 Содержит следующие данные: 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 admin) 							

Окно "Менеджер конфигурации" содержит следующие основные элементы интерфейса:

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.

Алминистрирование	Сертификаты (3)					
😤 Администраторы	Поиск					Q
Роли	Название	Кем выдан	Действителен с	Действителен по	Статус	Описание
🖂 🔚 Сертификаты	toot	root	10.05.2018 12:59	09.05.2023 12:59	Действителен	/C=RU /0=000 Test.corp /0U=0IT
Корневые центры се	Поверенный Изратерь КБ	Ловеренный Израт	30.05 2017 16:34	30 05 2028 16:44	Лействитерен	/ОнООО Кол Безопасности / нМо
Промежуточные це	Konuend centraties at RSA and	Кориевой септити	10.05 2018 13:18	09.05.2023.13:18	Пействителен	(C=BU/0=000 Test com /0U=0IT
Помень		Tophood out out internal	10.00.2010 10.10	00.00.2020 10.10	22010101010101	10-1010-000 104.000100-011
LDAP						
С Обновления						
Резервные копии						
📑 Лицензии						
🗾 Задачи						
I F						
Контроль доступа						
Виртуальные частные сети						
🔘 Система обнаружения втор						
🄯 Структура						Активация Windows
Администрирование						Чтобы активировать Windows, перейдите в

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.

Алминистрирование	Сертификаты (3)							
. Администраторы	Поиск							Q
В Роли		Сертифи	кат			E	Зладелец	
Сертификаты	Кем выдан 🗸 🗸 🗸	Название	Действителен с	Действителен по	Статус	Имя	Тип ресурса	
Промежуточные центры сертификации	Корневой сертификат RSA для LLVC №199	inon-aes	10.05.2018 13:19	10.05.2019 13:19	Действителен	🚥 mon-aes	Узел безопасности	
Персональные сертификаты	root	in managment	10.05.2018 12:59	10.05.2019 12:59	Действителен	- managment	Узел безопасности	
Домены	root	🕞 ub 188	10.05.2018 13:13	10.05.2019 13:13	Действителен	🚥 ub 188	Узел безопасности	
Ф LDAP								
Резервные копии								
📑 Лицензии								
🔳 Задачи								
Контроль доступа								
Виртуальные частные сети								
🔘 Система обнаружения вторжений								
🏟 Структура						Активация	a Windows	
Администрирование						Чтобы активи раздел "Пара	провать Windows, пе метры".	ерейдите в

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://aдрес_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:

- 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".
- Найдите в начальной части файла строку (для поиска целесообразно использовать сочетание клавиш <Ctrl> + <F>) и впишите адрес_мониторинга: monitoring_url="adpec_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".

Сертификаты	
Сертификаты 9Ц Сертификаты управления Корневые сертификаты RSA Сертификаты безопасности веб-сервера мониторинга (RSA) Сертификаты SSL/TLS-инспекции (RSA) Отозванные сертификаты Возврат в предыдущее меню	

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	і Кем выдан	і 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".



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	і Кем выдан	і Тип	I Действителен с			
mon-aes	¦ ∕C=RU∕O=org∕OU=dep∕CN=CA_RSA∕role=carsa	l 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".



16.Установите отметку клавишей <Пробел> и нажмите клавишу <Enter>.

На экране появится сообщение о подтверждении конфигурации.

Подтверх	кдено	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".

	iitara			
Название:				
Описание:				
Организация:		Подраз	деление:	
Регион:		Город:		
Электронная почта:		Страна:		RU
 Электронная подпись Неотрекаемость 	 Зашифрование данных Согласование ключей 		🗹 Прове □ Заши¢	рка подписи CRL урование при согласовании ключей
🗌 Зашифрование ключей	🗹 Проверка подписи сертиф	риката	🗌 Расши	фрование при согласовании ключе
ополнительно			(170)	
Алгоритм подписи: RSA (2048J - Cpo	ок действі	ия (ОТС):	05. Октябрь . 2023 07:05:04 🔻

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".

ртификат				
Тип сертификата: Админи	стратор	Ψ.		
Данные о владельц Пользо	стратор затель			
Введите данные д. Сервер	аутентификации доступа	ые из фа	айла запроса	
Название: Узел бе	зопасности			
Описание:	ner openn			
Организация:		Подразделение:		
Регион:		Город:		
Электронная почта:		Страна:	RU	
азначение ключа				
🖌 Электронная подпись	Зашифрование данных	Прове	рка подписи CRL	
🖌 Неотрекаемость	🔽 Согласование ключей	🗌 Зашия	рование при согласовании ключей	
🗹 Зашифрование ключей	🗌 Проверка подписи серти	фиката 🗌 Расши	фрование при согласовании ключе	
Дополнительно				
Корневой сертификат:	root66		•	
Алгоритм подписи:	FOCT 34.10-2012 (512)	Срок действия (L	JTC): 05. Октябрь .2019 07:07:31	
Экспортировать в файл:	Storage.p7b			
			Создать сертификат Отмен	

- 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".
- На панели отображения информации выберите компонент ЦУС. На панели инструментов нажмите кнопку "Свойства".
 Откроется окно "Узел безопасности".

Узел	1 безопасности	Серверные сертификаты			
C	Сертификаты				
V	1нтерфейсы	Сертификаты 96 и его комп	юнентов:	O	
N	Иаршруты	Название	Кем выдан	Роль	Ĺ
-12	астройки журналирования	mon-aes-66	root-aes-66	Web-монитор	wr f
Лок	альное хранилище		1001 003 00	web monimepi	
B⊢	ешнее хранилище	🔯 srvkdk66	root66	Узел безопас	4 C
)NS					
HCF	5				
18	IMP				
21					
4. Di	ſP				
11	Р іновления				
	ITP Обновления Иониторинг	4			
50 17 50 50	ГР бновления эниторинг	4			
	ТР бновления іониторинг	 Корневые сертификаты 			
0 0 0	ГР Яновления	 Корневые сертификаты Доверенные корневые серт 	ификаты для 95:		[•
70 76 70	Р новления ниториент	 Корневые сертификаты Доверенные корневые серт Название 	ификаты для УБ: Кем выдан	О.	c
чтр Эбно Ион	овления агоринг	 Корневые сертификаты Доверенные корневые серт Название Доверенный Издетель 	ификаты для УБ: Кем выдан КБ Доверенный І	С Действителен Издат 30.05.2017 16:	c

- 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".

		Название	Статус	Версия конфигурации		
		cluster	📀 Подключен	A 10059		
\checkmark	⊧	node-1066	📀 Подключен	10061		

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://adpec_cepвера.

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".

<u>₩</u>
Мониторинг
Приложение

На экране появится окно ввода имени и пароля администратора.

2. Введите имя и пароль администратора и нажмите кнопку "ОК".

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:

 Нажмите кнопку . На экране появится следующее окно:

G. 1.					
admin (Встроеннь	ій администр	ратор)			
Настройки					
Выйти					

2. Выберите пункт "Настройки".

На экране появится окно "Настройки пользователя".

Іользователь:	admin (Встроенный администратор)	
Часовой пояс:	Europe/Moscow	y
Язык интерфейса:	Русский	Ŧ

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.

	шаблон доступ			
Поиск по структуре	🖉 Редактировать			
Структура реалитировать	• Свои правила			
- Å domain-1065	Имя	Условие	Состояние	Причина
 Несортированные Удаленные 	SMART ошибки SDA: критично	Для sda Если filesystem.storage_devices.sda.smart.failures.count.critical > 0	 критический 	Узел безопасности %host%. Кри
	SMART ошибки SDA: предупреждение	Для sda Если filesystem.storage_devices.sda.smart.failures.count.casual > 0	• предупреждение	Узел безопасности %host%. Сбо
	SMART ошибки SDB: критично	Для sdb Если filesystem.storage_devices.sdb.smart.failures.count.critical > 0	 критический 	Узел безопасности %host%. Кри
	SMART ошибки SDB: предупреждение	Для sdb Если filesystem.storage_devices.sdb.smart.failures.count.casual > 0	 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.

Структура	редактировать
🔺 domain-1066	
📲 Несортированные	
• 🗙 cluster	
📰 node-1066	
• 1 Удаленные	

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".

состояние	ДЕТАЛЬНАЯ ИНФОРМАЦИЯ	ШАБЛОН	НАСТРОЙКИ	доступ
🕂 Добавити	ь	AL 19		

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

<		×
Правил	по - Новое правило	
Имя:	Новое правило	
Если:	Условие 1	
	лобавить еще одно условие	Ŧ
To	Контициски	-
	Отправить письмо	
		17
Для:		v
Причина:	host condition	
	Укажите причину	

- 4. Укажите имя правила и условие его применения. Для этого:
 - В поле "Имя" введите имя правила.

Примеч • прог • прог • циф • симе	ание. До писные и писные и ры 0 – 9; волы:	опускается и строчные буі строчные буі	спользова квы латин квы кириз	ание сле чского ал плицы А	дующих с пфавита А – Я, а – я;	имволо — Z, а —	B: Z;		
()	[]	_	-	*	?	!	%

• 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. Настра- ивается критичность события, генерируемого срабатыванием пра- вила, 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: %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.

PIMPA	Условие	Состояние	Причина	Действия
cpu	Для сри Если сри >= 90	• предупреждение	%host%	ØX

Примечание.

Пример правила мониторинга:

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

Правил	o - CPU_critical						
Имя:	CPU_critical						
Если:	Условие 1						
	cpu.load.avg1	>=	90				
	сри -	load -	avg1 -				
	добавить еще одно условие						
To:	Критичный		·				
	Отправить письмо						
Для:	cpu		v				
Причина:	host condition threshold (cpu.load.avg1) v	alue (cpu.load.avg1)					
	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:

- 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.

 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.

0	шавлон доступ			
Поиск по структуре	Редактировать + Добавить			
Структура	• Свои правила			
* Å domain-1065	Имя	Условие	Состояние	Причина
 Несортированные 	SMART ошибки SDA: критично	Для sda Если	критический	Узел безопасности %host%.
 Ш Удаленные 		filesystem.storage_devices.sda.smart.failures.count.critical > 0		
	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	ДЕТАЛЬНАЯ ИНФОРМА	ШАБЛОН	НАСТРОЙКИ	доступ	РЕЗЕРВИРОВАНИЕ	

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.

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

- 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.

32% озу	0% Swap	4% цп	100°С температура
03У			
использовано	4.18 Гбайт (54%)		
свободно	3.62 Гбайт (46%)		
использовано фактически	2.53 Гбайт (32%)		
свободно фактически	5.26 Гбайт (68%)		
буферизовано	104.67 Мбайт (1%))	
закэшировано	1.54 Гбайт (20%)		
всего	7.79 Гбайт		

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

• Подсистемы — сведения о состоянии СОВ, МЭ, системы журналирования, VPN, кластера.

Активный	78%	Активный	1
межсетевой экран	журнал	syslog	vpn
Активный	6%	Активный	Активный
межсетевой экран	журнал	syslog	кластер

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



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

				Трафик		Ошиб	ки	Отбро	шено
Интерфейс	IP адрес	МАС адрес	Состояние	Получено	Передано	Bx.	Иcx.	Bx.	Иcx.
• 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			Получа	атель					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:ed84::42f	15142		fc00:777:b380:ed84::1:a623	6432	tcp	05.06.2019 15:08:30	00:47:39	900.19 K6aйт	2.09 Мбайт
	fc00:777:b380:ed84::42f	46760		fc00:777:b380:ed84::1:a623	5432	tcp	05.06.2019 15:08:31	00:47:38	1022.06 Кбайт	1.51 M6aйr
node-1071.domain-108067	192.168.80.71	60828	cdc	192.168.80.67	8888	tcp	05.06.2019 15:08:00	00:48:09	100.24 Kőaĕrr	42.01 Кбайт

• Активные соединения VPN.

	Входящий трафик			Исходящий трафик			Ошибки		
Канал	Объем трафика	Скорость	Пакеты в секунду	Объем трафика	Скорость	Пакеты в секунду	Ошибки входящих пакетов	Ошибки исходящих пакетов	Ошибки имитозащиты
108067	3.39 Mбайт	163 бит/с	10	48.35 Мбайт	2.63 Кбит/с	6	0	8698055	0
• 108077	3.45 Mбайт	188 бит/c	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:	Время непрерывной работы:
08.10.2018 08:28:40 (UTC+00:00)	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.

≣	Все события	🖹 Генерация отчета
---	-------------	--------------------

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 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":

🖉 Редактировать	
Детальная инф	ормация
Контактное лицо:	

Для изменения данных:

1. Нажмите кнопку "Редактировать".

Рабочая область примет вид:

Детальная инф	ормация	
Контактное лицо	×	+

- **2.** Для добавления нового параметра нажмите кнопку "Добавить" **Ш**. 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".

lетальная инф	орм	ация	
Контактное лицо	Ψ.	Иванов	>
Телефон	Ŧ	8435555524	>
E-mail для уведо	Ŧ	aminemail@com	>

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 безопас	сности
Мониторинг узла безопасности:	\checkmark
Интервал сбора статистики:	5 мин 👻
Таймаут неактивности:	Отключить -
Список параметров мониторинга:	🗸 as
	🗸 сри
	✓ 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
сри	ЦП	ЦП и память
filesystem	SDA BOOT; DATA; SYSTEM; TEMPORARY	Жесткие диски Разделы жестких дисков
firewall	МЕЖСЕТЕВОЙ ЭКРАН	Подсистемы
ips	СОВ	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 администраторь	1	~
test (test1)	Администратор аудита	~
user (user)	Администратор аудита	

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	ШАБЛОН	доступ
🕂 Добавить		

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.

Редактиро	вать				
Объекты , выберите объ	доступа екты, к которь	ім будет разрешен доо	ступ		
🖌 Учитывать	узлы в подгру	лпах			
Объ	ект доступа	Администраторы			
	cluster5	admin2			
	node-1065	admin2			
	раторы				
Админист Отметьте адми Учетная запь	инистраторов, ись Ро	которым будет разрек уль	шен доступ Доступ	к выбранным объ	ьекта
Админист Отметьте адми Учетная запи Все админист	инистраторов, ись Ро граторы	которым будет разреі уль	шен доступ Доступ	к выбранным обт	ьекта

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".
- 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	🕂 Добавить 🛠 Вырезать 📋 Вставить 🗙 Удалить	🖉 Переименовать	🚨 Загрузить с ЦУС
Поиск Q	Редактор структуры		
Структура * domain-111111111 * Группа_3 * Группа_4 * Группа_5 • Группа 6	Имя ▲ [.] ✓ Группа_4 ▲ Группа_5 ▲ Группа_6		
 Несортированные Ш Удаленные 			

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:

 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.



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":

🖉 Редактировать	
Детальная инф	оормация
Контактное лицо:	

Для изменения данных:

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

🖉 Редактировать			
Детальная инф	ормац	ИЯ	

- **3.** Для добавления нового параметра нажмите кнопку "Добавить" **Ш**. 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 инф	орм	ация	
Контактное лицо	Ψ.	Иванов	×
Телефон	Ŧ	8435555524	×
E-mail для уведо	Ŧ	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		 Image: A start of the start of
test (test1)	Администратор аудита	~
user (user)	Администратор аудита	

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.

мони	торинг < >	система: 44332 1559	CETEBAR SEBORIACHOCTL	0 0 O YTPABNEH	R: 491
панель	монито 🗙 панель 2	× o			
Ø Pe	адактировать 🗋 дуб	лировать			
Стру doi Кла и Уз.	иктура main-1065 / Несорт астеры имееть иформация о о о о лы безопасности ode-1065	ированные /			Sarpyska ripoueccopa
Сист	гемный журнал				100 # 22 344
Сист	гемный журнал дата	Узел безопасности	Категория	Сообщение (срабатываний)	1000 a 223 kt
Сист	гемный журнал дата 14.03.2019 11:41:13	Узет безопасности node-1055	Категория Администрирование	Сообщение (срабатываний) 192.168.80.177 - admin [14/Mar/2019:08:4	100 m 22 54
Сист	темный журнал дата 14.03.2019 11:41:13 14.03.2019 11:41:12	Узет безопасности node:1055 node:1055	Категория Администрирование Администрирование	Сообщение (срабатываний) 192.168.80.177 - аdmin [14/Маг/2019:08.4 192.168.80.155 - admin [14/Маг/2019:08.4	1 60 or 22 342 113 -0003 (167 / Auddfogsvinght/Spager Spageszer-254nodz, JMSBND-1717 Brock, JMSBND-1073Bgroup, JMSBND-1 SourtFeld-Himestamp&ourtDrder-dez: HTTP1 1 12 -0003 (167 get rates to sync HTTP1 117 200 598 Thttps://mono.ses.db/magtatorg/sup/1acastrs* VestBark 0 isompatible. V68 F 7.0 Window H 6 11. W040K 1 Thterv17 0.3
Сист 6 6	темный журнал Алта 14.03.2019 11:41:13 14.03.2019 11:41:12 14.03.2019 11:41:12	Узел безопасности node-1055 node-1055 node-1055	Категория Администрирование Администрирование Администрирование	Сообщение (срабатываний) 192.168.80.177 - admin [14/Mar/2019.08.4 192.168.80.155 - admin [14/Mar/2019.08.4 192.168.80.177 - admin [14/Mar/2019.08.4	100 w 20 M 11 - 4000] "GT Austofrágovelger/hjage= kajageszer-55knoda, ahtólih0D=1071knoda, lahólih0D=10/24grug, ahtólih0D=1 kortfeleid-timestampkontDriete-desc HTT / 1 12 - 4000] "GT age states o gene (HTT // 12 00 SM Thegu/mono as & Khanagatonogina pil Austocates" Worklak ó Literapital. KKE 7 & Wriden Writ 18 - 11 WORk f. Trieter / 24 as 11 - 4000] "GT age states o gene (HTT // 12 00 SM Thegu/mono as & Khanagatonogina pil Austocates" Worklak ó Literapital. KKE 7 & Wriden Writ 18 - 11 WORk f. Trieter / 24 as 11 B ker
Сист 0 0	гемный журнал дята 14.03.2019 11.41.13 14.03.2019 11.41.12 14.03.2019 11.41.12 14.03.2019 11.41.12	Узет безопасности node-1055 node-1055 node-1055 node-1055	Категория Администрирование Администрирование Администрирование Администрирование	Сообщение (срабятываний) 192.168.80.177 - admin [14/Маг/2019.08.4 192.168.80.157 - admin [14/Маг/2019.08.4 192.168.80.177 - admin [14/Маг/2019.08.4 252.168.80.109 - admin [14/Маг/2019.08.4	1 60 in 20 44 11 - 0001 "GT / Audologuwight/bage-1 & Auguster-254.oods, MOBROD-1071&oods, JAKOBOD-11074&group, JAKOBOD-16.outField-timestamp&antDrifer-dec HT171 1 12 - 0001 "GT / get: state to-spic (HT171 12 20 658) theps://mon.ares.f5.nei/getros/prov/prof.accuts" Visualia4.0 Europatible, MSE 7.0. Window NT 8.1, WOHA4. Triferati 7.0. 3 11 - 0000 "GT / get: state to-spic (HT171 12 20 658) theps://mon.ares.f5.nei/getros/prov/prof.accuts" Visualia4.0 Europatible, MSE 7.0. Window NT 8.1, WOHA4. Triferati 7.0. 3 11 - 0000 "GT / get: state-to-spic (HT171 12 20 658) theps://mon.ares.f5.nei/getros/prof.accuts" Visualia4.0 Europatible (MSE 7.0. Window NT 8.1, WOHA4. Triferati 7.0. 3 11 - 0000 "GT / get exite-to-spic (HT171 12 20 658) theps://mag.mse.f5.nei/getros/prof.accuts" Visualia4.0 Europatible (MSE 7.0. Window NT 8.1, WOHA4. Triferati 7.0. 3 11 - 0000 "GT / getroster to-spic (HT171 12 20 658) theps://mag.mse.f5.8, App
Сист 0 0 0	гемный журнал дята 14.03.2019 11.41.13 14.03.2019 11.41.12 14.03.2019 11.41.12 14.03.2019 11.41.12 14.03.2019 11.41.10	Узет безопасности node-1055 node-1055 node-1055 node-1055 node-1055	Категория Администрирование Администрирование Администрирование Администрирование Администрирование Администрирование	Cooliagenae (cpa6strutaswak) 192-168.80.177 - admin [14/Mar/2019:08.4 192-168.80.175 - admin [14/Mar/2019:08.4 192-168.80.109 - admin [14/Mar/2019:08.4 192-168.80.109 - admin [14/Mar/2019:08.4	100 or 22 M 13 - 4000] 'GET Auddhögsveiget/Pager-Sapagester-Salanda, JANGBNGD-1071 lande, JANGBNGD-1073ligrup, JANGBNGD-1 Saurtfreid-rismestampikan/Dirder-des: HTT 1 ' 12 - 4000] 'GT aper anties oppie (HTT)', 12 00 GBT Thaper, Jamma es Könningstorongrup / Jackstram, "Machika (Jackmanning Kall, T.A. webown H.T. 10 NOVA, Hondrig A.V. 11 0 Net 13 - 4000] 'GT aper anties oppie (HTT)', 12 00 GBT Thaper, Jamma es Könningstorondurer/2008/24 562-5418 eS 24 Michika (Jackmanning Kall, T.A. Webown H.T. 10 NovA, Hondrig A.V. 11 0 Net 13 - 4000] 'GT aper anties oppie (HTT)', 12 00 GBT Thaper, Jamma es Könningstorondurer/2008/24 562-5418 eS 24 Michika/Dir Michika (Jackmanning Kall, Aper 13 - 4000] 'GT aper anties oppie (HTT)', 12 00 GBT Thaper, Jamma es Könningstorondurer/2008/24 562-5418 eS 24 Michika/Dir Michika (Jackmanning Kall, Aper 14 - 4000] 'GT aper anties oppie (HTT)', 12 00 GBT Thaper, Jamma es Könningstorondurer/2008/24 562-5418 eS 24 Michika/Dir Mi
Сист 0 0 0 0	темный журнал дата 14.03.2019 11.41.13 14.03.2019 11.41.12 14.03.2019 11.41.12 14.03.2019 11.41.12 14.03.2019 11.41.10 14.03.2019 11.41.10	Узен безопасности node-1085 node-1085 node-1085 node-1085 node-1085	Категория Адиинистрирование Адиинистрирование Адиинистрирование Адиинистрирование Адиинистрирование	Coodupmee (gasfaranasmeil) 192.0880.177 - admin [14/Mar/2019/08.4 192.18880.139 - admin [14/Mar/2019/08.4 192.1888.0199 - admin [14/Mar/2019/08.4 192.1888.0199 - admin [14/Mar/2019/08.4 192.1888.0199 - admin [14/Mar/2019/08.4	100 nr 22 94 13 - 4000] "CET Ausdöfogs/widget/bage=1 & gagester=254.node, sh068H0D=1071Bande, jsf068H0D=1074Egrung, sh068H0D=16andfeld=timestamp&andFord=rder, HTTP1 1 12 - 6000] "CET agestates orgen (HTTP1.12 00 6697 Thegu:/moneses & Khonkgenongurup/Lackers" ModBel & Distributed & Kitter 7.2 mindew HT & 100 Nove A 110 Mee 12 - 6000] "CET agestates orgen (HTTP1.12 00 6697 Thegu:/moneses & Khonkgenongurup/Lackers" ModBel & Distributed & Kitter 7.2 mindew HT & 100 Nove A 110 Mee 12 - 6000] "CET agestates orgen (HTTP1.12 00 6697 Thegu:/moneses & Khonkgenongurup/Lackers" ModBel & Distributed & Med A 2000 Mee 13 - 6000] "CET agestates orgen (HTTP1.12 00 6627 Thegu:/moneses & Khonkgenongurup/Lackers' ModBel & Distributed & Med A 2000 Mee 14 - 6000] "CET agestates orgen (HTTP1.12 00 Mee) "Thegu:/moneses & Khonkgenongurup/Lackers' Med Bel & Distributed & Mee 14 - 6000] "CET agestates orgen (HTTP1.12 00 Mee) "Thegu:/moneses & Khonkgenongurup/Lackers' Mee 14 - 6000] "CET agestates orgen (HTP1.12 00 Mee) "Thegu:/moneses & Khonkgenongurup/Lackers' Mee 14 - 6000] "CET agestates orgen (HTP1.12 00 Mee) "Thegu:/moneses & Khonkgenongurup/Lackers' Mee 14 - 6000] "CET agestates orgen (HTP1.12 00 Mee) "Thegu:/moneses & Khonkgenongurup/Lackers' Mee 14 - 6000] "CET agestates orgen (HTP1.12 00 Mee) "Thegu:/moneses & Khonkgenongurup/Lackers' Mee 14 - 6000] "CET agestates orgen (HTP1.12 00 Mee) "Thegu:/moneses & Khonkgenongurup/Lackers' Mee) # Mee 14 - 6000] "CET agestates orgen (HTP1.12 00 Mee) "Thegu:/moneses & Khonkgenongurup/Lackers' Mee) # Mee 14 - 6000] "CET agestates orgen (HTP1.12 00 Mee) "Thegu:/moneses & Khonkgenongurup/Lackers' Mee) # Mee) # Mee 14 - 6000] "CET agestates orgen (HTP1.12 00 Mee) "Thegu:/moneses & Khonkgenongurup/Lackers' Mee) #
Сист 6 6 6 6 6 6	гемный журнал Авта 14.03.2019 11.41:13 14.03.2019 11.41:12 14.03.2019 11.41:12 14.03.2019 11.41:12 14.03.2019 11.41:10 14.03.2019 11.41:09	Узет безопасности node-1005 node-1005 node-1005 node-1005 node-1005 node-1005 node-1005	Категория Администрирование Администрирование Администрирование Администрирование Администрирование Администрирование	Coolispinee (cpa6araaanee) 192, 168,80,177 - admin (1 - Maar 2019 084 192, 168,80, 175 - admin (1 - Maar 2019 084 192, 168,80, 173 - admin (1 - Maar 2019 084 192, 168,80, 109 - admin (1 - Maar 2019 084 192, 168,80, 109 - admin (1 - Maar 2019 084 192, 168,80, 155 - admin (1 - Maar 2019 1936	100 or 22 94 11 - 0001 (117 autohogu kegen Jaguer Laguer 2000 Autoba JABSHD - 1071 Kondu JABSHD - 1000 Autoba JABSHD - 10000 AUTOBA JABSHD - 1000 AUTOBA JABSHD - 10000 AUTOBA J
Сист 0 0 0 0 0	гемный журнал Дята 14.08.2019 11.41.12 14.08.2019 11.41.12 14.08.2019 11.41.12 14.08.2019 11.41.12 14.08.2019 11.41.10 14.08.2019 11.41.09 14.08.2019 11.41.09	Узет безопасности node-1005 node-1005 node-1005 node-1005 node-1005 node-1005 node-1005	Категория Администрирование Администрирование Администрирование Администрирование Администрирование Администрирование Администрирование	Cooliupmen (spaferusanell) 192. 68.80.17 admn [14/Mar/2019.06.4 192. 68.80.15 admn [14/Mar/2019.06.4 192. 68.80.19 admn [14/Mar/2019.06.4 192. 68.80.19 admn [14/Mar/2019.06.4 192. 68.80.19.5 admn [14/Mar/2019.06.4 192. 68.80.19.5 admn [14/Mar/2019.06.4	10 - 000] "GLT Ausdhögsvelger/"page-1 & pagester-"Skondel, afhößeD-1071 Bandel, JrKG/BIGD-1077Agrung, JrKG/BIGD-1 Bandel, JrKG/BI
Сист 6 6 6 6 6 6 6	темный журнал Авта 14.032019 11.41.13 14.032019 11.41.12 14.032019 11.41.12 14.032019 11.41.12 14.032019 11.41.09 14.032019 11.41.09 14.032019 11.41.09 14.032019 11.41.09	Ysen Resonacionni node-1085 node-1085 node-1085 node-1085 node-1085 node-1085 node-1085	Категория Адинистрирозание Адинистрирозание Адинистрирозание Адинистрирозание Адинистрирозание Адинистрирозание Адинистрирозание Адинистрирозание	Coologeneer (paforrunanoli) 192-08.80.177 - admin (14/Mar/2019.08.4 192.08.80.135 - admin (14/Mar/2019.08.4 192.08.80.193 - admin (14/Mar/2019.08.4 192.08.80.199 - admin (14/Mar/2019.08.4 192.08.80.199 - admin (14/Mar/2019.08.4 192.08.80.195 - admin (14/Mar/2019.08.4 192.08.80.195 - admin (14/Mar/2019.08.4 192.08.80.195 - admin (14/Mar/2019.08.4	100 er 22 94 11 - 0001 (11 / april 2006/0000 / april 2006/00000 / april 2006/00000 / april 2006/00000 / april 2006/0000
Сист 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Гемный журнал Арта 14.03.2019 11.41.13 14.03.2019 11.41.12 14.03.2019 11.41.12 14.03.2019 11.41.12 14.03.2019 11.41.12 14.03.2019 11.41.09 14.03.2019 11.41.09 14.03.2019 11.41.09 14.03.2019 11.41.07	Yaen Besonacinortiu node-1003 node-1003 node-1003 node-1003 node-1003 node-1003 node-1005 node-1005	Категория Адиничстрирование Адиничстрирование Адиничстрирование Адиничстрирование Адиничстрирование Адиничстрирование Адиничстрирование Адиничстрирование	Cooluginum (ppSicituationii) 192 - 168 (2017) - adam () 1648ar (2019) (2014 192 - 168 (2015) - adam () 1648ar (2019) (2014 192 - 168 (2015) - adam () 1648ar (2019) (2014 192 - 168 (2015) - adam () 1648ar (2019) (2014 192 - 168 (2015) - adam () 1648ar (2019) (2014 192 - 168 (2015) - adam () 1648ar (2019) (2014) 192 - 168 (2015) - adam () 1648ar (2019) (2014) 192 - 168 (2015) - adam () 1648ar (2019) (2014) 192 - 168 (2015) - adam () 1648ar (2019) (2014) 192 - 168 (2015) - adam () 1648ar (2019) (2014)	100 vr 20 44 113 - 4000] 'Gif Austologovietjer/'page-f Bagegester-554mole, JHOBHSO-1077.Bande, JHOBHSO-1077.Bgrup, JHOBHSO-18cortfield-timetamp&ontDider-dete: HTTP: 1 112 - 4000] 'Gif and the opin cittiff'': 120 05H Titige://mmansestbinargiono/juera/factors/**Molallak-06/empatible. Mill 7.4 mindee H 18, WOMAK Titieff'', A 113 Biel 112 - 4000] 'Gif and the opin cittiff'': 120 05H Titige://mmansestbinargiono/juera/factors/**Molallak-06/empatible. Mill 7.4 mindee H 18, WOMAK Titieff'', A 113 Biel 112 - 4000] 'Gif and the opin cittiff'': 120 05H Titige://mmansestbinargiono/juera/factors/**Molallak-06/empatible. Mill 7.4 mindee H 18, WOMAK Titieff'', A 113 Biel 112 - 4000] 'Gif and the opin cittiff'': 120 05H Titige://mmansestbinargiono/juera/factors/**Molallak-06/empatible. Mill 7.4 mindee H 18, Mill 7.4 mindee H 19, Mill 7.4 mindee H 10, Mill 7

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.

v	Дата 14.00.2019 12.20.30	Узел безопасности	Категория годиннистрирование	Сообщение (срабатываний) тэх тоо ох гээ - өмпнт (тинтин хэтэгэх хэээ тохиод тох гирин тэв нол наролнохил гл т г г г г хээ хэл - г сулсу
0	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&cortField=timestamp&sortDrder=desc HTTP/1.1* 200 109 "https://mon-aes-65/idashboard/predefined_dashboard
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-aes-65/dashboard/predefined_dashboard" "Mozilla/4.0 (compatible: MSIE 7.0; Windows NT 6.1; WOW64; Trid
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-aes-65/nav/gation/cluster/2a206924-362d-4028-a557-bb7d738880ch/info' 'Mozilla/5.0 (X11; Linux x86_64] Ag
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%58%5D=1071&node_id%58%5D=1073&group_id%58%5D=1&code_id%58%5B=1&code_id%58%5B=1&code_id%58%5B=1&code_id%58%5B=1&code_id%58%5B=1&code_id%58%5B=1&code_id%58%5B=1&code_id%58%5B=1&code_id%58%5B=1&code_id%58%5B=1&code_id%58%58%58%58%58%58%58%58%58%58%58%58%58%
0	14.03.2019 12:23:56	node-1073	Управление	(cluster_monitoring) Канал синхронизации кластера в поредке
0	14.03.2019 12:23:56	node-1073	Управление	[cluster_monitoring] Адрес синктронизации <192.168.90.71> доступен
•	14.03.2019 12:23:56	node-1065	Управление	(monitoring_analyzer.cluster) Состояние кластера «duster5»: критический (основной: исправный, резервный: остановленный)
•	14.03.2019 12:23:56	node-1065	Управление	(monitoring_analyzer.cluster] Состояние кластера «duster5»: критический (основной: исправный, резервный: остановленный)
	14.03.2019 12:23:56	node-1073	Управление	(cluster_monitoring) Состояние узла кластера: остановленный (статус: в охидании)
A	14.03.2019 12:23:56	node-1073	Управление	(cluster_monitoring) Канал синхронизации кластера неисправен
	14.03.2019 12:23:56	node-1073	Управление	[cluster_monitoring] Адрес синктронизации <192.168.90.71> недоступен
0	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-aes-65/dashboard/predefined_dashboard" "Mozilla/5.0 (X11; Linux x26_64] AppleWebKit/537.36 (KHTML, like

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.



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.

Структура
<u>domain-1065</u> / <u>Несортированные</u> /
Кластеры
cluster5 Информация
0 1 0
Узлы безопасности
node-1065 Информация

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
E	миджетов
а	аголовок:
[
	Создать Отмена

2. Введите название набора и нажмите "Создать".

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

⊠	панельмонито 🗙 123 — 🗙 новый дишеон 🗙 🔘				¥ ×
Ð	Редестировать		Настройк	и	
0	Заголовок виджета	φ×	Заголовок:	Baronosok avypiketa	
&			Тип видонта:		
~					
Ŵ					
16					
\sum					
97					
\mathbb{T}					
$\frac{1}{2}$					
9/					
.0	Софиниты Отнизна		Применить	Omesa	

Для настройки виджета:

1. Нажмите кнопку "Редактировать" в рабочей области.

🖉 Редактировать

Панель мониторинга перейдет в режим редактирования.

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

15.11.2017 050003 15.11.2017 050003 (UT node-11111111 Аудит Асполнительное пространство из-под бази данных исинторните успешно особождано 15.11.2017 050001 (UT node-11111111 Аудит Итоги прореживания степистки исинторните успешно возполнено 14.11.2017 050002 (UT node-111111111 Аудит Дополнительное пространство из-под бази данных исинторните успешно особождано 14.11.2017 050002 (UT node-111111111 Аудит Дополнительное пространство из-под бази данных исинторните успешно особождано 14.11.2017 050002 (UT node-11111111 Аудит Прореживания степисткии исинторните успешно особождано 14.11.2017 050002 (UT node-11111111 Аудит Поореживания степисткии исинторните успешно особождано 14.11.2017 050002 (UT node-11111111 Аудит Поореживания степисткии исинторните успешно особождано 14.11.2017 050002 (UT node-111111111 Аудит Поореживания степисткии исинторните успешно особождано 14.11.2017 050002 (UT node-111111111 Аудит Поореживания степисткии исинторните успешно особождано 14.11.2017 050002 (UT node-111111111 Аудит Поореживания степисткии исинторните успешно особождано 14.11.2017 050002 (UT node-111111111 Аудит Поореживания степисткии исинторните успешно особождано 14.11.2017 050002 (UT node-111111111 Аудит Поореживания степисткии исинторните успешно особождано 14.11.2017 050002 (UT node-111111111 Аудит Поореживания степисткии исинторните успешно особождано 14.11.2017 050002 (UT node-111111111 Аудит Поо из 2.45 ко 7 г >	15.11.2017 650003 15.11.2017 650003 (UT noce-11111111 Аудит Асполнительное пространство из-под беза данных исниторинта услешно осообокдано 15.11.2017 650001 (UT noce-11111111 Аудит Подекивания сталистики исниторинта услешно осообокдано 14.11.2017 050002 14.11.2017 150020 15.11.2017 150023 15.11.2017 150023 14.11.2017 150020 14.11.2017 150020 14.11.2017 150020 14.11.2017 150020 14.11.2017 150020 14.11.2017 150020 14.11.2017 150020 14.11.2017 150020 14.11.2017 150020 14.11.2017 150020 14.11.2017 150020 14.11.2017 150020 14.11.2017 150020 14.11.2017 150020 14.11.2017 150020 14.11.2017 150020 14.11.2017 150020 14.11.2017 150020 14.11.2017 150020 14.11.2017 15002	15.11.2017 650003 15.11.2017 650003 (UT node-11111111 Адалт Итот прореживание станстки и исниторните услешно вололено 15.11.2017 650001 (UT node-11111111 Адалт Итот прореживание станстки и исниторните услешно вололено 14.11.2017 050002 14.11.2017 0	 15.11.2017 68.00.03 15.11.2017 68.00.03 (∪П посе-111111111 Ауылт Долагинтель 15.11.2017 68.00.01 15.11.2017 68.00.01 (∪П посе-111111111 Ауылт Прореживен 14.11.2017 08.00.01 14.11.2017 05.00.02 14.1	ое простренство из-под безы данных мониторнита успешно освобождено навика статистики мониторнита: удалено 227 и 6962 записей в статистики мониторнита успешно выполнено е статистики мониторнита успешно выполнено навика статистики мониторнита: удалено 226 из 7187 записей в статистики мониторнита успешно выполнено в статистики мониторни в статистики монитор
15.11.2017 0520201 15.11.2017 0520201 15.11.2017 0520201 15.11.2017 0520201 15.11.2017 0520201 15.11.2017 0520201 15.11.2017 0520201 15.11.2017 0520201 15.11.2017 0520201 15.11.2017 0520201 15.11.2017 0520201 15.11.2017 0520201 15.11.2017 0520201 15.11.2017 0520201 15.11.2017 0520201 10.11.2017 0520201 10.11.2017 0520201 10.11.2017 0520201 10.11.2017 0520201 10.11.2017 0520201 11.11.20	15.11.2017 06.2020 15.11.2017 06.2020 (Л1 посе-111111111 Адалт Порекивение статистики мониторинте: уденно 227 из 582 записей 15.11.2017 06.2020 (Л1 посе-111111111 Адалт Порекивение статистики мониторинте: уденно 227 из 582 записей 14.11.2017 06.2020 (Л1 посе-111111111 Адалт Долагичительное простренство из-под беза денние мониторинте: уденно 227 из 582 записей 14.11.2017 06.2020 (Л1 посе-111111111 Адалт Долагичительное простренство из-под беза денние мониторинте: уденно 227 из 582 записей 14.11.2017 06.2020 (Л1 посе-111111111 Адалт Порекивение статистики мониторинте: уденно 235 из 7187 записей 14.11.2017 06.2020 (Л1 посе-111111111 Адалт Порекивение статистики мониторинте: услешно выпалено 14.11.2017 06.2020 (Л1 посе-111111111 Адалт Порекивение статистики мониторинте: услешно выпалено 14.11.2017 06.2020 (Л1 посе-111111111 Адалт Порекивение статистики мониторинте; услешно выпалено 14.11.2017 06.2020 (Л1 посе-111111111 Адалт Порекивение статистики мониторинте; услешно выпалено 14.11.2017 06.2020 (Л1 посе-111111111 Адалт Порекивение статистики мониторинте; услешно выпалено 16.11.2017 16.2024 15.11.2017 18.2024 (Л1 посе-111111111 Н ПТКИТ 15.11.2017 16.2024 15.11.2017 18.2028 (Л1 посе-111111111 Н ПТКИТ 15.11.2017 16.2023 15.11.2017 18.2028 (Л1 посе-111111111 Н ПТКИТ 15.11.2017 16.2023 15.11.2017 18.2028 (Л1 посе-111111111 Н ПТКИТ 15.11.2017 16.2023 15.11.2017 18.2038 (Л1 посе-111111111 Н ПТКИТ 15.11.2017 16.2023 15.11.2017 18.2038 (Л1 посе-111111111 Н ПТКИТ 15.11.2017 18.2038	15.11.2017 08.00.01 15.11.2017 08.00.01 (Л) посе.111111111 Адант Итоги прореживания статистики мониторинтя: удлячно 227 из 5802 записай 15.11.2017 08.00.01 (П) посе.111111111 Адант Дороживания статистики мониторинтя: удлячно 227 из 5802 записай 14.11.2017 08.00.02 (П) посе.111111111 Адант Дороживания статистики мониторинтя: удлячно 227 из 5802 записай 14.11.2017 08.00.02 (П) посе.111111111 Адант Дороживания статистики мониторинтя: удлячно 237 из 5802 записай 14.11.2017 08.00.02 (П) посе.111111111 Адант Дороживания статистики мониторинтя: удлячно 237 из 5802 записай 14.11.2017 08.00.01 (П) посе.111111111 Адант Прореживания статистики мониторинтя: удлячно 237 из 5802 записай 14.11.2017 08.00.01 (П) посе.111111111 Адант Прореживания статистики мониторинтя: удлячно 237 из 5802 записай 14.11.2017 08.00.01 (П) посе.111111111 Адант Прореживания статистики мониторинтя: удлячно 237 из 5802 записай 15.11.2017 18.00.01 (П) посе.111111111 Адант Прореживания статистики мониторинтя: удлячно 237 из 5802 обладено 16.11.2017 18.20.02 (П) посе.111111111 Адант (П) посе.111111111 (П) посе.111111111 16.11.2017 18.20.21 (П) посе.111111111 (П) посе.111111111	15.11.2017 05:00:01 15.11.2017 05:00:01 (UTI посе-111111111 Аудит Итоп проре 15.11.2017 05:00:01 15.11.2017 05:00:03 (UTI посе-111111111 Аудит Прореживен 14.11.2017 05:00:02 14.11.2017 05:00:02 (UTI посе-111111111 Аудит Прореживен 14.11.2017 05:00:01 14.11.2017 05:00:01 (UTI посе-111111111 Аудит Прореживен 15.11	изания сталистики мониторинта: удалено 227 из 5802 записай в сталистики мониторинта: удалено заличнето се простраество из-пад база даленах мониторинта; успешно особождено изания сталистики мониторинта: удалено 225 из 7187 записай с сталистики мониторинта: удалено 225 из 7187 записай с сталистики мониторинта; удалено 25 из 7187 записай с сталистики и мониторинта; удалено 25 из 7187 записай с сталистики и мониторинта; удалено 25 из 7187 записай ото из 2429 ото 1001 из 2429 ото 1017 143034 15.11.2017 1330.23 (ит посе.111111111 и ттанит ото 143034 15.11.2017 1330.23 (ит посе.111111111 и ттанит ото 143034 15.11.2017 1330.23 (ит посе.1111111111 и ттанит ото 143034 15.11.2017 1330.23 (ит посе.1111111111 и ттанит ото 143034 15.11.2017 1330.23 (ит посе.1111111111 и ттанит
15.11.2017 08.00.01 15.11.2017 08.00.01 10.11.2017 08.00.01 11.11.2017 08.00.01 Порекизание статистики мониторинта успешно заполнено Дополнительное пространство избази данных мониторинта успешно заполнено Дополнительное пространство избази данных мониторинта успешно заполнено 14.11.2017 08.00.02 14.11.2017 08.00.02 14.11.2017 08.00.01 15.01.2017 18.20.24 (UT noce-IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	В 11.2017 08.0001 15.11.2017 08.0001 Проремование станстики мониторинте успешно выпалнено Дополнительное простректов исяла бези далени мониторинте успешно возобидено 14.11.2017 08.0001 14.11.2017 08.0002 14.11.2017 08.0001 <td>В 11.2017 08.0001 15.11.2017 08.0001 (Дл поск-111111111 Адалт Прорекизение степистики мониторинте успешно выполнено Дополнительное простректся ципацие бези делена бези бези бези бези бези бези бези бези</td> <td>15.11.2017 08:00:01 15.11.2017 08:00:01 (UT) посе-111111111 Аудит Долалитель 14.11.2017 08:00:02 14.11.2017 08:00:02 (UT) посе-111111111 Аудит Итоги поре 14.11.2017 08:00:01 14.11.2017 08:00:01 (UT) посе-111111111 Аудит Прореживен 14.11.2017 08:00:01 (UT) посе-111111111 Аудит Пореживен 14.11.2017 08:00:01 (UT) посе-111111111 4/2/47 Пореживен 14.11.2017 08:00:01 (UT) посе-111111111 15.11</td> <td>е статистики мониторинга успешно выполнено ве пространство ис-пад бези данных мониторинга успешно освобождено какия статистики мониторинга уделено 225 из 7167 записей е статистики мониторинга успешно выполнено ме журналы 1000 из 2,439 000 Ф С Дата узла Узел базопасиссти Категори 1017 1630 34 15.11.2017 1830 34 (UT посе-111111111 НТТРИНТ 1017 1630 38 15.11.2017 1830 28 (UT посе-111111111 НТТРИНТ</td>	В 11.2017 08.0001 15.11.2017 08.0001 (Дл поск-111111111 Адалт Прорекизение степистики мониторинте успешно выполнено Дополнительное простректся ципацие бези делена бези бези бези бези бези бези бези бези	15.11.2017 08:00:01 15.11.2017 08:00:01 (UT) посе-111111111 Аудит Долалитель 14.11.2017 08:00:02 14.11.2017 08:00:02 (UT) посе-111111111 Аудит Итоги поре 14.11.2017 08:00:01 14.11.2017 08:00:01 (UT) посе-111111111 Аудит Прореживен 14.11.2017 08:00:01 (UT) посе-111111111 Аудит Пореживен 14.11.2017 08:00:01 (UT) посе-111111111 4/2/47 Пореживен 14.11.2017 08:00:01 (UT) посе-111111111 15.11	е статистики мониторинга успешно выполнено ве пространство ис-пад бези данных мониторинга успешно освобождено какия статистики мониторинга уделено 225 из 7167 записей е статистики мониторинга успешно выполнено ме журналы 1000 из 2,439 000 Ф С Дата узла Узел базопасиссти Категори 1017 1630 34 15.11.2017 1830 34 (UT посе-111111111 НТТРИНТ 1017 1630 38 15.11.2017 1830 28 (UT посе-111111111 НТТРИНТ
411.2017 08:00:03 1411.2017 08:00:03 (UT посе-111111111 Адил Дополнительное простренство из-под безы денных мониторинке уделень 2:5 из 7:187 зелисей 14.11.2017 08:00:02 (UT посе-111111111 Адил Итоги прореживания степистики мониторинке; уделень 2:5 из 7:187 зелисей 14.11.2017 08:00:01 (UT посе-111111111 Адил Итоги прореживания степистики мониторинке; уделень 2:5 из 7:187 зелисей 14.11.2017 08:00:01 (UT посе-111111111 Адил Прорекивания степистики мониторинке; уделень 2:5 из 7:187 зелисей 11.217 08:00:01 14.11.2017 08:00:01 (UT посе-111111111 Адил Прорекивание степистики мониторинке; уделень 2:5 из 7:187 зелисей 11.217 08:00:01 14.11.2017 08:00:01 (UT посе-111111111 Адил Прорекивание степистики мониторинке; уделень 8:10:00 из 2:450:00 Ф 11.217 08:00:01 14.11.2017 08:00:01 (UT посе-111111111 Адил Деле Деле Деле Узел безопасиски Категори 05ЫТИЯ МОНИТОРИНГА Ф Х Системиные журналы 1000 из 2:45:000 Ф 100:01/12:80:31 (UT посе-111111111 Н ПТРИ 11:10:17 1:80:31 (UT посе-111111111 Н ПТРИ 11:10:17 1:80:32 (UT посе-111111111 Н ПТРИ 11:11:11 1:80:31 (UT посе-111111111 Н ПТРИ 11:11:11:11:11:12:03:03:03 (UT посе-1111111111	1411.2017 08:00:03 1411.2017 08:00:03 (UT) пось111111111 Аудит Итоги прореживание степистики мониторните удинено 23 из 7187 записай 1411.2017 08:00:01 1411.2017 08:00:01 (UT) пось111111111 Аудит Итоги прореживание степистики мониторните удинено 23 из 7187 записай 1411.2017 08:00:01 1411.2017 08:00:01 (UT) пось111111111 Аудит Прорекивание степистики мониторните удинено 23 из 7187 записай 1411.2017 08:00:01 1411.2017 08:00:01 (UT) пось111111111 Аудит Прорекивание степистики мониторните услешно выпаличено 1 2 3 4 5 7 5 20бытия мониторинга Ф X Системиные журналы 1000 из 2.439 000 Ф 1511.2017 16:02:34 1511.2017 16:02:34 1511.2017 16:02:34 1511.2017 16:02:34 11111111 1111111 1511.2017 16:02:34 <	411.2017 08:00:03 14.11.2017 08:00:03 (UTI пось-111111111 Аудит Допалнительное простректею из-под базы данных мониторните услешно особондено 14.11.2017 08:00:02 14.11.2017 08:00:02 (UTI пось-111111111 Аудит Итоги прореживание статистики мониторните услешно выполнено 14.11.2017 08:00:01 14.11.2017 08:00:01 (UTI пось-111111111 Аудит Прорекивание статистики мониторните услешно выполнено 1 2 3 4 5 7 5 20быТИЯ МОНИТОРИНГА Ф X Системиные журналы 1000 из 2.439 000 X 1 51.12017 18:30:34 (UTI пось-111111111 Аудит Поотиз 2.439 000 X 1000 из 2.439 000 X 0 15.11.2017 18:30:34 (UTI пось-111111111 Аудит 1000 из 2.439 000 X 1000 из 2.439 000 X 1 15.11.2017 18:30:34 (UTI пось-1111111111 HTTPHIT 15.11.2017 18:30:34 (UTI пось-111111111111111111111111111111111111	1411.2017 05:00:03 1411.2017 05:00:23 (UT) пось-111111111 Аудит Дололинтель 1411.2017 05:00:22 1411.2017 05:00:23 (UT) пось-111111111 Аудит Ители проре 1411.2017 05:00:21 1411.2017 05:00:21 (UT) пось-111111111 Аудит Прорезилаен 1 2 3 4 5 0 7 8 > 256ЫТИЯ МОНИТОРИНГА	се прастренство из-пад базы данных мониторинта успешно освобондено навник статистики мониторинта: удалено 225 из 7187 записея с атанстики мониторинта: услешно выпалнано не журналы 1000 из 2430 000 Ф 0 Дата узая Узая базопасисти Категори 1017 1630 4 15.11.2017 1830 34 (UT посе-111111111 НТТРИП 1017 1630 38 15.11.2017 1830 38 (UT посе-111111111 НТТРИП
1411.2017 06:00.02 1411.2017 06:00.02 (UTi node-111111111 Аудит Итоги прореживание степистики мониторинке удинено 226 из 7187 записей 1411.2017 06:00.01 1411.2017 06:00.01 (UTi node-111111111 Аудит Прореживание степистики мониторинке удинено 226 из 7187 записей 18 2 3 4 5 0 7 0 05 2 3 4 5 0 7 0 05 Системиные журиалы 1000 из 2.49000 Ф 2 2 4 5 0 7 0 05 Системиные журиалы 1000 из 2.49000 Ф 2 2 2 2 2 3 4 5 0 0 2 05 Системиные журиалы 1000 из 2.49000 Ф 2 2 2 2 3 4 3 2 2 3 4 3 3 3 3 3 3 4 3	1411.2017 06:00.02 1411.2017 06:00.02 (UTI посе-111111111 Аудит Итоги прореживание статистнии мониторинех уданно 225 из 7187 записей 1411.2017 06:00.01 1411.2017 06:00.01 (UTI посе-111111111 Аудит Прореживание статистнии мониторинех уданно 225 из 7187 записей 10 2 3 4 5 6 7 5 205ыТИЯ МОНИТОРИНГА Ф X Системные журналы 1000 из 2.43500 Ф 10 11.2017 16:20.24 11.2017 16:20.24 11.2017 16:20.24 Уке базопасисти Китетери 10 15.11.2017 16:20.24 15.11.2017 16:20.24 1000 из 2.43500 Ф X Инте и посе 11111111 итте и посе 11111111 итте и посе 11111111 итте и посе 11111111 итте и посе 111111111 итте и посе 111	1411.2017 05:00:02 1411.2017 05:00:01 (UTI посе-11111111 Аудит Итапи прореживения сталистики мониториина; удалена 225 из 7187 записей 14.11.2017 05:00:01 14.11.2017 05:00:01 (UTI посе-111111111 Аудит Прореживения сталистики мониториина; удалена 225 из 7187 записей 1 2 3 4 5 0 7 0 2 3 4 5 0 7 0 2 3 4 5 0 7 0 2 3 4 5 0 7 0 2 3 4 5 0 7 0 205ЫТИЯ МОНИТОРИНГА Ф X Системные журналы 100 из 245000 Ф 1511.2017 16:30:34 1511.2017 18:30:34 (UT посе-11111111) НИТРИНТ 1511.2017 18:30:34 (UT посе-11111111) НИТРИНТ 1511.2017 16:30:31 1511.2017 18:30:32 (UT посе-11111111) НИТРИНТ 1511.2017 18:30:34 (UT посе-11111111) НИТРИНТ 1511.2017 16:30:31 1511.2017 18:30:31 (UT посе-11111111) НИТРИНТ 1511.2017 18:30:31 (UT посе-11111111) НИТРИНТ 1511.2017 16:30:31 1511.2017 18:30:31 (UT посе-11111111) НИТРИНТ	1411.2017 06:00:02 1411.2017 06:00:02 (UTI посе-111111111 Аушит Итоги проре 1411.2017 06:00:01 1411.2017 06:00:01 (UTI посе-111111111 Аушит Прореживен 1 2 3 4 5 6 7 5 2 5 4 5 6 7 5<	изание сиятистики мониторинге удалено 225 из 7187 записей статистики мониторинге услешно выполнено (е журналы Дата узла Узел баспасиссти Категори 1001 из 2430 00 У У Состановании Питини 017 163034 15.11.2017 183034 (UT посе-111111111 НТРИНТ 017 163038 15.11.2017 183038 (UT посе-111111111 НТРИНТ
1411.2017 05:0001 1411.2017 05:0001	141120170820001 141120170820001 ОП посе-111111111 Адал Прореживание саписнии мониторинка услешно выполнено 1 2 3 4 5 7 8 X Обытия мониторинка Ф X Системные журналы 100 из 2 43000 Ф 2 Обытия мониторинка Ф X Системные журналы 100 из 2 43000 Ф Нет данных Ф X Системные журналы 100 из 2 43000 Ф Нет данных Ф X Системные журналы 100 из 2 43000 Ф 15.11.2017 1630.34 (лл посе-111111111 нитенит 15.11.2017 1630.33 (лл посе-111111111 нитенит 15.11.2017 1630.33 15.11.2017 1630.33 (лл посе-111111111 нитенит 15.11.2017 1630.31 (лл посе-111111111 нитенит 15.11.2017 1630.33 15.11.2017 1630.31 (лл посе-111111111 нитенит 15.11.2017 1630.31 (лл посе-111111111 нитенит 15.11.2017 1630.31 (лл посе-111111111 нитенит 15.11.2017 1630.31 (лл посе-111111111 нитенит 15.11.2017 1630.31 15.11.2017 1630.31 (лл посе-111111111 нитенит 15.11.2017 1630.3	141120170820001 141120170820001 ОП посе-111111111 Аудит Прореживаение станстники мониторинге услешно выполнено 1 2 3 4 5 0 7 2 3 4 5 0 7 2 3 6 X Системные журналы 100/из 2 43:000 X Арте зале Арте зале Узая басопасности Татегори 100/из 2 43:000 X Арте зале Арте зале Узая басопасности Татегори 100/из 2 43:000 X Арте зале Арте зале Узая басопасности Татегори 100/из 2 43:000 X Арте зале Узая басопасности Татегори 100/из 2 43:000 X Арте зале Узая басопасности Татегори 15:11.2017 18:30:24 (UT посе-111111111 НТИРИНТВ 15:11.2017 18:30:33 (UT посе-1111111111 НТИРИНТВ 15:11.2017 18:30:33 (UT посе-111111111 НТИРИНТВ 15:11.2017 18:30:33 (UT посе-111111111 НТИРИНТВ 15:11.2017 18:30:33 (UT посе-111111111 НТИРИНТВ 0 15:11.2017 18:30:31 (UT посе-111111111 НТИРИНТВ 15:11.2017 18:30:31 (UT посе-111111111 НТИРИНТВ 0 1 <t< td=""><td>1411.2017050001 1411.2017050001 (Л1 поск-11111111 душит Прорениене 1 2 3 4 5 5 7 5 > обытия мониторинга</td><td>е сталистики мониторинга услещно выполнено IE ЖУРНАЛЫ 1000 из 2439 00 0 1 Дате урля Узел базопасности Категори 017 163034 15.11.2017 183034 (UT посе-111111111 НТРИПТ 017 163038 15.11.2017 1830.38 (UT посе-111111111 НТРИПТ</td></t<>	1411.2017050001 1411.2017050001 (Л1 поск-11111111 душит Прорениене 1 2 3 4 5 5 7 5 > обытия мониторинга	е сталистики мониторинга услещно выполнено IE ЖУРНАЛЫ 1000 из 2439 00 0 1 Дате урля Узел базопасности Категори 017 163034 15.11.2017 183034 (UT посе-111111111 НТРИПТ 017 163038 15.11.2017 1830.38 (UT посе-111111111 НТРИПТ
1 2 3 4 5 7 2 3 4 5 7 2 3 4 5 7 2 3 4 5 7 2 3 4 5 7 2 3 4 5 7 2 3 4 5 7 2 3 4 5 1000 rs2 425 000 Ф 1000 rs2 425 000 <	1 2 3 4 5 7 2 3 4 5 7 2 3 4 5 7 2 3 4 5 7 2 3 4 5 7 2 3 4 5 7 2 3 4 5 7 2 3 4 5 7 2 3 4 5 7 2 3 4 5 7 2 3 4 5 7 2 3 4 5 7 3 5 7 3 5 7 3 3 5 7 3 3 7 3 3 7 3 3 7 7 3 3 7 7 3 3 7 7 3 3 7 7 3 3 7 7 3 3 7 7 7 3 3 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7	Обытия мониторинга Ф × Системные журналы тор на 243000 Ф × Нет данных Ф хате данных Дате ули данных Дате ули данных 1511.2017 183034 (Л посе-111111111 Нитини и писка 0 15.11.2017 183034 (Л посе-111111111 Нитини и писка 15.11.2017 183034 (Л посе-111111111 Нитини и писка 0 15.11.2017 183034 (Л посе-111111111 Нитини и писка 15.11.2017 183034 (Л посе-111111111 Нитини и писка 0 15.11.2017 183034 (Л посе-111111111 Нитини и писка 15.11.2017 183034 (Л посе-111111111 Нитини и писка 0 15.11.2017 183034 (Л посе-1111111111 Нитини и писка 15.11.2017 183034 (Л посе-1111111111 Нитини и писка 0 15.11.2017 183034 (Л посе-1111111111 Нитини и писка 15.11.2017 183034 (Л посе-111111111 Нитини и писка 0 15.11.2017 183034 (Л посе-1111111111 Нитини и писка 15.11.2017 183034 (Л посе-111111111 Нитини и писка 1 2 3 4 5 ни > > Добавить виджет Добавить виджет Добавить виджет 100.0000000000000000000000000000000000	обытия мониторинга	е журналы 1000 из 2439 00 Ф С Алте узла Узал базопасности Интегнал 1017 163034 15.11.2017 183034 (UT посе-111111111 Н ПТРИНТ 017 163038 15.11.2017 183038 (UT посе-111111111 Н ПТРИНТ 017 163038 15.11.2017 183038 (UT посе-111111111 Н ПТРИНТ 017 163038 15.11.2017 183038 (UT посе-111111111 Н ПТРИНТ 017 163038 15.11.2017 183018 (UT посе-1111111111 Н ПТРИНТ
Алта дата улля Узел базопасности Клятегори 15.112017 163024 15.112017 133024 (UT node-111111111 Н НТТРИП 15.112017 163023 15.112017 133024 (UT node-111111111 Н НТТРИП 15.112017 163023 15.112017 133023 (UT node-111111111 Н НТТРИП (5.112017 163023 15.112017 133023 (UT node-111111111 Н НТТРИП	Алта узла узла базоласности категори 15.11.2017 18.3034 (15.11.2017 18.3034) (UT посе.111111111 НТТРИТ 15.11.2017 18.3033 (UT посе.11111111 НТТРИТ 15.11.2017 18.303 (UT п	Дата уляс зуляс зуляс базованаст катерии © 15.11.2017 18.30.24 (лл посе.11111111) 15.11.2017 18.30.24 (лл посе.111111111 н.ттянат © 15.11.2017 18.30.23 (лл посе.1111111111 н.ттянат © 15.11.2017 18.30.23 (лл посе.11111111111 н.ттянат © 15.11.2017 18.30.23 (лл посе.111111111 н.ттянат © 15.11.2017 18.30.23 (лл посе.111111111 н.ттянат © 15.11.2017 18.30.23 (лл посе.11111111 н.ттянат Посе.1111111 н.ттянат Посе.111111 н.ттянат По	Дате і і і і і Нет данных Нет данных (1511 (1511) (1511 (1511) (1511 (1511) (1511) (1511 (1511) (1	дата узла Узая базопасности Китегори 1017 (63034) 15.11.2017 (183034) (Л посе-111111111 НТТР/НТ 1017 (63038) 15.11.2017 (183034) (Л посе-111111111 НТТР/НТ 1017 (63038) 15.11.2017 (183038) (Л посе-111111111 НТТР/НТ 1017 (183038) 15.11.2017 (183038) (Л посе-111111111 НТТР/НТ 1017 (183038) 15.11.2017 (183038) (Л посе-1111111111 НТТР/НТ 1017 (183038) 15.11.2017 (183038) (Л посе-1111111111 НТТР/НТ
Нет данных (1) 15:11:2017 16:30:34 (UT node-111111111 нттент (1) 15:11:2017 16:30:34 (UT node-111111111 нттент (1) 15:11:2017 16:30:33 (UT node-111111111 нттент (1) 15:11:2017 16:30:33 (UT node-111111111 нттент (1) 15:11:2017 16:30:31 15:11:2017 13:30:31 (UT node-111111111 нттент	Нет данных Нет данных Нет данных Побация ризона Побация ризона Побация П	Нет данных Нет данных Добавить виджет	Нет данных (1) 1511 (1) 1511(017 163834 15.11.2017 1338334 (UT noce-111111111 НТРИТ 1017 163824 15.11.2017 1338334 (UT noce-111111111 НТРИТ 1017 163823 15.11.2017 1338338 (UT noce-111111111 НТРИТ 1017 16383 15.11.2017 1338338 (UT noce-1111111111 НТРИТ 1017 16383 15.11.2017 1338338 (UT noce-1111111111 НТРИТ
Нет данных Нет данных (1) 15:11.2017 1630-34 15:11.2017 1830:34 (UT noce-111111111 нттрит (1) 15:11.2017 1630-33 15:11.2017 1830:33 (UT noce-111111111 нттрит (1) 15:11.2017 1630:31 15:11.2017 1830:31 (UT noce-111111111 нттрит (1) 15:11.2017 1630:31 15:11.2017 1830:31 (UT noce-111111111 нттрит (1) 15:11.2017 1630:31 15:11.2017 1830:31 (UT noce-111111111 нттрит	Нет данных Нет данных Нет данных Пебация ризова Пебация ризова Пебация ризова Пебация ризова Пебация ризова Пебация ризова Петаданных Петад	Нет данных Нет данных Нет данных Добавить виджет	Нет данных (15.11 0 15.11 0 1	0071630234 15.11.20171330234 (UT node-1111111111 НТТРИТ 1071630233 15.11.20171330233 (UT node-1111111111 НТТРИТ 1071630233 15.11.20171330233 (UT node-111111111 НТТРИТ 1071630233 15.11.20171330236 (UT node-111111111 НТТРИТ
Нет данных () Is:11:2017 Is3033 IS:11:2017 Is3033 (UT nooe-11111111) нттрит () IS:11:2017 Is3033 IS:11:2017 Is3033 (UT nooe-111111111) нттрит () IS:11:2017 Is3031 IS:11:2017 Is3033 (UT nooe-111111111) нттрит () IS:11:2017 Is3033 IS:11:2017 Is3033 (UT nooe-111111111) нттрит	Нет данных (1) 1611207/162033 1511207/1620310 посе-111111111 нттент (1) 15112077/162031 15112017/162031 007 посе-111111111 нттент (1) 15112017/163031 15112017/163031 007 посе-111111111 нттент (1) 2 3 4 5 ··· 40)	Нет данных (1) 1:11:10:71:80:33 (5) нос-111111111111111111111111111111111111	Нет данных • тып • т	017/16/30/33 15.11.2017/13/30/33 (UT node-111111111 НПТРИП 1017/16/30/33 15.11.2017/13/30/33 (UT node-1111111111 НПТРИП 1017/16/30/31 15.11.2017/13/30/31 (UT node-1111111111)
ПСТ доптных ПСТ допт	11 C 1 401 1202 1 C 1201 1202 1 C 1002 1 C	Добавить виджет		017 16:30:31 15:11:2017 13:30:31 (UT node-111111111)
(1.2017 1630.31 15.11.2017 1630.31 (UT node-111111111 HTTP/HT (1.2017 1630.31 15.11.2017 1630.31 (UT node-111111111 HTTP/HT (1.2.3 4 5 40)		Добавить виджет	() (1) (1) (1) (1) (1) (1) (1) (1) (1) (
() 2 3 4 5 ··· 40 >		(1) 2 3 4 5 ··· 40 > Добавить виджет	(] 2	UTTEN
< 1 2 3 4 5 40 >	< 1 2 3 4 5 ··· 40 >	< 1 2 3 4 5 ··· 40 > Добавить виджет	< 1 2	
		Добавить виджет		3 4 5 … 40 >
Добавить виджет				

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

В правой части главного окна появится панель настроек виджета.

1	
Топ 10 геоисточников атак	
	Ŧ
	1 Топ 10 геоисточников атак

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.

Настройки	
Заголовок:	Заголовок виджета
Тип виджета:	Таблица
Тип информации:	События
Источник информации:	Система
Дата с:	Выберите дату
Дата по:	Выберите дату
Узлы безопасности/группы:	Начните набирать
Важность:	Начните набирать
Категория:	Начните набирать
Статус:	Начато Завершено
Параметр мониторинга:	
Сообщение:	
Фильтр:	Начните набирать
Столбцы:	Важность ✓) дата ✓) дата чауяе безопасности ✓) узел безопасности ✓) хог ✓) Категория ✓) Сообщение
Количество строк:	25
Поле сортировки:	дата
Порядок сортировки:	по убыванию
Применить Отмен	a

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.

=	Мониторинг < >	CACTERN: 350 528 CE	TTEMR REDORACHOCTL: 5524 5134 23096	этравление 187					G	±-
	предостановленный отчет 🗙	1 X 0								
	會 Печать ☆ Параметры	🖿 Открыть 🕞 Дублировать	Редактировать							
0	Топ 10 геоисточников	атак			Топ классов атак					
& \$	• Соединенные Штаты Амери	1322 2743 11 2004 © Китай © Япсния © Велиссой	23 - 550 - 550 - 750 -	м 😑 Франция 🌒 Канада	🕒 Утечка информа	цим 🝵 Попытка получе	133 1318 12 ния привилегия 0	анорания си	толокеры	
16	Топ 15 сбойных узлов				События монитори	нга				41 H3-41
2					Дата	Узел безопасности	Категория	Сообщение (срабатываний)		
1		30			14.11.2017 14:54:32	node-1062	Правила мон	итс (начато) Узел node-1052. Температура процессора 100С		
1					14.11.2017 14:53:49	node-1075	Правила мон	итс (начато) Узел node-1075. Температура процессора 100C		
21					III 14.11.2017 14:53:49	node-1075	Правила мон	итс (начато) node-1075 cpu.load.now != 1111 1111 1.97		
14					14.11.2017 14:52:15	node-1075	Правила мон	итс (завершено - 00:14:59) Узел node-1075. Температура процес	copa 100C	
					14.11.2017 14.52:15	node-1075	Правила мон	итс (завершено - 00.14:59) node-1075 cpu.load.now (= 1111 1111	2.56	
γ					14.11.2017 14:52:15	node-1062	Правила мон	итс (завершено - 00.20:07) Узел node-1062. Температура процес	copa 100C	
11tes					14.11.2017 14:37:15	node-1075	Правила мон	итс (начато) Узел node-1075. Температура процессора 100С		
		node-1	1075 🔵 node-1062		< 1 2 >					

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:

<			×
Сох	раненн	ые отчеты	
~	Предустанс Виджетов: 5	рвленный отчет Дата создания: 12.09.2017 09:36	×
~	Отчет 1 Виджетов: 0	Дата создания: 23.11.2017 10:16	×
~	Отчет 2 Виджетов: 0	Дата создания: 23.11.2017 10:16	×
~	Отчет 3 Виджетов: 0	Дата создания: 23.11.2017 10:16	×

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".

Добавить титульный лист
Добавить дату генерации отчёта
Добавить верхний колонтитул
Просмотреть список доступных макросо
Добавить нижний колонтитул
Просмотреть список доступных макросо
Ton 10 геоисточников атак (Топ геоисточников атак)
Ton 15 обнаруженных атак по сигнатурам (Ton сигнатур)
Топ 15 сбойных узлов (Топ сбойных узлов)
Konunector at a un toning (Konunector at av)

 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".

- 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".
- 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".

/зел безопасности	Петализация	18			
Сертификаты	Инализация				
Интерфейсы	регистрируе	мых в журналі	ации сведении, Вь	сокий	· · ·
Маршруты	Внешние сист	емные журнат	ы		
И Настройки журналирования			-		
Покальное хранилище					
Внешнее хранилище	Состояние	Адрес	Порт	Протокол	Временн
DNS		ШУС			Bcer
DHCP					
SNMP					
NTP					

Рис.З 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.

				OX
Состояние	Адрес	Порт	Протокол	Временной интер
	ЦУС			🖲 Всегда
~	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 пара-

метров. Для этого нажмите кнопку ២ в ячейке. Откроется окно "Временные интервалы".

Внешн	ние системные журн	алы		O×	Q
яние	Адрес	Порт	Протокол	Временной интер	
2	ЦУС				
	0.0.0.0	0	SYSLOG (TCP)	0	
		Временные инт	ервалы		
		Поиск (Ctrl + I	E)	0 0	здать
		Название	Описание		
			🚹 Нет элем	ентов.	
Очист	гка журналов —				
3ar	пускать процесс о				
Co	хранить				

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

икание ененной интервал дайте интервалы времени действия правил: подведите указатель мыши к требуемомому времени соответсвующего дня дайте интервалы времени можно с клавиатуры в формате время начала - время завершения (несколько интервала даются через разделитель ";"). Например: 10:00-12:00; 15:30-17:55	звание						
еменной интервал дайте интервалы времени действия правил: подведите указатель мыши к требуемомому времени соответсвующего дн дели, нажмите левую кнопку и, не отпуская, задайте интервал. кже задать интервалы времени можно с клавиатуры в формате время начала - время завершения (несколько интервали даются через разделитель ":"). Например: 10:00-12:00; 15:30-17:55 0 6 12 18 24 Пн	исание						
дайте интервалы времени действия правил: подведите указатель мыши к требуемомому времени соответсвующего дн дели, нажмите левую кнопку и, не отпуская, задайте интервал. Ккех задать интервалы время начала - время завершения (несколько интервал даются через разделитель ";"). Например: 10:00-12:00: 15:30-17:55 0 6 12 18 24 Пи Вт Вт Вторник Ччими - ччими Вторник Ччими - ччими Среда Ччими - ччими Четверг Ччими - ччими Четверг Ччими - ччими Суббота Ччими - ччими Восфесенье Ччими - ччими	еменной интер	вал					
кже задать интервалы времени можно с клавиатуры в формате время начала - время завершения (несколько интервали даются через разделитель ":"). Например: 10:00-12:00: 15:30-17:55 О 6 12 18 24 Пи ватПи недели: Понедельник ччими ччими Вторник ччими - ччими Среда ччими - ччими Четверг ччими - ччими Четверг ччими - ччими Суббота ччими - ччими Восресеные ччими - ччими	дайте интерва дели, нажмите	лы времени действ элевую кнопку и. н	зия правил: подведи е отпуская, задайте	ите указатель мыш интервал.	и к требуема	омому времени с	оответсвующего дня
0 6 12 18 24 Пи 1 1 1 1 Вт 1 1 1 1 Сре 1 1 1 1 14 1 1 1 1 17 1 1 1 1 18 1 1 1 1 19 1 1 1 1 10 1 1 1 1 11 1 1 1 1 12 1 1 1 1 14 1 1 1 1 15 1 1 1 1 16 1 1 1 1 17 1 1 1 1 16 1 1 1 1 17 1 1 1 1 18 1 1 1 1 19 1 1 1 1 10 1 1 1 1 11 1 1 1 1 12 1 1 1 1 13 1	кже задать ин	тервалы времени и	иожно с клавиатурь	ы в формате время	начала - врем	ия завершения (н	есколько интервалов
0 6 12 18 24 Дни недели: Пн Пн Пн Пн Пн Пн Пн Зат Пн Пн Пн Пн Пн Пн Пат Пн Пн Пн Пн Пн Пн Пат Пат Пн Пат Пат Пат Пат Сб Пат Пат Пат Пат Пат Сб Пат Пат Пат Пат Пат Сб Пат Пат Пат Пат Пат Сост Пат Пат Пат Пат Пат Сост Пат Пат Пат Пат Пат	даются через	зазделитель ,). п	апример. 10.00-12.0	10, 10.50-17.55			
Пи Понедельник ччлии ат Понедельник ччлии Сре Вторник ччлии чили Члии ччлии чили Ччлии ччлии чили чилии чилии суббота чилии чилии чилии чилии чилии	°	6	12	18	24	Дни недели:	
ата са	Тн					Понедельник	44:MM - 44:MM
Среда Ччлии - ччлии Нт Среда ччлии - ччлии Пт Па Па Па Сб Собота ччлии - ччлии Зас Па Воскресенье ччлии - ччлии	Вт			0	100	Вторник	441MM - 441MM
IT Четверг ччим Tr Па Па Па Чийм - ччим C6 Субота ччим - ччим чим - ччим Bac Па Каканананананананананананананананананана	Cp					Среда	44:MM - 44:MM
Тт Пятница ичени - ччени 26 Суббота ичени - ччени 36 Воскресеные ичени - ччени	IT .					Четверг	440MM - 440MM
Сб Суббота чч:мм Зас Воскресенье чч:мм	Т					Пятница	44:MM - 94:MM
Воскресенье чч:ни	D6					Суббота	44:MM - 44:MM
	Вс					Воскресенье	44:MM - 44:MM
	I.			1			
емя 05:15	OM 05-15						

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

4				O×
Состояние	Адрес	Порт	Протокол	Временной интер
	ЦУС			🕒 Всегда
V	110.220.101.10	100	SYSLOG (TCP)	🖲 Всегда

- 3. Для отмены хранения журналов на сервере снимите отметку состояния.
- 4. Нажмите кнопку "ОК" в окне "Узел безопасности" (см. Рис.3 на стр.43).
- 5. 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":

Узел безопасности - node-188						×
 Узел безопасности Сертификаты Интерфейсы Маршруты Настройки хириалирования 	✓ Локально Хранение ж Ежедневно	е хранилище курналов в локальной б е расписание очистки ж	азе данны: курналов:	к узла безопас	СНОСТИ.	
Локальное хранилище	Статус	Журнал	Старт	Оповещать	Период хранения	
Внешнее хранилище		Управления	23:00		365	
DNS		Системный	23:00		365	
SNMP		Сетевой безопасно	. 23:00		365	-
NTP	Запускать і Сохранить	процесс очистки при	80 10 2	² Занятого З Записей	места на диске журналов	
				ОК	Отмена Прим	енить

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.
- **4.** Поставьте отметку в поле "Оповещать" для отправки почтовых уведомлений о выполнении операции очистки.
- 5. Настройте количество дней хранения записей журналов. Для этого выделите двойным щелчком мыши ячейку столбца "Период хранения данных (дней)" и внесите изменения с помощью клавиатуры.
- 6. 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".

Ежедневно	ре расписание очистки жур	налов		216
Статус	Журнал	Старт	Оповещать	Период хранения
\checkmark	Администрирования	11:29	\checkmark	112
\checkmark	Системный	08:00	\checkmark	10
\checkmark	Сетевой безопасности	03:00		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.

Узел безопасности Сертификаты	☑ Использовать внешнюю БД	
Сертификаты Интерфейсы Статические маршруты Динамические маршруты И настройки хурналирования Локальное хранилище Внешнее хранилище DNS DHCP	Внешняя база данных Адрес: Название базы данных: Имя пользователя: Пароль: Поисковая мащина	Порт. 5432
SNMP Дата и время Обновления Мониторинг	Адрес:	Порт: 9200

2. Установите отметку "Внешняя база данных".

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

3. Введите параметры настройки и нажмите кнопку "Применить".

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

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

CUCTEMA CETER	АЯ БЕЗОПАСНОСТЬ УПРАВЛЕНИ	• • •		
🔅 Удалить *				
• Фильтры				
Источник	Система ч	Sanpoc:		
Дата с	Выберите дату	и или не	по важность категория параметр, мониторинга продолжительность сообщение срабатываний статус узел, без	юпасности хост
Дата по	Выберите дату			
Группировать события по:		Применить	Сбросить	
Reproductive to LIVCu:	1077			
• Журнал				
• Журнал	5 ··· 40 >		иносичение 💽 С знакед з на вспосемний назв	 количество стиок. (25) 50
• Журнал (1 2 3 4 Дата 2602 2019 00:51 5	5 ··· 40 > > ysen 6esonschottni 2 071 mode/077	Категория Управление	AETOGRAGERAN DE COMUNICATION DE LA COMUNICATIONE DE L	 количество стиок: (25) 50
 Журнал 1 2 3 4 Дята 4 26.02.2019 09:31:5 2 6.02.2019 09:31:5 	5 ··· 40 ≯ Узел безопасности 2.971 поде-1077 9.50 поде-1077	Категория Управление Управление	Attocondutive Configure Projection property like of foods 1007 (bit local provinces) Configure	 количество стгок (25) 50
 WypHaл 1 2 3 4 Дита 26.02.2019.09513 26.02.2019.09513 26.02.2019.09513 	5 ··· 40 ≯ Узел безопасности 2.971 поde1077 9.529 поde1077 7.727 поde1077	Категории Управление Управление Управление	Antoconserver D C source 2 10	 д количество стгок (26) 50
 * Журнал 1 2 3 4 Дята 26.02.2019.09513 26.02.2019.09530 26.02.2019.09530 26.02.2019.09530 	5 ··· 40 >	Категории Управление Управление Управление Управление	Attocendations C which is a set occurrent in the se	 колнаство сток (35) 50
 Wyphan 1 2 3 4 Arta 2602.2019 09515 2602.2019 09512 2602.2019 09502 2602.2019 09502 2602.2019 09502 2602.2019 09502 	5 ··· 40 >	Категория Управление Управление Управление Управление Бызовая плятформа	Anticoprocestives Configurate Configurate Projection progress state of (node 1007) has became (psychronzed) (replacetor,-unrotating) Replication progress state of (node 1007) has became (psychronzed) (replacetor,-unrotating) Replication progress state of (node 1007) has became (psychronzed) (replacetor,-unrotating) Replication progress state of (node 1007) has became (psychronzed) (replacetor,-unrotating) Replication progress state of (node 1007) has became (psychronzed) (replacetor,-unrotating) Replication progress state of (node 1007) has became (psychronzed) (replacetor,-unrotating) Replication progress state of (node 1007) has became (psychronzed) (replacetor,-unrotating) Replication progress state of (node 1007) has became (psychronzed) (replacetor,-unrotating) Replication progress state of (node 1007) has became (psychronzed) (replacetor,-unrotating) Replication progress state of (node 1007) has became (psychronzed)	 колнество стгос. 25 50
XypHan 1 2 3 4 Aora Aora 2602201909513 2602201909513 2602201909513 2602201909503 2602201909503 2602201909500 2602201909500 0 2602201909500	5 ··· 40 > 3/3en/6esonacoiectu 2/971 node-1077 9.539 node-1077 7.727 node-1077 1.687 node-1077 1.682 node-1077	Категория Управление Управление Управление Управление Базовая платформа Базовая платформа	ARTOGENERATIVO CON SUBJECT OF SUB	2 КОЛЧЕСТВО СТОК (3) 50
Xyphan	5 ··· 40 > ysen 6esonacoiocru 2.971 node-1077 5.539 node-1077 7.727 node-1077 1.687 node-1077 1.682 node-1077 1.682 node-1077	Категория Управление Управление Управление Даровая полформа Баровая полформа Баровая полформа	Attocardentree Or which 2 at Extra countrel Performance	• KOMACTECTTOR (8) 50
Xyphan 1 2 3 4 Ars Ars Z602.019 0951 Z602.019 0951 Z602.019 0952 Z602.019 0952 Z602.019 0952 Z602.019 0952 Z602.019 0952 Z602.019 0955 Z602.019 0955 Z602.019 0955 Z602.019 0955 Z602.019 0955	5 ··· 40 5 V3en Gesonaciocra 2.971 mode-1077 2.983 mode-1077 2.931 mode-1077 .	Категория Управление Управление Управление Базова плятформа Базовая плятформа Базовая плятформа Базовая плятформа	ARDGORDENSING C ANNEL 2011 C ANNEL 2012 C ANNEL 2013 C AN	D KONNETBOLITOR (B) 10
Kyphan (1 2 3 4 Arra Arra Arra Arra Accolor 90915 A 260201909915 A 260201909915 A 260201909915 A 260201909905 A 260201909905 B 260201909905 B 260201909905 C 360201909405 B 260201909405 B 260201909405 B 260201909405	5	Категория Управление Управление Управление Вазова плятформа Базовая плятформа Базовая плятформа Базовая плятформа Базовая плятформа	Electronautrixe	Restruction (3) 10

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:

• X	Курна	ал					
<	1	2	3	4	5	 26	>

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

кол-во строк: 25 50 100

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

При работе с несколькими вариантами фильтрации или разными журналами наж-

мите 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 l



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, по-казываемая соответствующим значком.

	Важность сообщения							
Иконка	Уровень	Иконка	Уровень					
*	Авария	ä	Тревога					
•	Критическая ошибка	Δ	Ошибка					
Ę0	Предупреждение		Оповещение					
0	Информация	2	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 опреде- ленных 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 сооб-• шение.
- 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, ІРадрес и порт источника атаки, порт и IP-адрес, на который проводилась атака.

Детальная информаці	ия 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 MI ME 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.

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:[Оповещать/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 под- системы
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 сра- батыванием сигнатуры с определенной вер- сией
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

Для фильтрации записей используют следующие теги:

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	ä	Тревога	
•	Критическая ошибка	Δ	Ошибка	
ų,	Предупреждение		Оповещение	
0	Информация	2	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 опреде- ленным 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.

• Ж	урнал				
<	1 2 3 4 5	20	>		
	Дата	Действие	Узел безопасности (интерфейс)	Компонент	Адрес отправителя
	26.02.2019 10:22:35.493	Разрешить	node-1065	Межсетевой эк	93.191.9.124
	26.02.2019 10:22:35.493	Оповещать	node-1065 (eth2)	СОВ	39.69.76.51
	26.02.2019 10:22:35.492	Оповещать	node-1065	VPN	93.191.9.124
~	26.02.2019 10:22:35.492	Разрешить	node-1065 (eth3)	КП	77.104.1.22
~	26.02.2019 10:22:35.492	Блокировать	node-1065 (eth0)	СОВ	39.69.76.51
~	26.02.2019 10:22:35.492	Обнаружить	node-1065 (eth1)	КП	93.191.9.124
	26.02.2019 10:22:35.492	Перенаправить	node-1065	VPN	77.104.1.22
	26.02.2019 10:22:35.492	Оповещать	node-1065	VPN	39.69.76.51
	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 активна:



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.

Журналы	
Просмотр системного журнала Просмотр хирнала сетевой безопасности	
Просмотр журнала управления	
Возврат в предыдущее меню	

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.

Data Part Exteroples H Excerptes 66. 66. 19 86:13:09 1 1111 i mode-1111.dom i (U) Ansenuerymposaume: Программе очастки хирналов завершиля свою работу 66. 66. 19 86:13:09 1 1111 i mode-1111.dom i (U) Базовая платформа: рад.unix(sa-1:session): session opened for user 68. 66. 19 86:13:09 1 1111 i mode-1111.dom i (U) Базовая платформа: pan.unix(sa-1:session): session cypese 3 panyo sessi 68. 66. 19 86:13:09 1 1111 i mode-1111.dom i (E) Базовая платформа: panyo opening D/ango session (type: 5) panyo sessi 68. 66. 19 86:13:09 1 i mode-1111.dom i (E) Базовая платформа: panyo (tssi) (tssi) i session errors: "(ITTP status = 3 68. 66. 19 86:13:09 1 i mode-1111.dom i (E) Базовая платформа: panyo (tssi) (tssi) i session errors: "(ITTP status = 3 69. 66. 19 86:13:00 1 i mode-1111.dom i (E) Базовая платформа: panyo (tssi) (tssi) i session errors: "(ITTP status = 3 69. 66. 19 86:13:05 1 i mode-1111.dom i (I) Базовая платформа: panyonix(sa-1:session): session errors: " 86. 66. 19 86:13:05 1 i mode-1111.dom i (I) Базовая платформа: panyonix(sa-1:session): session errors: "				Просн	отр системного журнала (события: 1 - 8)
<pre>b6.6.19 80:13400 1111 inde-1111.dom i [U] Aremuertynynsene: []perjamen excerna zgwanno samepusin come paidory 80:66.19 80:13400 1111 inde-1111.dom i [U] Базовая полутория: [marunis(su-1):session] is session opened for user 80:66.19 80:13400 1111 inde-1111.dom i [U] Базовая полутория: [marunis(su-1):session trype:]]pagen session 80:66.19 80:13400 1111 inde-1111.dom i [E] Базовая полутория: [marunis(su-1):session trype:]]pagen session 80:66.19 80:13400 1111 inde-1111.dom i [E] Базовая полутория: [marunis(su-1):session trype:]]pagen session 80:66.19 80:13400 1111 inde-1111.dom i [E] Базовая полутория: [marunis(su-1):session trype:]]pagen session 80:66.19 80:13400 1111 inde-1111.dom i [I] Базовая полутория: [marunis(su-1):session records regioned for user 80:66.19 80:13405 1111 inde-1111.dom i [I] Базовая полутория: [marunis(su-1):session records regioned for user 80:66.19 80:13405 1111 inde-1111.dom i [I] Базовая полутория: [marunis(su-1):session]: session closed for user 80:66.19 80:13405 1111 inde-1111.dom i [I] Базовая полутория: [marunis(su-1):session]: session closed for user 80:66.19 80:13405 1111 inde-1111.dom i [I] Базовая полутория: [marunix(su-1):session]: session closed for user 80:86.19 80:13405 1111 inde-1111.dom i [I] Базовая полутория: [marunix(su-1):session]: session closed for user 80:86.19 80:13405 1111 inde-1111.dom i [I] Базовая полутория: [marunix(su-1):session]: session closed for user 80:86.19 80:13405 1111 inde-1111.dom i [I] Базовая полутория: [marunix(su-1):session]: session closed for user 80:86.19 80:13405 1111 inde-1111.dom i [I] Базовая полутория: [marunix(su-1):session]: session opened for user 80:80:19 80:13405 1111 inde-1111.dom i [I] Базовая полутория: [marunix(su-1):session]: session discreterees [marunix(su-1):session]: session opened for user</pre>	Дата/Время		1 9зел	1 Хост	I Категория и сообщение
	10476478 Upuesa 66.68.13 6 66.68.13 6 66.68.13 6 66.68.13 6 66.68.13 6 66.68.13 6 66.68.13 6 66.68.13 6 66.68.13 6	8:13:89 8:13:89 8:13:89 8:13:89 8:13:89 8:13:89 8:13:89 8:13:85 8:13:85	i 1111 i 1111 i 1111 i 1111 i 1111 i 1111 i 1111 i 1111 i 1111 i 1111	i xocr i node-1111.dom. node-1111.dom. node-1111.dom. node-1111.dom. i node-1111.dom. i node-1111.dom.	 Kaveropsk & Coduşture (U) Agresuczyposana: Dorpowa owczna zgloba zasepska cose padoty. (11) Gaosa natychysi jam.unix(su-lisession): session opened for user. (12) Gaosa natychysis: Error opening Djang session (type: Djang session): 121 Gaosas natychysis: start_djang.session error: ('01TT status '3). (13) Essanas natychysis: pam.unix(su-lisession): session (opened for user '101 Gaosas natychysis: pam.unix(su-lisession): session (opened for user '101 Gaosas natychysis: pam.unix(su-lisession): session (opened for user '101 Gaosas natychysis: pam.unix(su-lisession): session opened for user '101 Gaosas natychysi

В окне просмотра отображается список всех хранящихся в журнале событий. 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.

		Подробные сведения о событии
Дата/время:	06.06.19, 08:13:09.463	
Время на цзле:	06.06.19, 08:13:09.463	(UTC+00:00)
Xoct:	node-1111.domain-1111	
ID устройства:	1111	
Уровень важности:	Предупреждение	
Категория:	Администрирование	
Отправитель:	local_menu	
Количество срабатываний:	1	
Диск переполнен, выполнен	на очистка журналов. Уда	алено записей: О

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.

	Поиск
Строка	

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.

- 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:

 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.

		Категории событий
I r	1	Администрирование
Ē	i	Удаленный доступ
] [1	Обнаружение вторжений Контроль достипа
I	i	Контроль целостности
L E	1	Нудит и мониторинг Правила мониторинга
E r	1	Защищенные коммуникации Базовая платформа
Ľ	-	

• 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.



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;
- ІР-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.

	Подробные сведения о событии
Дата/время:	06.06.19, 08:54:21.480
Время на узле:	06.06.19, 08:54:21.480 (UTC480266)
Узел:	1061
Ин терфейс:	eth2
Действие:	Заблокировано
Адрес отправителя:	184.129.63.12
Порт отправителя:	5745
Адрес получателя:	183.115.232.108
Порт получателя:	40555
Компонент:	ДА —
Количество срабатываний:	
Протокол:	icmp
Класс:	Веб-атаки
Идентификатор сигнатуры:	2026131
Сигнатура:	WEB_SPECIFIC_APPS Campsite article_id Parameter INSERT INTO
	SQL Injection Attempt

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.

	Поиск
Строка	

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.

- 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:

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

Фильтр	
<u>Пата∕вреня</u> Узел Компонент	
Применить	

- 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:

	Ko	омпоне	нт
E	1	ДA	
E	1	ВЧС	
E	1	MC3	
E]	ПΦ	
E]	кп	
E	1	MIA	

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.

119-06-06 08:57:6	30 LUC ILATI		Контине	энт
		Проснотр	журнала управлен	ния (события: 1 - 913)
ата∕Вреня	1 Узел	1 Хост	і Субъект	I Категория и сообщение
6.86.19 08:56:36	5 1054	node-1054.doma	. superuser	I []] Администрирование: Просмотр журнала управлен
6.06.19 08:55:29	9 1054	node-1054.doma	. superuser	I III Администрирование: Просмотр журнала сетевой
6.06.19 08:55:21	1 1054	node-1054.doma	. Ladmin	I [1] Управление: Администратор выполнил Взятие бл
5.06.19 08:55:19	9 1054	node-1054.doma	. I admin	 [1] Управление: Администратор выполнил вход. Рез
.06.19 08:55:19	9 1054	node-1054.doma	. admin	III Управление: Администратор выполнил вход. Рез
.06.19 08:55:17	7 1054	node-1054.doma		I []] Администрирование: Вход в систему
.06.19 13:23:50	3 1054	node-1054.doma	. Ladmin	 [1] Управление: Администратор выполнил выход. Ре
.86.19 13:23:56	3 : 1054	i node-1054.doma	. i admin	111 Эправление: Администратор выполнил Снятие бл
.06.19 13:23:13	3 1054	i node-1054.doma	. i admin	1 [1] Управление: Администратор выполнил Формирова
.86.19 13:23:80	5 1054	i node-1854.doma	. I admin	 [1] П. Эправление: Администратор выполнил Формирова
.86.19 13:22:5	7 1054	i node-1054.doma	. i admin	1 [1] Эправление: Наминистратор выполнил формирова
00.10 13:22:13	0 1 1007	1 node-1007.doma	. i aamin	I III Эправление: НДМИНИСТРАТОР ВЫПОЛНИЛ ФОРМИРОВА
06 40 40.22.43	0 1 1001 0 1 10EA	i nuae-1051.auma	. i domin	 ГГТ эправление: ндминистратор выполнил формирова ГГТ Чарав социе: Асминистратор выполния Формирова
00.17 13:22:13	0 I 1004	1 1000-1054.00md	. i damin	ттт статор выполнил формирова
96 19 13-22-01	7 1 1051	1 1000-1051.00md	, i admin	 ГГТ эправление: нднинистратор выполнил формирова ГГТ Управление: Авминистратор выполнил формирова
86 19 13-21-3	2 1 1055	1 node-1055.doma	: admin	 [1] Эправление: Администратор выполнил формирова [1] Чоравление: Администратор выполнил формирова
R6 19 13-21-26	5 1 1005	1 node-1996 down	. r admin	 ГГТ Эправление: нднинистратор выполнил формирова ГГТ Управление: Авминистратор выполнил формирова
86 19 13:21:20	5 1 1050	1 node=1954 doma	: admin	 [1] Управление: Администратор выполнил формирова [1] Управление: Администратор выполнил формирова
R6 19 13:21:16	5 1 1054	1 node-10511doma	i admin	 [1] Чправление: Администратор выполния формирова [1] Чправление: Администратор выполния Пормирова
86 19 13:21:16	5 1 1054	1 node-1054 doma	l admin	1 [1] Чаравление: Алиминстратор выполния формирова
R6 19 13:28:54	1 1954	i node-10511doma	l admin	1 П.1. Управление: Администратор выполния формирова 1 П.1. Чправление: Администратор выполния Дормирова
.86.19 13:28:56	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	I node=1861.doma	ladmin	1 111 Управление: Алминистратор выполния Пормирова
R6.19 13:19:39	1 1954	1 node-1954 doma	admin	[11] Управление: Алминистратор выполнил Пормирова
.86.19 13:19:38	3 1854	node-1854.doma	admin	[11] Управление: Администратор выполнил Сохранени
.86.19 13:19:30	5 1054	node-1054.doma	admin	[]] Управление: Администратор обновил объект тиг
.86.19 13:16:07	7 1006	node-1996.doma	. admin	[11] Управление: Администратор выполнил Формирова
.06.19 13:16:03	3 1007	node-1007.doma	l admin	[[]] Управление: Администратор выполнил Формирова
.86.19 13:12:44	1 1054	node-1054.doma	. I admin	I III Управление: Администратор выполнил Перезагру
.86.19 13:12:01	1 1007	node-1007.doma		III Администрирование: Вход в систему
.06.19 13:09:53	3 1054	node-1054.doma	. I admin	I III Управление: Администратор выполнил Формирова
.06.19 13:09:42	2 1054	node-1054.doma	. admin	I III Управление: Администратор выполнил Формирова
.06.19 13:09:42	2 1054	node-1054.doma	. Ladmin	III Управление: Администратор выполнил Формирова
.06.19 13:09:00	3 1054	node-1054.doma	. i admin	I [1] Управление: Администратор выполнил Формирова
.06.19 13:08:52	2 1007	node-1907.doma	. i admin	I III Управление: Администратор выполнил Формирова
.06.19 13:08:48	3 1054	node-1054.doma	. i admin	I [1] Управление: Администратор выполнил Формирова
.06.19 13:08:42	2 1054	node-1054.doma	. Ladmin	I III Управление: Администратор выполнил Формирова
.06.19 13:07:51	1 1054	node-1054.doma	. i admin	1111 Эправление: Администратор выполнил Формирова
0.06.19 13:07:51	1 1054	node-1054.doma	. i admin	1 [1] Эправление: Администратор выполнил Формирова
5.06.19 13:07:50	1055	i node-1055.doma	. i admin	1 111 Эправление: Администратор выполнил Формирова

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.

		Подробные сведения о событии
Дата/время:	06.06.19, 08:22:12.487	
Время на узле:	06.06.19, 08:22:12.487	(UTC+00:00)
Xoct:	node-1111.domain-1111	
ID устройства:	1111	
Уровень важности:	Информация	
Субъект:	superuser	
Категория:	Администрирование	
Просмотр журнала (управления	

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.

Поиск				
Строка				

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.

- 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.

Выберите журнал для очистки	
<mark>Системный журнал</mark> Журнал сетевой безопасности Журнал управления Возврат в предыдущее меню	

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.

	Период	
Начало	01.01.05	
Конец	31.01.2005	

• 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:

 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:

 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.

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 CRLфайла в доверенные корневые центры сертификации.

Для подключения оснастки "Сертификаты" в консоли ММС:

- 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...".

		-		beroperindic ochocinor.	
Оснастка	Поставщик	^		Корень консоли	Изменить расширения
Анализ и настро	Корпораци				Mannum
Диспетчер автор	Корпораци				удалить
Диспетчер устро	Корпораци				
💂 Локальные поль	Microsoft C				Вверх
• Монитор IP-безо	Microsoft C				
монитор брандм	Microsoft C		Reference >		Вниз
🕺 Общие папки	Microsoft C		цоодыны >		
🗋 Папка	Корпораци				
🕑 Планировщик за	(с) Корпора				
🛃 Просмотр событий	(с) Корпора				
📑 Редактор объек	Microsoft C				
📑 Результирующа	Microsoft C				
🚽 Сертификаты	Корпораци	~			Лополнительно

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

снастка диспетч	ера сертификатов			
Эта оснастка все	егда будет управлят	ь сертификата	чидля:	
О моей учетной	записи пользовател	пя		
О учетной запис	си службы			
• учетной запис	си компьютера			
			< Hasan	Отмена

- 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.

\overline Консоль1 - [Корень консоли]										
🚟 Файл Действие Вид Избранное Окно Справка										
📔 Корень консоли Имя										
Сертификаты (локальный компьютер) Сертификаты (локальный ко										
> СЛИЧНОЕ										
> Доверенные кор	Поиск сертификатов									
> Промежуточные	Все залани	>	Поиск сертифика	TOR						
> 📔 Доверенные изд	осе задачи	· · ·	поиск сертифика	105						
> 🚞 Сертификаты, к	Новое окно отсю	да	Импорт							
> 📋 Сторонние корн	Обновить									
> Доверенные лиц	~									
> Поставщики сер	орнавые а паменты предварительной си									
Другие пользователи										
> MSIEHistoryJournal										
» 📔 Удаленный рабочий стол										
> 📋 Доверенные корнев	> 📋 Доверенные корневые сертификаты сма									
> 🧰 Доверенные устройства										
> Windows Live ID Toke	en Issuer									

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