Эшелон
комплексная безопасность

КОМРАД

Система управления событиями ИБ

РУКОВОДСТВО АДМИНИСТРАТОРА

НПЕШ.60010-03

Аннотация

В документе содержатся сведения о назначении изделия «Программный комплекс «KOMRAD Enterprise SIEM» НПЕШ.60010-03 (далее — ПК «Комрад», Изделие, Комплекс, Система), его архитектуре, условиях применения, последовательности действий администратора, обеспечивающих установку, запуск, конфигурирование, выполнение и завершение программы. Также приведены тексты сообщений, выдаваемых администратору в ходе работы с ПК «Комрад».

В настоящем руководстве приняты следующие обозначения.

	Пример/совет/подсказка.
	Важная информация, которую стоит принять во внимание.
	Сообщения администратору.
Кнопка	Элемент графического интерфейса «Кнопка».
`Клавиша`	Клавиша или сочетание клавиш на клавиатуре.
Жирный шрифт	Названия разделов, страниц, вкладок, диалоговых окон, файлов, терминов.

Содержание

1 Общие сведения

В данной главе содержатся общие сведения о ПК «Комрад», его функциональных возможностях и архитектуре. Рассмотрены варианты конфигурации аппаратной платформы в зависимости от необходимой производительности. Приведены базовые термины, которые используются в остальной части Руководства.

1.1 Список сокращений

В настоящем руководстве приняты следующие сокращения.

ARP — Address Resolution Protocol, протокол, который позволяет определить физический адрес по адресу сетевого уровня;
CEF — Common Event Format, формат представления записей о событиях;
CSV — Comma-Separated Values, формат представления табличных данных;
DDR — Double Data Rate, тип компьютерной памяти, используемой в вычислительной технике в качестве оперативной и видеопамяти;
DHCP — Dynamic Host Configuration Protocol, протокол динамического конфигурирования сетевого узла;
DNS — Domain Name System, распределенный механизм, используемый в сети Интернет для преобразования логических имен в сетевые адреса;
GRUB — GRand Unified Bootloader, загрузчик операционной системы;
HTML — HyperText Markup Language, стандартизированный язык разметки документов в сети Интернет;
HTTP — HyperText Transfer Protocol, протокол прикладного уровня передачи данных;
ICMP — Internet Control Message Protocol, протокол, используемый для контроля за ошибками и сообщениями на уровне сети;
EPS — Events Per Second, количество событий в секунду;
(S)FTP — (Secure) File Transfer Protocol, (защищенный) протокол передачи файлов;
GbE — Gigabit Ethernet, технология, предусматривающая передачу данных со скоростью 1 Гбит/с;
IP — Internet Protocol, основной протокол сетевого уровня;
JPEG — Joint Photographic Experts Group, растровый графический формат;
ODBC — Open Database Connectivity, стандарт доступа к базам данных;
PDF — Portable Document Format, формат электронных документов;
PNG — Portable Network Graphics, растровый графический формат;
PCI — Peripheral component interconnect, шина ввода-вывода для подключения периферийных устройств к материнской плате компьютера;
RAID — Redundant Array of Independent Disks, избыточный массив независимых дисков;
RDP — Remote Desktop Protocol, протокол прикладного уровня для обеспечения удаленной работы пользователя с сервером, на котором запущен сервис терминальных подключений;

RPC — Remote Procedure Call, класс технологий, позволяющих компьютерным программам вызывать функции или процедуры в другом адресном пространстве;
SFP — Small Form-factor Pluggable, стандарт модульных компактных трансиверов;
SNMP — Simple Network Management Protocol, стандартный интернет-протокол для управления устройствами в IP-сетях на основе архитектур TCP/UDP;
SSH — Secure Shell, протокол прикладного уровня, позволяющий производить удаленное управление операционной системой и туннелирование TCP-соединений;
SQL — Structured Query Language, язык работы с реляционными базами данных;
SVG — Scalable Vector Graphics, векторный графический формат;
TCP — Transmission Control Protocol, протокол, предназначенный для управления передачей данных с гарантированной доставкой;
UDP — User Datagram Protocol протокол, предназначенный для управления передачей данных без гарантированной доставки;
USB — Universal Serial Bus, последовательный интерфейс для подключения периферийных устройств к вычислительной технике;
UTF — Unicode Transformation Format, кодировка текста, которая позволяет хранить символы Юникода;
WMI — Windows Management Instrumentation,технология управления ОС Windows;
XSS — Cross-Site Scripting, тип атаки на веб-системы;
YAML — Yet Another Markup Language, формат сериализации данных;
Вт — ватт;
Гбайт — гигабайт, 10^9 байт;
ИБ — информационная безопасность;
ИТ — информационные технологии;
ОЗУ — оперативное запоминающее устройство;
ОС — операционная система;
ПЗУ — постоянное запоминающее устройство;
СМИБ — система менеджмента информационной безопасности;
Тбайт — терабайт, 10^{12} байт.

1.2 Термины и определения

В настоящем руководстве используются следующие термины с соответствующими определениями.

NoSQL — совокупность подходов, направленных на реализацию хранилищ баз данных, обеспечивающих следующие свойства:

- каждый запрос гарантированно завершается;

- состояние системы может изменяться со временем, даже без ввода новых данных, для достижения согласования данных;
- данные могут быть некоторое время не согласованы, но приходят к согласованию через некоторое время.

Администратор — выделенный персонал, в обязанности которого входит выполнение технологических функций по обслуживанию ПК «Комрад» и осуществление мониторинга информационной безопасности.

Актив — все, что имеет ценность для организации [ГОСТ Р ИСО/МЭК 13335-1-2006]. В контексте настоящего руководства под активом понимается конечное или сетевое устройство, имеющее IP-адрес.

База фактов — структурированное множество данных, используемых для поиска и корреляции данных.

Виджет — интерактивный блок визуализации данных, отражающий динамику их изменения в системе.

Группа реагирования на инциденты информационной безопасности — группа обученных и доверенных членов организации [ГОСТ Р ИСО/МЭК ТО 18044-2007].

Директива корреляции (RBR, rule-based reasoning) — логическая совокупность правил, построенная по иерархическому принципу, в соответствии с которыми осуществляется сравнение параметров событий ИБ, а также их количества и частоты, с заданными показателями для выявления инцидентов информационной безопасности.

Инцидент информационной безопасности (инцидент ИБ) — появление одного или нескольких нежелательных или неожиданных событий ИБ, с которыми связана значительная вероятность компрометации бизнес-операции и создания угрозы ИБ [ГОСТ Р ИСО/МЭК ТО 18044-2007].

Источник события — конечное устройство, на котором фиксируется изменение контролируемых параметров (возникновение событий ИБ).

Карточка события (инцидента, запроса, актива) — страница со сводной информацией по отдельному событию ИБ (инциденту, запросу, активу).

Конструктор запросов — элемент графического интерфейса для построения запросов на выборку данных о событиях (инцидентах) ИБ.

Корреляция данных — сравнение параметров данных о событиях ИБ с заданными граничными показателями для выявления инцидентов ИБ.

Нормализация данных — преобразование и приведение данных к единому формату для упрощения последующей обработки.

Панель виджетов — рабочая область веб-интерфейса администратора, на которой расположены виджеты; в системе может быть несколько панелей виджетов.

Плагин модуля доступности — небольшая программа, предназначенная для мониторинга доступности одного сервиса.

Плагин модуля сбора событий — программа, выполняющая сбор и первичную обработку событий ИБ.

Режим сенсора – режим, при котором коллекторы принимают события ИБ от источников событий самостоятельно.

Событие информационной безопасности (событие ИБ) — идентифицированное появление определенного состояния системы, сервиса или сети, указывающего на возможное нарушение политики ИБ или отказ защитных мер, или возникновение неизвестной ранее ситуации, которая может иметь отношение к безопасности [ГОСТ Р ИСО/МЭК ТО 18044-2007].

1.3 Назначение системы

ПК «Комрад» предназначен для мониторинга результатов регистрации событий безопасности и реагирования на них.

1.4 Основные функции

ПК «Комрад» предоставляет следующие функциональные возможности:

- сбор и хранение информации о событиях ИБ в течение установленного времени хранения;
- выборка записей событий ИБ на основе предустановленных и пользовательских фильтров;
- обнаружение, идентификация и регистрация инцидентов ИБ;
- генерация отчетов о возникших инцидентах ИБ;
- своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов;
- мониторинг доступности технических средств по протоколам ICMP, SSH, HTTP, HTTPS, SMTP;
- управление (администрирование) комплексом;
- метод управления доступом, предусматривающий присвоение субъектам доступа (операторам ПК «Комрад») прав на использование объектов доступа (пунктов меню).

1.5 Архитектура

ПК «Комрад» состоит из следующих подсистем (Рисунок 1):

- подсистема событий ИБ;

- подсистема инцидентов ИБ;
- подсистема хранения и поиска;
- подсистема мониторинга доступности;
- подсистема аналитики;
- подсистема администрирования.

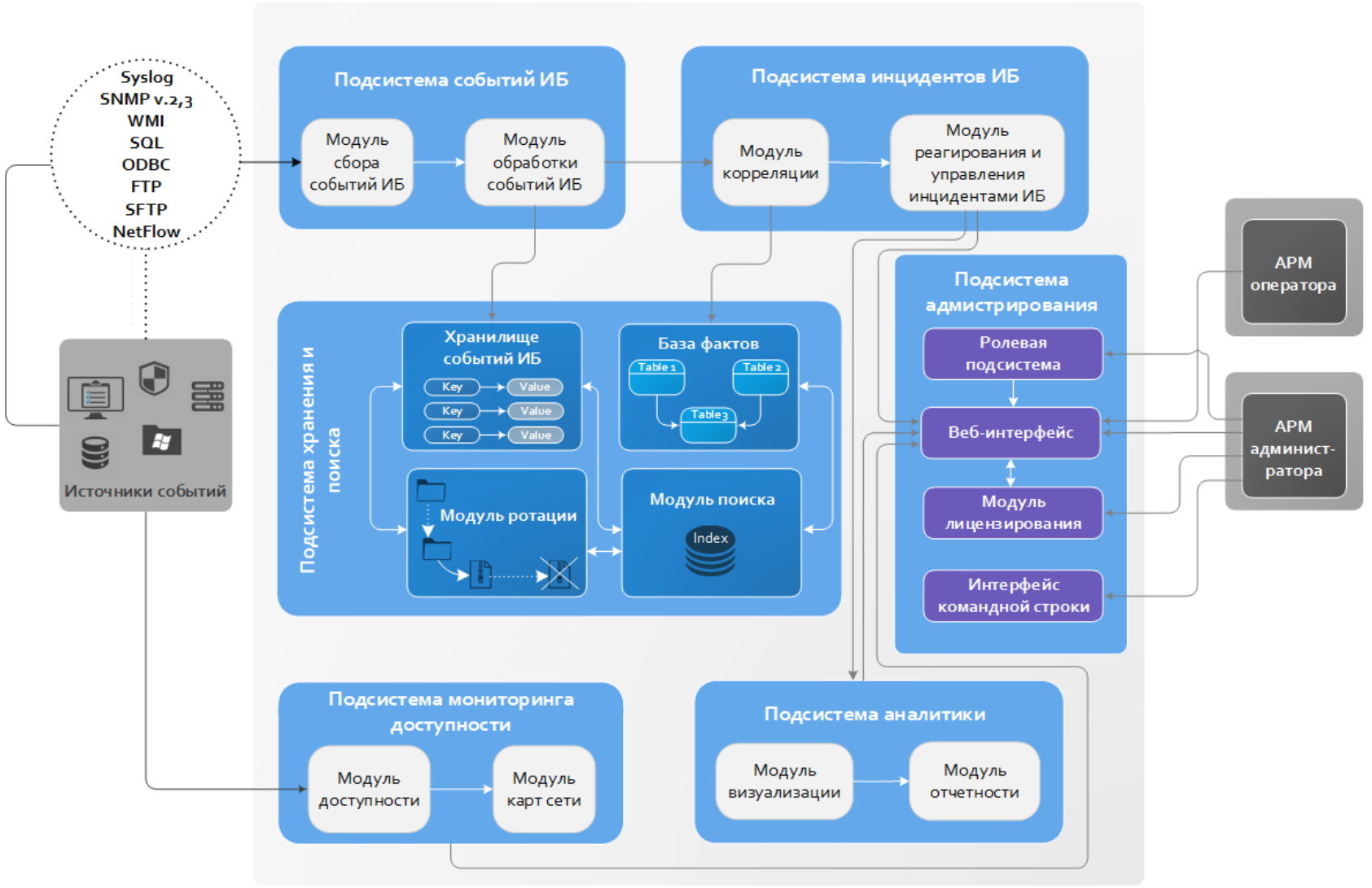


Рисунок 1. Архитектура ПК «Комрад»

1.5.1 Подсистема событий ИБ

Подсистема включает *модуль сбора событий ИБ* и *модуль обработки событий ИБ*.

1.5.1.1 Модуль сбора событий ИБ

Модуль сбора событий ИБ предназначен для оперативного сбора событий ИБ, регистрируемых источниками. Модуль сбора осуществляет свою работу посредством средств сбора и передачи информации — агентов, собственных средств конечных устройств и систем или запросов от модуля обработки событий ИБ. Сбор событий возможен посредством агента OSSEC, по протоколам и стандартам Syslog (включая формат CEF), SNMPv2, SNMPv3, методами SQL, WMI, FTP, SFTP, SSH, NetFlow.

Для получения информации о подключении источников событий ИБ см. раздел Подключение источников событий.

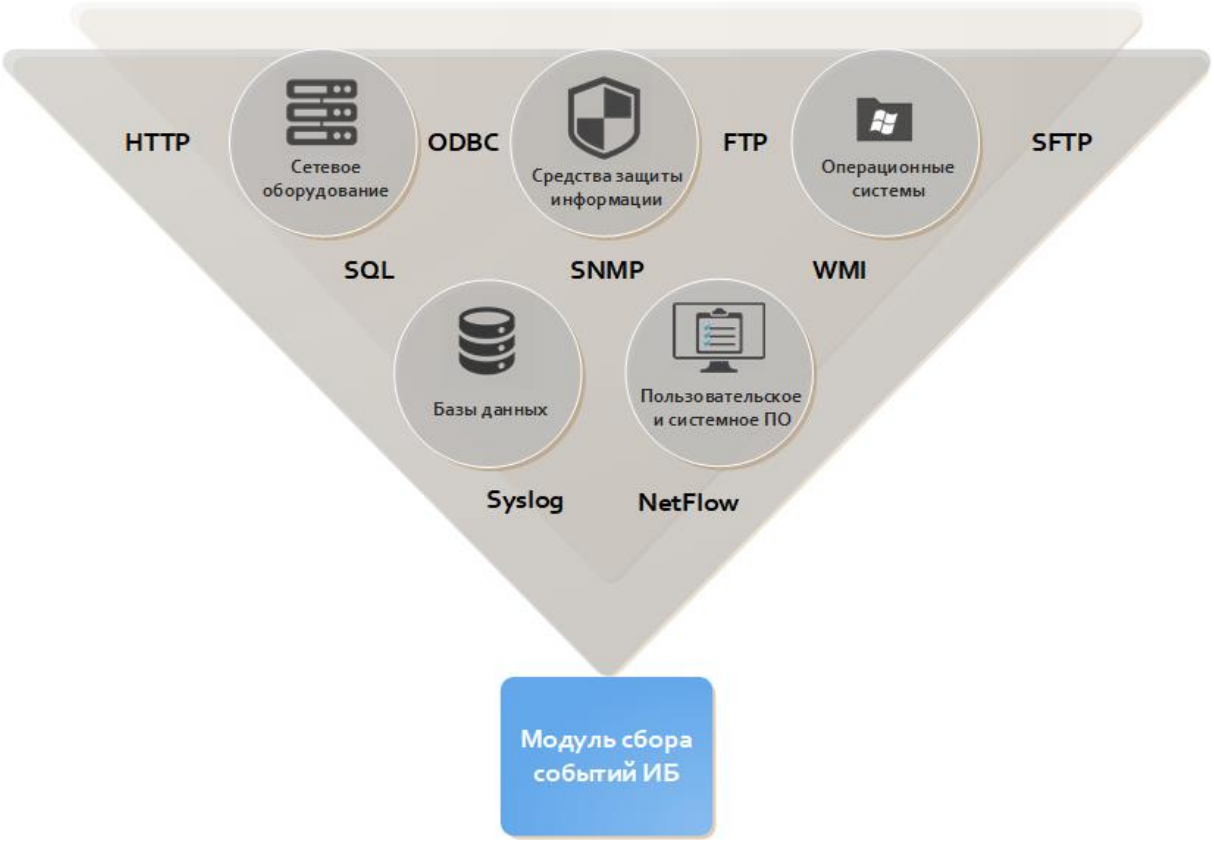


Рисунок 2. Виды источников событий ИБ

1.5.1.2 Модуль обработки событий ИБ

Модуль производит нормализацию событий в соответствии с наборами инструкций — преобразование и приведение данных к единому формату для

упрощения дальнейшего анализа — после чего передает их в хранилище событий ИБ, где каждому событию ИБ присваивается уникальный идентификатор. Для определенных событий может производиться их обогащение: например, автоматическое определение географического положения источника события по его IP-адресу.

1.5.2 Подсистема инцидентов ИБ

Подсистема включает *модуль корреляции* и *модуль реагирования и управления инцидентами ИБ*.

1.5.2.1 Модуль корреляции

Модуль предназначен для обнаружения, идентификации и регистрации инцидентов. Корреляция осуществляется в соответствии с директивами корреляции. Директива корреляции может включать цепочки правил. В системе имеется как ряд предустановленных директив, так и возможность создавать пользовательские директивы. При их создании используется визуальный конструктор. Предоставляются механизмы управления директивами: возможность приостановить/возобновить работу директивы, изменить состав и содержание ее правил, удалить. Предусмотрена возможность создания правил типа «отсутствие событий». Если в течение заданного времени не поступило ни одного события, удовлетворяющего критериям этого правила, будет сформирован инцидент ИБ. Описанный механизм позволяет отслеживать нарушение доступности актива.

1.5.2.2 Модуль реагирования и управления инцидентами ИБ

Модуль предназначен для управления жизненным циклом инцидента (workflow). При возникновении инцидента группа реагирования на инциденты информационной безопасности получает всплывающее уведомление в графическом интерфейсе. Оповещение об инциденте может быть автоматически отправлено ответственному лицу или группе лиц по E-mail, согласно заданному шаблону письма. При обнаружении инцидента в системе создается задача для расследования инцидента, задаче могут быть присвоены различные статусы. Предусмотрена возможность исполнения пользовательских сценариев при возникновении инцидента.

1.5.3 Подсистема хранения и поиска

Подсистема включает *хранилище событий ИБ*, *базу фактов*, *модуль поиска* и *модуль ротации*.

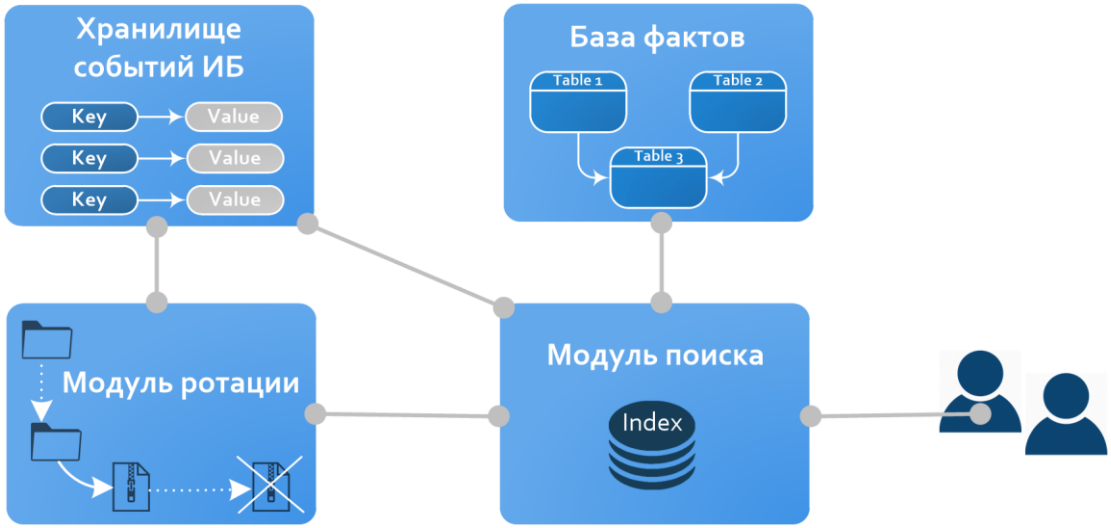


Рисунок 3. Подсистема хранения и поиска

1.5.3.1 Хранилище событий ИБ

Нормализованные события ИБ, данные об инцидентах ИБ и информация о настройках системы хранятся в нереляционной (NoSQL) базе данных, что позволяет более эффективно осуществлять выборку большого количества данных.

1.5.3.2 База фактов

База фактов представляет собой структурированное множество данных, используемых для поиска и корреляции событий ИБ.

1.5.3.3 Модуль поиска

Модуль позволяет осуществлять выборку событий при помощи визуального конструктора запросов. Используется механизм индексации для ускорения полнотекстового поиска.

1.5.3.4 Модуль ротации

Модуль позволяет управлять временем хранения событий безопасности, архивировать события, управлять временем хранения архивов. События, помещенные в архив, занимают меньший объем памяти, но недоступны для поиска. Минимальное время хранения событий составляет 1 день, максимальное время зависит от объема используемого дискового пространства. Подробнее см. раздел Хранилище событий.

1.5.4 Подсистема мониторинга доступности

Подсистема включает *модуль доступности* и *модуль карт сети*.

1.5.4.1 Модуль доступности

Модуль позволяет осуществлять контроль функционирования технических средств, обнаружение и локализацию отказов функционирования. Подробнее см. раздел Доступность.

1.5.4.2 Модуль карт сети

Модуль позволяет располагать технические средства, контролируемые модулем доступности, на карте, устанавливать в качестве карты пользовательское фоновое изображение. Подробнее см. раздел Карта.

1.5.5 Подсистема аналитики

Подсистема включает *модуль визуализации* и *модуль отчетности*.

1.5.5.1 Модуль визуализации

Возможности модуля визуализации позволяют отображать события в виде графиков и диаграмм (линейные, столбчатые, круговые, радиальные и др.). В системе есть следующие диаграммы:

- диаграмма событий в реальном времени: позволяет видеть распределение событий во времени и отслеживать «всплески», которые могут свидетельствовать об инциденте ИБ;
- диаграмма событий на странице запросов к базе событий: предназначена для повышения эффективности и скорости поиска нужных событий;
- диаграмма событий инцидента: отражает распределение событий отдельно взятого инцидента во времени.

Администратор может создавать и настраивать собственные виджеты и менять настройки панели виджетов.

Модуль предоставляет интерфейс для контроля соответствия защищаемой информационной системы нормативным документам, включающий диаграмму со сводной статистикой по выполнению требований ГОСТ Р ИСО/МЭК 27001-2006. Подробнее см. раздел Контроль соответствия.

Модуль включает инструментарий для расследования инцидентов — визуализатор событий. Он предназначен для построения визуальной модели инцидента, выявления аномалий и поведенческого анализа, может быть задействован при расследовании инцидента. Подробнее см. раздел Визуализатор событий.

1.5.5.2 Модуль отчетности

Модуль предоставляет следующие возможности по экспорту данных и созданию отчетов:

- экспорт данных виджета (в формате PDF);
- экспорт событий ИБ в соответствии с заданными критериями поиска (в форматах CSV, PDF);
- сводный отчет по инцидентам (в форматах CSV, PDF);
- отчет по отдельно взятому инциденту, включая изменение его состояния и свойств на протяжении всего жизненного цикла (в формате PDF);
- экспорт диаграммы соответствия ГОСТ Р ИСО/МЭК 27001-2006 (в формате PDF).

Взаимодействие администратора безопасности с ПК «Комрад» осуществляется с использованием веб-интерфейса и интерфейса командной строки.

1.5.6 Подсистема администрирования

Подсистема включает *веб-интерфейс*, *ролевую подсистему*, *модуль лицензирования* и *интерфейс командной строки*.

1.5.6.1 Ролевая подсистема

Ролевая подсистема позволяет создавать, настраивать и удалять учетные записи пользователей, роли и группы. Подробнее см. раздел Пользователи.

1.5.6.2 Веб-интерфейс

Веб-интерфейс предназначен для взаимодействия администратора безопасности с ПК «Комрад».

1.5.6.3 Модуль лицензирования

Модуль лицензирования предназначен для активации установленных модулей посредством веб-интерфейса. Подробнее см. раздел Активация.

1.5.6.4 Интерфейс командной строки

Интерфейс командной строки предназначен для обеспечения администратору безопасности возможности управления системой и предоставления данных об ошибках и сбоях компонентов ПК «Комрад». Подробнее см. раздел Интерфейс командной строки.

1.6 Конфигурация аппаратной части платформы

Ниже представлена рекомендуемая конфигурация аппаратной платформы в зависимости от производительности.

EPS	Аппаратная платформа	Процессор	ОЗУ	RAID	ПЗУ	Доп. возможности
500 1000 2000	SL1500/1U4G2 (1U, 2 сетевых интерфейса GbE, 1 блок питания 350 Вт)	6-ядерный процессор Xeon-E5-2603V4	2x8 Гб DDR 4	10	4x2000 Гбайт	Резервируемый блок питания (2x400 Вт), увеличение объема ОЗУ до 256 Гб, установка дополнительного сетевого адаптера (4xSFP или 4xRJ45), возможность увеличения времени хранения данных
5000	SL2500/2U8LG3 (2U, 2 сетевых интерфейса GbE, 1 блок питания 563 Вт, 3xPCI-E (8x)), низкопрофильный 3xPCI-E (4x)	два 6-ядерных процессора Xeon-E5-2603V4	4x8 Гб DDR 4	10	4x10 Тбайт	Резервируемый блок питания (2x740 Вт), увеличение объема ОЗУ до 256 Гб, установка дополнительного сетевого адаптера (4xSFP или 4xRJ45), возможность увеличения времени хранения данных

2 Установка и загрузка

В данной главе содержатся сведения об этапах установки ПК «Комрад» и его загрузке.

2.1 Шаг 1. Начало

Для установки запустите ISO-образ на аппаратной платформе, конфигурация которой соответствует рекомендуемой (раздел Конфигурация аппаратной части платформы). Откроется начальное окно установки (Рисунок 4), в котором необходимо выбрать один из вариантов установки, представленных в таблице ниже.

Вариант установки	Описание
Полная установка	Полная установка ПК «Комрад»
Выборочная установка	Установка ПК «Комрад» с выбором устанавливаемых модулей

Выберите вариант установки и нажмите клавишу `Enter`.

Рисунок 4. Начальное окно установки ПК «Комрад»

2.2 Шаг 2. Подготовка к установке

Необходимо дождаться окончания загрузки дополнительных компонентов (Рисунок 5). На данном шаге от администратора не требуется никаких действий.

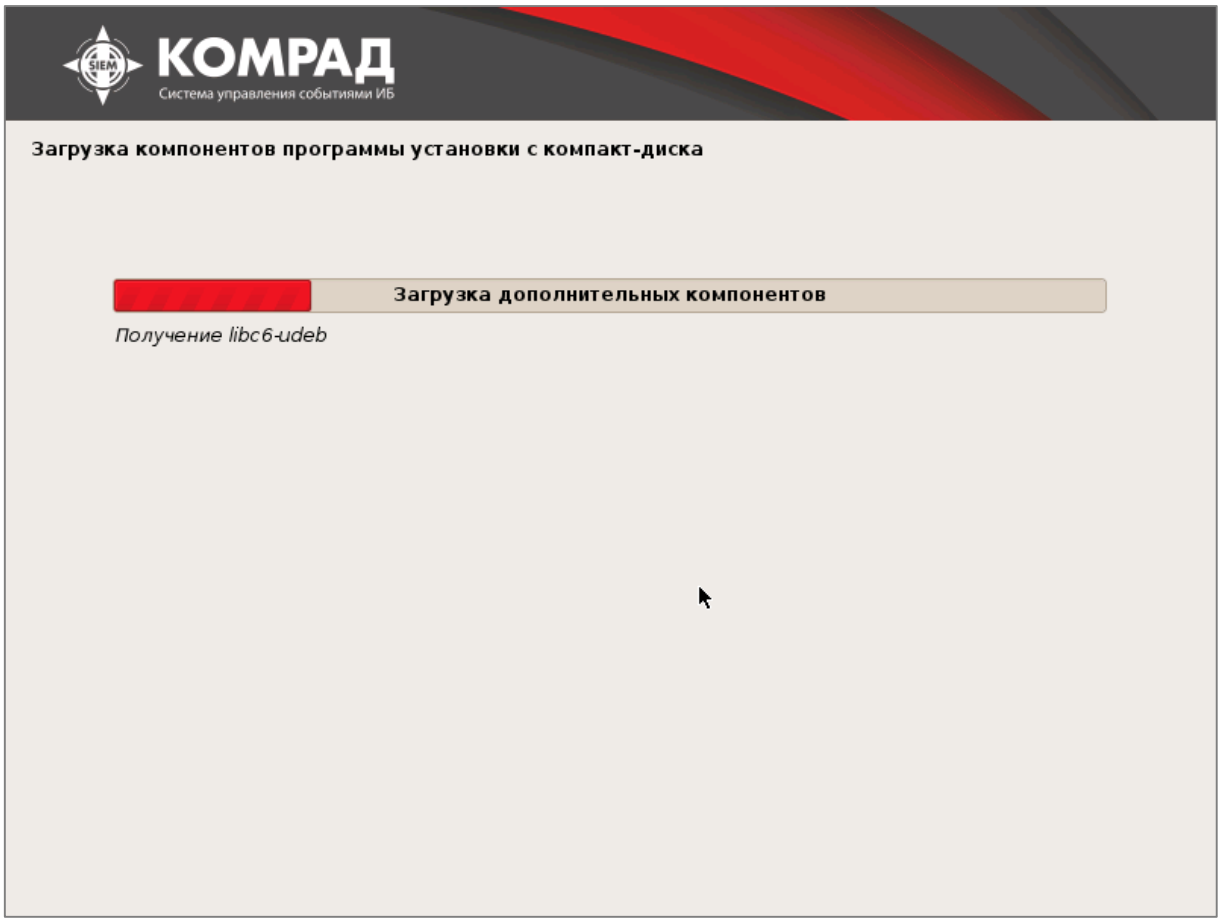


Рисунок 5. Загрузка дополнительных компонентов

2.3 Шаг 3. Настройка сети

2.3.1 Выбор сетевого интерфейса

Если на платформе более одного сетевого интерфейса, необходимо выбрать, какой из них будет использован как основной (Рисунок 6). По умолчанию, выбран первый обнаруженный интерфейс. Для перехода к следующему шагу нажмите кнопку **Продолжить**, для возврата к предыдущему шагу нажмите кнопку **Вернуться**.

Если сетевой интерфейс один, данный шаг будет пропущен.

В ходе установки существует возможность сделать снимок экрана, нажав кнопку **Снимок экрана** в интерфейсе мастера установки.

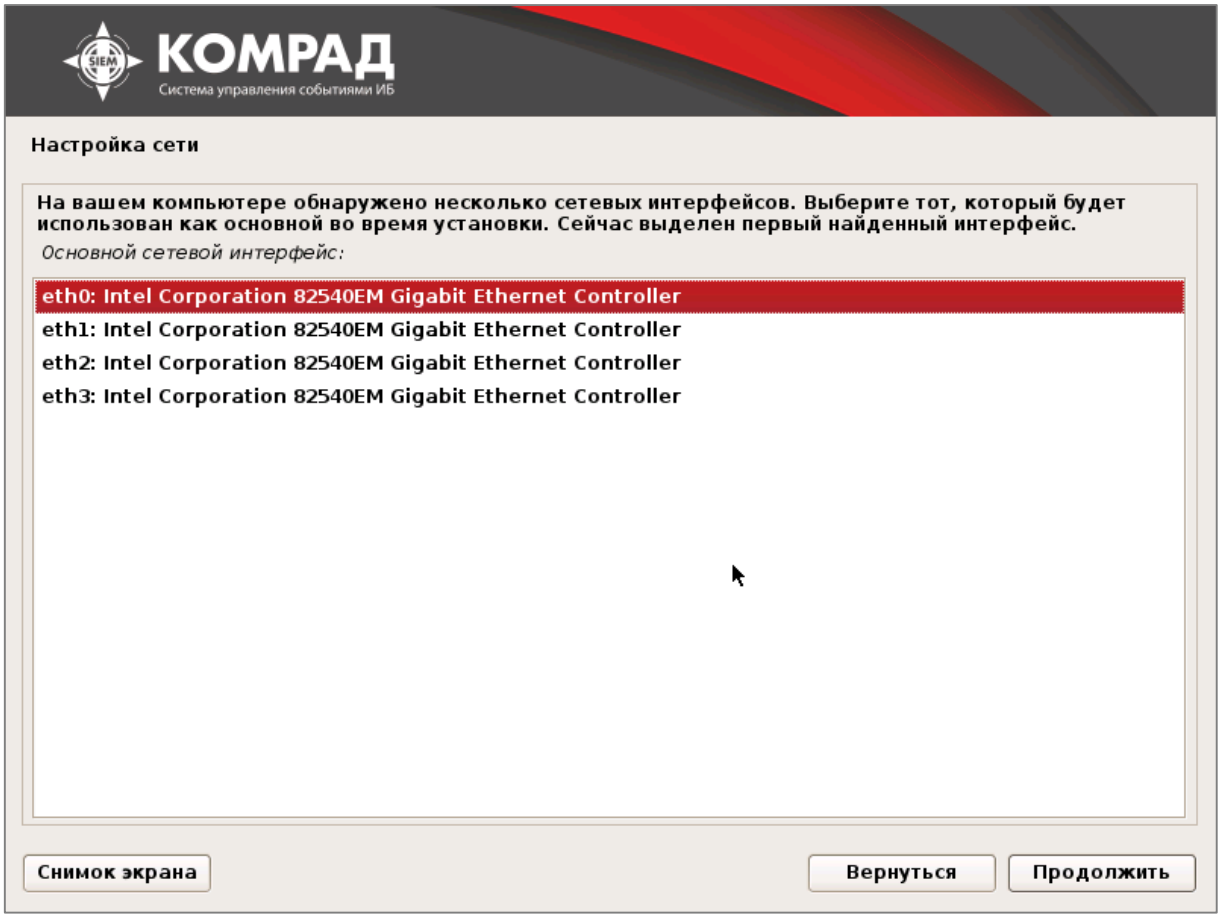


Рисунок 6. Выбор сетевого интерфейса

2.3.2 Настройка сетевых параметров

2.3.2.1 Вариант 1. Автоматическая настройка сети

Если в вашей сети используется DHCP-север, сетевые настройки будут установлены автоматически (Рисунок 7). В противном случае переходите к Варианту 2 Ручная настройка сети.

Рисунок 7. Получение настроек сети по DHCP

2.3.2.2 Вариант 2. Ручная настройка сети

Укажите метод настройки сети **Настроить сеть вручную** (Рисунок 8). Для перехода к следующему шагу нажмите кнопку **Продолжить**, для возврата к предыдущему шагу нажмите кнопку **Вернуться**.

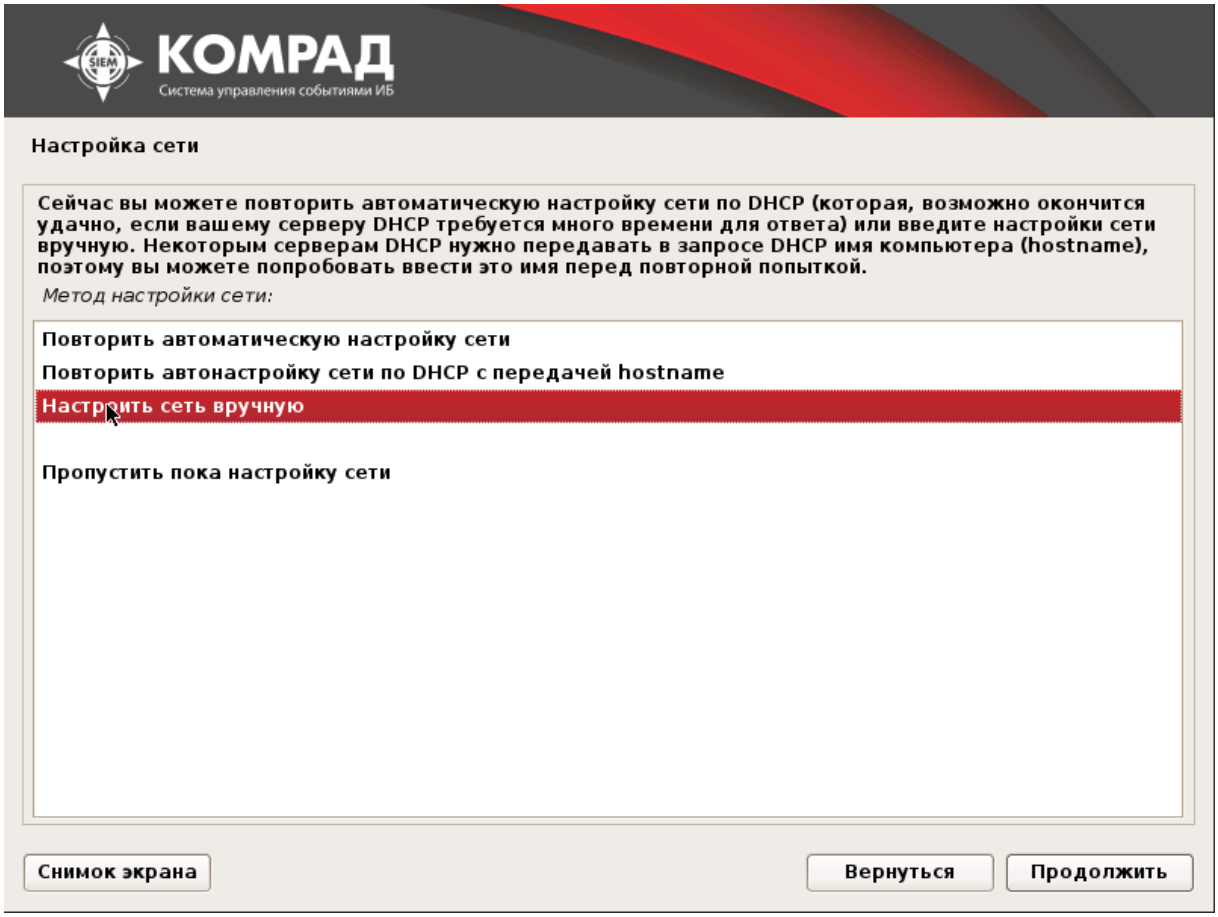


Рисунок 8. Выбор метода настройки сети

2.3.2.2.1 IP-адрес сети

Задайте IP-адрес ПК «Комрад» в Вашей сети (Рисунок 9). Для перехода к следующему шагу нажмите кнопку **Продолжить**, для возврата к предыдущему шагу нажмите кнопку **Вернуться**.

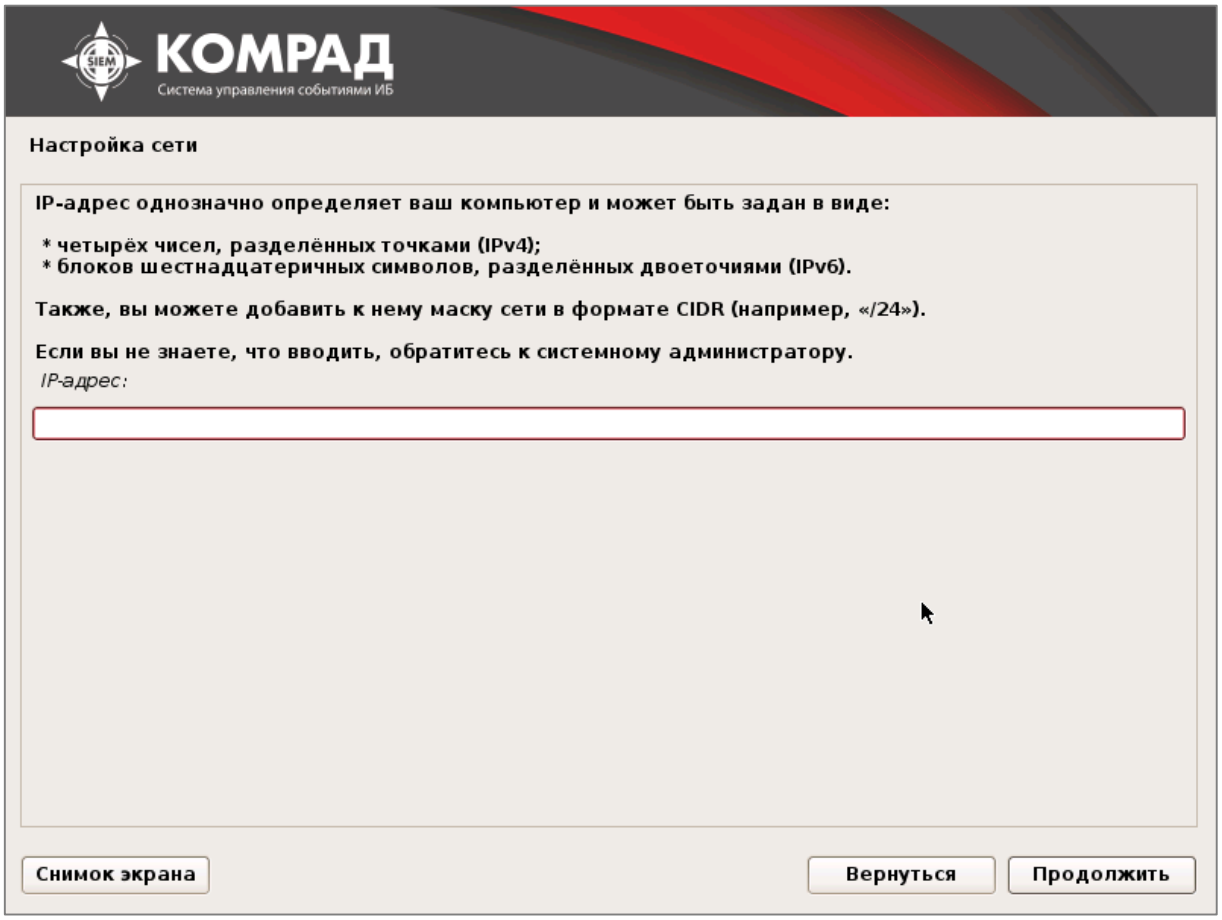


Рисунок 9. Назначение IP-адреса

2.3.2.2.2 Маска подсети

Укажите маску подсети (Рисунок 10). Для перехода к следующему шагу нажмите кнопку **Продолжить**, для возврата к предыдущему шагу нажмите кнопку **Вернуться**.

Рисунок 10. Назначение маски подсети

2.3.2.2.3 IP-адрес маршрутизатора

Укажите шлюз (Рисунок 11). Для перехода к следующему шагу нажмите кнопку **Продолжить**, для возврата к предыдущему шагу нажмите кнопку **Вернуться**.

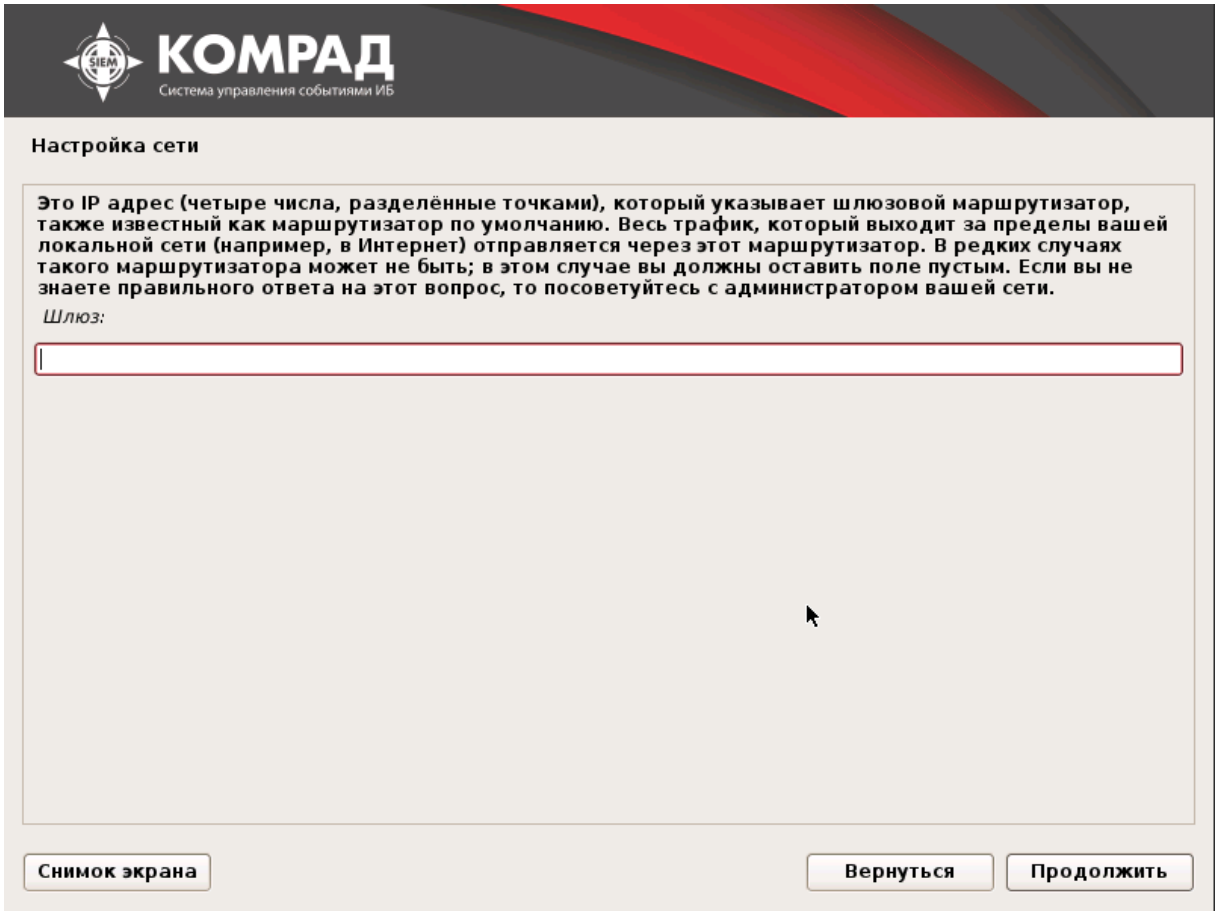


Рисунок 11. Назначение IP-адреса маршрутизатора

2.3.2.2.4. IP-адреса DNS серверов

Укажите IP-адреса DNS-серверов (Рисунок 12). Для перехода к следующему шагу нажмите кнопку **Продолжить**, для возврата к предыдущему шагу нажмите кнопку **Вернуться**.

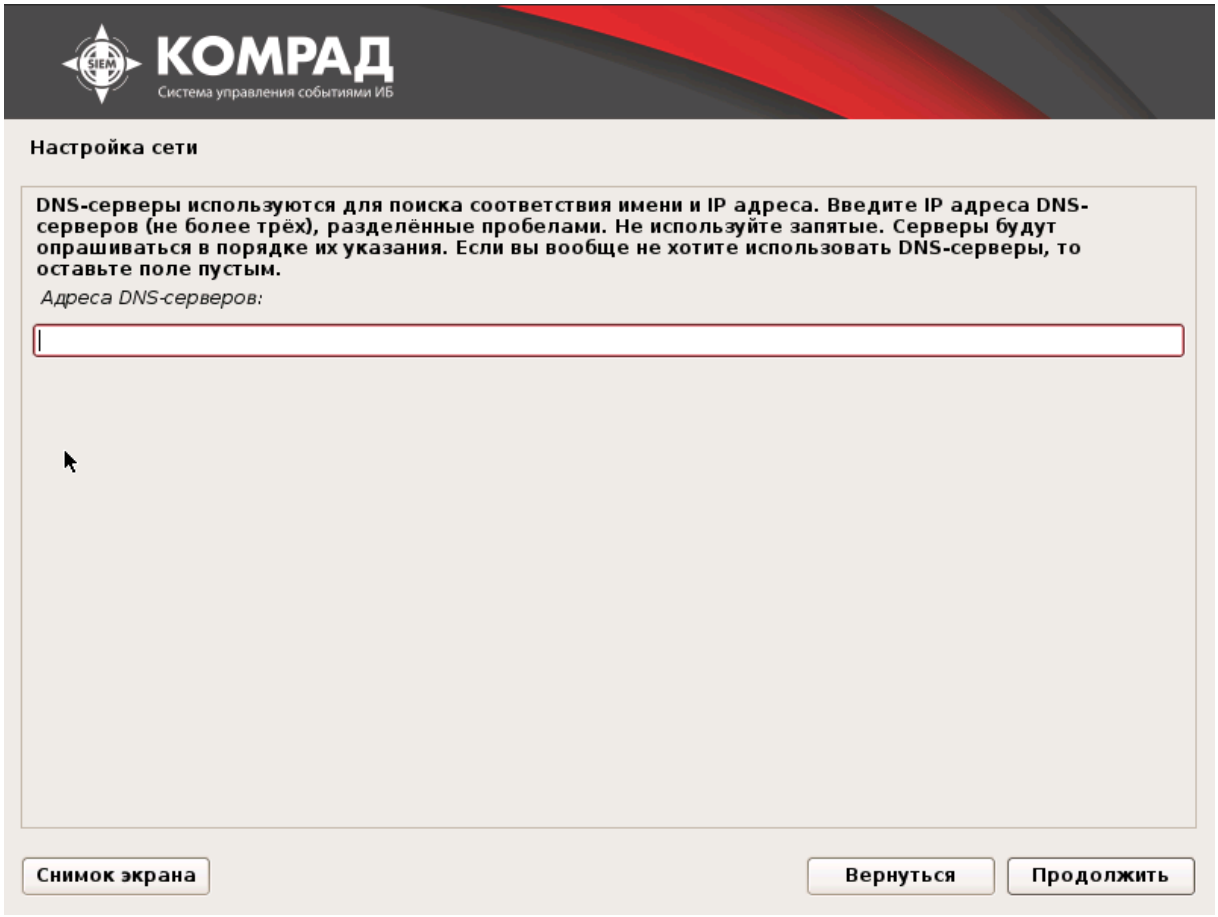


Рисунок 12. Назначение IP-адресов DNS серверов

2.3.3 Назначение идентификатора

Назначьте идентификатор (имя компьютера) для ПК «Комрад» (Рисунок 13). Для перехода к следующему шагу нажмите кнопку **Продолжить**, для возврата к предыдущему шагу нажмите кнопку **Вернуться**.

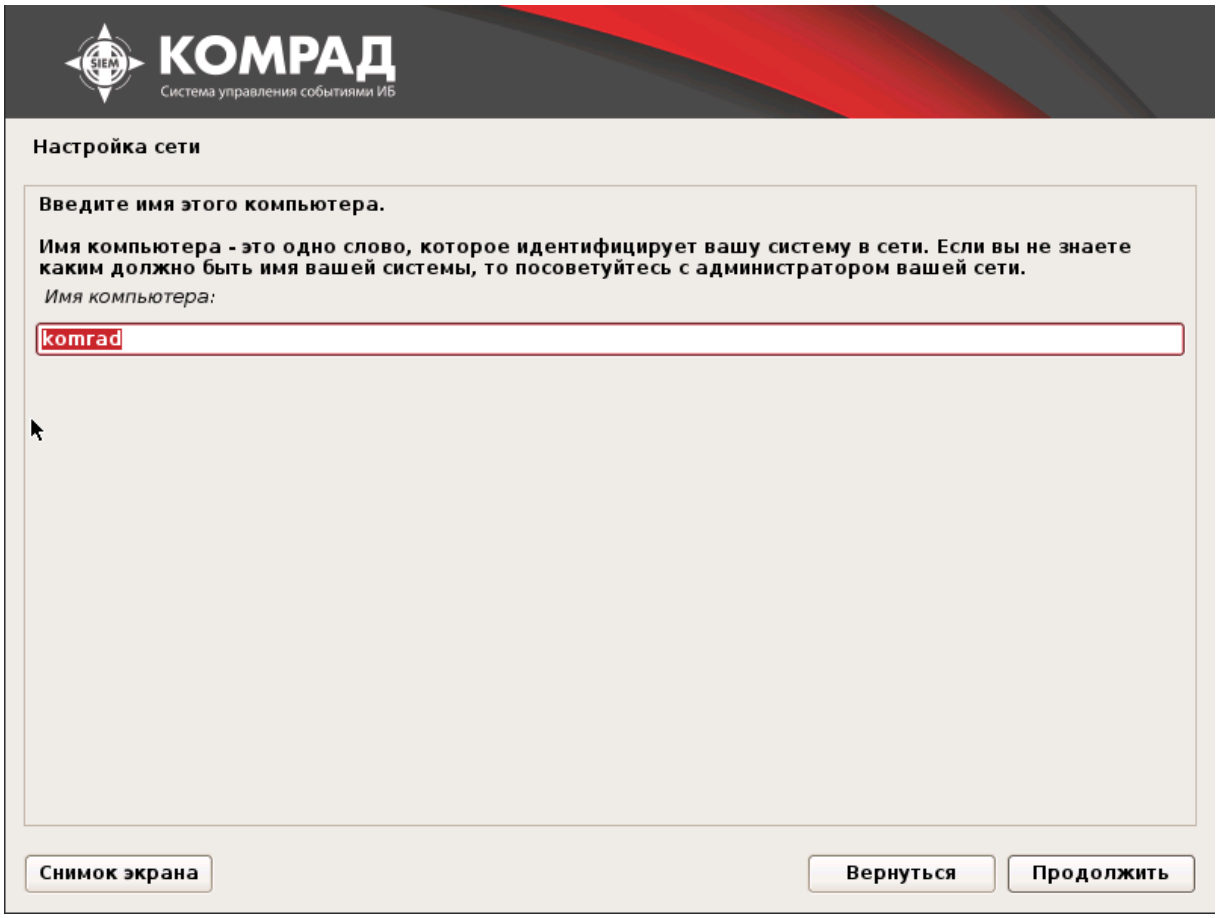


Рисунок 13. Назначение имени устройства

2.4 Шаг 4. Настройка учетной записи

Назначьте пароль пользователя **admin** (Рисунок 14). Учетная запись admin будет использоваться для доступа к интерфейсу командной строки. Для перехода к следующему шагу нажмите кнопку **Продолжить**, для возврата к предыдущему шагу нажмите кнопку **Вернуться**.

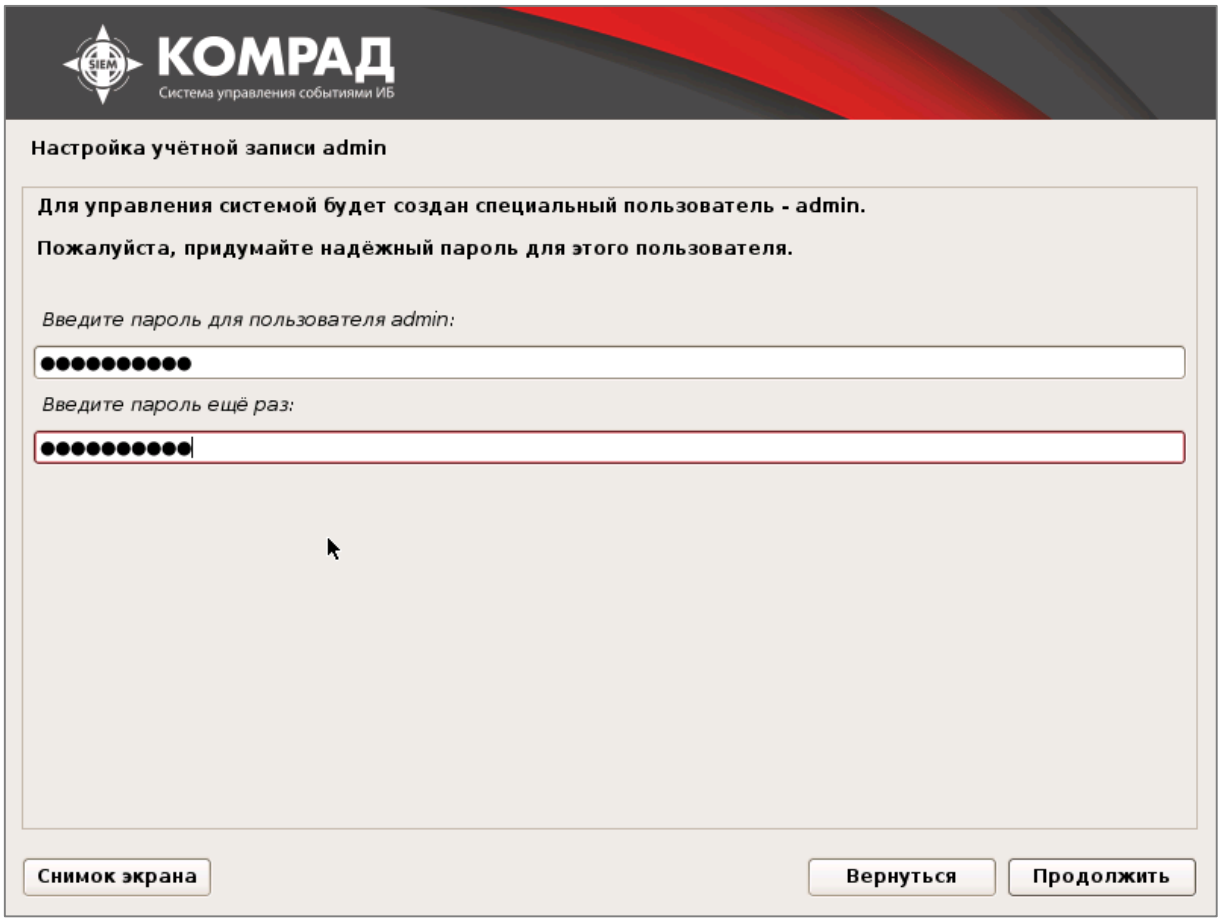


Рисунок 14. Настройка пароля пользователя admin

2.5 Шаг 5. Настройка часового пояса

Укажите часовой пояс (Рисунок 15). Для перехода к следующему шагу нажмите кнопку **Продолжить**, для возврата к предыдущему шагу нажмите кнопку **Вернуться**.

Рисунок 15. Настройка часового пояса

2.6 Шаг 6. Разметка дисков

2.6.1Автоматическая разметка

2.6.1.1 Выбор метода разметки

Для автоматической разметки жесткого диска выберите метод разметки **Авто – использовать весь диск** (Рисунок 16). Для перехода к следующему шагу нажмите кнопку **Продолжить**, для возврата к предыдущему шагу нажмите кнопку **Вернуться**.

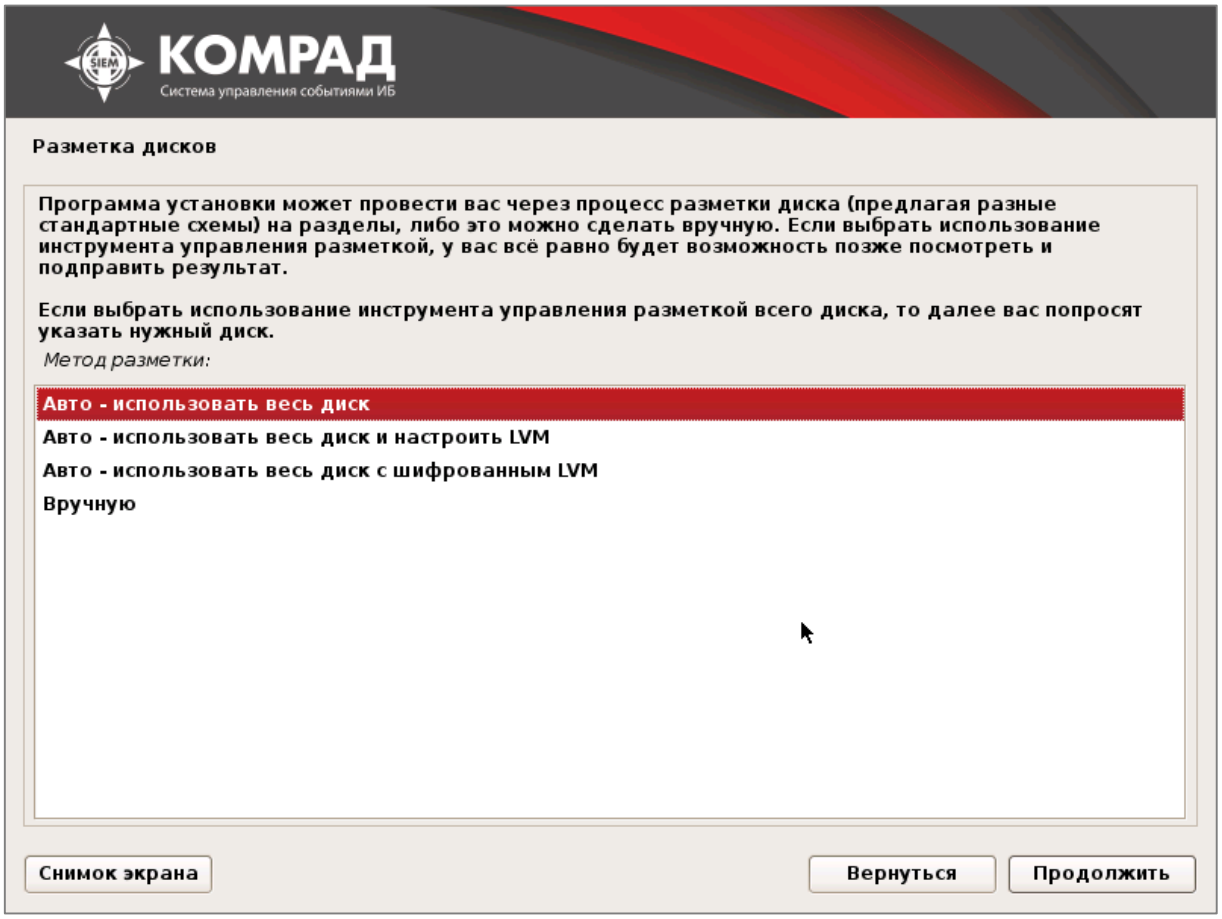


Рисунок 16. Выбор метода автоматической разметки диска

2.6.1.2 Выбор диска

Выберите жесткий диск, на который будет установлен комплекс (Рисунок 17). Для перехода к следующему шагу нажмите кнопку **Продолжить**, для возврата к предыдущему шагу нажмите кнопку **Вернуться**.

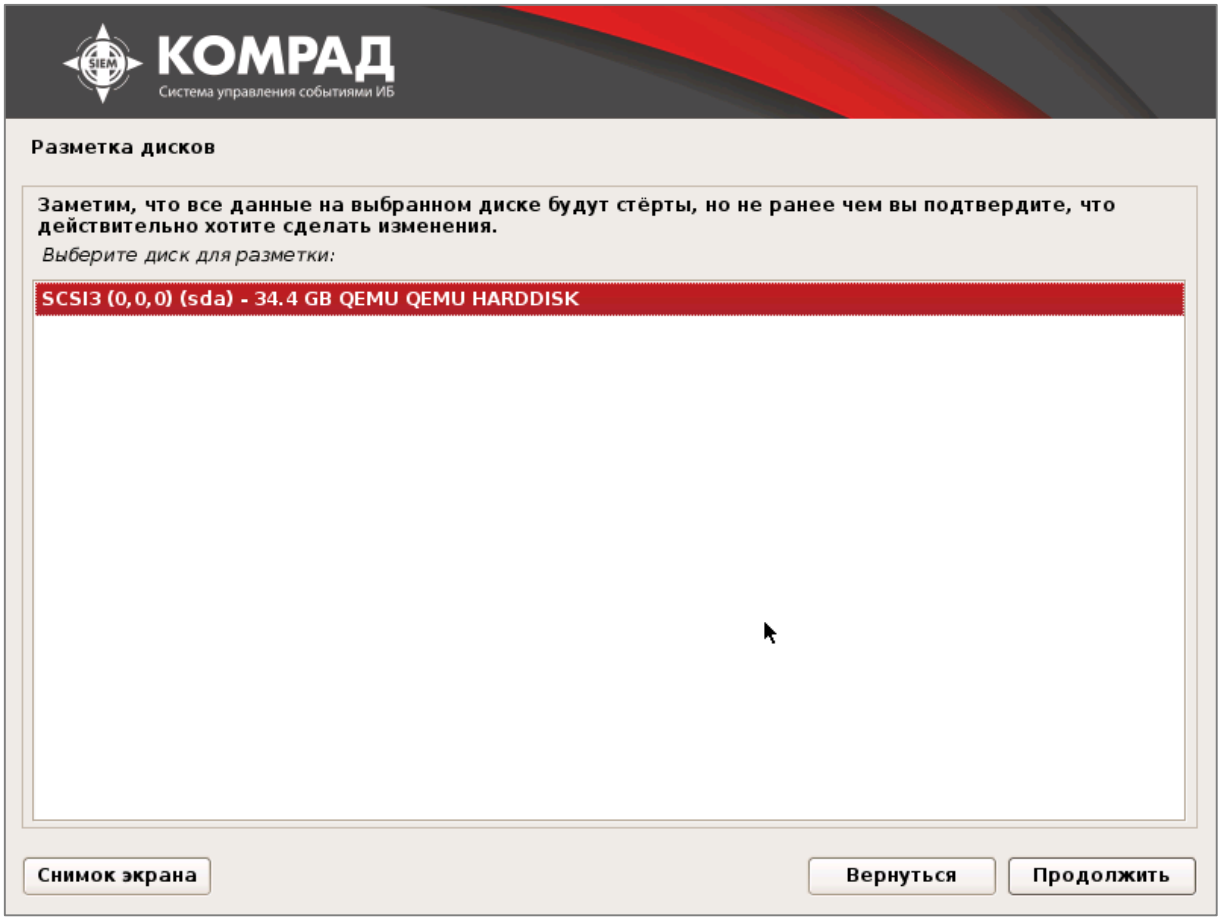


Рисунок 17. Выбор диска

2.6.1.3 Выбор схемы разметки

Выберите схему разметки жесткого диска (Рисунок 18). Для перехода к следующему шагу нажмите кнопку **Продолжить**, для возврата к предыдущему шагу нажмите кнопку **Вернуться**.

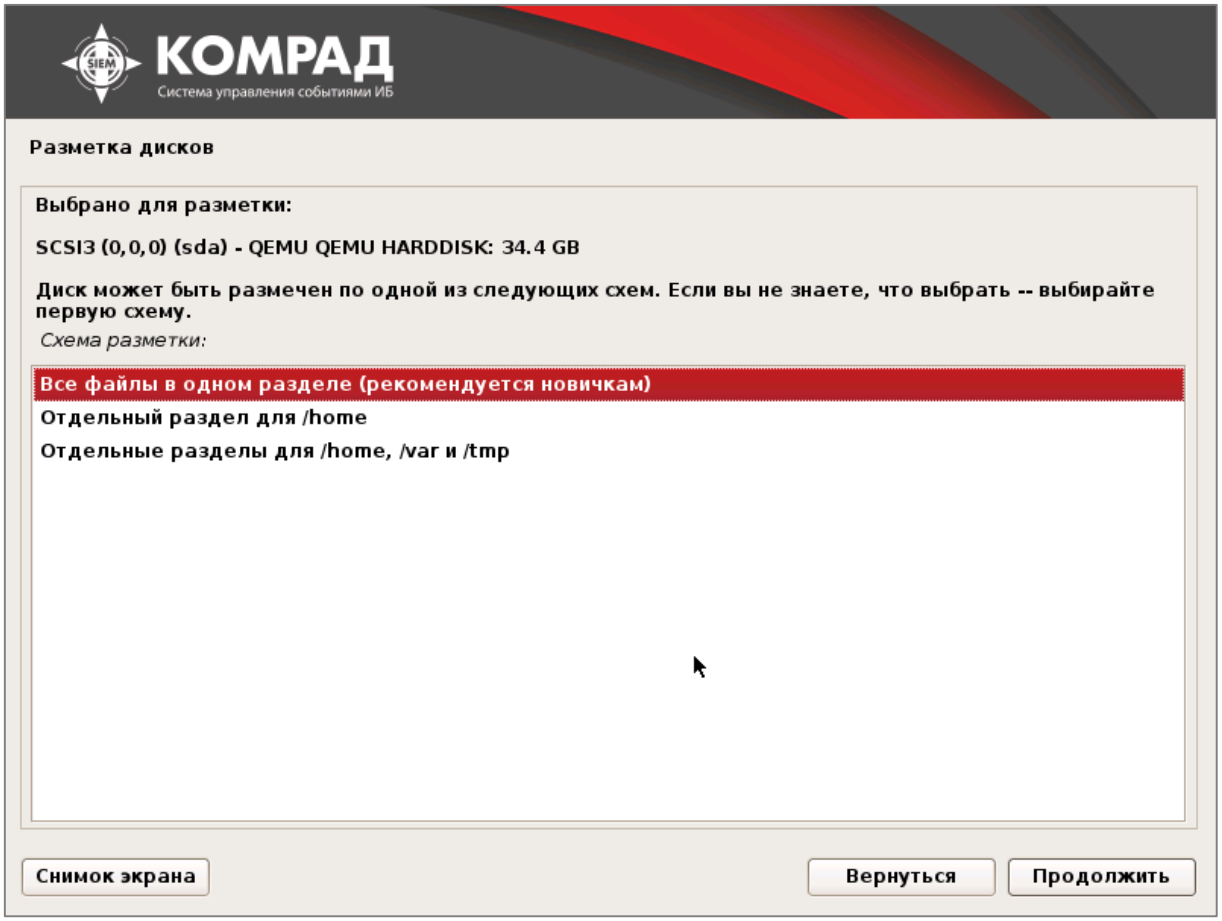


Рисунок 18. Выбор схемы разметки диска

2.6.1.4 Завершение разметки дисков

Завершите разметку дисков, выбрав пункт меню **Закончить разметку и запись изменения на диск** (Рисунок 19). Для перехода к следующему шагу нажмите кнопку **Продолжить**, для возврата к предыдущему шагу нажмите кнопку **Вернуться**.

При нажатии на кнопку **Справка** выводится основная информация по разметке дисков (Рисунок 20).

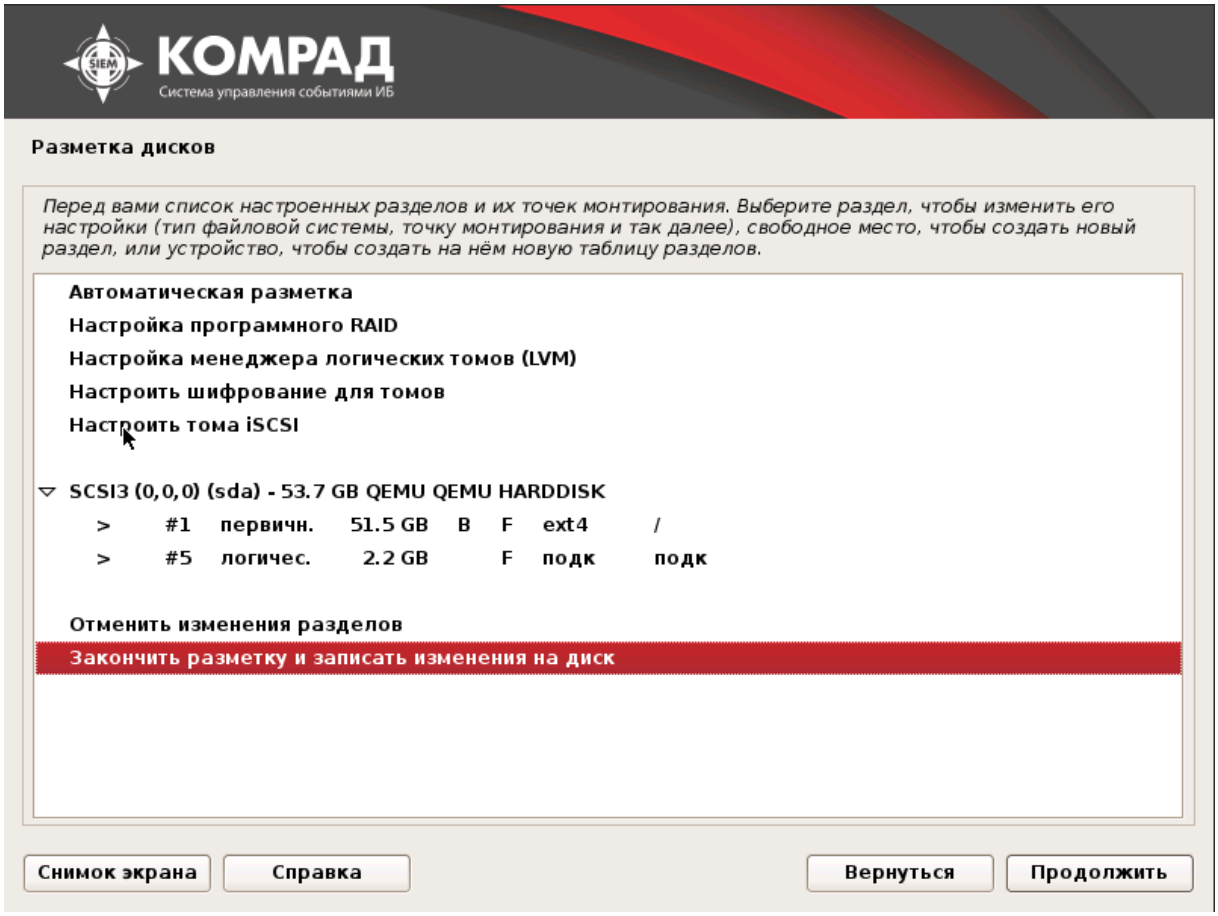


Рисунок 19. Завершение разметки дисков

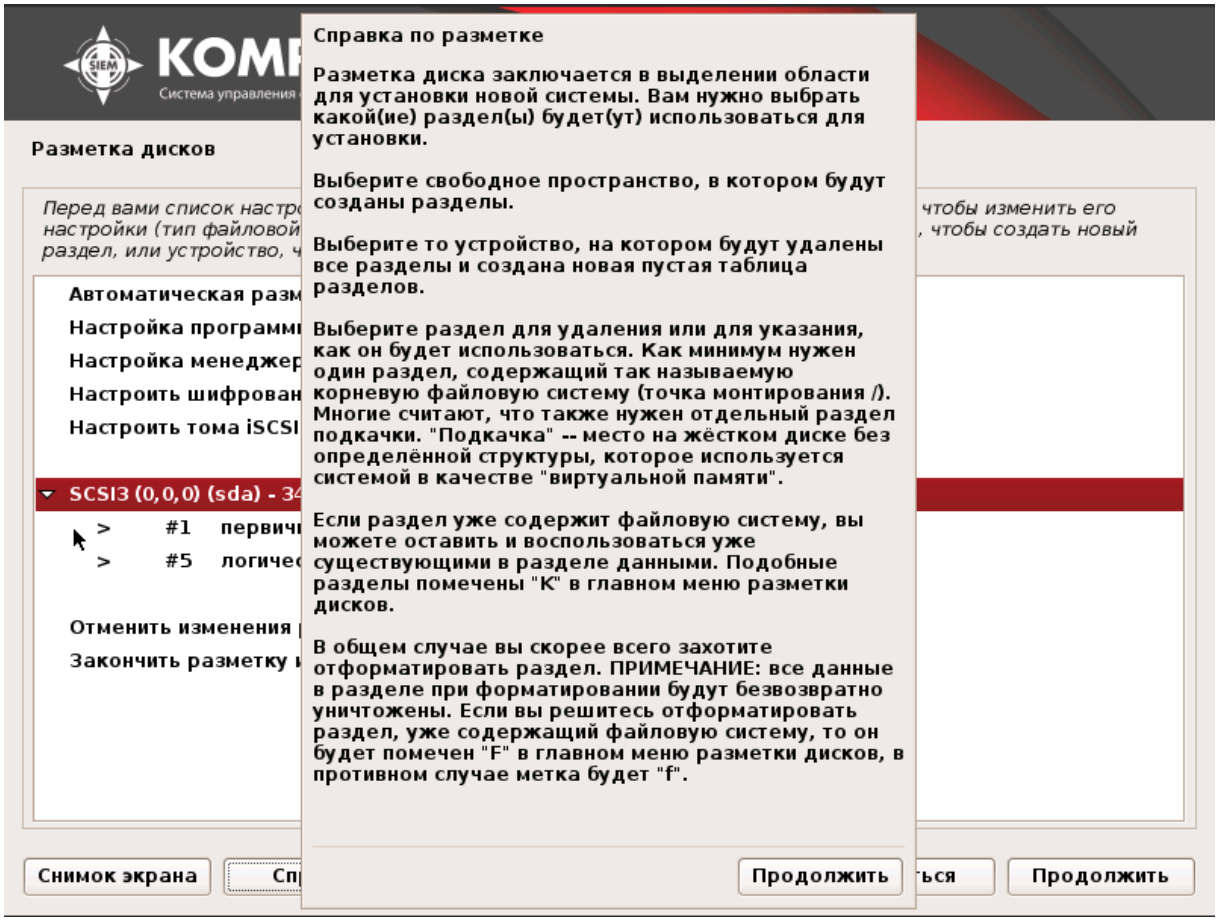


Рисунок 20. Справка по разметке

2.6.1.5 Сохранение автоматической разметки дисков

Подтвердите или отклоните сохранение разметки дисков (Рисунок 21). Для перехода к следующему шагу нажмите кнопку **Продолжить**.

Рисунок 21. Сохранение автоматической разметки

2.6.2Разметка диска вручную

2.6.2.1 Выбор метода разметки

Выберите метод разметки диска **Вручную** (Рисунок 22). Для перехода к следующему шагу нажмите кнопку **Продолжить**, для возврата к предыдущему шагу нажмите кнопку **Вернуться**.

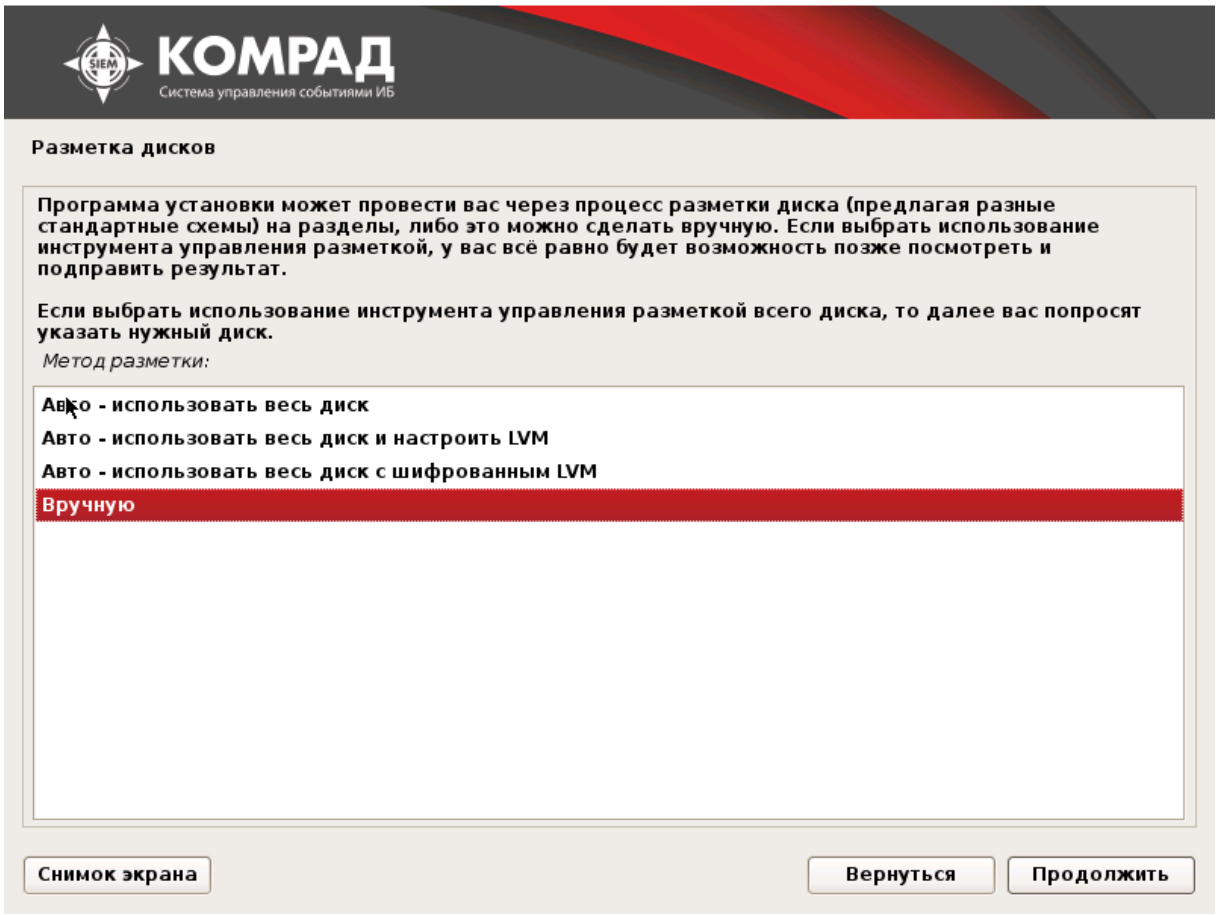


Рисунок 22. Выбор метода ручной разметки диска

2.6.2.2 Выбор диска

Выберите жесткий диск, на который будет установлен комплекс (Рисунок 23). Для перехода к следующему шагу нажмите кнопку **Продолжить**, для возврата к предыдущему шагу нажмите кнопку **Вернуться**.

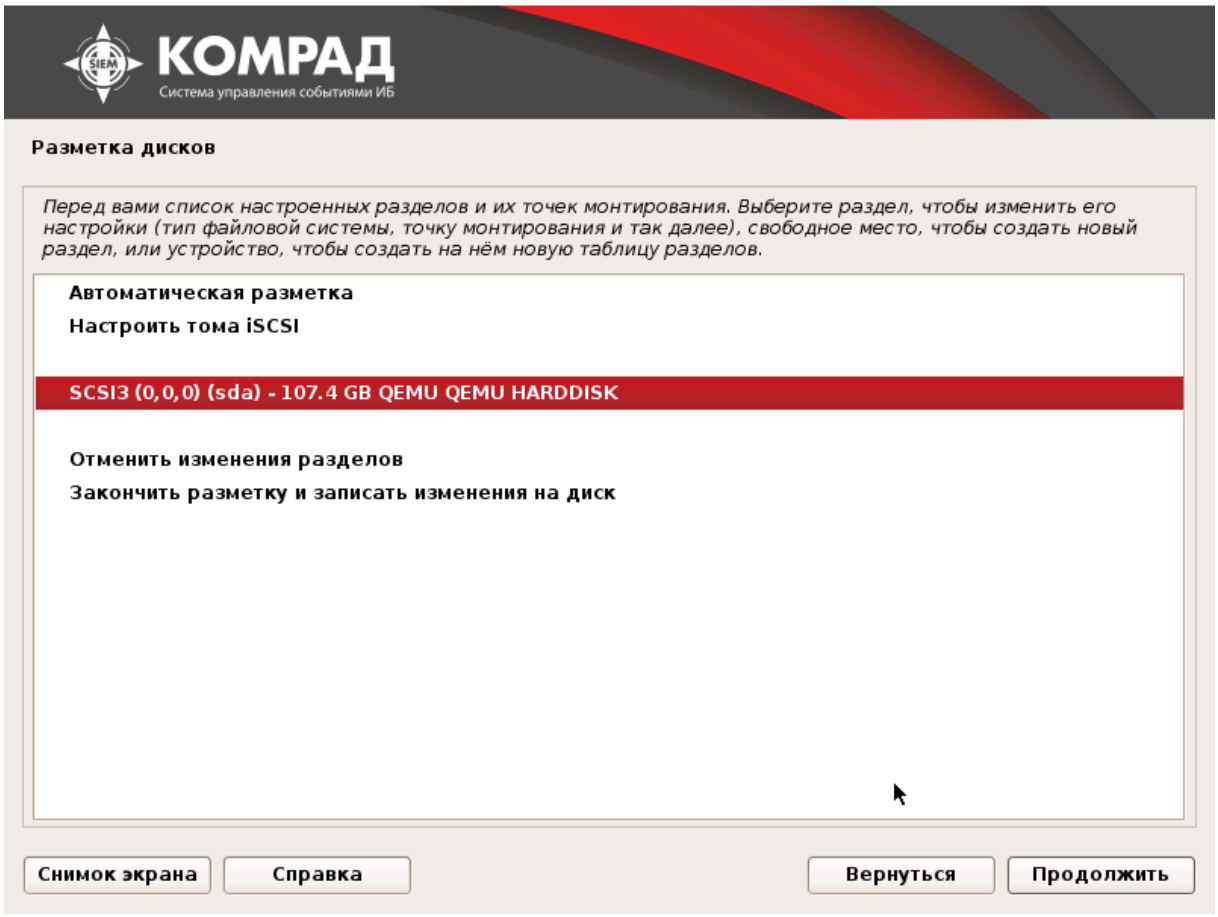


Рисунок 23. Выбор диска

2.6.2.3 Создание новой таблицы разделов

Подтвердите создание новой таблицы разделов, выбрав **Да** (Рисунок 24). Для перехода к следующему шагу нажмите кнопку **Продолжить**, для возврата к предыдущему шагу нажмите кнопку **Вернуться**.

Рисунок 24. Создание новой таблицы разделов

2.6.2.4 Выбор свободного места

Выберите свободное место, которое необходимо разметить (Рисунок 25), нажмите кнопку **Продолжить**, для возврата к предыдущему шагу нажмите кнопку **Вернуться**.

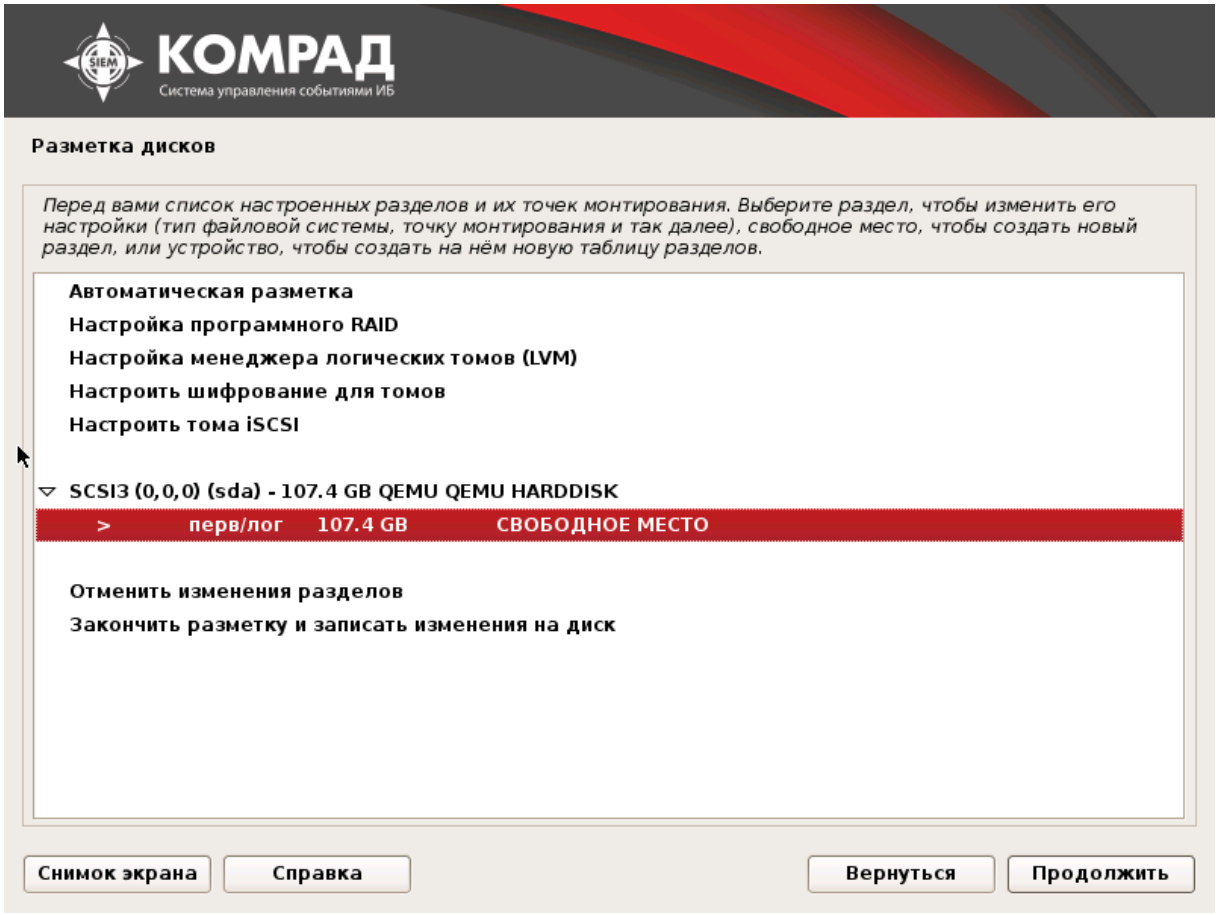


Рисунок 25. Выбор свободного пространства

2.6.2.5 Создание загрузочного раздела

Выберите пункт **Создать новый раздел**. При помощи мастера разметки создайте загрузочный раздел со следующими параметрами.

Параметр	**Значение**
Новый размер раздела	200 MB
Тип нового раздела	Первичный
Местоположение нового раздела	Начало
Использовать как	Журналируемая файловая система Ext4
Точка монтирования	/boot
Параметры монтирования	defaults
Метка	отсутствует
Зарезервированные блоки	5%
Обычное использование	стандарт
Метка ‘загрузочный’	вкл

Данные параметры представлены в качестве примера.

Завершите создание загрузочного раздела, выбрав пункт меню **Настройка раздела закончена** (Рисунок 26).

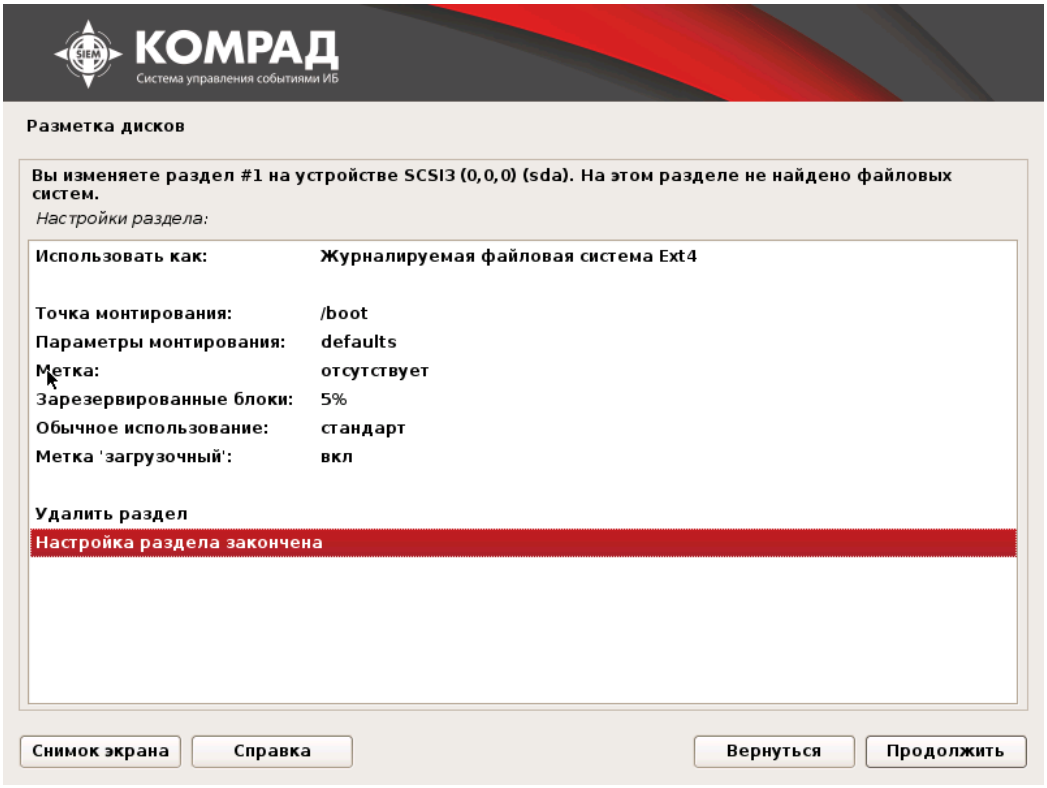


Рисунок 26. Создание загрузочного раздела

2.6.2.6 Создание раздела подкачки

Выберите свободное место, которое необходимо разметить, нажмите кнопку **Продолжить**. Выберите пункт **Создать новый раздел**. При помощи мастера разметки создайте раздел подкачки (swap) со следующими параметрами.

Параметр	Значение
Новый размер раздела	8 GB
Тип нового раздела	Логический
Местоположение нового раздела	Начало
Использовать как	раздел подкачки
Метка ‘загрузочный’	выкл

Данные параметры представлены в качестве примера.

Завершите создание раздела подкачки, выбрав пункт меню **Настройка раздела закончена** (Рисунок 27).

Рисунок 27. Создание раздела подкачки

2.6.2.7 Создание корневого раздела

Выберите свободное место, которое необходимо разметить, нажмите кнопку **Продолжить**. Выберите пункт **Создать новый раздел**. При помощи мастера разметки создайте корневой раздел со следующими параметрами.

Параметр	**Значение**
Новый размер раздела	<всё доступное свободное место>
Тип нового раздела	Первичный
Местоположение нового раздела	Начало
Использовать как	Журналируемая файловая система Ext4
Точка монтирования	/
Параметры монтирования	defaults
Метка	отсутствует
Зарезервированные блоки	5%
Обычное использование	стандарт
Метка ‘загрузочный’	выкл

Данные параметры представлены в качестве примера.

Завершите создание корневого раздела, выбрав пункт меню **Настройка раздела закончена** (Рисунок 28).

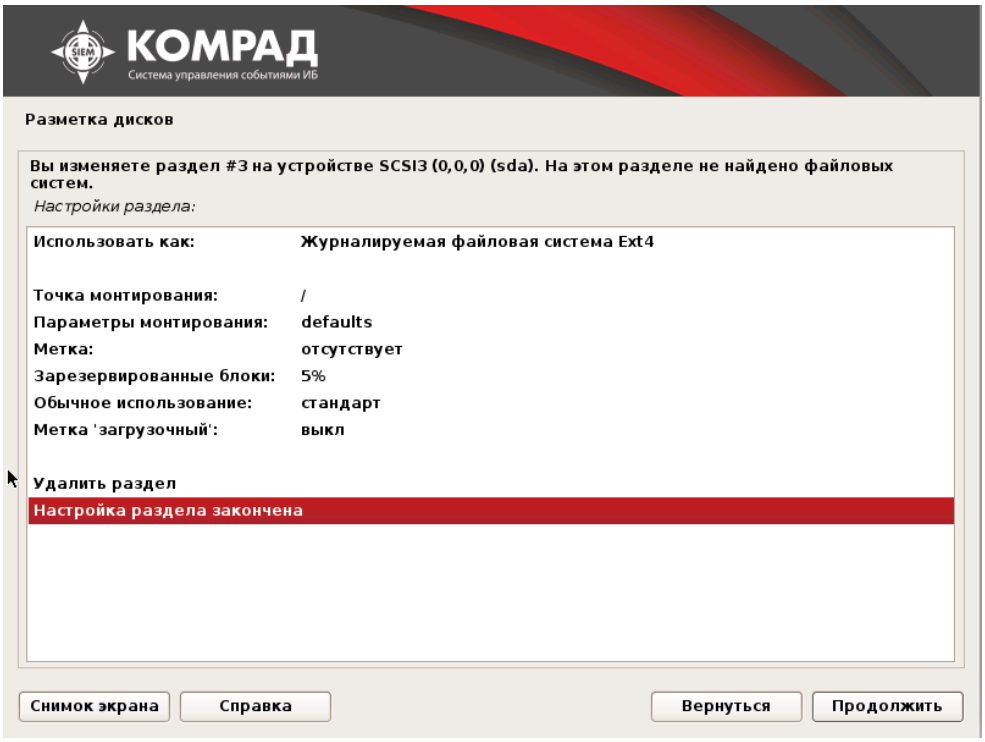


Рисунок 28. Создание корневого раздела

2.6.3 Окончание разметки

Завершите разметку диска (Рисунок 29). Для перехода к следующему шагу нажмите кнопку **Продолжить**, для возврата к предыдущему шагу нажмите кнопку **Вернуться**.

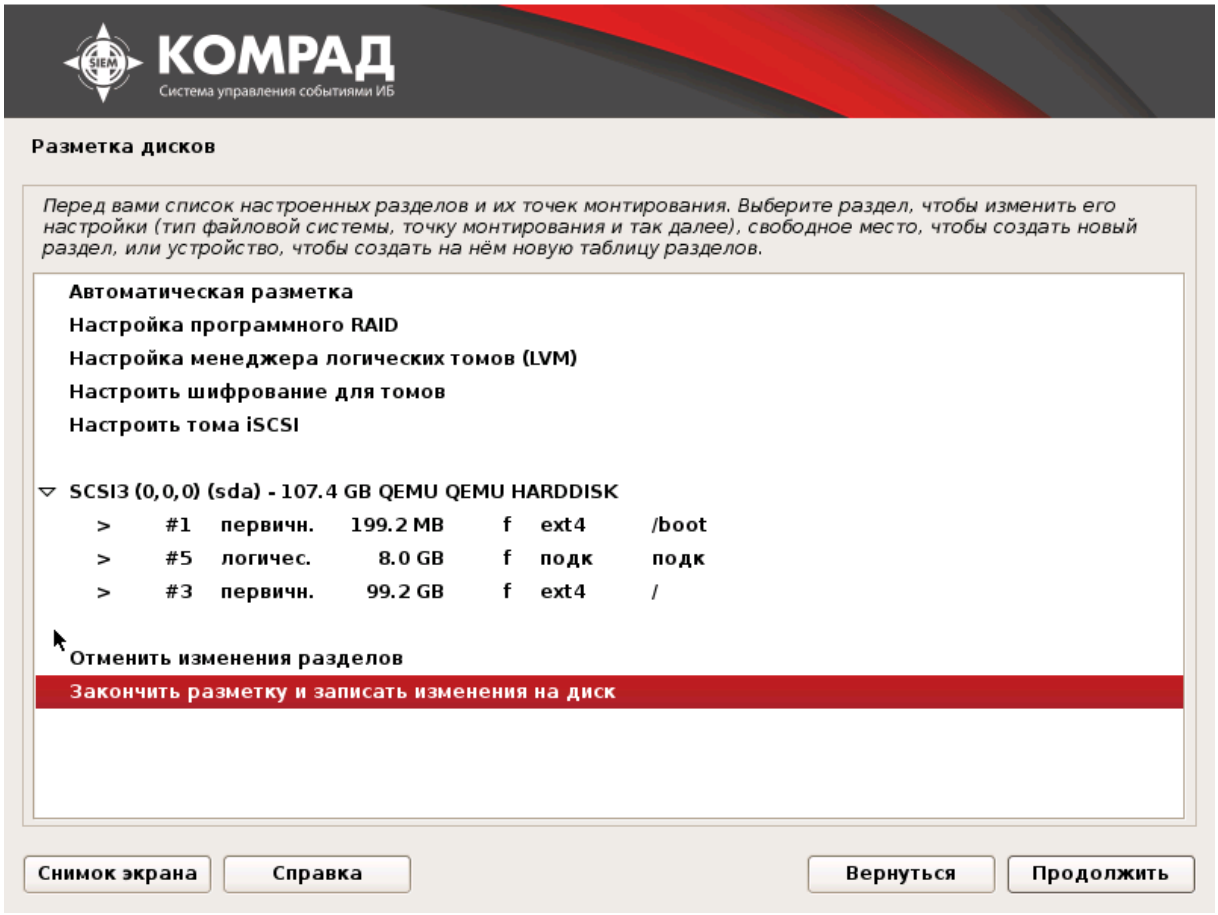


Рисунок 29. Завершение разметки

Для подтверждения записи изменений на диск и окончания процедуры разметки выберите **Да**. Нажмите кнопку **Продолжить**.

2.7 Шаг 7. Установка базовой системы и программного обеспечения

Дождитесь окончания процесса установки базовой системы (Рисунок 30).

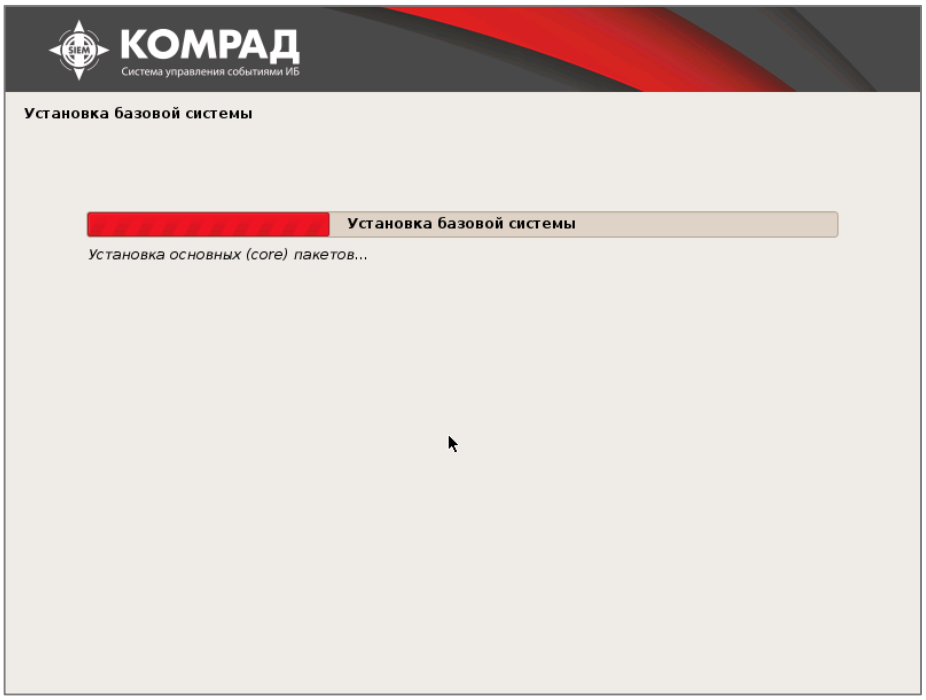


Рисунок 30. Установка базовой системы

Выберите устанавливаемое программное обеспечение (Рисунок 31). Для перехода к следующему шагу нажмите кнопку **Продолжить**.

Если установка происходит впервые, то обязательным условием является выбор пункта **Центр управления КОМРАД SIEM**.

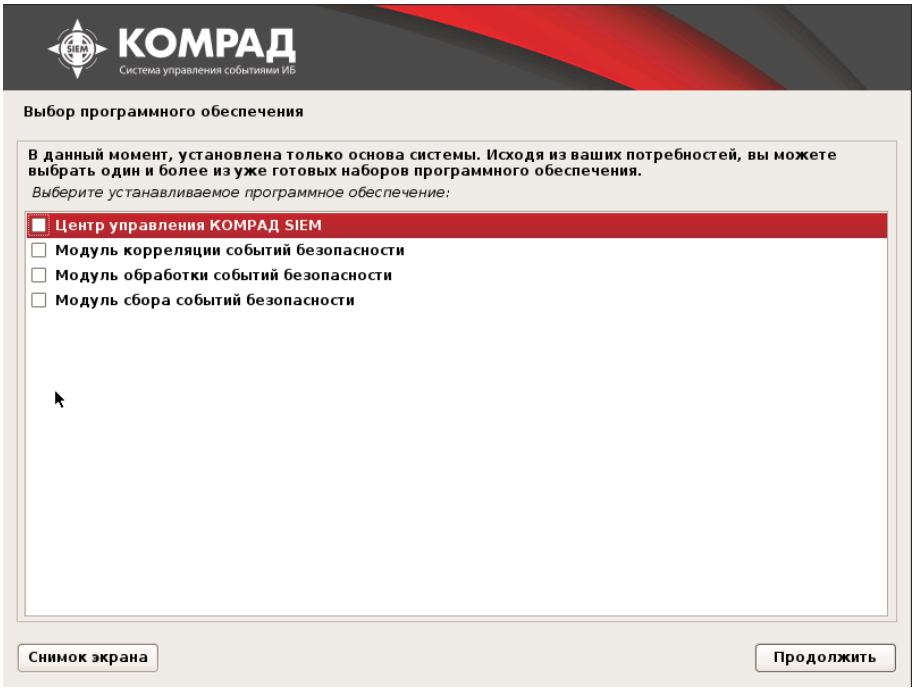


Рисунок 31. Выбор программного обеспечения

2.7.1 Установка главного узла

Выберите пункт меню **Центр управления КОМРАД SIEM** (Рисунок 32). Для перехода к следующему шагу нажмите кнопку **Продолжить**.

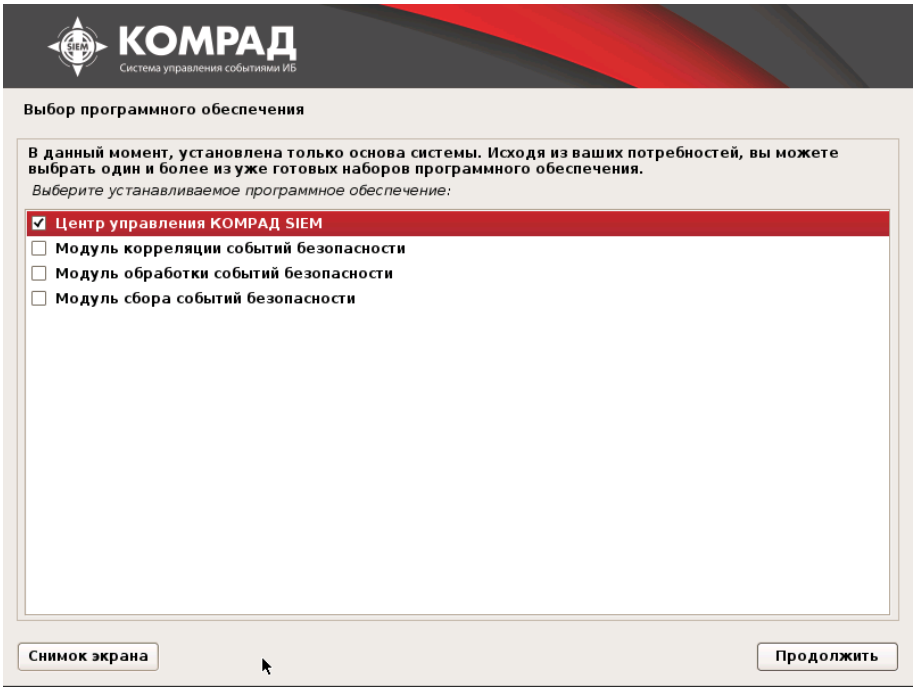


Рисунок 32. Выбор главного узла

Дождитесь установки программного обеспечения (Рисунок 33).

Рисунок 33. Установка главного узла

2.7.2 Установка узла с модулем корреляции событий безопасности

Выберите пункт меню **Модуль корреляции событий безопасности** (Рисунок 34). Для перехода к следующему шагу нажмите кнопку **Продолжить**.

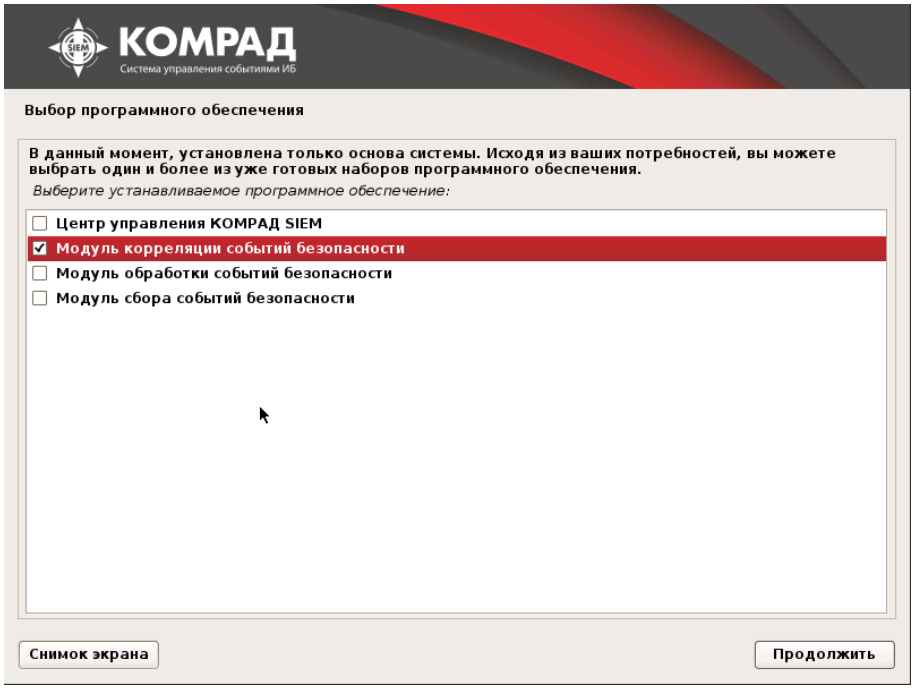


Рисунок 34. Выбор узла с модулем корреляции

Дождитесь установки программного обеспечения (Рисунок 35).

Рисунок 35. Установка узла с модулем корреляции

Назначьте имя узла с модулем корреляции для ПК «Комрад» (Рисунок 36). Для перехода к следующему шагу нажмите кнопку **Продолжить**.

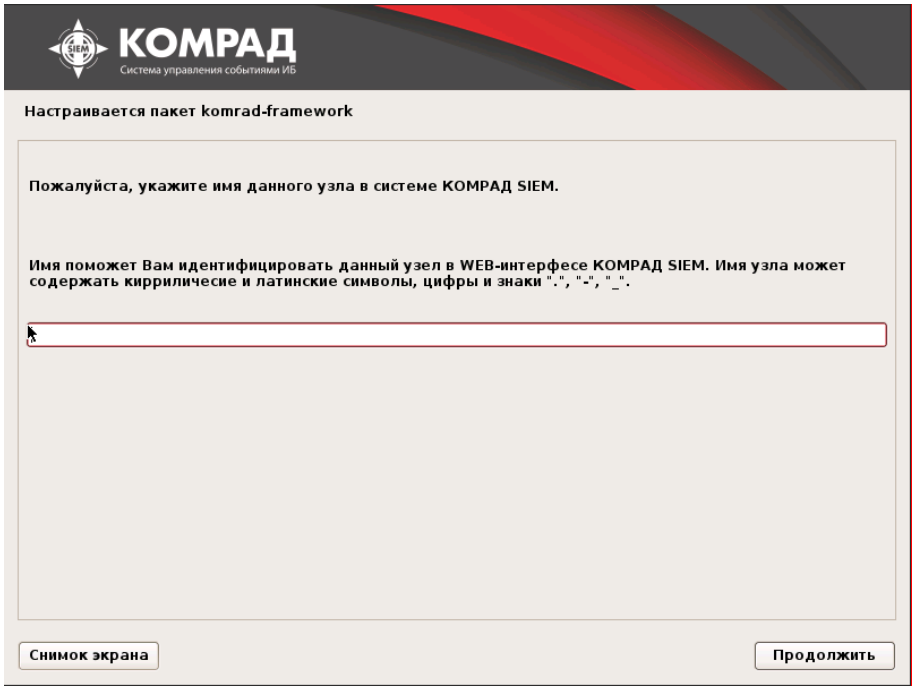


Рисунок 36. Назначение имени узла с модулем корреляции

Задайте IP-адрес главного узла ПК «Комрад» (Рисунок 37). Для перехода к следующему шагу нажмите кнопку **Продолжить**.

Рисунок 37. Назначение IP-адреса Главного узла

Узел с модулем корреляции успешно зарегистрирован в ПК «Комрад» (Рисунок 38). Для перехода к следующему шагу нажмите кнопку **Продолжить**.

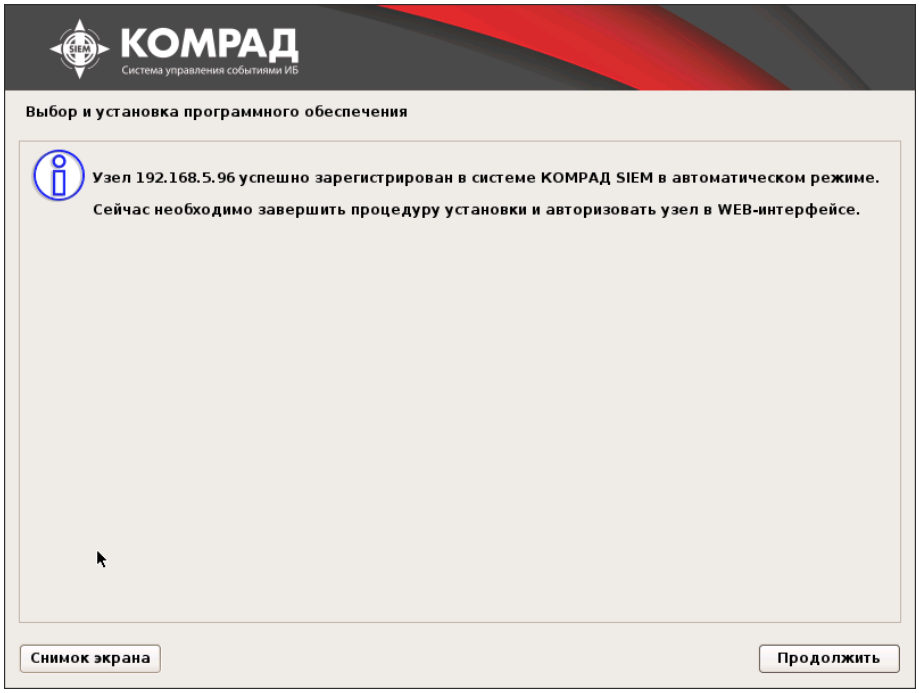


Рисунок 38. Регистрация узла с модулем корреляции в системе

Дождитесь установки программного обеспечения (Рисунок 39).

Рисунок 39. Установка узла с модулем корреляции

Выберите режим сетевой доступности узла с модулем корреляции (Рисунок 40). Для перехода к следующему шагу нажмите кнопку **Продолжить**.

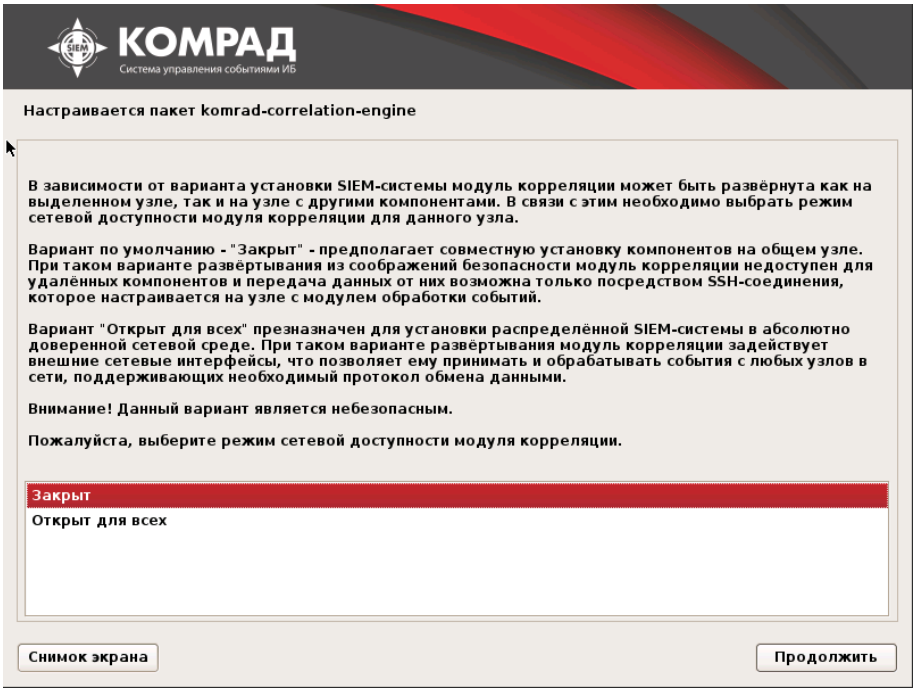


Рисунок 40. Выбор режима сетевой доступности

Дождитесь установки программного обеспечения (Рисунок 41).

Рисунок 41. Установка узла с модулем корреляции

2.7.3 Установка узла с модулем обработки событий безопасности

Выберите пункт меню **Модуль обработки событий безопасности** (Рисунок 42). Для перехода к следующему шагу нажмите кнопку **Продолжить**.

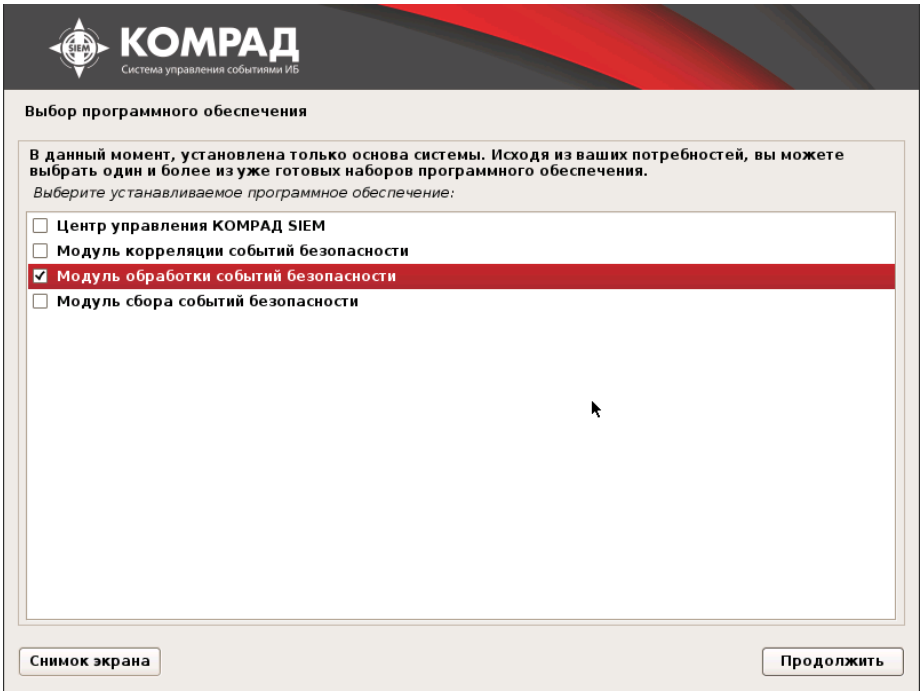


Рисунок 42. Выбор узла с модулем обработки событий

Дождитесь установки программного обеспечения (Рисунок 43).

Рисунок 43. Установка узла с модулем обработки событий

Назначьте имя узла с модулем обработки событий для ПК «Комрад» (Рисунок 44). Для перехода к следующему шагу нажмите кнопку **Продолжить**.

Рисунок 44. Назначение имени узла с модулем обработки событий

Задайте IP-адрес главного узла ПК «Комрад» (Рисунок 45). Для перехода к следующему шагу нажмите кнопку **Продолжить**.

Рисунок 45. Назначение IP-адреса главного узла

Узел с модулем обработки событий успешно зарегистрирован в ПК «Комрад» (Рисунок 46). Для перехода к следующему шагу нажмите кнопку **Продолжить**.

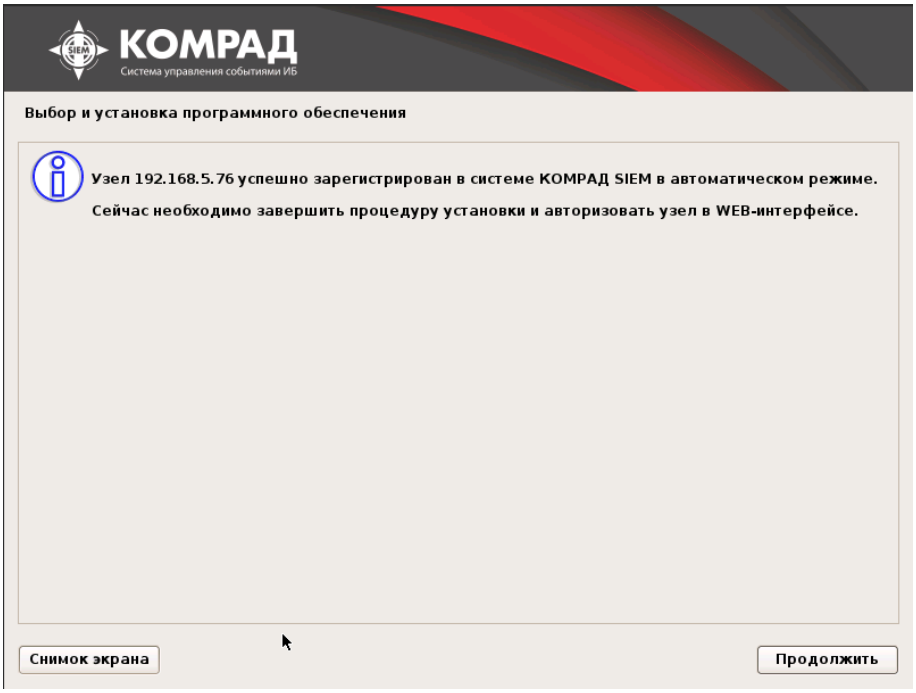


Рисунок 46. Регистрация узла с модулем обработки событий

Дождитесь установки программного обеспечения (Рисунок 47).

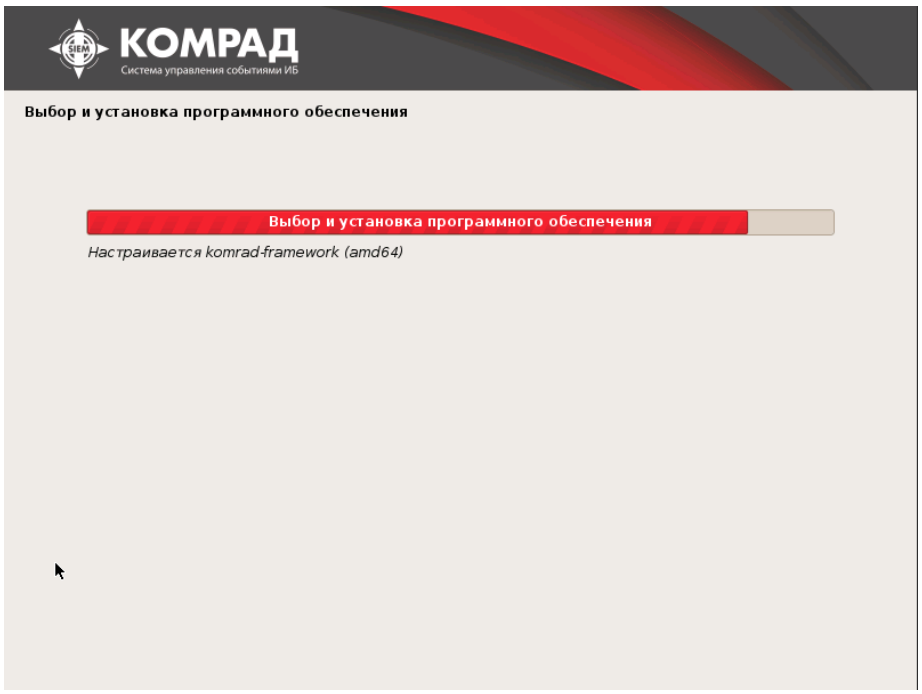


Рисунок 47. Установка узла с модулем обработки событий

Выберите режим сетевой доступности узла с модулем обработки событий (Рисунок 48). Для перехода к следующему шагу нажмите кнопку **Продолжить**.

Рисунок 48. Выбор режима сетевой доступности

Выберите IP-адрес узла с установленным модулем корреляции (Рисунок 49). Для перехода к следующему шагу нажмите кнопку **Продолжить**.

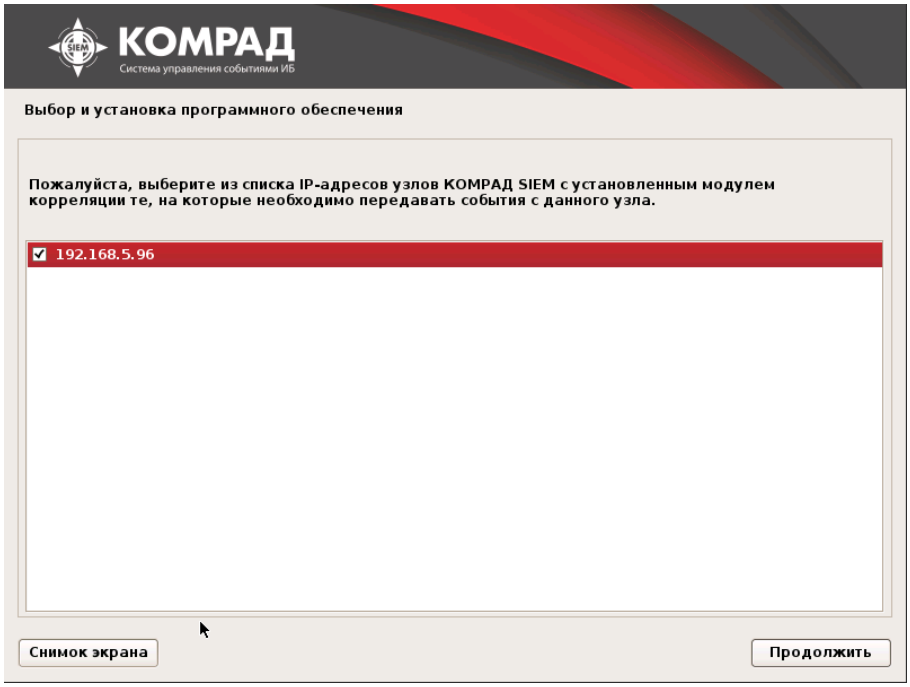


Рисунок 49. Выбор узла с коррелятором

Задайте IP-адрес главного узла ПК «Комрад» (Рисунок 50). Для перехода к следующему шагу нажмите кнопку **Продолжить**.

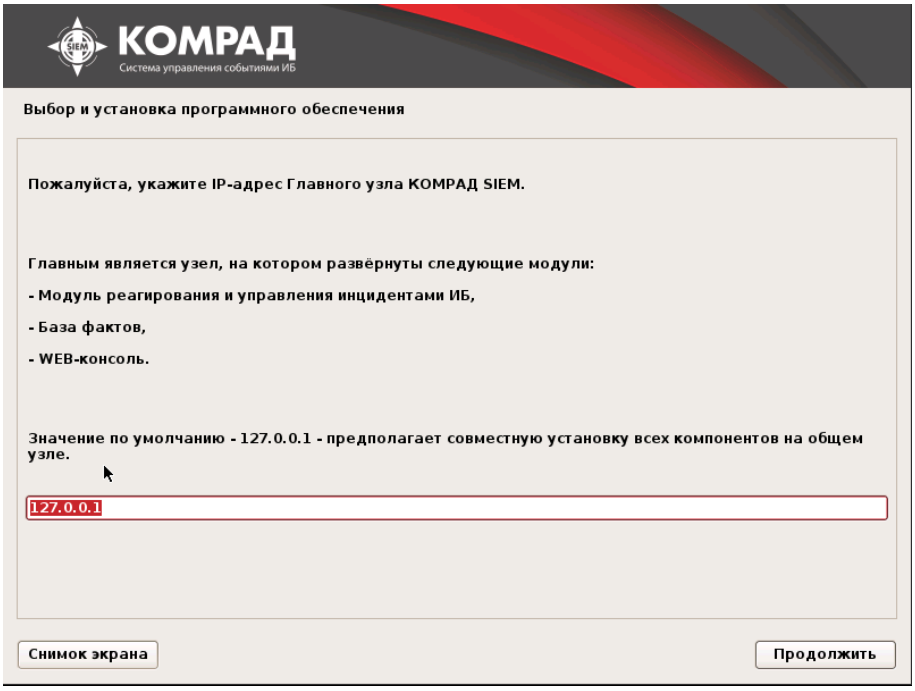


Рисунок 50. Назначение IP-адреса главного узла

2.7.4 Установка узла с модулем сбора событий безопасности

Выберите пункт меню **Модуль сбора событий безопасности** (Рисунок 51). Для перехода к следующему шагу нажмите кнопку **Продолжить**.

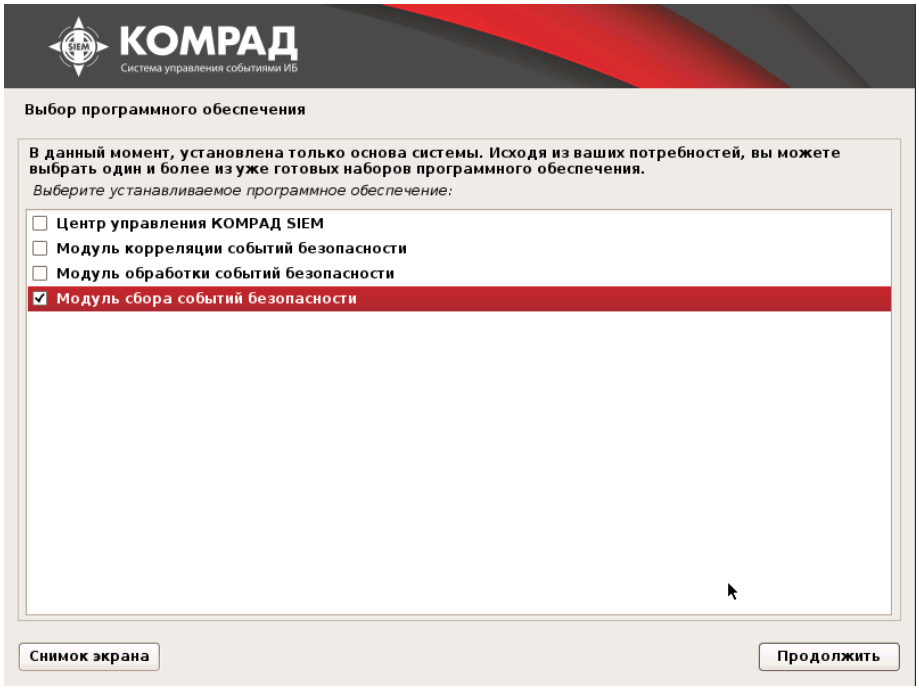


Рисунок 51. Выбор узла с модулем сбора событий

Дождитесь установки программного обеспечения (Рисунок 52).

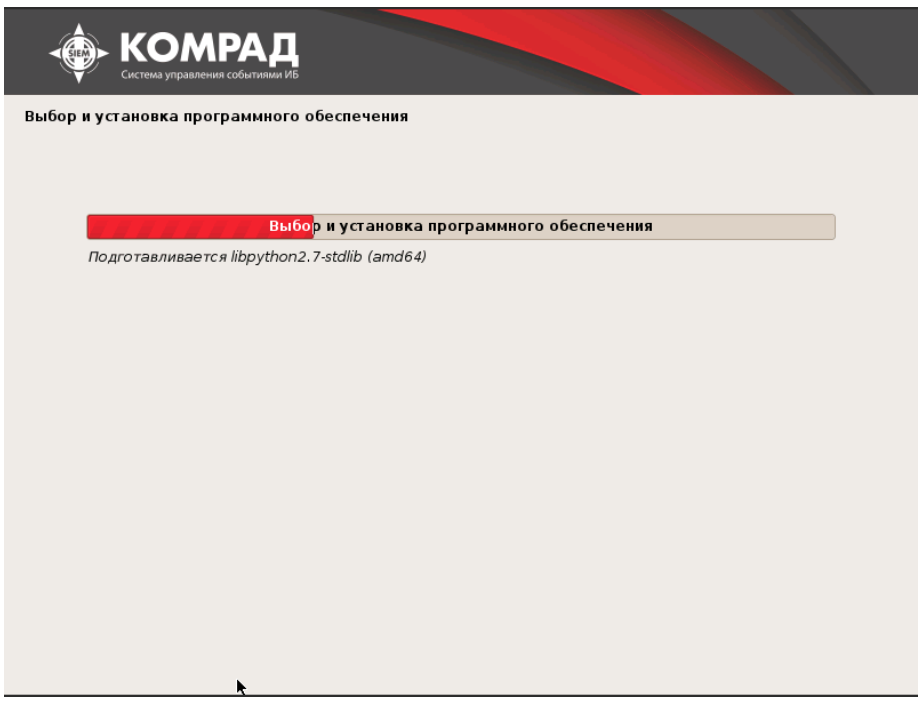


Рисунок 52. Установка узла с модулем сбора событий

Назначьте имя узла с модулем сбора событий для ПК «Комрад» (Рисунок 53). Для перехода к следующему шагу нажмите кнопку **Продолжить**.

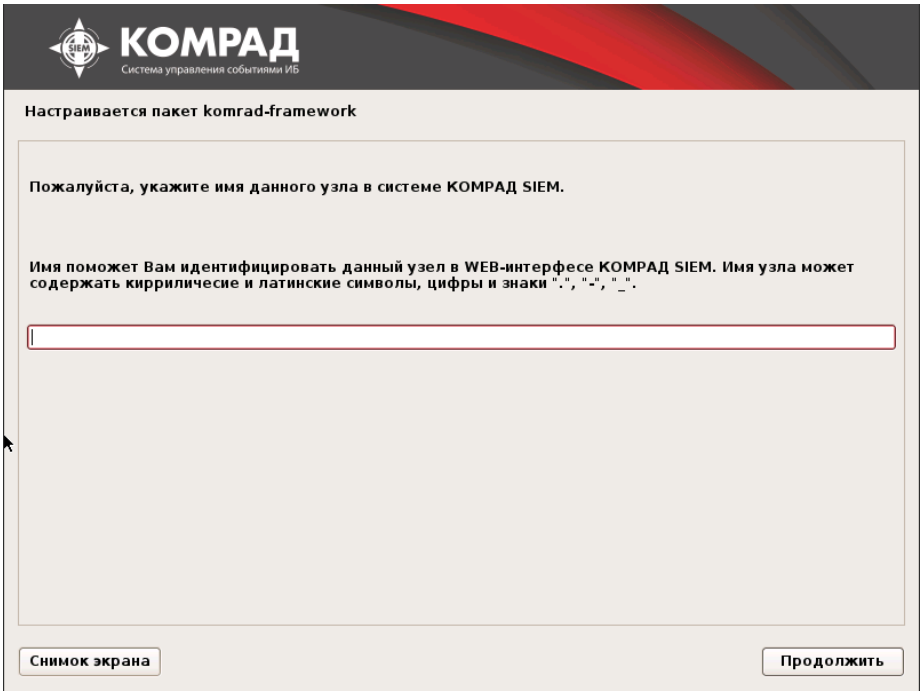


Рисунок 53. Назначение имени узла с модулем сбора событий

Задайте IP-адрес главного узла ПК «Комрад» (Рисунок 54). Для перехода к следующему шагу нажмите кнопку **Продолжить**.

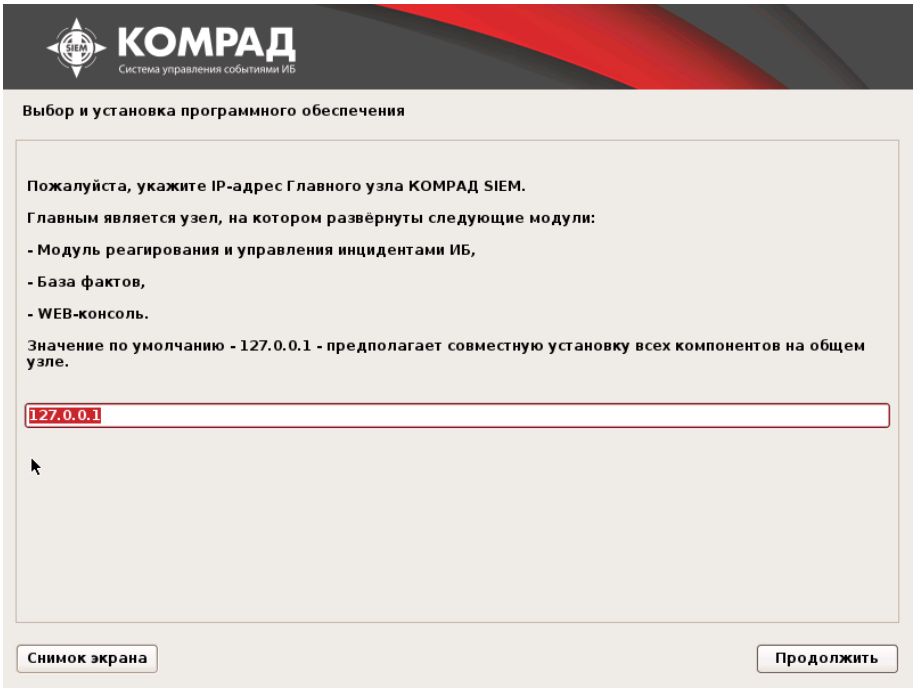


Рисунок 54. Назначение IP-адреса главного узла

Узел с модулем сбора событий успешно зарегистрирован в ПК «Комрад» (Рисунок 55). Для перехода к следующему шагу нажмите кнопку **Продолжить**.

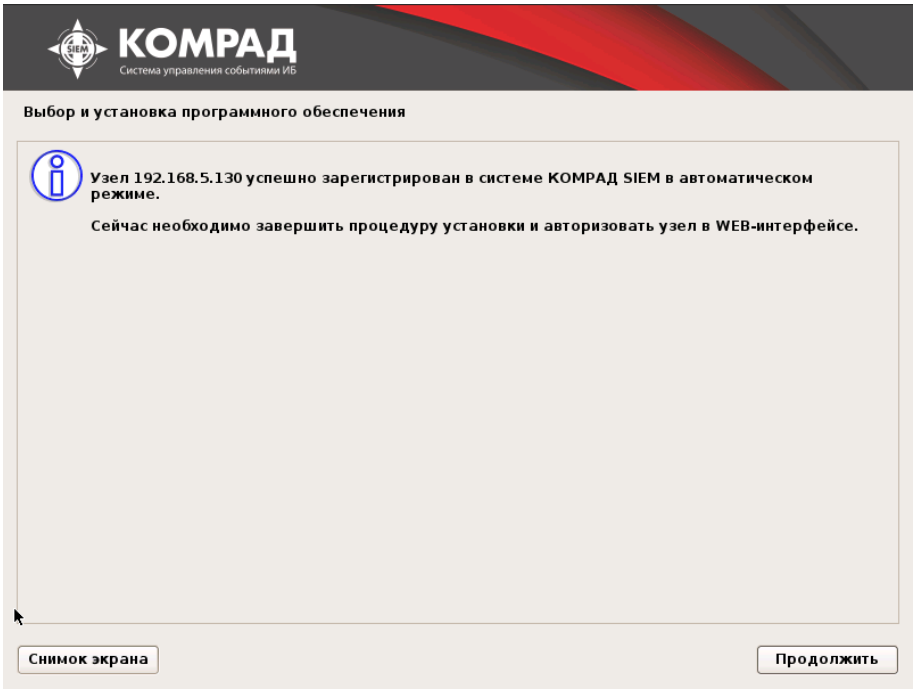


Рисунок 55. Регистрация узла с модулем сбора событий

Дождитесь установки программного обеспечения (Рисунок 56).

Рисунок 56. Установка узла с модулем сбора событий

2.8 Шаг 8. Установка системного загрузчика

Установите системный загрузчик GRUB (Рисунок 57). Для перехода к следующему шагу нажмите **Продолжить**, для возврата к предыдущему шагу нажмите **Вернуться**.

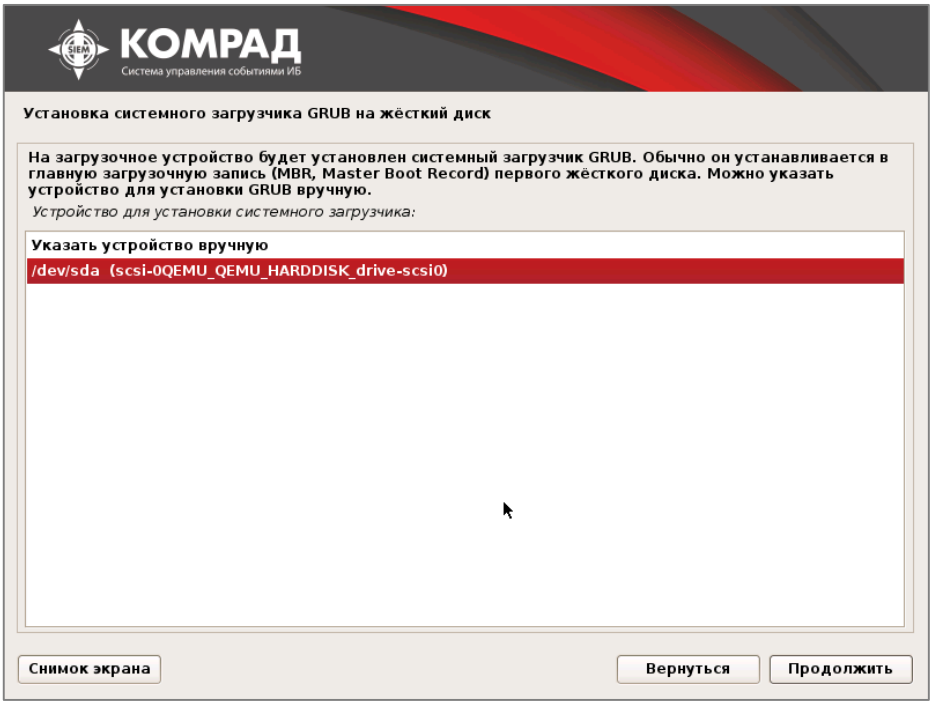


Рисунок 57. Выбор места установки загрузчика

Дождитесь окончания установки (Рисунок 58).

Рисунок 58. Окончание установки

По окончании установки система автоматически перезагружается. В случае успешной установки появится экран загрузки системы (Рисунок 59).

2.9 Загрузка системы

После включения питания аппаратной платформы начинается загрузка ПК «Комрад» (Рисунок 59).

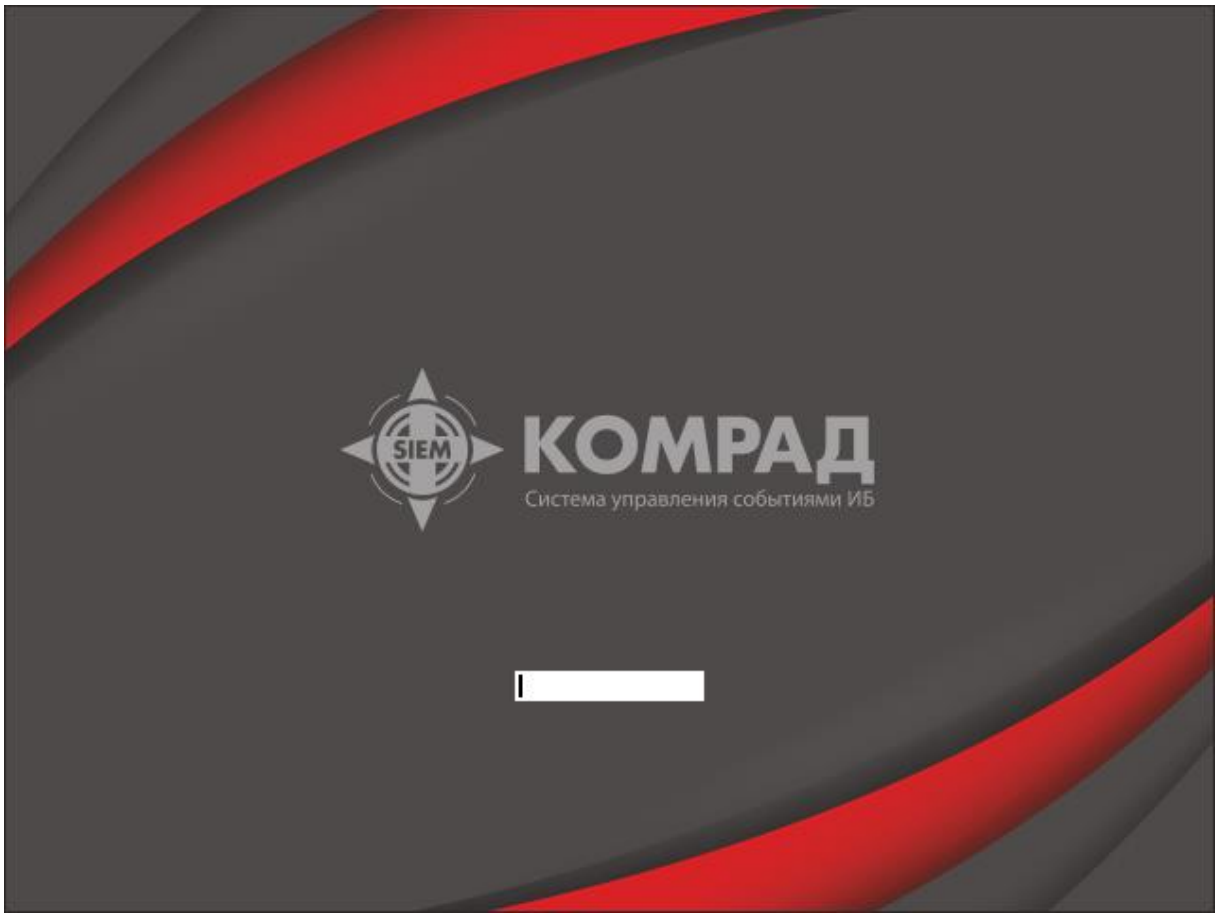


Рисунок 59. Окно загрузки системы

Процесс загрузки завершается приглашением ко входу в систему (Рисунок 175). На данном этапе ПК «Комрад» готов к работе администратора с веб-интерфейсом. Для конфигурирования и управления ПК «Комрад» администратору необходимо авторизоваться в интерфейсе командной строки.

2.10 Активация

После установки ПК «Комрад» и прохождения процедуры авторизации администратором система осуществит переход на страницу **Компоненты** (Рисунок 60).

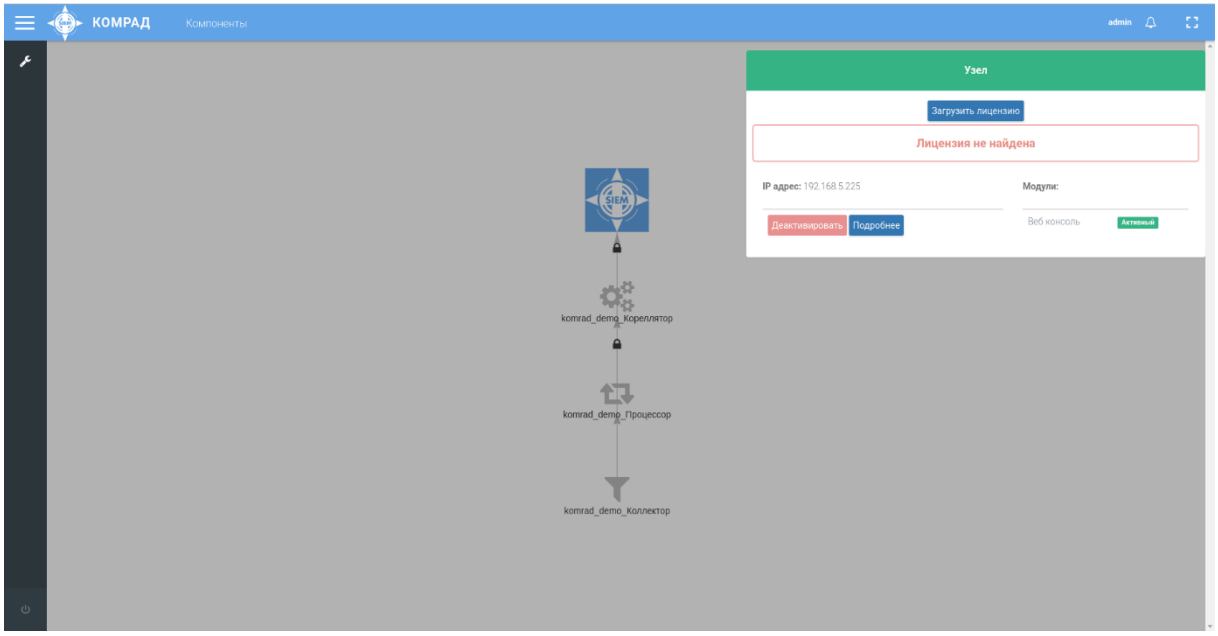


Рисунок 60. Страница Компоненты

Для отображения полного веб-интерфейса ПК «Комрад» необходимо загрузить лицензионный файл и пройти процедуру активации установленных узлов.

2.10.1 Загрузка лицензии

Для загрузки лицензионного файла выполните следующие действия:

1. Нажмите кнопку **Загрузить лицензию** в диалоговом окне (Рисунок 60).
2. Через проводник выберите лицензионный файл с расширением *.licsign.lic* и нажмите кнопку **Открыть**.

При успешной загрузке файла администратор получит всплывающее сообщение **Операция успешна** и в диалоговом окне отобразится информация о лицензии (Рисунок 61).

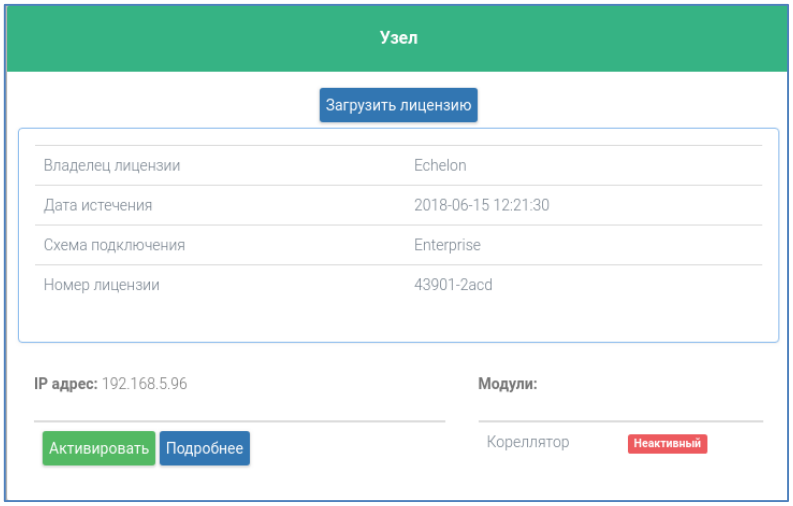


Рисунок 61. Информация о лицензии

В случае неудачной загрузки файла система отобразит сообщение, представленное на Рисунок 62. Попробуйте загрузить другой файл.

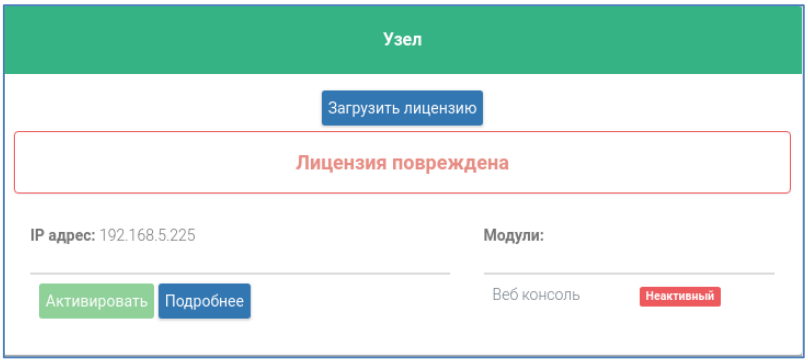


Рисунок 62. Ошибка при загрузке файла лицензии

2.10.2 Активация узлов

После успешной загрузки файла лицензии необходимо активировать установленные узлы.

На схеме компонентов (Рисунок 63) активные узлы имеют зеленый цвет, неактивные – серый.

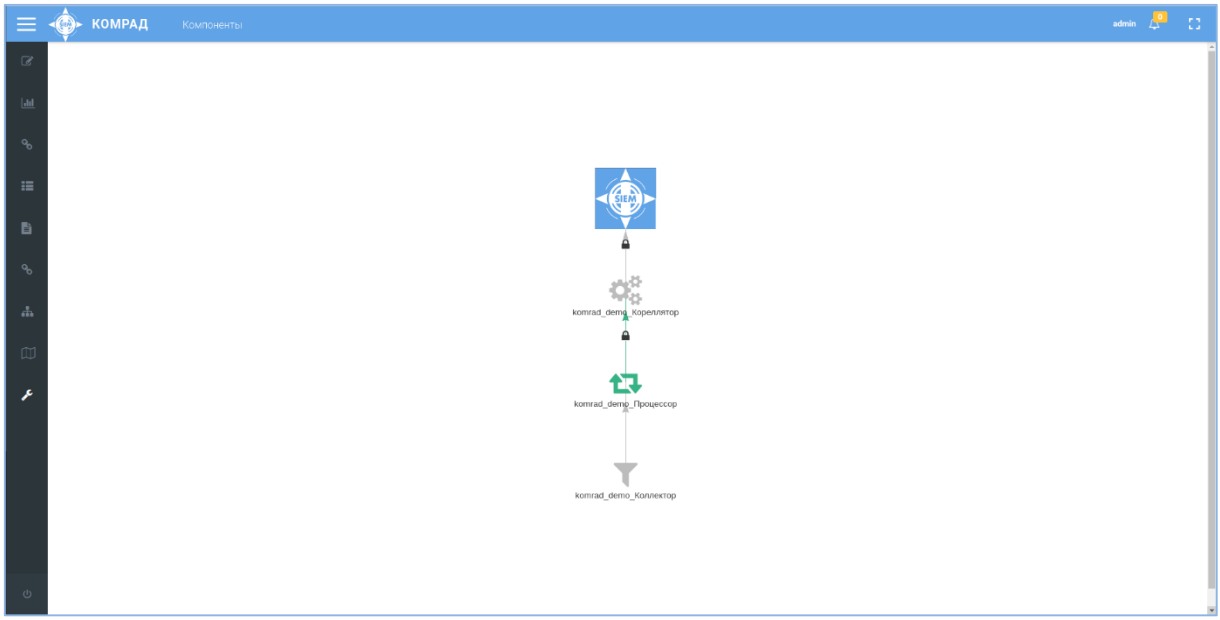


Рисунок 63. Пример схемы компонентов

Для активации выполните следующие действия:

1. На схеме компонентов выберите узел, который необходимо активировать, нажав на него левой кнопкой мыши (Рисунок 60).

Активация главного узла, содержащего веб-интерфейс, происходит автоматически после загрузки файла лицензии.

2. В диалоговом окне нажмите кнопку **Активировать** (Рисунок 61); статусы модулей, установленных на данном узле, будут изменены на **Активный** (Рисунок 64).

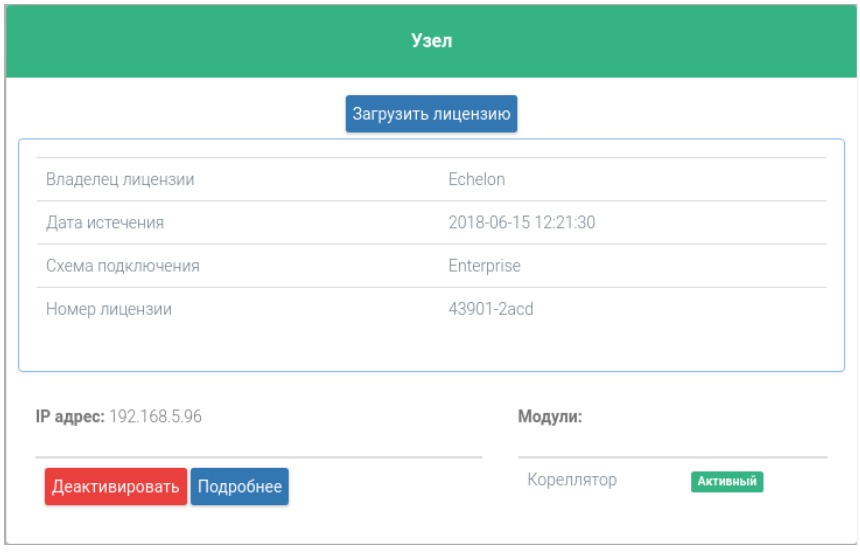


Рисунок 64. Активация узла

После активации цвет узла на схеме компонентов станет зеленым.

2.10.3 Деактивация узлов

Для деактивации узла выполните следующие действия:

1. На схеме выберите узел, который необходимо деактивировать, нажав на него левой кнопкой мыши.
2. В диалоговом окне нажмите кнопку **Деактивировать** (Рисунок 64); статусы модулей, установленных на данном узле, будут изменены на **Неактивный** (Рисунок 61).

После деактивации цвет узла на схеме компонентов станет серым.

3 Настройка источников событий

В данной главе содержатся сведения о настройках, которые необходимо произвести администратору для конфигурирования источников на передачу событий в ПК «Комрад».

3.1 Сбор событий WMI

Технология WMI (Windows Management Instrumentation) используется для удаленного сбора событий с ОС Windows. Для настройки сбора событий по протоколу WMI необходимо настроить источник событий и внести изменения в конфигурационный файл модуля сбора событий.

3.1.1 Настройка устройства с ОС Windows

3.1.1.1 ОС Windows 7/8/10

3.1.1.1.1 Создание пользователя с ограниченными правами

В целях безопасности необходимо создать отдельную учетную запись пользователя с ограниченными правами. Ниже представлен пример для пользователя *wmiuser*.

1. Вызовите диалоговое меню **Выполнить**, нажав `WinKey+R`, введите команду **compmgmt.msc**, нажмите кнопку **ОК**. Появится окно **Управление компьютером**.
2. В левой области окна **Управление компьютером** выберите **Локальные пользователи и группы**. Щелкните правой кнопкой мыши по пункту **Пользователи** и выберите в контекстном меню пункт **Новый пользователь...** (Рисунок 65).

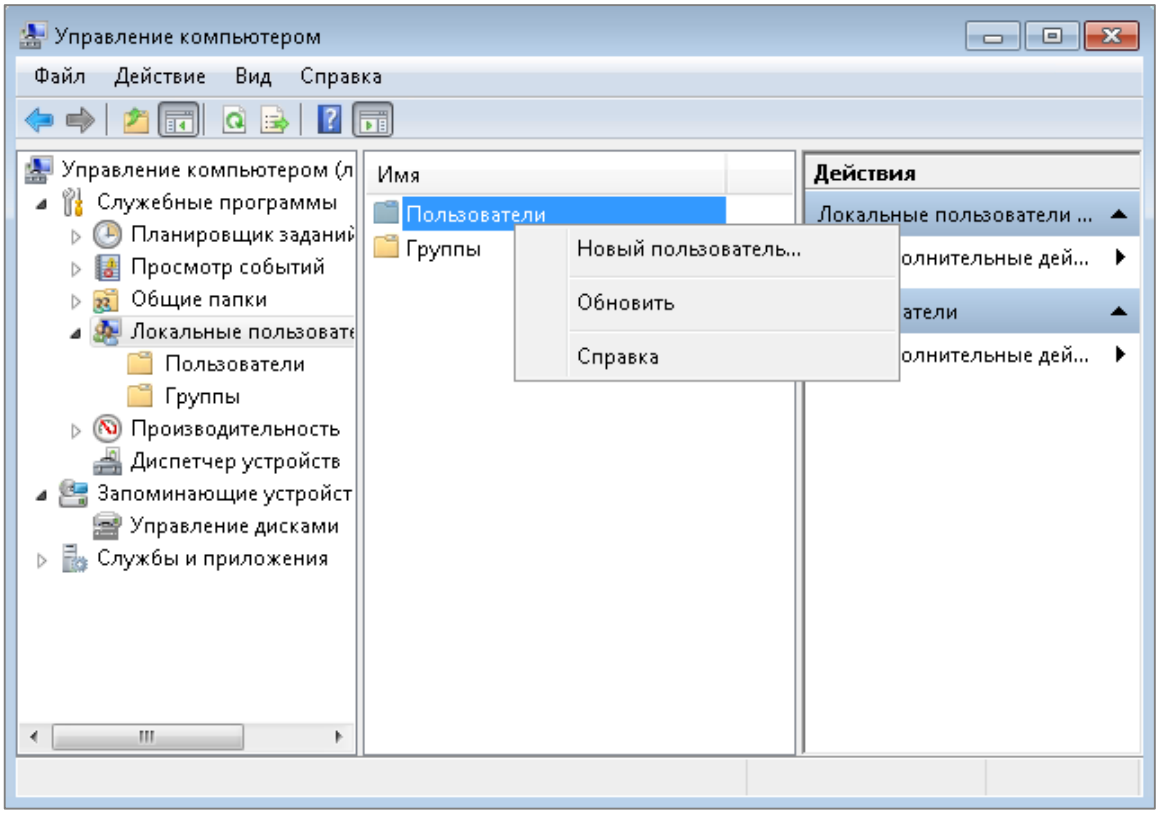


Рисунок 65. Создание нового пользователя

3. Введите имя пользователя (wmiuser), укажите пароль, выберите пункт **Срок действия пароля не ограничен** (Рисунок 66). Нажмите кнопки **Создать** и **Закрыть**.

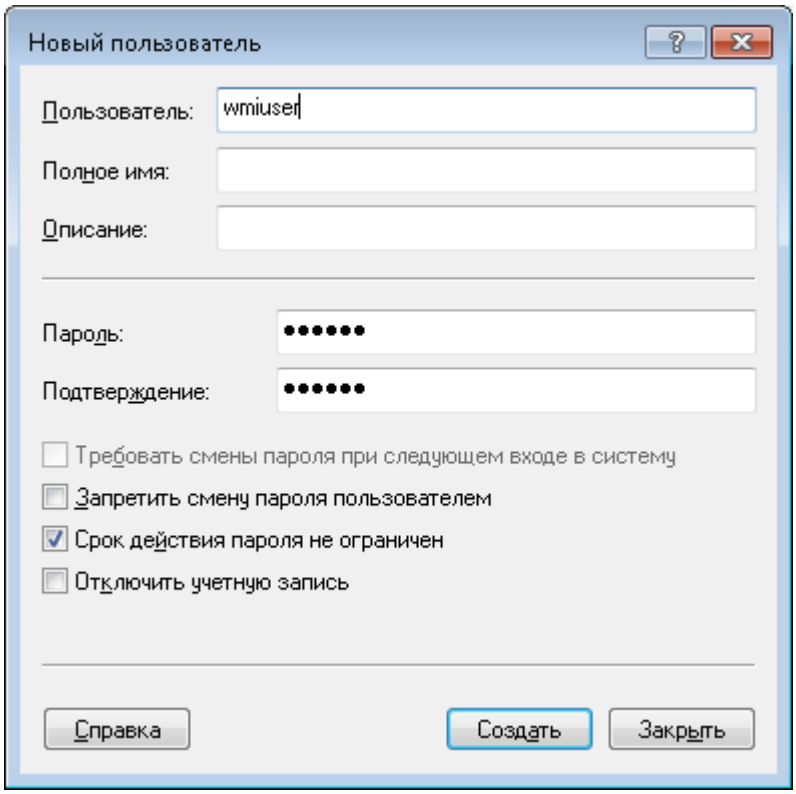


Рисунок 66. Ввод данных нового пользователя

4. Щелкните правой кнопкой мыши по пользователю wmiuser и выберите в контекстном меню пункт **Свойства**.
5. Перейдите во вкладку **Членство в группах** и нажмите кнопку **Добавить**.
6. Нажмите кнопку **Дополнительно**. В открывшемся окне нажмите кнопку **Поиск** и выберите группы **Читатели журнала событий** и **Пользователи DCOM**. Нажмите кнопку **OK**.

3.1.1.1.2 Настройка прав пользователя на управление WMI

1. Вызовите диалоговое меню **Выполнить**, нажав `WinKey+R`, введите команду **compmgmt.msc**, нажмите кнопку **OK**. Появится окно **Управление компьютером**.
2. В левой области окна **Управление компьютером** выберите **Служба и приложения > Управляющий элемент WMI**, щелкните по записи **Управляющий элемент WMI** правой кнопкой мыши и выберите в контекстном меню пункт **Свойства**.
3. В открывшемся окне выберите вкладку **Безопасность** и раскройте дерево **Root**.

4. Выделите ветвь **CIMV2** и нажмите кнопку **Безопасность** в нижнем правом углу.
5. Добавьте пользователя wmiuser в раздел **Группы или пользователи** и отметьте пункты **Включить учетную запись**, **Включить удаленно**, **Прочесть безопасность** (Рисунок 67). Нажмите кнопку **ОК**.

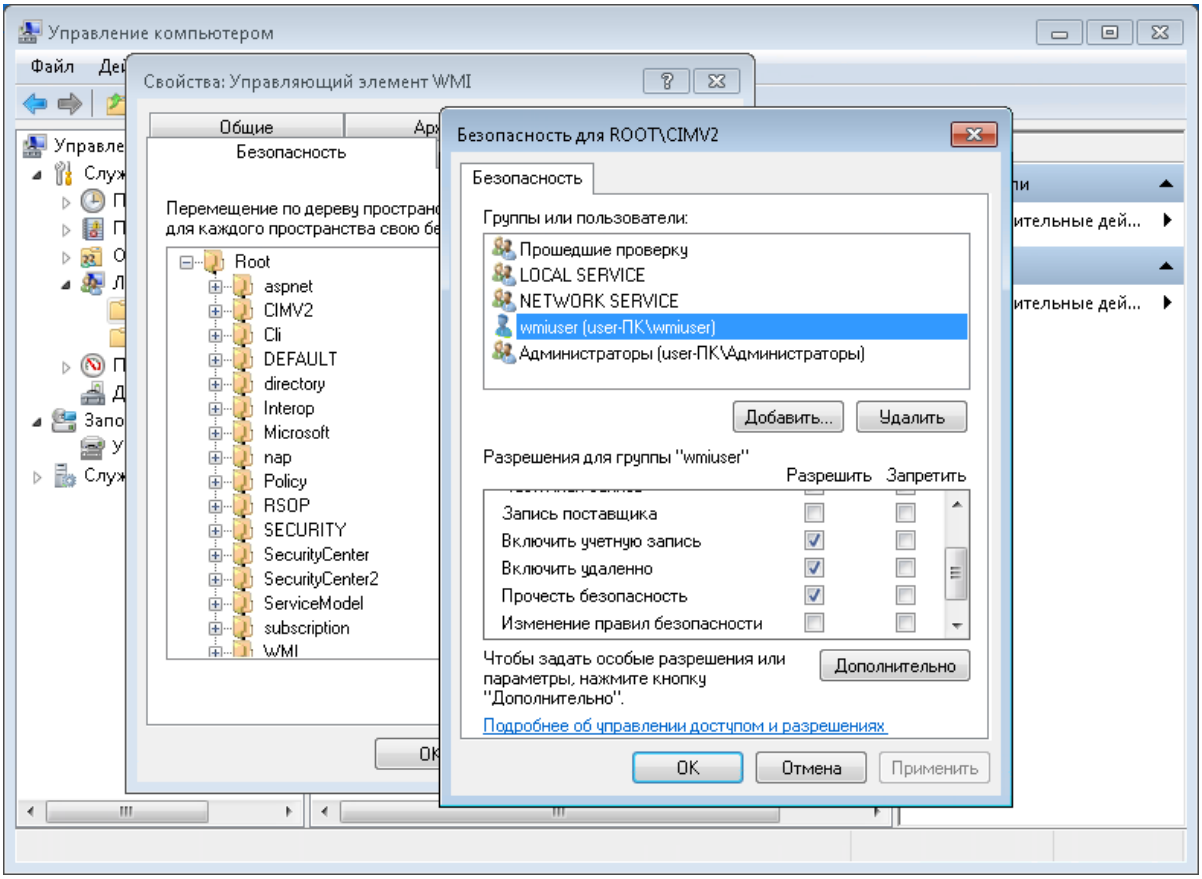


Рисунок 67**.** Настройка разрешений пространства имен

3.1.1.1.3 Предоставление прав доступа

Для предоставления пользователю прав для удаленного доступа и сбора логов, необходимо произвести следующие настройки DCOM.

1. Вызовите диалоговое меню **Выполнить**, нажав `WinKey+R`, введите команду **dcomcnfg**, нажмите кнопку **ОК**.
2. В разделе **Службы компонентов** выберите **Компьютеры > Мой компьютер**, щелкните правой кнопкой мыши по записи **Мой компьютер** и выберите в контекстном меню пункт **Свойства**.
3. В открывшемся окне выберите вкладку **Безопасность COM**.
4. В разделе **Разрешения на запуск и активацию** нажмите кнопку **Изменить ограничения...**
5. В диалоговом окне **Разрешение на запуск и активацию** нажмите кнопку **Добавить**.
6. В открывшемся окне введите имя пользователя wmiuser в раздел **Введите имена выбираемых объектов** и нажмите кнопку **ОК**.

7. В диалоговом окне **Разрешение на запуск и активацию** в разделе **Группы или пользователи** выберите пользователя wmiuser и отметьте пункты **Локальный запуск**, **Удаленный запуск**, **Локальная активация**, **Удаленная активация** (Рисунок 68). Нажмите кнопку **ОК**.
8. В разделе **Права доступа** диалогового окна **Свойства: Мой компьютер** нажмите кнопку **Изменить ограничения...**
9. В диалоговом окне **Права доступа** выберите пункт «АНОНИМНЫЙ ВХОД» в разделе **Группы или пользователи** и отметьте пункты **Локальный доступ**, **Удаленный доступ** (Рисунок 69). Нажмите кнопку **ОК**.

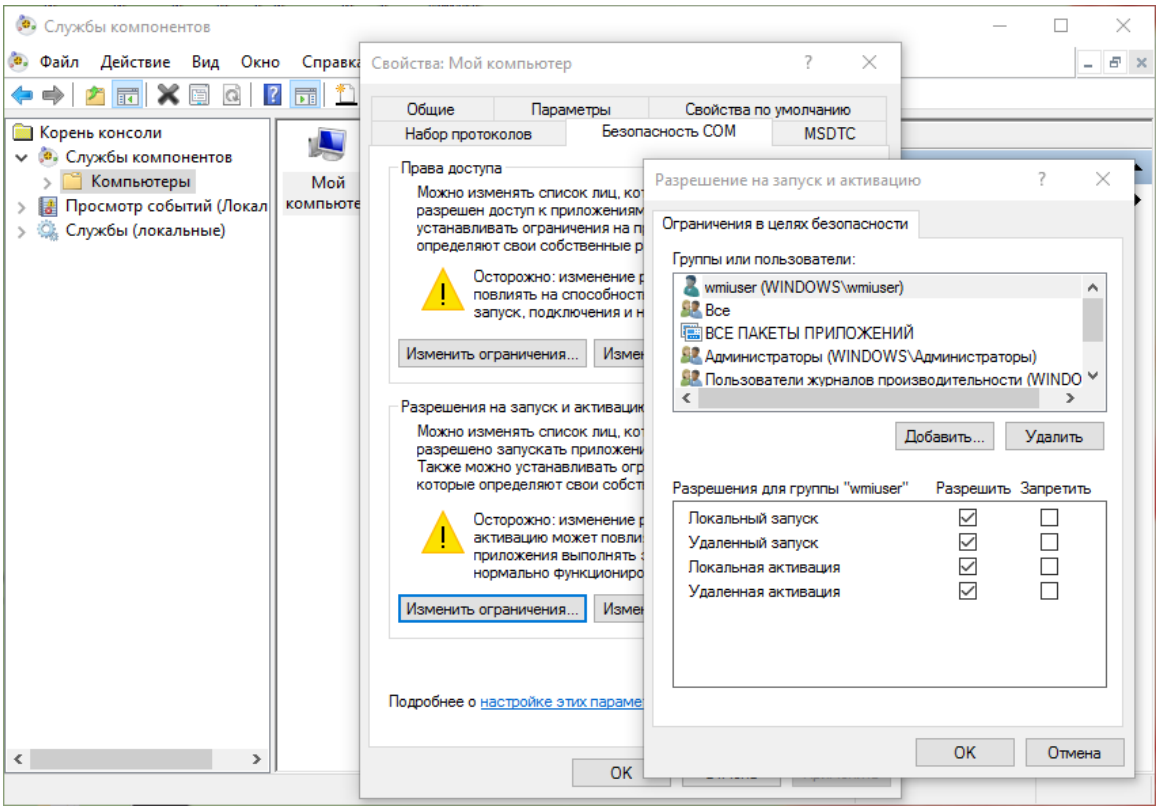


Рисунок 68. Разрешения для пользователя wmiuser

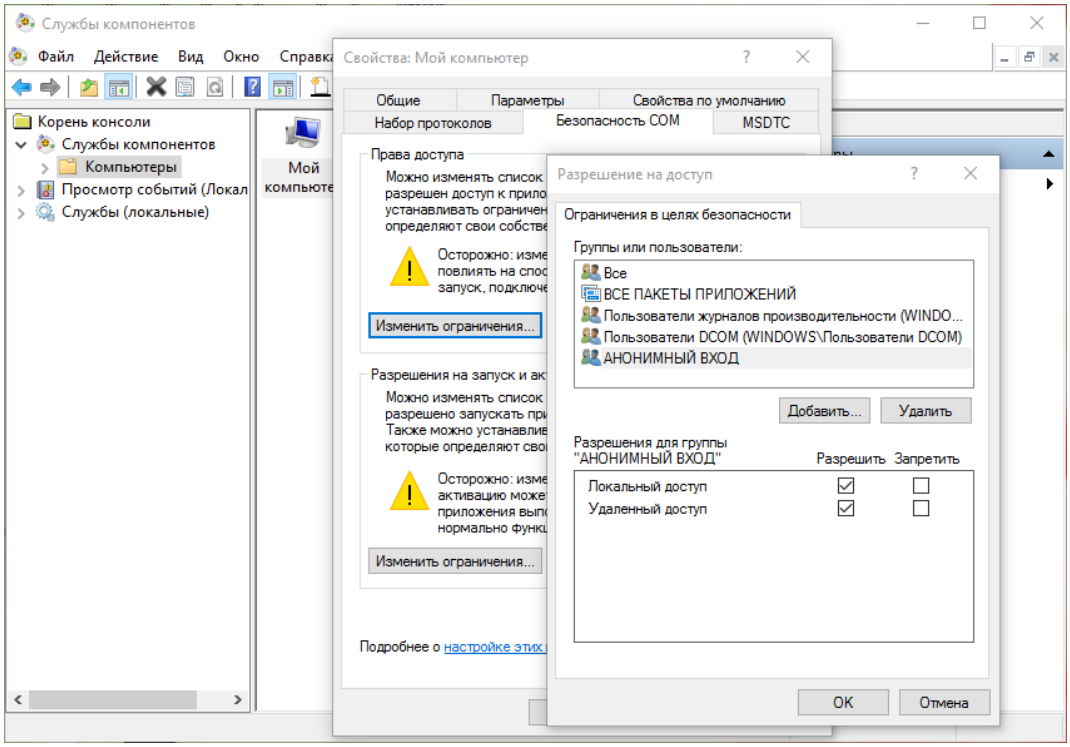


Рисунок 69. Разрешение на анонимный вход

3.1.1.2 ОС Windows Server

Описание последовательности действий приведено на примере Windows Server 2008 R2.

3.1.1.2.1 Создание пользователя с ограниченными правами

В целях безопасности необходимо создать отдельную учетную запись пользователя с ограниченными правами. Ниже представлен пример для пользователя *wmi_user*.

1. Откройте диспетчер сервера.
2. В левой области окна диспетчера выберите **Роли > Доменные службы Active Directory > Имя домена**. Щелкните правой кнопкой мыши по пункту **Users** и выберите в контекстном меню пункт **Создать > Пользователь** (Рисунок 70).

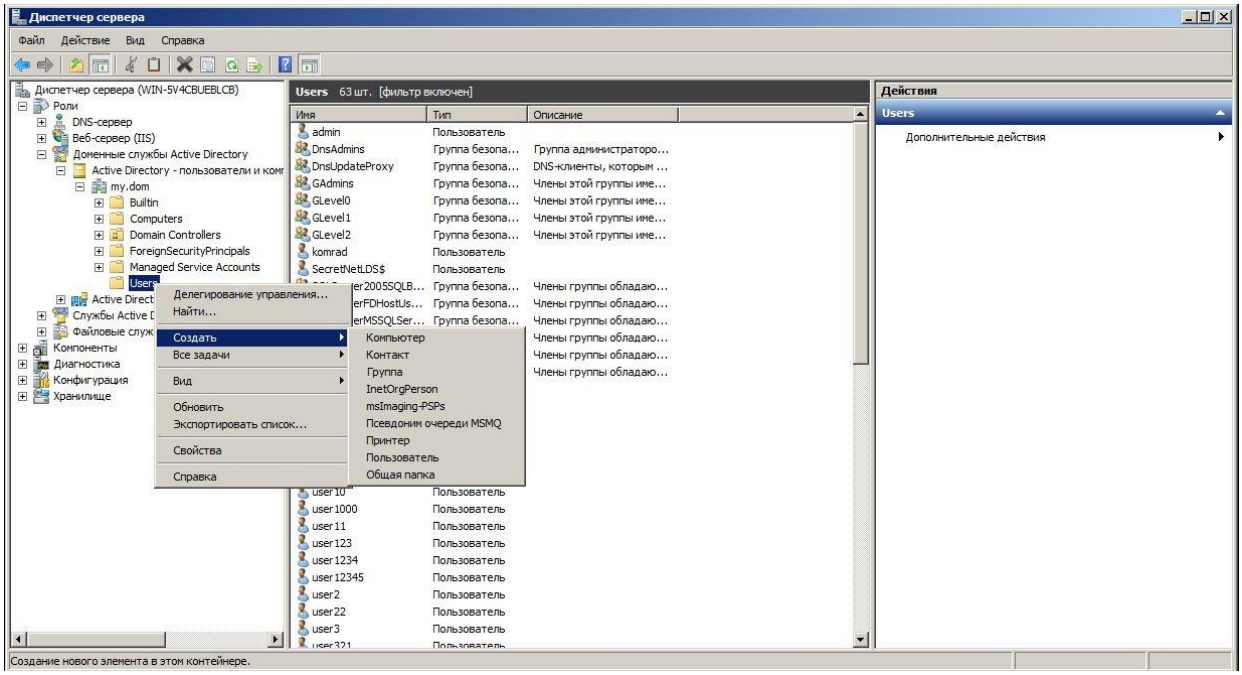


Рисунок 70. Создание нового пользователя

3. Укажите имя и имя входа пользователя (wmi_user), нажмите кнопку **Далее** (Рисунок 71).

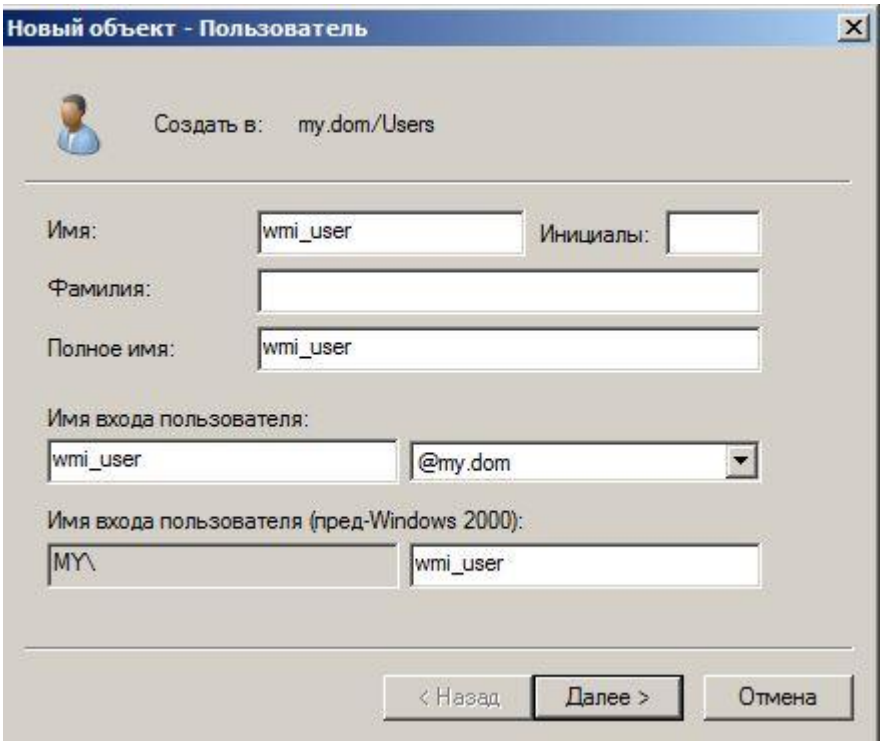


Рисунок 71. Ввод данных нового пользователя

4. Укажите пароль пользователя wmi_user, выберите пункт **Срок действия пароля не ограничен**. Нажмите кнопки **Далее** и **Готово** (Рисунок 72).

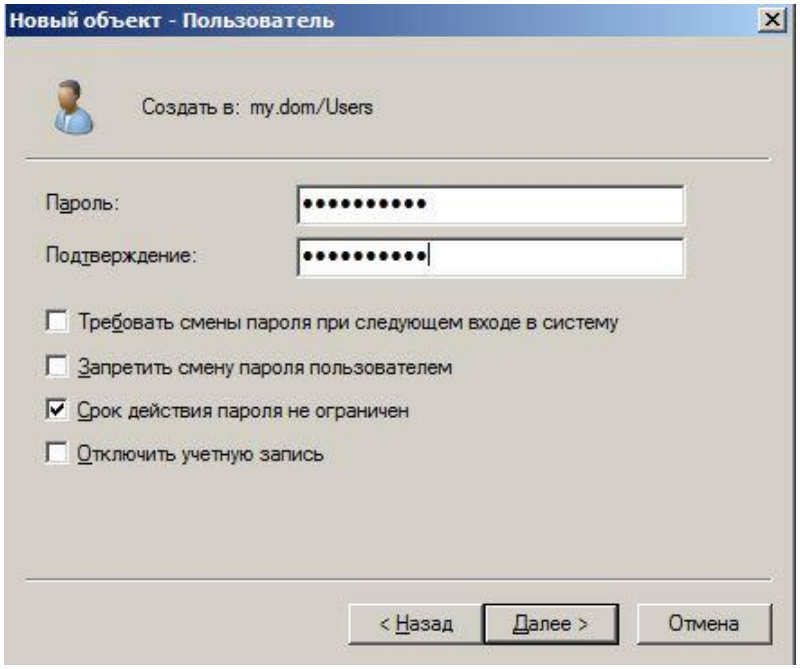


Рисунок 72. Настройка учетной записи wmi_user

5. Щелкните правой кнопкой мыши по пользователю wmi_user и выберите в контекстном меню пункт **Свойства**.
6. Перейдите во вкладку **Член групп** и нажмите кнопку **Добавить** (Рисунок 73).

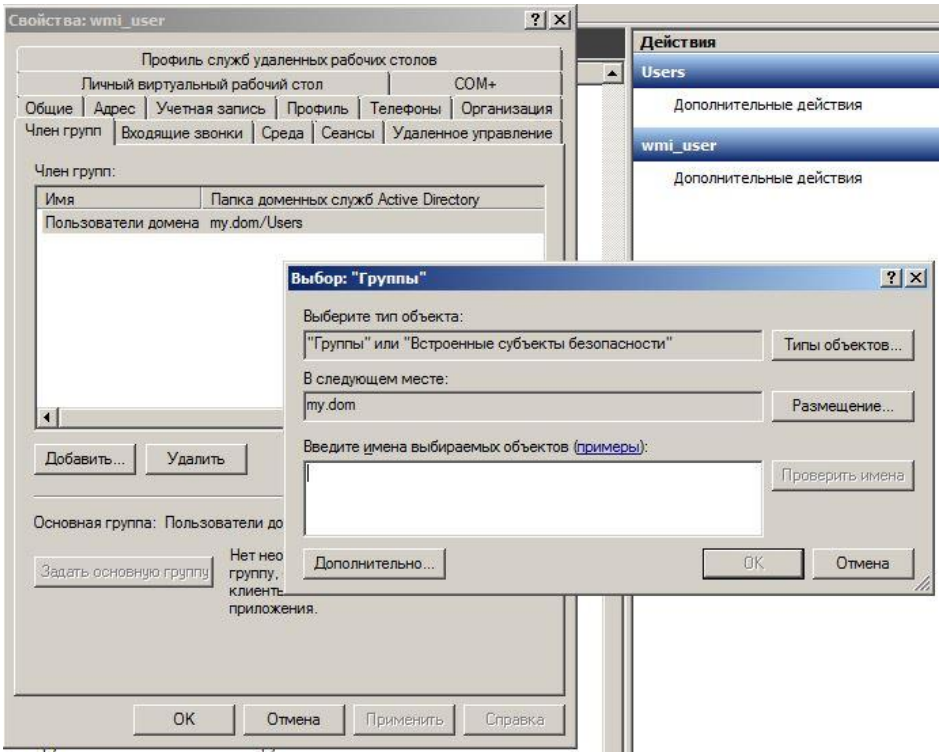


Рисунок 73. Настройка членства в группах

1. Нажмите кнопку **Дополнительно**. В открывшемся окне нажмите кнопку **Поиск** и выберите группы **Читатели журнала событий** и **Пользователи DCOM**. Нажмите кнопку **OK**.

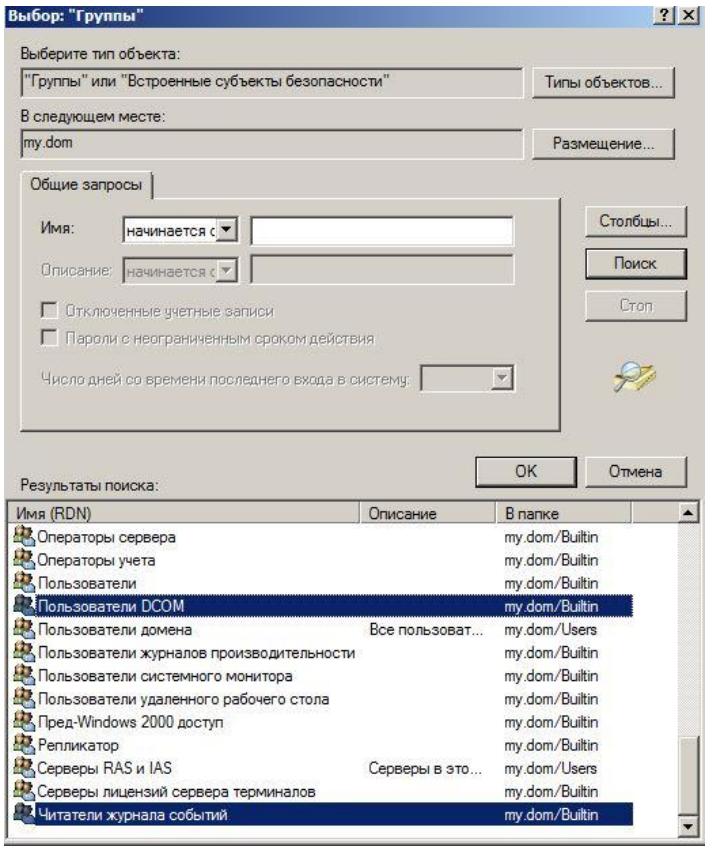


Рисунок 74. Выбор групп «Читатели журнала событий» и «Пользователи DCOM»

3.1.1.2.2 Настройка прав пользователя на управление WMI

1. В левой области окна диспетчера сервера выберите **Конфигурация > Управляющий элемент WMI**, щелкните по записи **Управляющий элемент WMI** правой кнопкой мыши и выберите в контекстном меню пункт **Свойства**.
2. В открывшемся окне выберите вкладку **Безопасность** и раскройте дерево **Root**.
3. Выделите ветвь **CIMV2** и нажмите кнопку **Безопасность** в нижнем правом углу (Рисунок 75).

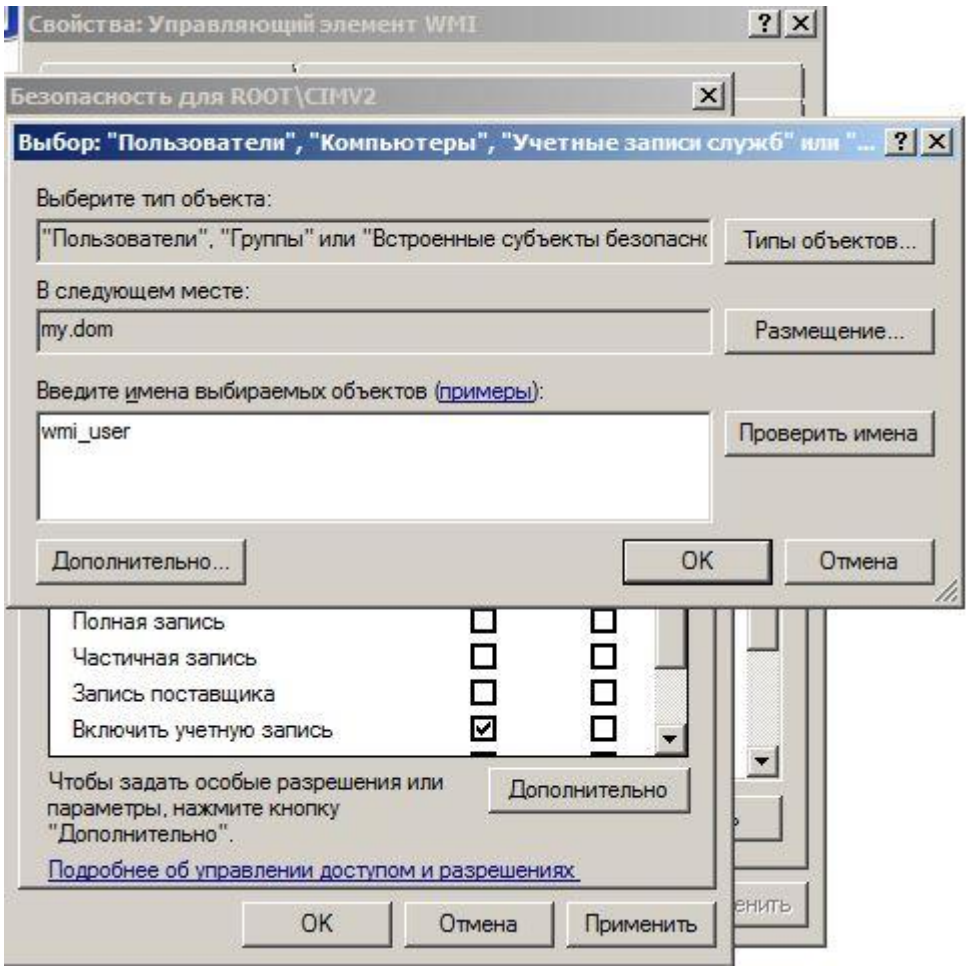


Рисунок 75. Настройки безопасности для ветви Root\CIMV2

4. Добавьте пользователя wmi_user в раздел **Группы или пользователи** и отметьте пункты **Включить учетную запись**, **Включить удаленно**, **Прочесть безопасность** (Рисунок 76). Нажмите кнопку **OK**.

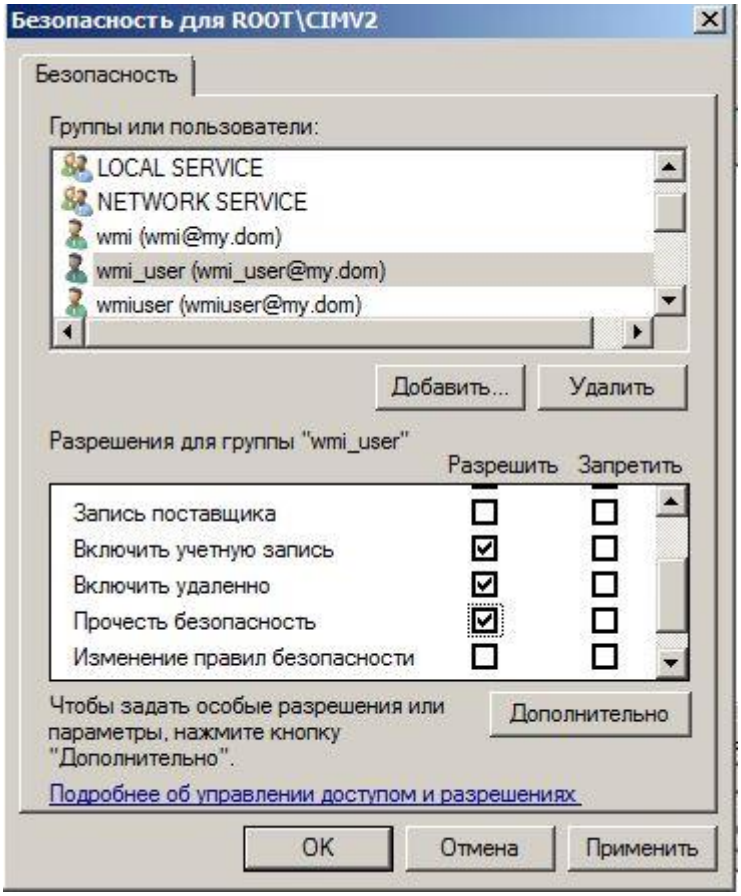


Рисунок 76**.** Настройка разрешений пространства имен

3.1.1.2.3 Предоставление прав доступа

Действия, которые необходимо выполнить на данном этапе, аналогичны действиям в ОС Windows 10.

3.1.1.3 Проверка корректности настроек

Выполните на ПК «Комрад» команду **wmic** с соответствующими параметрами:

```
wmic -U имя_пользователя%пароль //ip_адрес "select * from
Win32_ComputerSystem"
```

Например,

```
wmic -U admin%Seclab1234 //192.168.5.70 "select * from
Win32_ComputerSystem"
```

Результатом выполнения команды должны быть данные:

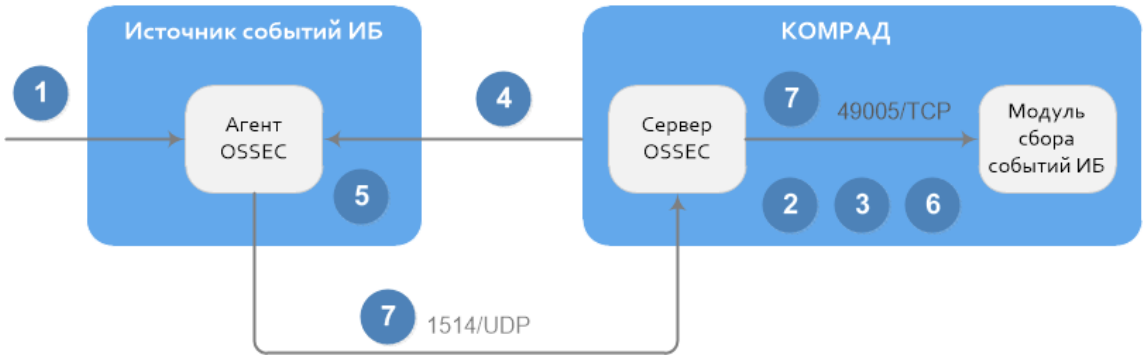
```
CLASS: Win32_ComputerSystem

AdminPasswordStatus|AutomaticManagedPagefile|AutomaticResetBootOption|Aut
omaticResetCapability|BootOptionOnLimit|BootOptionOnWatchDog|BootROMSuppo
rted|BootStatus|BootupState|Caption|ChassisBootupState|
```

```
ChassisSKUNumber|CreationClassName|CurrentTimeZone|DaylightInEffect|Descr
iption|DNSHostName|Domain|DomainRole|EnableDaylightSavingsTime|FrontPanel
ResetStatus|HypervisorPresent|InfraredSupported|InitialLoadInfo|

InstallDate|KeyboardPasswordStatus|LastLoadInfo|Manufacturer|Model|Name|N
ameFormat|NetworkServerModeEnabled|NumberOfLogicalProcessors|NumberOfProc
essors|OEMLogoBitmap|OEMStringArray|PartOfDomain|PauseAfterReset|

PCSystemType|PCSystemTypeEx|PowerManagementCapabilities|PowerManagementSu
pported|PowerOnPasswordStatus|PowerState|PowerSupplyState|PrimaryOwnerCon
tact|PrimaryOwnerName|ResetCapability|ResetCount|ResetLimit|Roles|

Status|SupportContactDescription|SystemFamily|SystemSKUNumber|SystemStart
upDelay|SystemStartupOptions|SystemStartupSetting|SystemType|ThermalState
|TotalPhysicalMemory|UserName|WakeUpType|Workgroup

3|True|True|True|0|0|True|{0,0,0,0,0,0,0,0,0,0}|Normal boot|DESKTOP-
749LDN2|3|To be filled by O.E.M.|Win32_ComputerSystem|180|False|AT/AT
COMPATIBLE|DESKTOP-749LDN2|WORKGROUP|0|

True|3|False|False|NULL|(null)|3|(null)|ASUSTeK COMPUTER
INC.|N76VB|DESKTOP-
749LDN2|(null)|True|8|1|NULL|{CL4Ega2fZyBF6,nKZzHrUAm9U9L,2QXu4D9gfKlOw,9
0NB0131-M00840, , , , , , }

|False|-1|2|2|NULL|False|3|0|3|(null)|admin|1|-1|-
1|{LM_Workstation,LM_Server,NT,Potential_Browser}|OK|NULL|N|ASUS-
NotebookSKU|0|NULL|0|x64-based PC|3|17060139008|(null)|6|WORKGROUP
```

Если выполнение команды завершилось с ошибкой, необходимо проверить выполненные настройки.

3.2 Сбор событий от OSSEC

Существует возможность настроить ПК «Комрад» на сбор событий от агента OSSEC, установленного на источнике событий. Для настройки сбора событий от OSSEC необходимо настроить агент OSSEC на источнике событий и сервер OSSEC на ПК «Комрад» (предустановлен). Общая схема настройки и работы сбора событий от OSSEC представлена на рисунке 77.



1	Установка агента OSSEC на источнике событий
2	Добавление агента OSSEC на ПК «Комрад»
3	Генерация ключа для агента OSSEC
4	Импорт ключа на агент OSSEC

5	Настройка агента OSSEC на источнике событий
6	Настройка сервера OSSEC на ПК «Комрад»
7	Передача событий ИБ от источника в ПК «Комрад»

Рисунок 77. Схема настройки сбора событий от OSSEC

3.2.1 Установка агента OSSEC на источнике событий

Для сбора событий с помощью OSSEC на источнике событий должен быть установлен агент. Инструкции по установке агента OSSEC в ОС Linux приведены в приложении В.

3.2.2 Добавление агента OSSEC на ПК «Комрад»

Для добавления агента OSSEC на ПК «Комрад» выполните следующие действия:

1. Запустите на ПК «Комрад» утилиту **/var/ossec/bin/manage_agents** для добавления агента OSSEC.
2. Введите "A" (Add an agent).
3. Введите имя агента.
4. Укажите IP-адрес агента (источника событий).
5. Выберите идентификатор ID (можно оставить по умолчанию).
6. Подтвердите изменения и нажмите `Enter`.

3.2.3 Генерация ключа для агента OSSEC

Для генерации ключа для агента OSSEC выполните следующие действия:

1. В утилите manage_agents введите "E" (Extract key for an agent).
2. Выберите ID агента.
3. Скопируйте сгенерированный ключ и нажмите `Enter`.
4. Завершите работу с утилитой, нажав "Q" (Quit).
5. Перезапустите службу OSSEC командой:

```
/etc/init.d/ossec restart
```

3.2.4 Импорт ключа на агент OSSEC

Для импорта ключа на агент OSSEC выполните следующие действия:

1. Запустите на источнике событий утилиту **/var/ossec/bin/manage_agents** для импорта сгенерированного ключа.
2. Введите "I" (Import key from the server).

3. Вставьте скопированный ранее ключ.
4. Подтвердите изменения и нажмите `Enter`.
5. Завершите работу с утилитой, нажав "Q" (Quit).

3.2.5 Настройка агента OSSEC на источнике событий

Для настройки агента OSSEC на источнике событий выполните следующие действия:

1. Откройте конфигурационный файл **ossec.conf**:

```
sudo nano /var/ossec/etc/ossec.conf
```

2. Укажите IP-адрес ПК «Комрад»:

```
  <client>
    <server-ip>192.168.0.1</server-ip>
  </client>
```

3. Добавьте секцию syslog_output, в которой необходимо указать IP-адрес ПК «Комрад» для перенаправления событий OSSEC в rsyslog:

```
<syslog_output>
  <level>1</level>
  <server>192.168.0.1</server>
</syslog_output>
```

4. Сохраните изменения и закройте конфигурационный файл.
5. Перезапустите службу OSSEC командой:

```
/etc/init.d/ossec restart
```

3.2.6 Настройка сервера OSSEC на ПК «Комрад»

Каталог установки OSSEC в ПК «Комрад»: **/var/ossec/**.

Путь	Описание
/var/ossec/bin/	директория с бинарными файлами
/var/ossec/etc/	директория с конфигурационными файлами
/var/ossec/logs/	директория с событиями (логами)

Сервер OSSEC записывает данные в журнал текущего дня **/var/ossec/logs/alerts/<год>/<месяц>/ossec-alerts-<день>.log**. Журнал за текущие сутки хранится в файле **/var/ossec/logs/alerts/alerts.log**.

Для работы агентов с сервером необходимо открыть UDP-порт 514.

Для настройки сервера OSSEC выполните следующие действия:

1. Откройте конфигурационный файл **rsyslog.conf**:

```
sudo nano /etc/rsyslog.conf
```

2. Раскомментируйте строки:

```
$ModLoad imudp
$UDPServerRun 514
```

3. В секцию rules добавьте правило:

```
*.*     @@127.0.0.1:49005;RSYSLOG_TraditionalFileFormat
```

4. После настройки необходимо перезапустить службу командой:

```
/etc/init.d/rsyslog restart
```

5. Активируйте запись журналов в Syslog командой:

```
/var/ossec/bin/ossec-control enable client-syslog
```

6. Перезапустите сервис командой:

```
/var/ossec/bin/ossec-control restart
```

4 Начало работы

Для начала использования ПК «Комрад» необходимо выполнить следующие действия:

1. Запустите на компьютере администратора совместимый браузер. Список совместимых браузеров приведен ниже.

Тип браузера	Минимально допустимая версия
Google Chrome	48
Safari	10.1
Mozilla Firefox	53
Opera	29
Microsoft Edge	41
Yandex Browser	15.12

2. Введите в адресной строке IP-адрес ПК «Комрад», заданный при его установке, администратор будет переадресован на страницу авторизации (Рисунок 78).

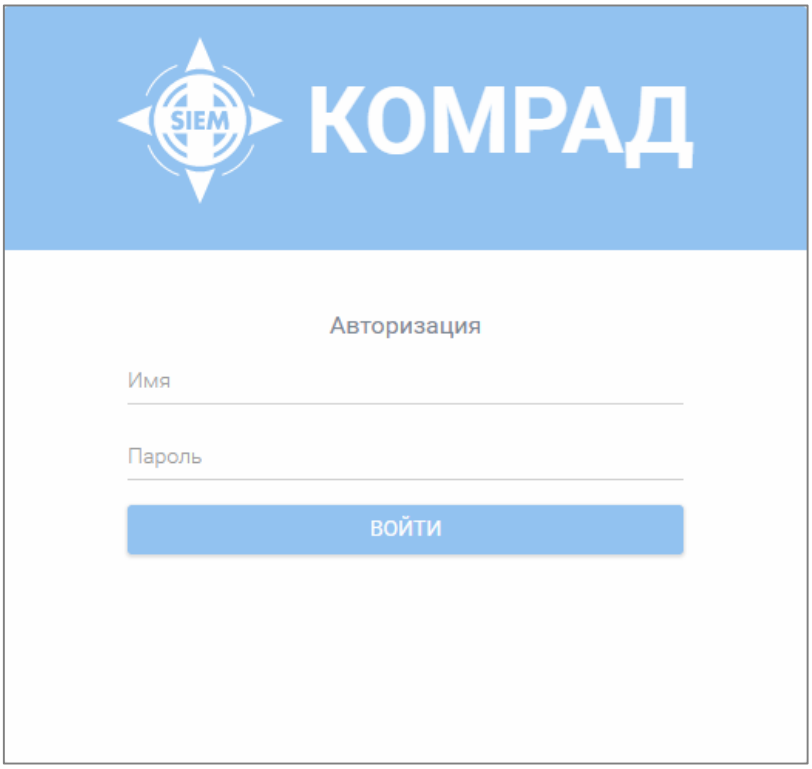


Рисунок 78. Окно авторизации ПК «Комрад»

3. Введите имя пользователя и пароль по умолчанию.

Имя пользователя	admin
Пароль	admin

После успешного входа откроется страница **Виджеты**. Изменить имя пользователя и пароль можно на странице **Администрирование > Пользователи**.

5 Виджеты

В данной главе содержатся сведения о работе с пунктом меню **Виджеты**. Раздел **Виджеты** представляет собой панели визуализации событий ИБ в виде различных графиков и диаграмм и предоставляет возможности по настройке отображаемых данных и их положению на странице.

5.1 Рабочая область виджета

Рабочая область виджета представлена на Рисунок 79.

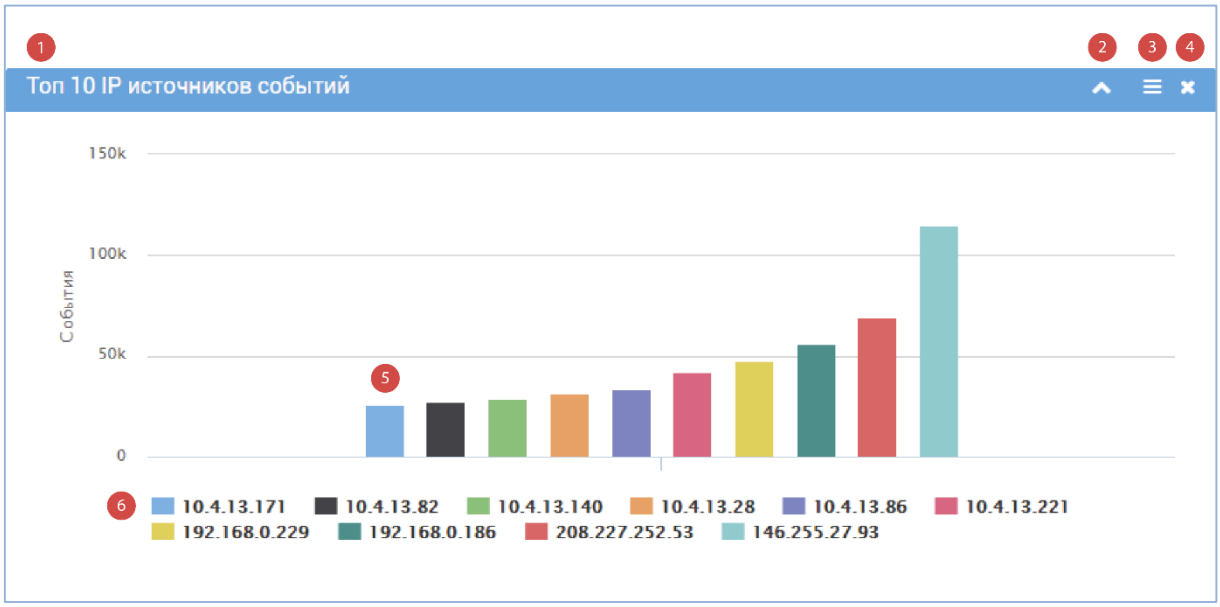


Рисунок 79. Рабочая область виджета

Виджет состоит из следующих элементов:

1) заголовок виджета;
2) кнопка сворачивания/разворачивания виджета;
3) кнопка меню виджета;
4) кнопка удаления виджета;
5) график;
6) легенда.

При нажатии на кнопку открывается панель меню виджета (Рисунок 80).

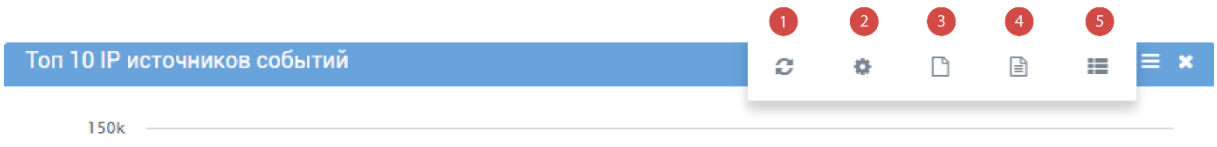


Рисунок 80. Меню виджета

Панель меню состоит из следующих элементов:

1) пересчет виджета (см. раздел Пересчет виджета);
2) настройки виджета (см. раздел Настройка виджета);
3) добавить в шаблоны (см. раздел Добавление шаблона);
4) сгенерировать отчет (см. раздел Экспорт данных виджета);

5) загрузить запрос (см. раздел Запрос для виджета).

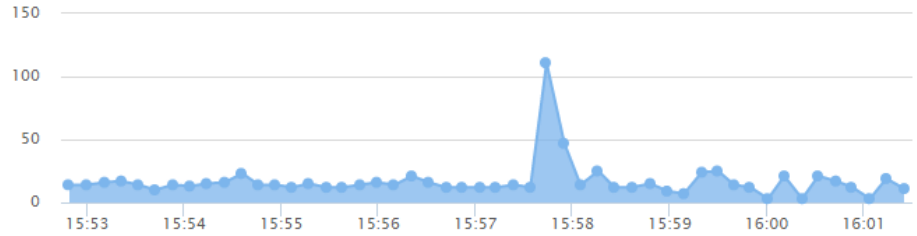
5.2 Типы виджетов

В зависимости от задачи анализа могут использоваться различные типы виджетов.

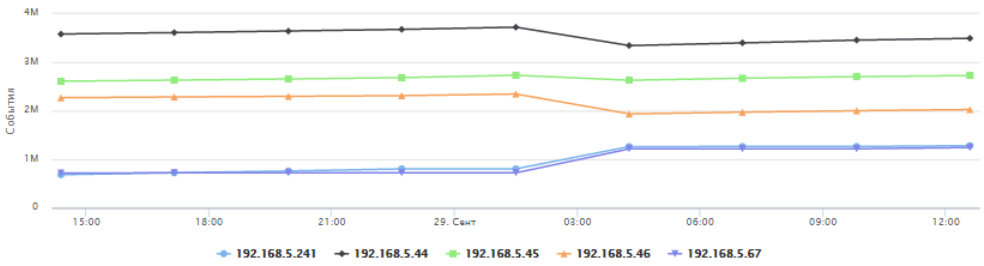
5.2.1 Линейный график

На Рисунок 81 представлены примеры линейных графиков.

а)



б)



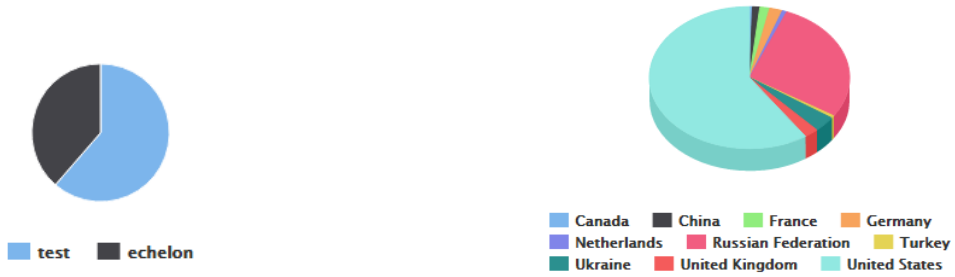
в)

Рисунок 81. Пример линейного графика:
а) — без заливки; б) — с заливкой; в) — множественный без заливки

Точками на линейном графике обозначено количество событий за указанный период времени. Все точки соединяются отрезками. Линейный график наилучшим образом отражает динамику потока событий во времени, а также позволяет отслеживать тренды. «Быстрый» рост графика означает резкое увеличение активности в сети, что может свидетельствовать об инциденте информационной безопасности.

5.2.2 Круговая диаграмма

На Рисунок 82 представлены примеры круговых диаграмм.



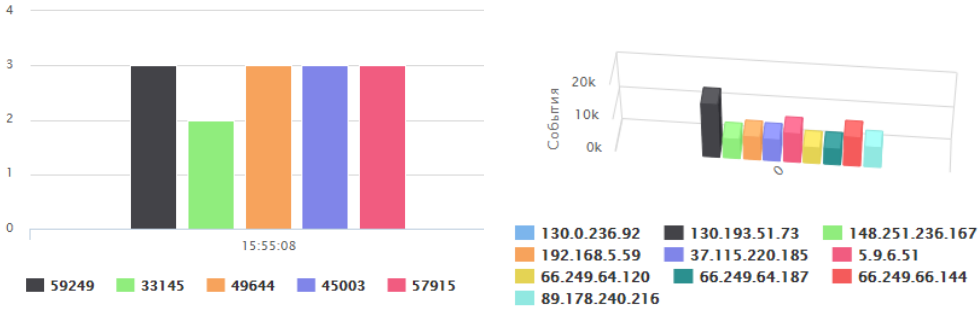
а) б)

Рисунок 82. Пример круговой диаграммы:
а) — плоская; б) — объемная

Каждый сектор круговой диаграммы отражает группу событий с одинаковым значением одного из полей. Площадь сектора пропорциональна количеству событий. Круг соответствует общему количеству событий за указанный период. Виджет типа «Круговая диаграмма» удобно использовать для наглядного отображения соотношения между количеством событий в группе, обладающих одинаковым значением поля, и общим количеством событий за период. Круговая диаграмма сохраняет наглядность только в том случае, если задано небольшое количество групп. Если количество групп событий большое, человеческому глазу сложно различать сектора маленькой площади.

5.2.3 Гистограмма

На Рисунок 83 представлены примеры гистограмм.



а) б)

Рисунок 83. Пример гистограммы:
а) — плоская; б) — объемная

Столбец гистограммы по своему значению аналогичен сектору круговой диаграммы. Высота столбца равна количеству событий соответствующей группы. Гистограмму рекомендуется применять в случае, когда необходимо

сравнить количество событий в разных группах относительно друг друга. Гистограмма, в отличие от круговой диаграммы, не дает наглядного представления о соотношении между количеством событий в группе и общим количеством событий за период. Как и в случае круговой диаграммы, большое количество групп событий с небольшим количеством событий в группе усложняет визуальный анализ.

5.2.4 Список

На Рисунок 84 представлен пример списка.

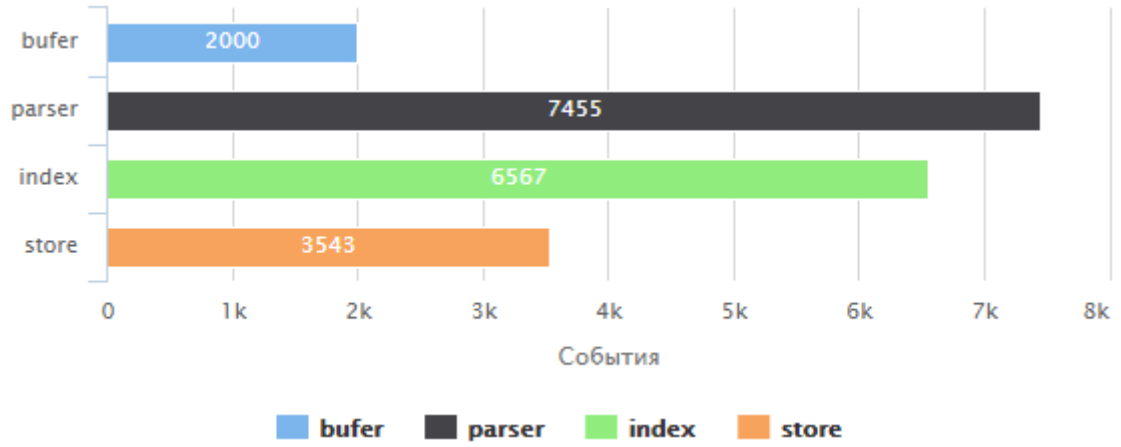


Рисунок 84. Пример списка

Список аналогичен гистограмме. В отличие от гистограммы количество событий соответствующей группы в списке пропорционально не высоте столбца, а длине горизонтальной линии. Для удобства точное количество событий в группе указано непосредственно на линии списка. Гистограмма и список являются взаимозаменяемыми виджетами. Выбор того или иного типа графика зависит исключительно от предпочтений администратора.

5.2.5 Радиальная диаграмма

На Рисунок 85 представлен пример радиальной диаграммы.

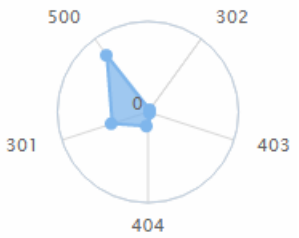


Рисунок 85. Пример радиальной диаграммы

В центре радиальной диаграммы находится начало координат, из которого расходятся оси количества событий ИБ. Количество осей зависит от групп событий ИБ с одинаковым значением поля. Точки на осях соединяются отрезками прямых линий. Полученная таким образом геометрическая фигура позволяет оценивать, к примеру, состояние сетевой активности. Отклонение от симметрии в геометрической фигуре свидетельствует об аномалиях и может сигнализировать об инциденте информационной безопасности.

5.2.6 Таблица

На Рисунок 86 представлен пример таблицы.

Данные	Количество
XMAS сканирование	1
Несанкционированное соединение TeamViewer	1
Несанкционированный вход ROOTa	8
Подбор пароля SSH	2
Попытка повышения привилегий	9

Рисунок 86. Пример таблицы

Таблица позволяет отобразить события, сгруппированные по одному из полей, и число событий в каждой группе. Этот тип виджета рекомендуется использовать в тех случаях, когда есть потребность оперативно получать информацию о точном количестве событий в группе.

5.2.7 Числовой индикатор

Числовой индикатор позволяет отслеживать количество событий, соответствующих запросу виджета (Рисунок 87).

Рисунок 87. Пример числового индикатора

5.3 Настройка виджета

Настройка виджета включает задание его параметров и составление запроса на выборку событий ИБ.

5.3.1 Параметры

Параметр	Описание	Примечание
Имя виджета	название виджета	обязательный параметр
Описание	комментарии администратора	необязательный параметр
Тип графика	подробное описание см. в разделе Типы графиков	обязательный параметр
Источник	источником данных для виджета могут быть база данных событий безопасности или база фактов	обязательный параметр
Объемная	диаграмма будет преобразована в трехмерную	только для типов виджетов Круговая диаграмма, Гистограмма
С заливкой	область под графиком заполняется цветом	только для типов виджетов Линейный, Радиальная диаграмма
Множественный	группировать события на одном виджете	только для типа виджета Линейный
Период	период обновления виджета на странице	единицы измерения: секунды, минуты, часы

Длительность	временной интервал, за который отображаются события	только для типов виджетов Линейный, Гистограмма; единицы измерения: секунды, минуты, часы
Данные события	поле, по которому будут сгруппированы события	только для типов виджетов Круговая диаграмма, Гистограмма, Радиальная диаграмма, Список, Таблица
Топ	количество отображаемых групп событий	
Использовать разницу значений	отображать относительное количество событий	используется разница значений между числом событий в предыдущем периоде и текущем
Сортировать по значению	области на графике будут отображаться в порядке увеличения количества событий	только для типов виджетов Круговая диаграмма, Гистограмма, Радиальная диаграмма, Список, Таблица

Минимальные значения параметров **длительность** и **период** составляют 5 секунд. Значение длительности не должно быть меньше периода.

5.3.2 Запрос для виджета

Виджет отражает статистику по событиям безопасности, подходящим под указанный в виджете запрос к базе данных событий. Существует возможность создать виджет для ранее сохраненного запроса.

5.3.2.1 Запрос к базе фактов

Чтобы загрузить запрос, нажмите кнопку на панели меню виджета (Рисунок 80). Система выполнит переход на страницу **Поиск по событиям**. Если необходимый запрос был ранее создан и сохранен в базе фактов ПК «Комрад», щелкните левой кнопкой мыши в поле **Загрузить запрос** и найдите его по названию.

5.3.2.2 Запрос к базе событий при помощи конструктора запросов

5.3.2.2.1 Сохраненный запрос

Если необходимый запрос был ранее создан и сохранен в ПК «Комрад», щелкните левой кнопкой мыши в поле **Загрузить запрос** и найдите его по названию. При выборе сохраненного запроса он загрузится в конструкторе запросов и станет доступен для редактирования.

5.3.2.2.2 Новый запрос

Мастер создания/настройки виджета содержит встроенный конструктор запросов, в котором необходимо создать запрос для отображения его результатов в виджете. Подробнее о работе с Конструктором запросов см. в разделе Поиск по событиям.

5.4 Настройка панели виджетов

Для удобной группировки виджетов предусмотрена возможность их размещения на пользовательских панелях виджетов (dashboard). Администратор может создать и настроить рабочую область любой панели для удобной работы по своему усмотрению. Предусмотрена возможность перемещать виджеты по рабочей области, изменять размеры виджетов. Осуществить настройку рабочей области возможно только в режиме настройки панели виджетов. Для переключения между режимами используйте кнопку в правой верхней части экрана.

- 

Переход в режим настройки панели виджетов. В данном режиме возможно перемещение виджета по рабочей области и изменение размеров виджета.
- 

Выход из режима настройки панели виджетов, переход в обычный режим. В обычном режиме перемещение и изменение размеров виджетов невозможно.

5.4.1 Создание новой панели

Для создания новой панели виджетов выполните следующие действия:

1. Нажмите кнопку  в верхней части страницы **Виджеты**.
2. Введите новое название панели.
3. Нажмите `Enter`.

Новая панель виджетов создана. Для добавления виджета на панель см. раздел Создание нового виджета.

5.4.2 Переименование панели

Для переименования панели виджетов выполните следующие действия:

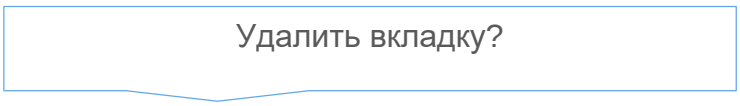
1. Выберите панель, которую необходимо переименовать.
2. Щелкните по ней тройным щелчком левой кнопкой мыши для включения режима редактирования.
3. Введите новое название панели.
4. Нажмите `Enter`.

Панель «Общие» нельзя переименовать.

5.4.3 Удаление панели

Для удаления панели виджетов выполните следующие действия:

1. Перейдите на панель, которую необходимо удалить.
2. Нажмите кнопку  рядом с названием панели.
3. В открывшемся диалоговом окне в ответ на вопрос



нажмите кнопку **Удалить** для подтверждения и кнопку **Отмена** для отмены удаления.

Удаление панели приведет к удалению всех виджетов, которые на ней расположены.

Панель «Общие» удалить нельзя.

5.5 Предустановленные виджеты

5.5.1 Панель «Общие»

Панель визуализации **Общие** содержит предустановленные виджеты:

- события за последний час (см. раздел События за последний час);
- топ 10 IP источников событий (см. раздел Топ 10 IP источников событий);
- топ 10 IP назначения событий (см. раздел Топ 10 IP назначения событий);
- активность пользователей (см. раздел Активность пользователей);
- топ 10 источников событий (см. раздел Топ 10 источников событий).

5.5.1.1 События за последний час

На Рисунок 88 приведен пример графика виджета «События за последний час».

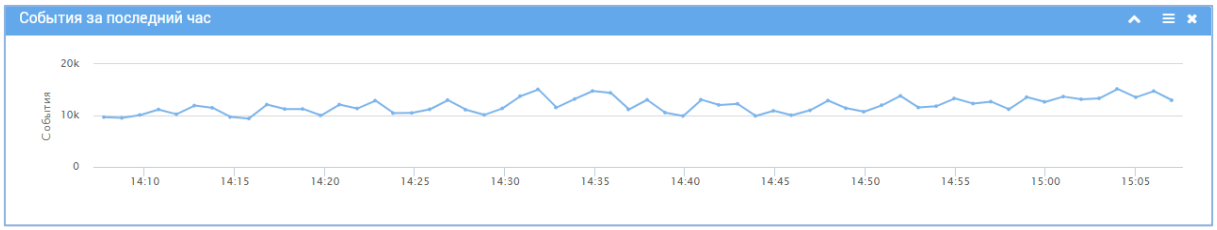


Рисунок 88.Пример графика предустановленного виджета «События за последний час»

Источником данных для виджета является база событий безопасности. Запрос на выборку данных имеет следующий вид (Рисунок 89).

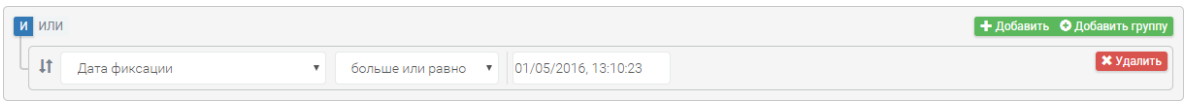


Рисунок 89. Запрос на выборку данных для виджета «События за последний час»

Виджет имеет следующие параметры.

Параметр	**Значение**
Имя виджета	События за последний час
Описание	Отсутствует

Тип графика	Линейный
Источник	База событий
Период (сек)	60
Длительность (сек)	3600
Использовать разницу значений	Включено

5.5.1.2 Топ 10 IP источников событий

На Рисунок 90 приведен пример графика виджета «Топ 10 IP источников событий.

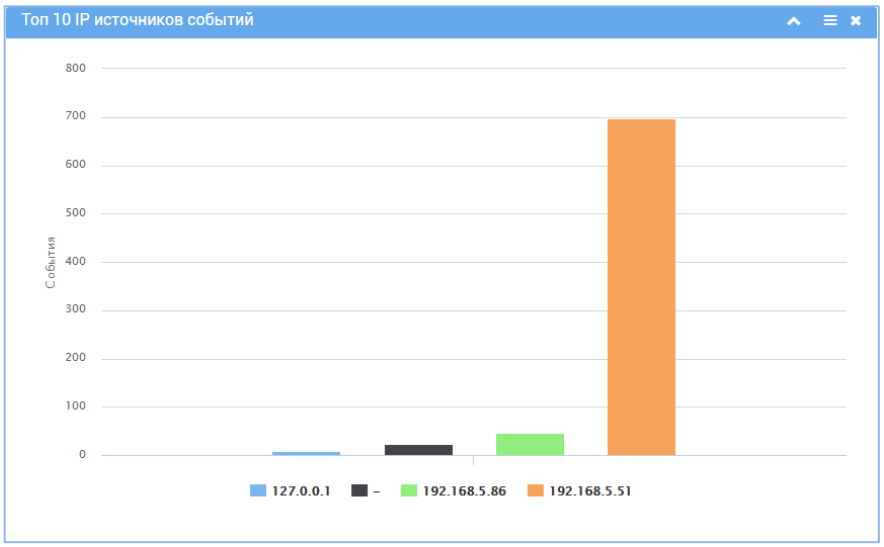


Рисунок 90. Пример графика предустановленного виджета «Топ 10 IP источников событий»

Источником данных для виджета является база событий безопасности. Запрос на выборку данных имеет следующий вид (Рисунок 91).

Рисунок 91. Запрос на выборку данных для виджета «Топ 10 IP источников событий

Виджет имеет следующие параметры.

Параметр	**Значение**
Имя виджета	Топ 10 IP источников событий
Описание	Отсутствует
Тип графика	Гистограмма
Источник	База событий
Период (сек)	60
Длительность (сек)	60
Данные события	IP источника

Использовать разницу значений	Выключено
Сортировать по значению	Включено

5.5.1.3 Топ 10 IP назначения событий

На Рисунок 92 приведен пример графика виджета «Топ 10 IP назначения событий».

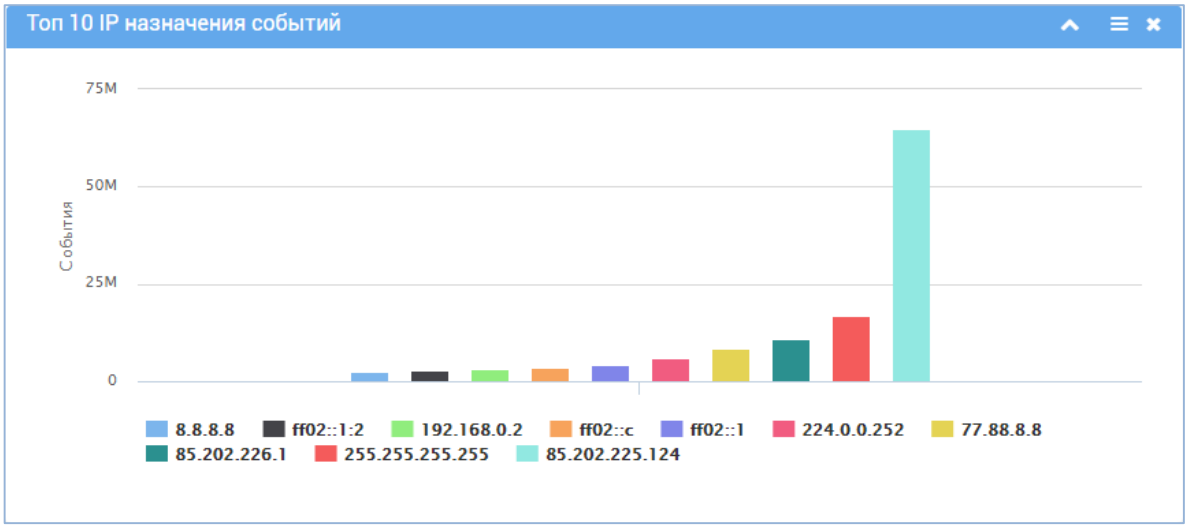


Рисунок 92. Пример графика предустановленного виджета «Топ 10 IP назначения событий»

Источником данных для виджета является база событий безопасности. Запрос на выборку данных имеет следующий вид (Рисунок 93).

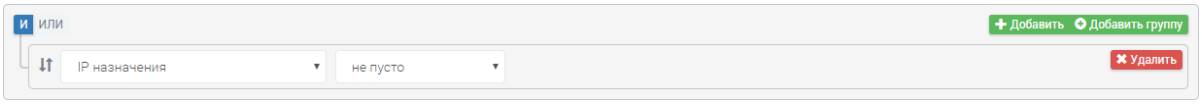


Рисунок 93. Запрос на выборку данных для виджета «Топ 10 IP назначения событий»

Виджет имеет следующие параметры.

Параметр	**Значение**
Имя виджета	Топ 10 IP назначения событий
Описание	Отсутствует
Тип графика	Гистограмма
Источник	База событий
Период (сек)	60
Длительность (сек)	60
Данные события	IP назначения
Использовать разницу значений	Выключено
Сортировать по значению	Включено

5.5.1.4 Активность пользователей

На Рисунок 94 приведен пример графика виджета «Активность пользователей».

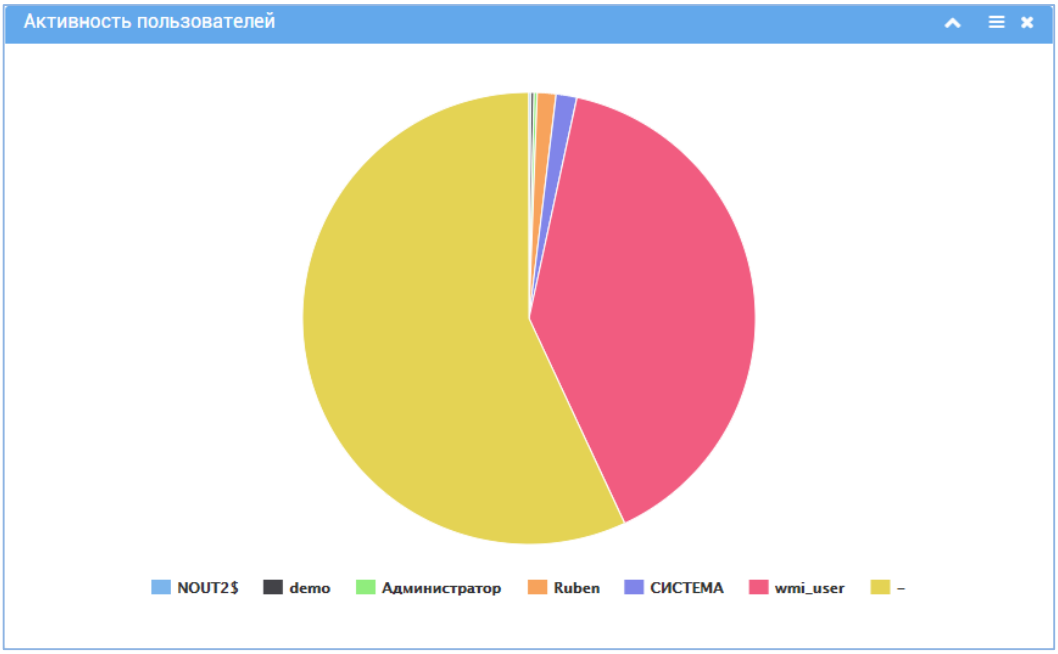


Рисунок 94. Пример графика предустановленного виджета «Активность пользователей»

Источником данных для виджета является база событий безопасности. Запрос на выборку данных имеет следующий вид (Рисунок 95).

Рисунок 95. Запрос на выборку данных для виджета «Активность пользователей»

Виджет имеет следующие параметры.

Параметр	**Значение**
Имя виджета	Активность пользователей
Описание	Отсутствует
Тип графика	Круговая диаграмма
Источник	База событий
Период (сек)	60
Данные события	Имя пользователя
Использовать разницу значений	Выключено
Сортировать по значению	Включено

5.5.1.5 Топ 10 источников событий

На Рисунок 96 приведен пример графика виджета «Топ 10 источников событий».

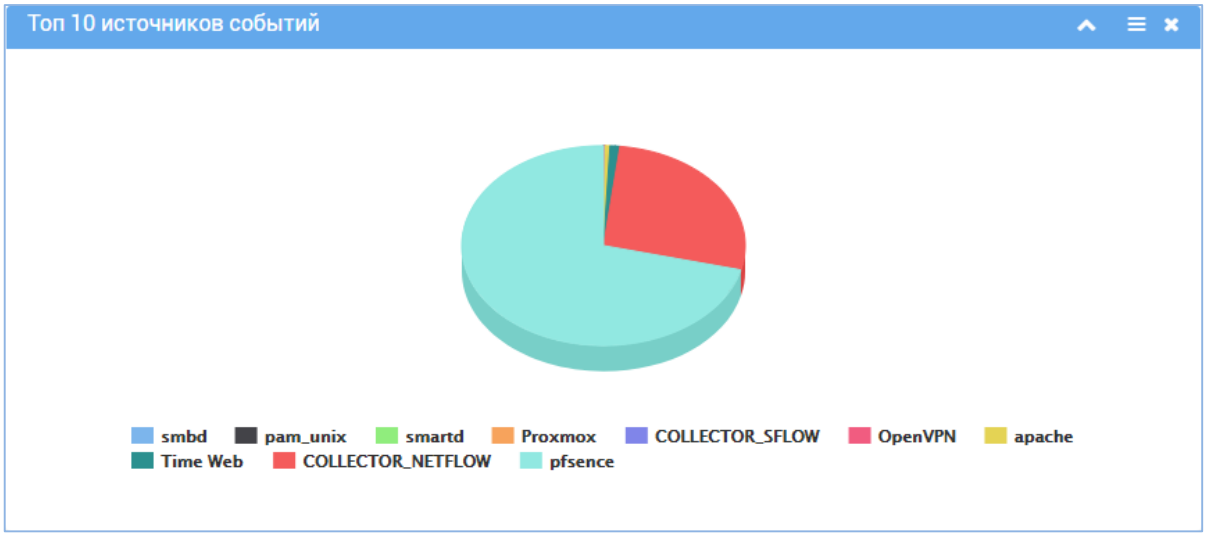


Рисунок 96. Топ 10 источников событий

Источником данных для виджета является база событий безопасности. Запрос на выборку данных имеет следующий вид (Рисунок 97).

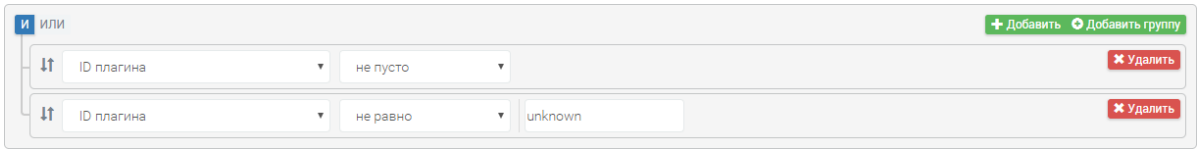


Рисунок 97. Пример графика предустановленного виджета "Топ 10 источников событий"

Виджет имеет следующие параметры

Параметр	**Значение**
Имя виджета	Топ 10 источников событий
Описание	Отсутствует
Тип графика	Объемная круговая
Источник	База событий
Период (сек)	60
Длительность (сек)	60
Данные события	ID плагина
Использовать разницу значений	Выключено
Сортировать по значению	Включено

5.5.2 Панель «Статистика по инцидентам»

Панель визуализации **Статистика по инцидентам** содержит предустановленные виджеты:

- статус инцидентов (см. раздел Статус инцидентов);
- статистика по инцидентам (см. раздел Статистика по инцидентам);
- средняя длительность инцидентов (в секундах)(см. раздел Средняя длительность инцидентов (в секундах));
- среднее время (в секундах) реакции на инцидент (см. раздел Среднее время (в секундах) реакции на инцидент).

5.5.2.1 Статус инцидентов

На Рисунок 98 приведен пример графика виджета «Статус инцидентов».

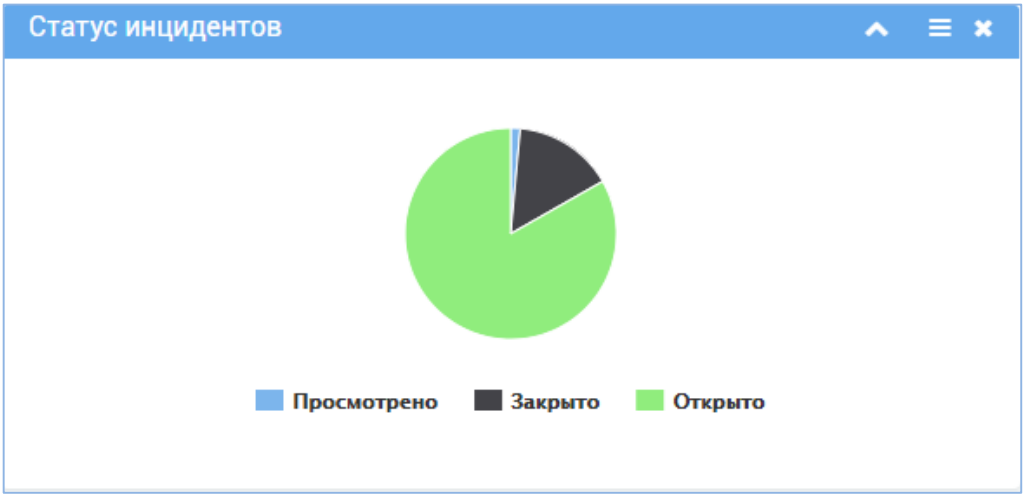


Рисунок 98. Пример графика виджета «Статус инцидентов»

Виджет имеет следующие параметры.

Параметр	**Значение**
Имя виджета	Статус инцидентов
Описание	Отсутствует
Тип графика	Круговая диаграмма
Источник	База фактов
Период (сек)	60
Использовать разницу значений	Выключено
Сортировать по значению	Включено

5.5.2.2 Статистика по инцидентам

На Рисунок 99 приведен пример графика виджета «Статистика по инцидентам».

Рисунок 99. Пример графика виджета «Статистика по инцидентам»

Виджет имеет следующие параметры.

Параметр	**Значение**
Имя виджета	Статистика по инцидентам
Описание	Отсутствует
Тип графика	Таблица
Источник	База фактов
Период (сек)	1
Использовать разницу значений	Выключено
Сортировать по значению	Включено

5.5.2.3 Средняя длительность инцидентов (в секундах)

На Рисунок 100 приведен пример графика виджета «Средняя длительность инцидентов (в секундах)».

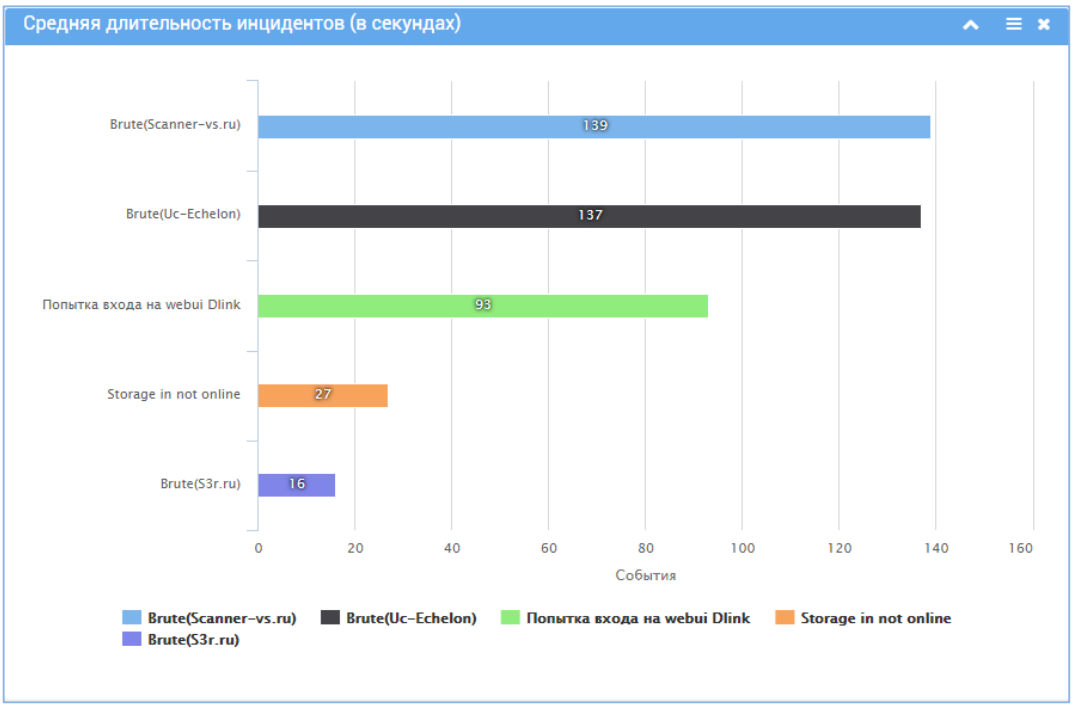


Рисунок 100. Пример графика виджета «Средняя длительность инцидентов (в секундах)»

Виджет имеет следующие параметры.

Параметр	**Значение**
Имя виджета	Средняя длительность инцидентов (в секундах)
Описание	Отсутствует
Тип графика	Список
Источник	База фактов
Период (сек)	60
Использовать разницу значений	Выключено
Сортировать по значению	Включено

5.5.2.4 Среднее время (в секундах) реакции на инцидент

На Рисунок 101 приведен пример графика виджета «Среднее время (в секундах) реакции на инцидент»

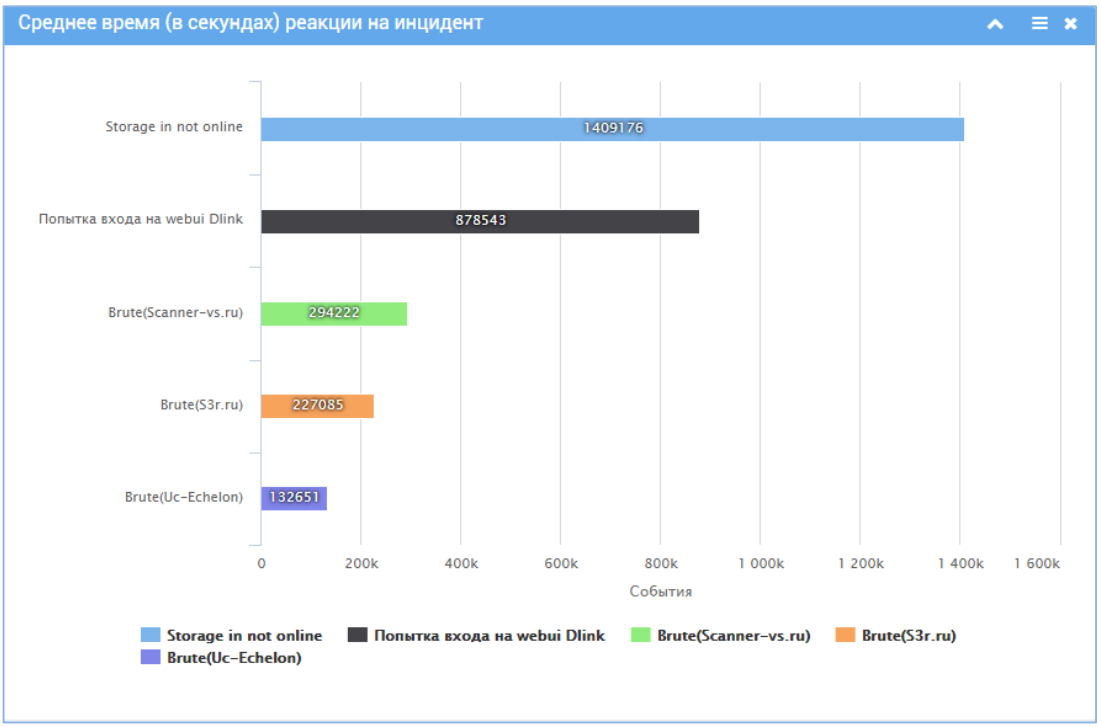


Рисунок 101. Пример графика виджета «Среднее время (в секундах) реакции на инцидент»

Виджет имеет следующие параметры.

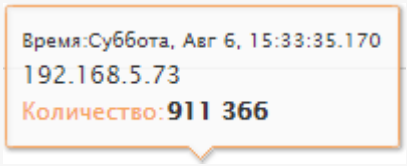
Параметр	**Значение**
Имя виджета	Среднее время (в секундах) реакции на инцидент
Описание	Отсутствует
Тип графика	Список
Источник	База фактов
Период (сек)	60
Использовать разницу значений	Выключено
Сортировать по значению	Включено

5.6 Работа с виджетами

5.6.1 Уточнение информации на графике

Существует возможность получения подробной информации по каждой из точек (столбцу, сектору) диаграммы. При наведении курсора мыши на интересующую точку (столбец, сектор) на диаграмме событий отображается всплывающее информационное сообщение.

Пример информационного сообщения:



По клику на точку графика открывается страница поиска по событиям. На этой странице отображены события, соответствующие временной метке и типу выбранной точки.

Для скрытия/отображения группы событий щелкните по ее заголовку левой кнопкой мыши в легенде виджета.

5.6.2 Создание нового виджета

Для создания нового виджета выполните следующие действия:

1. Нажмите кнопку **Добавить** в правой верхней части страницы.
2. **Название и тип**:
   а) выберите тип графика из предложенного слева списка, при выборе графика доступен его предварительный просмотр;
   б) укажите имя виджета и при необходимости его описание;
   в) для перехода к следующему шагу нажмите кнопку **Далее**, для отмены создания виджета нажмите кнопку **Отмена**.
3. **Данные**. Настройте сбор данных:
   а) выберите источник данных:

База фактов	данные будут сформированы на основе одного из сохраненных в базе фактов запросов
Конструктор запросов	данные будут сформированы при помощи конструктора запросов к базе данных событий

   б) укажите запрос, результат выполнения которого будет отображаться в виджете (подробнее о запросах для виджета см. раздел Запрос для виджета);
   в) для перехода к следующему шагу нажмите кнопку **Далее**, для возврата к предыдущему шагу нажмите кнопку **Назад**, для отмены создания виджета нажмите кнопку **Отмена**.
4. **Параметры**. Укажите параметры виджета (список параметров и их описание доступно в разделе Параметры).

Описание параметра доступно при наведении курсора на пиктограмму .

Для перехода к следующему шагу нажмите кнопку **Далее**, для возврата к предыдущему шагу нажмите кнопку **Назад**, для отмены создания виджета нажмите кнопку **Отмена**.

5. **Результат**. Сводная информация по виджету, который будет создан. Для завершения создания виджета нажмите кнопку **Завершить**, для возврата к предыдущему шагу нажмите кнопку **Назад**, для отмены создания виджета нажмите кнопку **Отмена**.

Новый виджет добавится в нижнюю область панели виджетов. Для получения информации о способе перемещения виджета обратитесь к разделу Перемещение виджета.

5.6.3 Пересчет виджета

Для обновления диаграммы виджета нажмите кнопку  на панели меню виджета (Рисунок 80). Процесс может занять несколько минут.

5.6.4 Редактирование виджета

Для редактирования параметров виджета нажмите кнопку  на панели меню виджета (Рисунок 80). В открывшемся диалоговом окне отредактируйте параметры виджета (работа с интерфейсом подробно описана в разделе Создание нового виджета).

5.6.5 Создание виджета по шаблону

Для создания виджета по шаблону выполните следующие действия:

1. Нажмите кнопку **Шаблоны** в правой верхней части страницы.
2. В открывшемся диалоговом окне выберите нужный шаблон из списка слева, щелкнув на него левой кнопкой мыши.
3. Нажмите кнопку **ОК**, чтобы создать виджет, для отмены создания виджета нажмите кнопку **Отмена**.

5.6.6 Управление шаблонами виджетов

5.6.6.1 Добавление шаблона

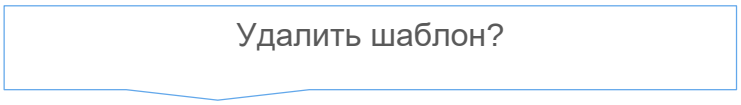
Для добавления виджета в шаблоны с заданным набором параметров нажмите кнопку  на панели меню виджета (Рисунок 80).

Виджет добавится в список шаблонов (см. раздел Создание виджета по шаблону).

5.6.6.2 Удаление шаблона

Для удаления шаблона виджета выполните следующие действия:

1. Нажмите кнопку **Шаблоны** в правой верхней части страницы.
2. В открывшемся диалоговом окне выберите нужный шаблон из списка и нажмите кнопку  в его строке.
3. В открывшемся диалоговом окне в ответ на вопрос



нажмите кнопку **Удалить** для подтверждения и кнопку **Отмена** для отмены удаления.

4. Нажмите кнопку **Отмена**, чтобы закрыть окно.

5.6.7 Перемещение виджета

Для перемещения виджета выполните следующие действия:

1. Перейдите в режим настройки панели виджетов, подробнее о режиме настройки виджетов см. раздел Настройка панели виджетов.
2. Нажмите и удерживайте левую кнопку на области виджета, который необходимо переместить; переместите виджет в нужную область; отпустите кнопку мыши, когда перемещение виджета завершено.
3. Выйдите из режима настройки панели виджетов.

5.6.8 Изменение размера виджета

Для изменения размера виджета выполните следующие действия:

1. Перейдите в режим настройки панели виджетов, подробнее о режиме настройки виджетов см. раздел Настройка панели виджетов.
2. Подведите курсор мыши к краю рабочей области виджета, размер которого необходимо изменить; удерживая левую кнопку мыши, настройте размер виджета; отпустите кнопку мыши, когда изменение размера виджета завершено.
3. Выйдите из режима настройки панели виджетов.

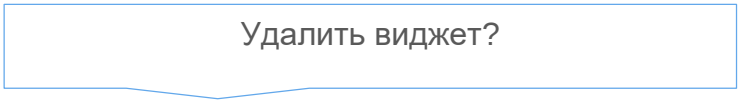
5.6.9 Экспорт данных виджета

Для экспорта данных, отображаемых в виджете, нажмите кнопку  на панели меню виджета (Рисунок 80). В новой вкладке браузера отобразится окно предпросмотра готового отчета, который можно отправить на печать или сохранить на компьютер в формате PDF средствами браузера.

5.6.10 Удаление виджета

Для удаления виджета выполните следующие действия:

1. Выберите виджет, который необходимо удалить.
2. Нажмите кнопку  в правом верхнем углу виджета.
3. В открывшемся диалоговом окне в ответ на вопрос



нажмите кнопку **Удалить** для подтверждения и кнопку **Отмена** для отмены удаления.

6 События в реальном времени

В данной главе содержатся сведения о работе с пунктом меню **События в реальном времени**. Раздел **События в реальном времени** позволяет отслеживать события безопасности, поступающие в ПК «Комрад», в режиме реального времени.

6.1 Диаграмма событий в реальном времени

В верхней части страницы располагается гистограмма количества событий безопасности (Рисунок 102). График обновляется каждую секунду и отображает количество событий, зафиксированных в ПК «Комрад», за прошедшую минуту. Цена деления шкалы времени — 5 секунд.

Рисунок 102. Диаграмма событий в реальном времени

Диаграмма событий в реальном времени соответствует виджету со следующими параметрами.

Тип графика	Гистограмма
Период (сек)	1
Длительность (сек)	60

6.2 Таблица событий в реальном времени

Под диаграммой событий в реальном времени располагается таблица зафиксированных событий. Описание полей таблицы и настройки отображаемых полей см. в разделе Поиск по событиям.

6.3 Работа с событиями в реальном времени

Работа с событиями в реальном времени подразумевает:

- настройку таблицы событий (подробнее см. раздел Настройка таблицы событий в реальном времени);
- остановка и запуск отображения событий в реальном времени (подробнее см. раздел Остановка отображения событий);
- обращение к диаграмме событий для уточнения информации за интересующий интервал времени (подробнее см. раздел Информационные сообщения).

6.3.1 Настройка таблицы событий в реальном времени

Для настройки таблицы событий в реальном времени выполните следующие действия:

1. Нажмите кнопку ⚙ в правом верхнем углу диаграммы событий в реальном времени.
2. Укажите размер таблицы (размер таблицы равен количеству отображаемых на странице событий).

Минимальный размер таблицы — 1. При указании неверного значения диаграмма и таблица событий в реальном времени прекратят обновление.

3. Для сохранения настройки нажмите кнопку **ОК**, для отмены настройки нажмите кнопку **Отмена**.

6.3.2 Остановка отображения событий

Для детального анализа событий, наблюдаемых в реальном времени, предусмотрена возможность временной остановки записи событий в таблицу событий. Чтобы остановить обновление таблицы событий, нажмите кнопку **Стоп**. Чтобы возобновить режим реального времени и продолжить отображение событий в таблице, нажмите **Пуск**.

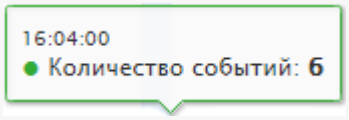
После нажатия кнопки **Стоп** прекратится запись событий в таблицу событий в реальном времени. Однако все события сохраняются в хранилище событий и доступны для поиска на странице **Поиск по событиям**.

Все события, зафиксированные в ПК «Комрад» в период остановки, продолжают отображаться на диаграмме более светлым цветом.

6.3.3 Информационные сообщения

При наведении курсора мыши на столбец, соответствующий интересующему периоду времени, на диаграмме событий отображается всплывающее информационное сообщение, содержащее количество событий, зафиксированных в ПК «Комрад» в эту секунду.

Пример информационного сообщения:



7 Активы

В данной главе содержатся сведения о работе с пунктом меню **Активы**. Раздел **Управление активами** предназначен для создания, редактирования и удаления активами. Под активом понимается конечное или сетевое устройство, имеющее IP-адрес. Если необходимо осуществлять мониторинг доступности технического средства, оно должно быть предварительно добавлено в систему в раздел **Активы**.

7.1 Просмотр активов

Список активов отображается в левой части страницы (Рисунок 103). Для поиска по списку активов введите его имя или часть имени в строку поиска, расположенную в верхней части списка.

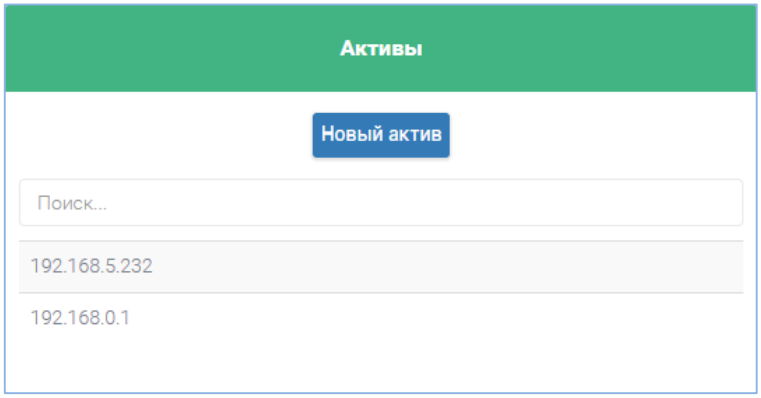


Рисунок 103. Список активов

7.1.1 Список полей актива

Поле	Описание
Имя хоста	уникальное название актива
IP-адрес	сетевой идентификатор актива

К активу может быть подключен один или несколько плагинов модуля мониторинга доступности.

7.1.2 Список полей плагина

Поле	Описание
Имя плагина	название подключенного плагина модуля мониторинга доступности
Порт	порт, который будет контролироваться соответствующим плагином
Описание	комментарий администратора

Все поля являются обязательными для заполнения.

7.2 Создание нового актива

На Рисунок 104 представлено диалоговое окно создания нового актива.

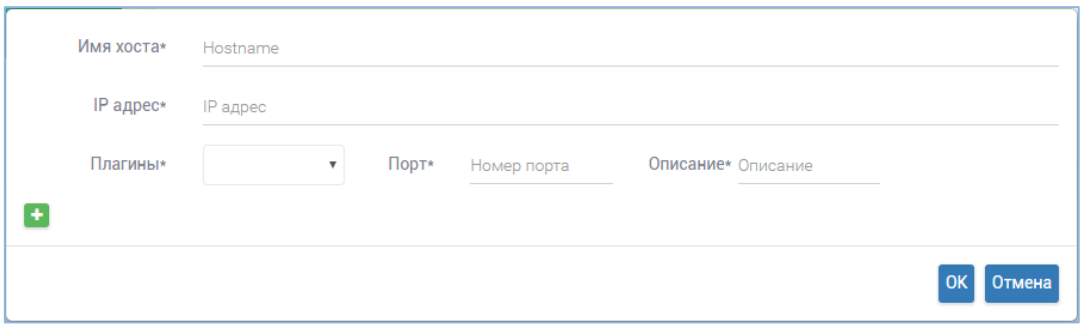


Рисунок 104. Диалоговое окно «Новый актив»

Для создания нового актива выполните следующие действия:

1. Нажмите кнопку **Новый актив** (Рисунок 103).
2. Заполните поля актива.
3. Заполните поля плагина для мониторинга доступности сервиса данного актива.
4. При необходимости мониторинга доступности двух и более сервисов нажмите кнопку  и заполните поля остальных плагинов.
5. Для завершения создания актива нажмите кнопку **OK**, для отмены создания актива нажмите кнопку **Отмена**.

Созданный актив отобразится в списке активов на страницах **Активы** и **Доступность**.

7.3 Редактирование актива

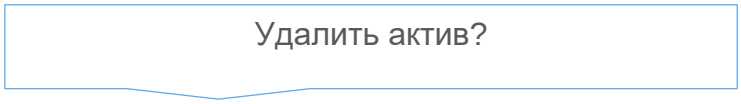
Для изменения актива выполните следующие действия:

1. Выберите актив, поля которого необходимо изменить (Рисунок 103).
2. Нажмите кнопку  .
3. Отредактируйте необходимые данные; для добавления нового плагина нажмите кнопку  и заполните поля плагина, для отключения плагина от актива нажмите кнопку  .
4. Для завершения редактирования актива нажмите кнопку **OK**, для отмены внесенных изменений нажмите кнопку **Отмена**.

7.4 Удаление актива

Для удаления актива выполните следующие действия:

1. Выберите актив, который необходимо удалить (Рисунок 103).
2. Нажмите кнопку **Удалить** в правой верхней части страницы.
3. В открывшемся диалоговом окне в ответ на вопрос



нажмите кнопку **Удалить** для подтверждения и кнопку **Отмена** для отмены удаления.

8 События безопасности

В данной главе содержатся сведения о работе с пунктом меню **События безопасности**, который включает следующие разделы:

- **Поиск по событиям** предназначен для осуществления выборок данных по событиям ИБ при помощи конструктора запросов;
- **Все запросы** позволяет управлять сохраненными запросами на выборку событий.

8.1 Поиск по событиям

Страница **Поиск по событиям** позволяет:

- просматривать события ИБ в соответствии с пользовательскими запросами;
- сохранять пользовательские запросы;
- загружать на компьютер пользователя результаты поиска.

8.1.1 Просмотр событий

Поля таблицы событий безопасности настраиваются пользователем:

- ☑ поле будет включено в таблицу;
- ☐ поле не будет включено в таблицу.

8.1.1.1 Список основных полей таблицы

Поле	**Описание**
№ события	уникальный идентификатор события
Дата фиксации	дата поступления события в ПК «Комрад»
Дата генерации	дата генерации сообщения на источнике событий
Данные	полное сообщение от источника событий
Тип сообщения	пара ID плагина:SID плагина
ID плагина	идентификатор плагина
SID плагина	идентификатор подгруппы правил плагина модуля обработки событий
Протокол	протокол обмена данными
IP источника	IP-адрес узла-источника
IP назначения	IP-адрес узла-назначения
Порт источника	порт узла-источника
Порт назначения	порт узла-назначения
Имя источника	символическое имя узла-источника
Имя назначения	символическое имя узла-назначения
MAC источника	MAC-адрес узла-источника
MAC назначения	MAC-адрес узла-назначения
Имя файла	название файла (если оно присутствует в событии)
Имя пользователя	пользователь, от имени которого совершалось действие, повлекшее за собой генерацию сообщения
Устройство	IP-адрес или символическое имя промежуточного сетевого устройства

В зависимости от конфигурации и используемых источников событий могут появляться дополнительные поля.

8.1.1.2 Карточка события

Для просмотра информации о событии щелкните по нему левой кнопкой мыши в таблице событий. Откроется карточка события, содержащая разделы с полями нормализации. Для удобного отображения полей необходимо использовать кнопки  и  . Чтобы закрыть карточку, щелкните левой кнопкой мыши в любую точку окна за ее пределами.

8.1.2 Конструктор запросов к базе событий

Конструктор позволяет составлять запросы к базе данных событий безопасности.

8.1.2.1 Рабочие элементы конструктора

-  перемещение запроса (группы запросов);
-  включено логическое «И»;
-  включено логическое «ИЛИ»;
-  добавить новое условие текущего уровня;
-  добавить новый уровень;
-  удалить условие или группу условий запроса;
-  удалить все критерии запроса, очистить поля конструктора;
-  сохранить список событий безопасности в формате CSV;
- **Поиск** найти все события безопасности, соответствующие критериям запроса;
- **Сохранить** сохранить запрос для оперативного обращения к нему при дальнейшей работе.

8.1.2.2 Построение запроса

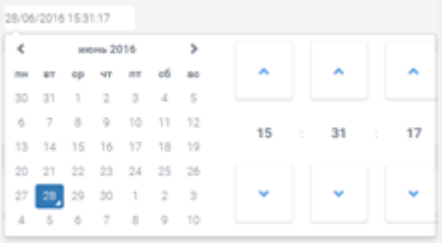
Строить запросы можно по любому полю таблицы. Ниже приведено описание возможных значений полей.

Поле	Оператор	Описание
№ события	равно	точное значение поля
	не равно	любое значение поля, кроме указанного

Поле	Оператор	Описание
	начинается с	значение поля начинается с указанных символов
	не начинается с	значение поля начинается с любых символов, кроме указанных
	содержит	значение поля содержит указанные символы
	не содержит	значение поля не содержит указанные символы
	оканчивается на	значение поля оканчивается указанными символами
	не оканчивается на	значение поля оканчивается любыми символами, кроме указанных
Порт источника Порт назначения	равно	точное значение поля
	не равно	любое значение поля, кроме указанного
	меньше	значение поля меньше указанного
	больше	значение поля больше указанного
	содержит	значение поля содержит указанные символы
	не содержит	значение поля не содержит указанные символы
	пусто	поле не содержит значения
	не пусто	поле содержит какое-либо значение
Дата фиксации Дата генерации	равно	точное значение поля
	не равно	любое значение поля, кроме указанного
	меньше	значение поля меньше указанного
	меньше или равно	значение поля меньше указанного или совпадает с ним
	больше	значение поля больше указанного
	больше или равно	значение поля больше указанного или совпадает с ним
	между	значение поля лежит в указанном интервале
	пусто	поле не содержит значения
	не пусто	поле содержит какое-либо значение
Другие	равно	точное значение поля
	не равно	любое значение поля, кроме указанного
	начинается с	значение поля начинается с указанных символов
	не начинается с	значение поля начинается с любых символов, кроме указанных
	содержит	значение поля содержит указанные символы

Поле	Оператор	Описание
	не содержит	значение поля не содержит указанные символы
	оканчивается на	значение поля оканчивается указанными символами
	не оканчивается на	значение поля оканчивается любыми символами, кроме указанных
	пусто	поле не содержит значения
	не пусто	поле содержит какое-либо значение

Для ввода данных формата даты и времени предусмотрен календарь. Прочие поля редактируются в текстовом виде.



8.1.2.2.1 Поиск по одному полю таблицы

Выборку событий ИБ по одному из полей таблицы можно выполнить с помощью простого запроса. Для создания простого запроса выполните следующие действия:

1. Выберите поле, по которому необходимо построить запрос (полный список полей доступен в разделе Список основных полей таблицы).
2. Выберите критерий запроса.
3. Укажите значение поля.
4. Нажмите кнопку **Поиск**.

8.1.2.2.2 Поиск по нескольким полям таблицы

Выборку событий ИБ по нескольким полям таблицы можно выполнить при помощи составного запроса. Составной запрос представляет собой объединение простых запросов. Для создания составного запроса выполните следующие действия:

1. Создайте простой запрос, указав в качестве поля одно из полей, по которым необходимо осуществить выборку (см. раздел Поиск по одному полю таблицы).
2. Нажмите кнопку **Добавить**.
3. Добавьте необходимое количество простых запросов.
4. Укажите, какой логический оператор необходимо применить к результатам простых запросов (см. раздел Рабочие элементы конструктора):

а) логическое «И», если необходимо найти события на пересечении результатов всех простых запросов;
б) логическое «ИЛИ», если необходимо объединить результаты простых запросов в одно множество событий ИБ.

5. Нажмите кнопку **Поиск**.

8.1.2.2.3 Подзапрос

Подзапрос является простым либо составным запросом, выполненным внутри другого запроса, и представляет собой инструмент для построения сложных запросов на выборку событий ИБ. Для создания подзапроса выберите нужный запрос и нажмите кнопку **Добавить группу**.

8.1.2.2.4 Перемещение запроса (группы запросов)

Для перемещения запроса (группы запросов) с одного уровня на другой нажмите и удерживайте кнопку ⇵ в левой части запроса (группы запросов), который необходимо переместить. Переместите запрос (группу запросов) на нужный уровень. Отпустите кнопку мыши, когда перемещение запроса (группы запросов) завершено.

8.1.2.2.5 Примеры

Пример 1. События ИБ, поступившие от источника с именем siem (Рисунок 105).

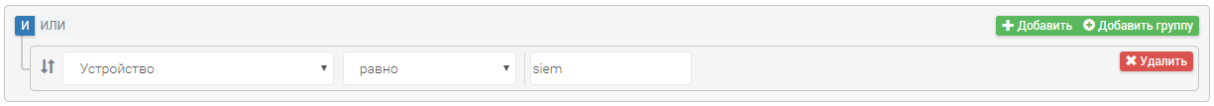


Рисунок 105. Директива корреляции для примера 1

Пример 2. События ИБ, поступившие от источника с именем siem в период времени с 20 по 21 июня 2016 года (Рисунок 106).

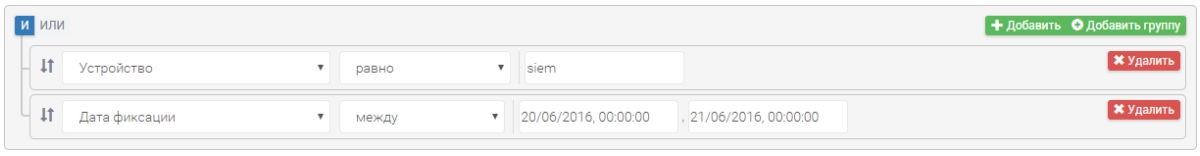


Рисунок 106. Директива корреляции для примера 2

Пример 3. События ИБ, сформированные для пользователя root или любого пользователя, имя которого начинается с символов «us» (Рисунок 107).

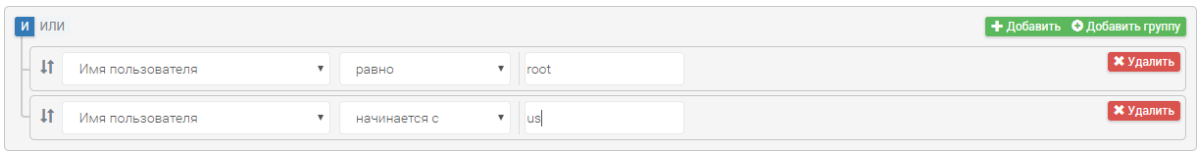


Рисунок 107. Директива корреляции для примера 3

Пример 4. События ИБ, поступившие от любого источника в подсети 192.168.1.0/24, инициаторы которого — пользователи user1 или user2 (Рисунок 108).

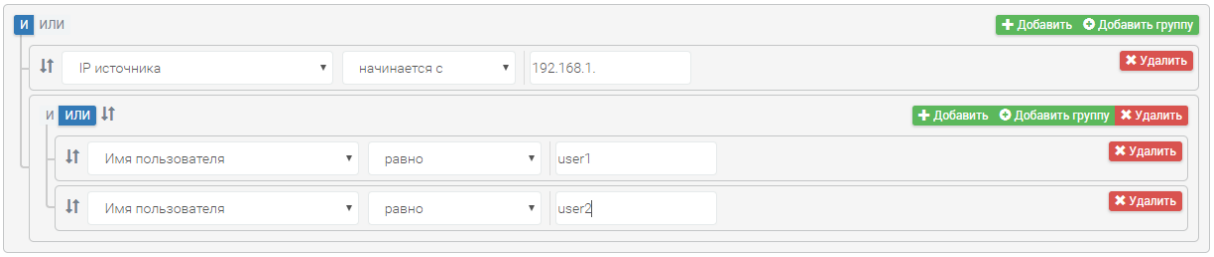


Рисунок 108. Директива корреляции для примера 4

Пример 5. События ИБ, связанные с веб-ресурсами, которые происходили в выходные дни 18 и 19 июня 2016 года, сформированные для сотрудников, работавших в указанный период из офиса (локальная сеть 192.168.0.0/16), за исключением администратора безопасности (security_admin), если только последний не работал удаленно (через VPN) (Рисунок 109).

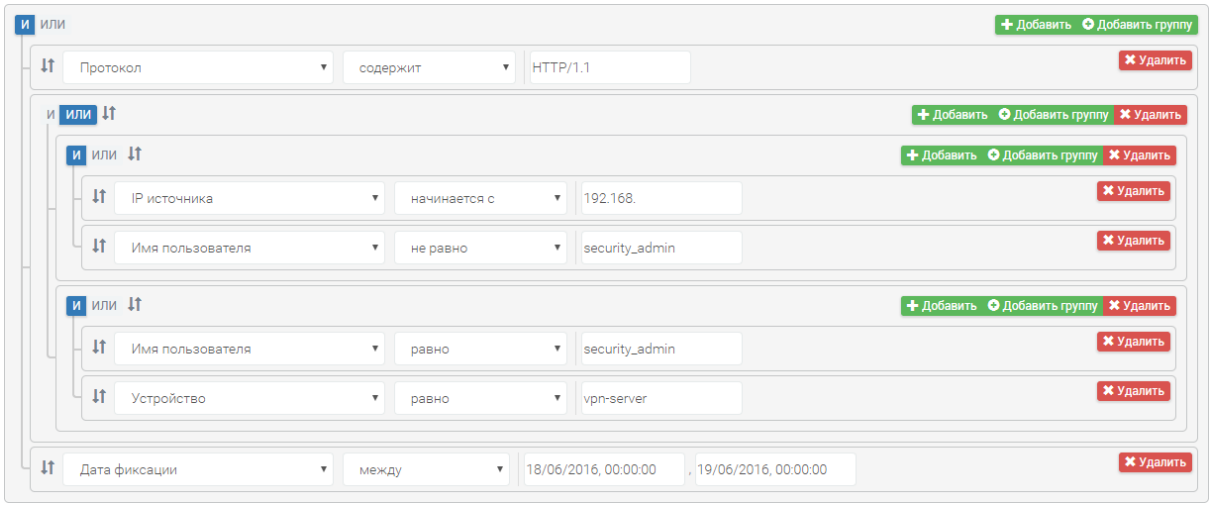


Рисунок 109. Директива корреляции для примера 5

8.1.2.3 Удаление элементов запроса

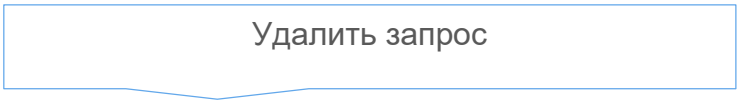
Для удаления элемента запроса нажмите кнопку **Удалить**. Удалить можно как запрос, так и любой подзапрос.

Удаление подзапроса приведет к удалению всех вложенных в него элементов.

8.1.2.4 Отмена запроса

Предусмотрена возможность быстрого удаления всех элементов запроса, отображаемого в конструкторе запросов в данный момент.

1. Нажмите кнопку ✖.
2. В открывшемся диалоговом окне в ответ на вопрос



нажмите кнопку **ОК** для подтверждения и кнопку **Отмена** для отмены удаления.

8.1.2.5 Сохранение запроса

Существует возможность сохранить запрос для удобного обращения к нему в процессе работы. Для этого выполните следующие действия:

1. Нажмите кнопку **Сохранить**.
2. В открывшемся диалоговом окне введите имя запроса в поле **Имя запроса** и краткое описание результата выполнения запроса в поле **Описание**.
3. Для сохранения запроса нажмите кнопку **ОК**, для отмены сохранения запроса нажмите кнопку **Отмена**.

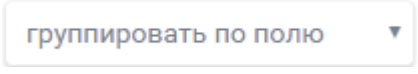
Сохраненные запросы доступны на странице **Все запросы**. Подробное описание работы с сохраненными запросами см. в разделе Все запросы.

8.1.2.6 Применение сохраненного запроса

Для того, чтобы использовать для выборки событий ранее созданный запрос (см. раздел Сохранения запроса), выберите его название в выпадающем списке поля **Загрузить запрос**. Запрос отобразится на странице.

8.1.2.7 Группировка событий

Существует возможность сгруппировать события выборки по любому из полей.

1. Постройте запрос (см. пункт Построение запроса).
2. Выберите поле, по которому необходимо сгруппировать, в выпадающем списке 

.
3. Нажмите кнопку **Поиск**.

В интерфейсе отобразятся первые (по количеству событий) 25 групп.

8.1.2.8 Автообновление результата запроса

Существует возможность настроить автоматическое обновление результатов запроса. Запрос к базе событий будет выполняться с периодичностью, заданной администратором.

Для активации автообновления запроса отметьте пункт **Обновление** и укажите период обновления (Рисунок 110). Минимальный период обновления — 30 секунд.

Рисунок 110. Настройка автообновления

8.1.3 Диаграмма событий

После построения запроса в конструкторе запросов установите флажок **Построить график** и нажмите кнопку **Поиск**. Система построит диаграмму событий, соответствующую заданному запросу (Рисунок 111). Процесс может занять несколько минут.

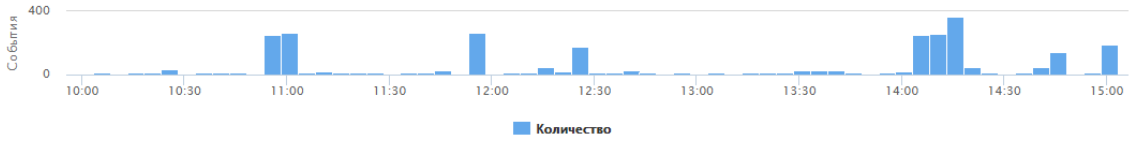
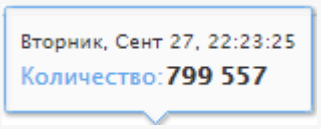


Рисунок 111. Пример диаграммы событий

8.1.3.1 Информационные сообщения

При наведении курсора мыши на столбец, соответствующий интересующему периоду времени, на диаграмме событий отображается всплывающее информационное сообщение, содержащее количество событий, зафиксированных в ПК «Комрад» в этот период времени.

Пример информационного сообщения:



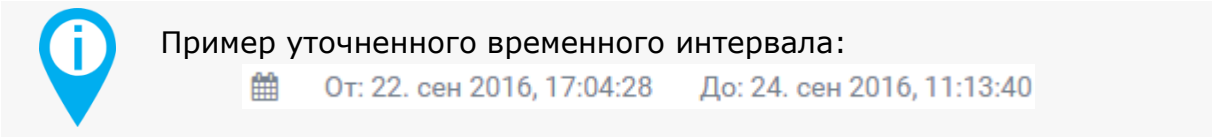
8.1.3.2 Работа с диаграммой событий

8.1.3.2.1 Уточнение запроса

Предусмотрена возможность уточнения интервалов времени в запросе при помощи диаграммы событий.

Выберите дату и время начала и окончания интересующего периода времени. Нажмите и удерживайте левую кнопку мыши на области диаграммы, соответствующей дате начала интересующего периода. Не отпуская левую кнопку мыши, переместите курсор в область, соответствующую дате окончания интересующего периода. Отпустите кнопку мыши.

В результате будет построена диаграмма распределения событий в уточненный период времени. В выборке событий будут только те события, которые соответствуют уточненному интервалу. Период времени уточненного запроса отображается в верхней части диаграммы.



8.1.3.2.2 Отмена уточнения

Для возврата к первоначальной (неуточненной) выборке событий нажмите кнопку ✖ справа от уточненного временного интервала.

8.2 Все запросы

Раздел **Все запросы** позволяет оперировать сохраненными запросами к базе данных событий безопасности.

8.2.1 Таблица списка запросов

Все сохраненные запросы отражаются в таблице со следующими полями.

Поле	Описание
№	порядковый номер запроса
Имя запроса	название запроса
Описание	комментарии пользователя (может быть пустым)
Время создания	дата и время сохранения запроса в системе

8.2.2 Рабочие элементы

-  переход к редактированию и поиску по запросу на странице Поиск по событиям;
-  удалить сохраненный запрос;
- **Поиск по таблице...** строка ввода для поиска запроса по ключевому слову/части слова.

8.2.3 Сортировка списка запросов

Предусмотрена возможность сортировки в лексикографическом порядке по любому из полей таблицы списка запросов.

Для осуществления сортировки выполните следующие действия:

1. Щелкните левой кнопкой мыши по нужному полю таблицы списка запросов.
2. Выберите кнопками  и  прямой или обратный порядок сортировки.

9 Контроль соответствия

В данной главе содержатся сведения о работе с пунктом меню **Контроль соответствия**. Раздел **ГОСТ Р ИСО/МЭК 27001-2006** позволяет осуществлять контроль соответствия требованиям ГОСТ Р ИСО/МЭК 27001-2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования».

9.1 Цели и меры

Рабочее поле отображает цели и меры управления, перечисленные в Приложении А ГОСТ Р ИСО/МЭК 27001-2006, на конкретную систему менеджмента информационной безопасности (СМИБ).

9.1.1 Состояния мер управления

Состояние меры управления формируется из сочетания ее статусов. Возможны следующие состояния.

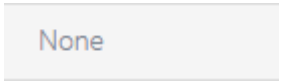
- 

мера управления не применяется к СМИБ;
- 

мера управления применяется к СМИБ, но не реализована;
- 

мера управления применяется к СМИБ и реализована.

9.1.2 Рабочие элементы

- 

текстовое поле для ввода комментария;
- 
кнопка «Печать», с помощью которой можно распечатать отчет или сохранить на компьютер средствами браузера.

9.1.3 Управление целями и мерами

Управление целями и мерами производится по следующему сценарию:

1. Отметьте меры управления, которые применяются к СМИБ.
2. Среди мер, которые применяются к СМИБ, отметьте реализованные (Подробнее о возможных состояниях мер см. раздел Состояния мер управления).
3. При необходимости оставьте комментарии в текстовых полях напротив мер.

Примеры текстовых комментариев:

1. обоснование применимости/неприменимости меры управления;
2. планируемая дата реализации меры.

4. Для сохранения отчета в формате PDF нажмите кнопку **Сохранить**.

9.2 Статистика

Статистика отражает количество мер управления в каждой из групп А.5-А.15 Приложения А ГОСТ Р ИСО/МЭК 27001-2006, которые применяются к СМИБ и реализованы в ней.

9.2.1 Работа со статистикой

Статистика отображается в виде столбчатой диаграммы (Рисунок 112). Каждому столбцу соответствует группа мер управления А.5-А.15. Число над столбцом диаграммы соответствует общему количеству мер управления в группе. В рамках одной группы цветом выделяются блоки мер с одинаковым состоянием.

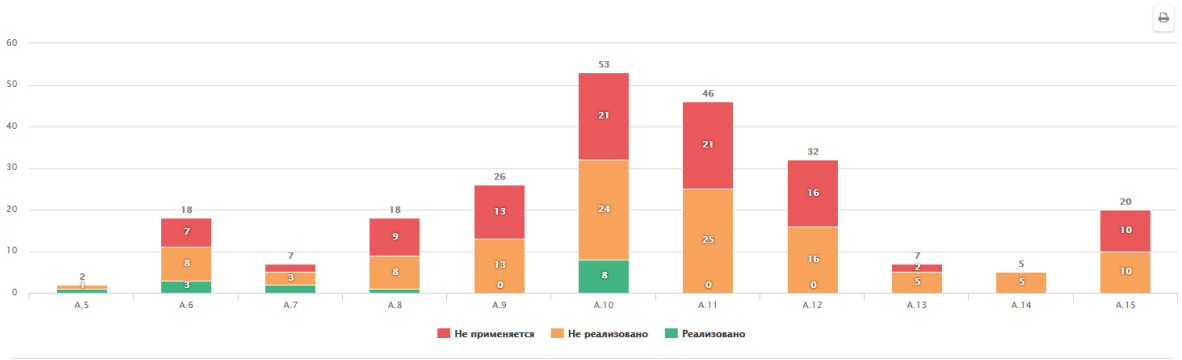


Рисунок 112. Пример диаграммы статистики

Ниже представлено соответствие цвета блока статусу меры.

Цвет	Состояние меры	
	Не применяется	Не реализовано
	Применяется	Не реализовано
	Применяется	Реализовано

Блок дополнительно сопровождается числом, соответствующим количеству мер в блоке.

При наведении курсора на блок мер всплывает окно со сводной информацией:

- идентификатор группы мер;
- количество мер в данном блоке;
- количество мер в группе.

Для скрытия/отображения блока мер щелкните по его цвету левой кнопкой мыши.

Для быстрого перехода к группе мер в рабочем поле Цели и меры управления щелкните левой кнопкой мыши по столбцу диаграммы с идентификатором интересующей группы мер.

9.2.2 Работа со статистикой вне интерфейса ПК «Комрад»

Для работы со статистикой вне графического интерфейса ПК «Комрад» предусмотрены возможности:

- напечатать график;
- скачать в формате PDF.

Данные возможности вызываются по нажатию на  .

9.3 Панель навигации

В правой части страницы располагается перечень мер управления A.5-A.15 для удобного переключения между блоками мер. Для перехода к нужному блоку мер достаточно щелкнуть по нему левой кнопкой мыши на панели навигации.

10Корреляция

В данной главе содержатся сведения о работе с пунктом меню **Корреляция**, который включает следующие разделы:

- **Конструктор директив** предназначен для управления директивами корреляции;
- **Инциденты** предназначен для просмотра инцидентов ИБ и управления процессом их расследования.

10.1 Конструктор директив

Каждая директива корреляции предназначена для выявления одного типа инцидента информационной безопасности. Она включает одно правило верхнего (нулевого) уровня и неограниченное количество правил, образующих логические маршруты директивы. Под логическим маршрутом директивы понимается цепочка правил, в которой выполнение каждого следующего правила возможно только при условии выполнения предыдущего. Под выполнением правила подразумевается наступление количества событий, заданного счетчиком событий, за период времени, указанный в таймере правила. Правила, принадлежащие разным логическим маршрутам, но имеющие одинаковый порядковый номер в соответствующих цепочках правил, образуют один уровень директивы корреляции. Поступление события верхнего уровня влечет за собой активацию правил первого уровня на всех логических маршрутах. Инцидент ИБ будет сгенерирован при выполнении всех правил хотя бы одного логического маршрута.

Рассмотрим пример (Рисунок 113). Данная директива корреляции позволяет выявлять инцидент информационной безопасности, который имеет следующий сценарий. Злоумышленник сканирует службу SSH на защищаемых ресурсах, данное действие фиксируется межсетевым экраном «Рубикон» (Правило#0). Далее злоумышленник проводит попытки удаленной авторизации на защищаемых ресурсах (атака подбора пароля методом перебора). Сообщения о попытках авторизации могут поступать как от операционной системы (Правило#1), так и от системы обнаружения вторжений OSSEC (Правило#2). Правило#0 является правилом верхнего (нулевого) уровня. Директива имеет два логических маршрута: Правило#0 — Правило#1 и Правило#0 — Правило#2, при этом правила #1 и #2 относятся к одному уровню директивы корреляции, так как имеют одинаковый порядковый номер в соответствующих маршрутах.

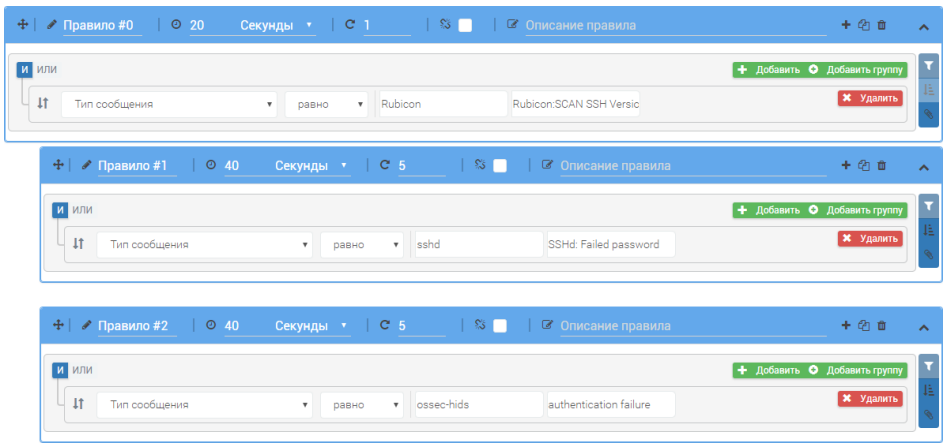


Рисунок 113. Двухуровневая директива корреляции с двумя логическими маршрутами

10.1.1 Рабочая область правил и директив корреляции

Рабочая область правила корреляции представлена на Рисунок 114.

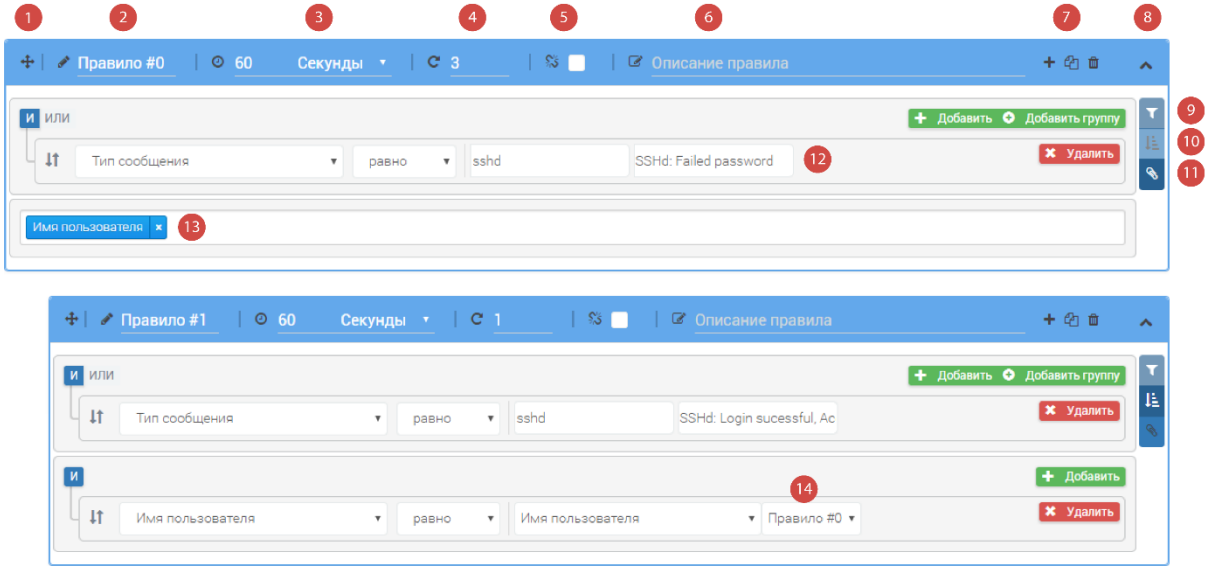


Рисунок 114. Пример рабочей области правила корреляции

Рабочая область состоит из следующих элементов:

1) кнопка перемещения правила;
2) название правила;
3) таймер правила;
4) счетчик событий;
5) тип правила «отсутствие событий»;
6) описание;
7) блок управления правилом;
8) кнопка «свернуть правило»;
9) операция «фильтрация»;
10) операция «наследование»;
11) операция «модальность»;
12) блок «фильтрация»;
13) блок «модальность»;
14) блок «наследование».

Для удобного просмотра директивы используйте ^ и v.

10.1.1.1 Параметры

10.1.1.1.1 Название правила

Название правила задается администратором в текстовом виде и может быть использовано в блоке правила с типом наследование. Название правила отображается в разделе **Инциденты**.

10.1.1.1.2 Таймер правила

Таймер правила запускается при поступлении первого события, попадающего под критерии правила. Если в течение этого времени не произойдет указанное в счетчике количество событий, он будет обнулен.

10.1.1.1.3 Счетчик событий

Счетчик определяет количество событий, которое должно произойти в течение времени, заданном в таймере правила, для активации следующего уровня.

10.1.1.1.4 Описание

Комментарий администратора является необязательным параметром.

10.1.1.2 Тип правила «отсутствие событий»

Правило типа «отсутствие событий» считается выполненным, если в течение времени, заданном в таймере правила, не наступило ни одного события, удовлетворяющего критериям данного правила. Для этого типа правила игнорируется счетчик событий.

10.1.1.3 Блоки правила

Каждое правило формируется из набора (блоков) критериев. Каждый блок может быть отнесен к одному из типов: фильтрация, наследование или модальность.

10.1.1.3.1 Фильтрация

Блок типа «фильтрация» формируется при помощи инструментария конструктора запросов (см. раздел Поиск по событиям). Позволяет фильтровать события, удовлетворяющие ограничениям, заданным в конструкторе.

10.1.1.3.2 Наследование

Если значение полей фильтрации не может быть задано константой, а зависит от значения, полученного на предыдущем уровне директивы, применяется Наследование.

Пример использования: необходимо, чтобы события второго уровня директивы имели то же значение поля IP-адрес, что и события, составившие первый уровень директивы.

10.1.1.3.3 Модальность

Блок типа «модальность» позволяет группировать события по значению параметра, указанного в блоке. В этом случае под область действия правила попадут только те события, у которых значение параметра, указанного в блоке Модальность, одинаковое.

10.1.1.4 Управление правилом

10.1.1.4.1 Создание правила текущего уровня

Для создания правила на текущем уровне нажмите кнопку  в рабочей области любого из правил текущего уровня.

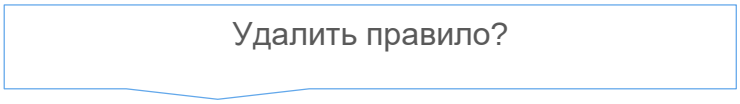
10.1.1.4.2 Создание правила следующего уровня

Для создания правила на следующем уровне нажмите кнопку  в рабочей области любого из правил текущего уровня.

10.1.1.4.3 Удаление правила

Для удаления правила корреляции выполните следующие действия:

1. Нажмите кнопку  в рабочей области правила, которое необходимо удалить.
2. В открывшемся диалоговом окне в ответ на сообщение



нажмите кнопку **ОК** для подтверждения и кнопку **Отмена** для отмены удаления.

10.1.1.5 Перемещение правила

Для перемещения правила с одного уровня на другой нажмите и удерживайте кнопку  в рабочей области правила, которое необходимо переместить. Переместите правило на нужный уровень. Отпустите кнопку мыши, когда перемещение правила завершено.

10.1.2 Директивы корреляции

Список доступных в системе директив корреляции имеет древовидную структуру, расположен в левой части страницы. Для удобного управления директивами они хранятся в каталогах.

10.1.2.1 Каталоги

Каждый каталог имеет название и снабжается символом . Каталог может содержать как директивы корреляции, так и другой каталог (подкаталог). Каталог **Предустановленные** содержит список директив корреляции, которые создаются автоматически при установке ПК «Комрад» (см. раздел Предустановленные директивы корреляции).

10.1.2.1.1 Просмотр каталогов

Для отображения содержимого каталога нажмите . Для того, чтобы скрыть содержимое каталога, нажмите .

10.1.2.1.2 Создание каталога

Для создания каталога директив корреляции выполните следующие действия:

1. Выберите каталог, в котором необходимо создать новый каталог.
2. Нажмите кнопку в левой верхней части страницы.
3. В открывшемся диалоговом окне введите имя нового каталога.

Имя каталога не может быть пустым. При попытке указать пустое имя каталога ПК «Комрад» выдаст сообщение

> Пустые имена не могут быть использованы

и каталог не будет создан.

4. Для сохранения каталога нажмите кнопку **ОК**, для отмены создания каталога нажмите кнопку **Отмена**.

10.1.2.1.3 Удаление каталога

Для удаления каталога директив корреляции выполните следующие действия:

1. Выберите каталог, который необходимо удалить.
2. Нажмите кнопку **Удалить** в левой верхней части страницы.
3. В открывшемся диалоговом окне в ответ на вопрос

> Удалить элемент?

нажмите кнопку **ОК** для подтверждения или кнопку **Отмена** для отмены удаления.

Удаление непустых каталогов невозможно.

10.1.2.2 Управление директивами корреляции

10.1.2.2.1 Просмотр директив

Для отображения директивы корреляции найдите и выберите нужную директиву в левой части страницы. Активные директивы снабжены символом  . Если действие директивы в данный момент времени отключено, ее название сопровождается символом  .

10.1.2.2.2 Создание директивы

Для создания новой директивы корреляции выполните следующие действия:

1. Выберите каталог, в котором необходимо создать новую директиву.
2. Нажмите кнопку  в левой верхней части страницы.
3. В открывшемся диалоговом окне введите название новой директивы.

Название директивы не может быть пустым. При попытке указать пустое имя директивы ПК «Комрад» выдаст сообщение

> Пустые имена не могут быть использованы

и директива не будет создана.

4. Для сохранения директивы нажмите кнопку **ОК**, для отмены создания директивы нажмите кнопку **Отмена**.
5. Создайте правила директивы (см. разделы Рабочая область правила корреляции, Управление правилом).
6. Нажмите кнопку **Сохранить директиву** для завершения процедуры создания директивы.
7. При необходимости продолжить без сохранения изменений после любого действия в ответ на сообщение

> Директива была изменена. Несохраненные изменения будут потеряны. Вы действительно хотите продолжить?

нажмите кнопку **ОК** для подтверждения. При необходимости сохранить изменения нажмите кнопку **Отмена** и перейдите к шагу 6.

Созданная директива включена: события, удовлетворяющие критериям правил, будут формировать инцидент. Для отключения действия директивы нажмите кнопку **Приостановить**.

10.1.2.2.3 Редактирование директивы

Для изменения директивы корреляции выполните следующие действия:

1. Выберите директиву, которую необходимо изменить.
2. Внесите необходимые изменения (см. разделы Рабочая область правила корреляции, Управление правилом).
3. Нажмите кнопку **Сохранить директиву** для завершения процедуры создания директивы.

10.1.2.2.4 Включение (отключение) директивы

Для включения (отключения) работы директивы корреляции выполните следующие действия:

1. Выберите директиву, которую необходимо включить (отключить).
2. Нажмите кнопку **Возобновить** (**Приостановить**).

10.1.2.2.5 Экспорт директивы

Для экспорта директивы выполните следующие действия:

1. Выберите директиву, которую необходимо экспортировать.
2. Нажмите кнопку **Экспорт**.
3. В открывшемся диалоговом окне нажмите кнопку **Копировать**, чтобы скопировать код директивы.
4. Нажмите кнопку **ОК**, чтобы завершить действие.

10.1.2.2.6 Импорт директивы

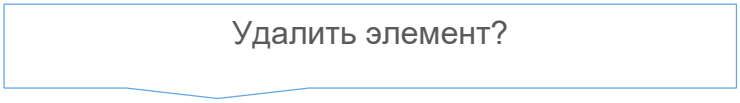
Для импорта директивы выполните следующие действия:

1. Нажмите кнопку **Импорт**.
2. В открывшемся диалоговом окне нажмите сочетание клавиш `Ctrl + V`, система добавит в текстовое поле ранее скопированный код директивы.
3. Для завершения действия нажмите кнопку **ОК**, для отмены действия нажмите кнопку **Cancel**.

10.1.2.2.7 Удаление директивы

Для удаления директивы корреляции выполните следующие действия:

1. Выберите директиву, которую необходимо удалить.
2. Нажмите кнопку  в левой верхней части страницы.
3. В открывшемся диалоговом окне в ответ на вопрос



нажмите кнопку **ОК** для подтверждения и кнопку **Отмена** для отмены удаления.

10.1.3 Предустановленные директивы корреляции

10.1.3.1 Подкаталог KAV

Подкаталог **KAV** содержит директивы корреляции на основе событий от Kaspersky Security 10.

Директива	Описание
Не установлено антивирусное ПО	На клиентском узле не установлено средство антивирусной защиты
Неполная комплектация AV-средства	Некоторые компоненты средства антивирусной защиты не используются (отключены)
Базы устарели	Базы данных сигнатур давно не обновлялись, есть угроза
Сторонний источник баз	Попытка использования недоверенных ресурсов для обновления баз данных сигнатур
Сбой обновления	При обновлении средства антивирусной защиты произошла ошибка
Остановка задачи	Приостановлено выполнение задачи
Срабатывание самозащиты	Сработал компонент самозащиты антивируса от вредоносных программ, пытающихся заблокировать его или удалить с компьютера
Срабатывание защиты	Средство антивирусной защиты обнаружило вредоносное ПО
Ошибка активации	При активации средства антивирусной защиты произошла ошибка
Режим ограниченной функциональности	Средство антивирусной защиты перешло в режим ограниченной функциональности

10.1.3.2 Подкаталог Dallas Lock

Подкаталог **Dallas Lock** содержит директивы корреляции на основе событий от СЗИ Dallas Lock 8.0.

Директива	Описание

Нарушение целостности файла	Обнаружено нарушение целостности контролируемого объекта
Нарушение целостности реестра	Обнаружено нарушение целостности реестра
Удаление файла	Файл был удален
Отключение аудита	Аудит был отключен
Сброс мандатных уровней	Настройки мандатных уровней были сброшены
Нарушение КС на нескольких машинах	Целостность файла была нарушена на нескольких рабочих станциях

10.1.3.3 Подкаталог Континент

Подкаталог **Континент** содержит директивы корреляции на основе событий от АПКШ «Континент» (с использованием SIEM-коннектора 1.0).

Директива	**Описание**
Недоступность криптошлюза	Криптошлюз перестал присылать события очистки журнала
Сбой обновления ключей	После команды на удаленную смену ключей криптошлюз перестал быть доступен

10.1.4 Примеры

Пример 1. Директива, состоящая из двух уровней, на каждом из которых по одному правилу (Рисунок 115).

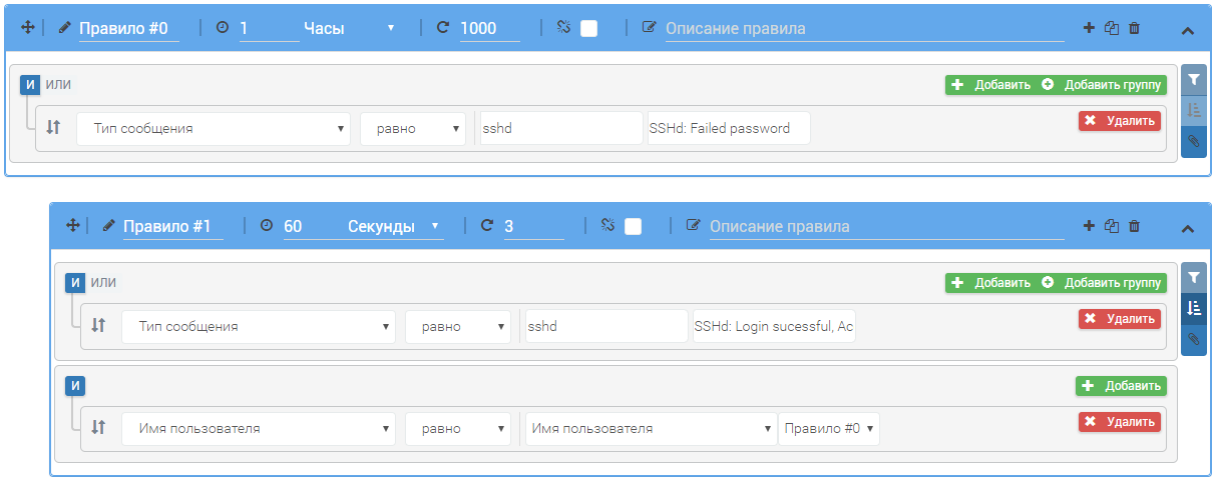


Рисунок 115. Директива корреляции для примера 1

- **Правило 1**. В течение 1 часа ожидается не менее 1000 событий неуспешной авторизации одного и того же пользователя.

Параметр правила	**Значение**

Название правила	Правило #0
Таймер правила	1 час
Счетчик событий	1000
Блоки правила	
Фильтрация	Тип сообщения|равно|sshd|SSHD: Failed password
Модальность	Имя пользователя

- **Правило 2**. В течение 60 секунд ожидается не менее 3 событий успешной авторизации от имени пользователя, зафиксированного при выполнении правила 1.

Параметр правила	**Значение**
Название правила	Правило #1
Таймер правила	60 секунд
Счетчик событий	3
Блоки правила	
Фильтрация	Тип сообщения|равно|sshd|SSHD: Login sucessful, Accepted password
Наследование	Имя пользователя|равно|Имя пользователя|Правило #0

Пример 2. Директива, состоящая из двух уровней, на каждом из которых по одному правилу (Рисунок 116).

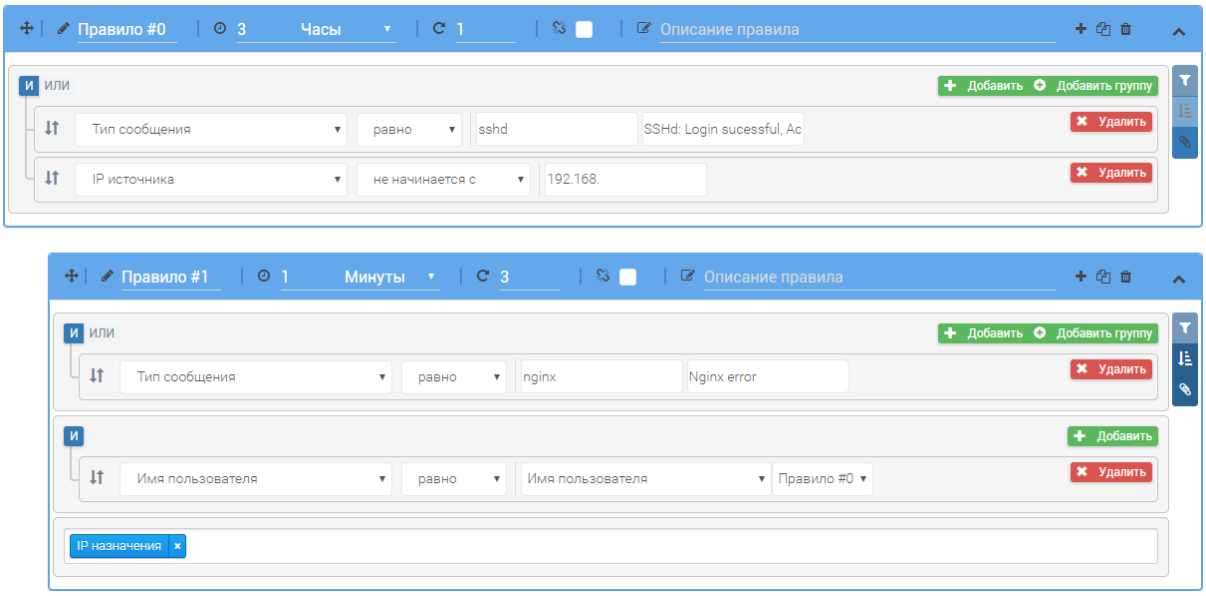


Рисунок 116. Директива корреляции для примера 2

- **Правило 1**. В течение 3 часов ожидается хотя бы одно событие успешной авторизации из внешней сети.

Параметр правила	Значение
Название правила	Правило #0
Таймер правила	3 часа
Счетчик событий	1
Блоки правила	
Фильтрация	Тип сообщения | равно | sshd | SSHD: Login sucessful, Accepted password **И** IP источника|не начинается с | 192.168

- **Правило 2**. В течение 1 минуты ожидается не менее 3 событий от одного и того же веб-сервера nginx. Событие заключается в возникновении ошибки при обработке запросов от имени пользователя, зафиксированного при выполнении правила 1.

Параметр правила	Значение
Название правила	Правило #1
Таймер правила	1 минута
Счетчик событий	3
Блоки правила	
Фильтрация	Тип сообщения | равно | nginx | Nginx error
Наследование	Имя пользователя | равно | Имя пользователя | Правило #0
Модальность	IP назначения

10.1.5 Реакция на инцидент

При обнаружении инцидента ИБ его расследование может быть назначено пользователю или группе пользователей. Оповещение о возникновении инцидента может быть отправлено на электронную почту. Возможна настройка вызова пользовательского сценария: например, для оповещения по SMS, создания правила блокировки для межсетевого экрана и т.п.

Настройка реакции на инцидент производится на вкладке **Реакция** (Рисунок 117).

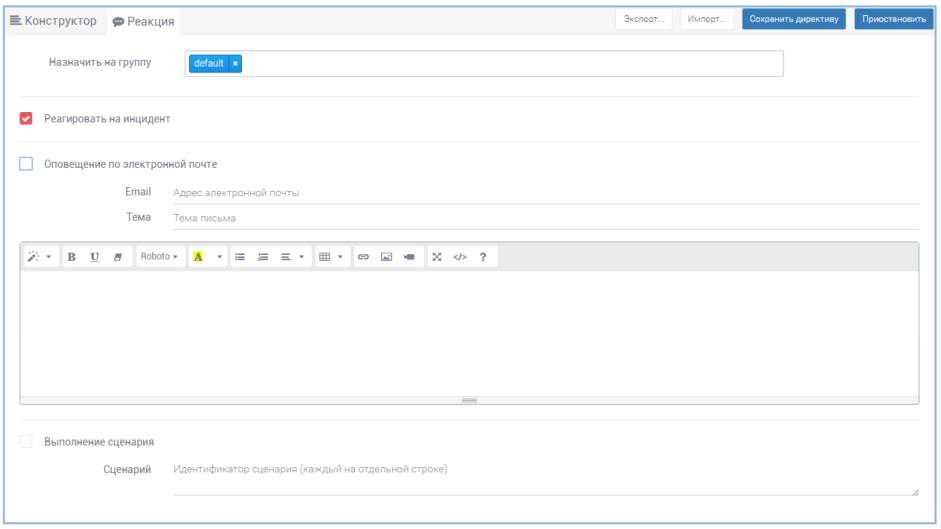


Рисунок 117. Вкладка «Реакция»

Для настройки реакции при возникновении инцидента выполните следующие действия:

1. Перейдите на вкладку **Реакция**.
2. Выберите пользователя или группу пользователей, на которых будет назначено расследование инцидента, в разделе **Назначить на группу**.
   Отметьте пункт **Реагировать на инцидент**.
3. При необходимости оповещения по электронной почте:
   3.1. отметьте пункт **Оповещение по электронной почте**;
   3.2. укажите электронный адрес получателя;
   3.3. укажите тему письма.
4. Введите текст, который будет генерироваться для оповещения об инциденте. В тексте могут быть использованы следующие псевдонимы (alias).

Поле	**Псевдоним**
№ инцидента	INCIDENT_ID
Название директивы	DIRECTIVE_NAME
Дата генерации инцидента	INCIDENT_TIME
Количество событий в инциденте	INCIDENT_EVENTS_NUMBER
Длительность	INCIDENT_DURATION
Назначено	INCIDENT_ASSIGNED

Псевдонимы обрамляются знаками процента. Например, %INCIDENT_ID%.

5. При необходимости выполнения сценария:
   5.1. отметьте пункт **Выполнение сценария**;

5.2. укажите имя и параметры сценария (через пробел);
5.3. при необходимости вызова более одного сценария укажите имена и параметры каждого сценария с новой строки.

Сценарии должны располагаться в каталоге:
/usr/share/komrad-reaction-block/scripts/.

При вызове сценария могут быть использованы псевдонимы.
Пример вызова сценария:
notify_by_SMS.sh %DIRECTIVE_NAME%.

10.2 Инциденты

Страница **Инциденты** предназначена для просмотра информации об инцидентах ИБ, сформированных ПК «Комрад».

10.2.1 Просмотр инцидентов

Страница **Инциденты** состоит из двух таблиц.

- Сводка по всем инцидентам (Рисунок 118). Для удобного просмотра инциденты сгруппированы по директивам, в результате работы которых они были сформированы. Существует возможность сортировки списка директив по количеству инцидентов. Для этого щелкните левой кнопкой мыши по полю **Всего** и выберите кнопками и прямой или обратный порядок сортировки.

- Краткая информация об инцидентах (Рисунок 119). Таблица отражает перечень инцидентов, зарегистрированных в системе, а также общую информацию по ним. Полная информация об инциденте доступна в карточке инцидента.

Рисунок 118. Сводная таблица по всем инцидентам

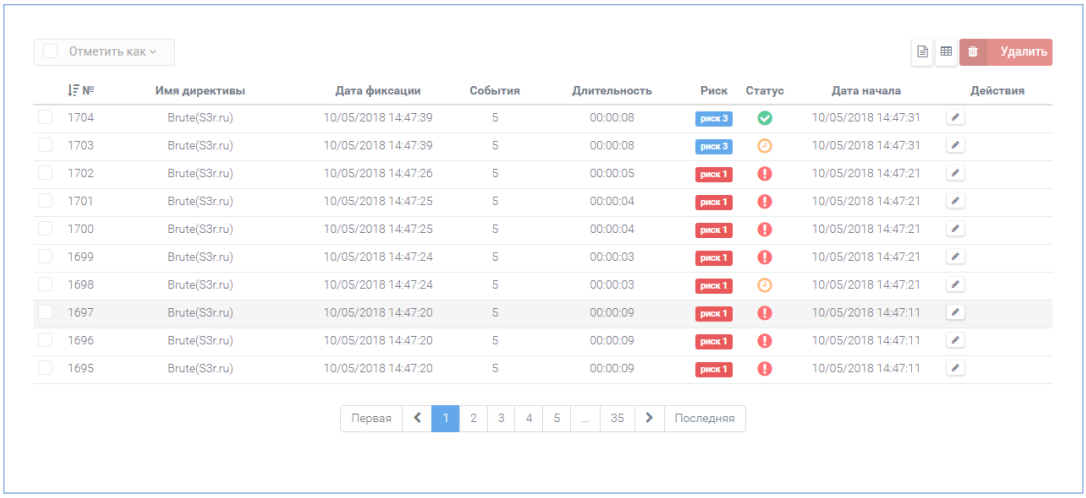


Рисунок 119. Общая таблица инцидентов

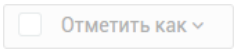
Также доступна сводная информация по статусам инцидентов:

- открытые;
- просмотренные;
- закрытые.

10.2.1.1 Список полей таблицы инцидентов

Поле	Описание
№	идентификатор инцидента
Имя директивы	название директивы, срабатывание которой привело к формированию инцидента
Дата фиксации	дата и время формирования инцидента (последнего события)
События	общее количество событий ИБ в инциденте
Длительность	разница между датой фиксации и датой начала
Риск	показатель критичности инцидента
Статус	статус расследования инцидента: • новый — инцидент зафиксирован, но еще не просмотрен • просмотрен — карточка инцидента была открыта • закрыт — расследование инцидента завершено
Дата начала	дата и время активации директивы (поступления события, удовлетворяющего критериям правила нулевого уровня)

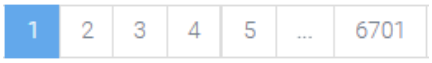
10.2.1.2 Рабочие элементы

-  переход к директиве в конструкторе директив;
-  экспорт отчета в формате PDF;
-  экспорт отчета в формате CSV;
- 

позволяет отметить все инциденты и присвоить им статус;
- **Удалить** удаление инцидента.

10.2.1.3 Навигация

Для удобной навигации по таблице инцидентов предусмотрена порядковая нумерация страниц. Блок порядковой нумерации располагается в нижней части страницы.

- 

кнопки перемещения по страницам;
-  переход на предыдущую страницу;
-  переход на следующую страницу;
- **Первая** переход на первую страницу;
- **Последняя** переход на последнюю страницу.

10.2.2 Поиск по инцидентам

Поиск по инцидентам осуществляется при помощи конструктора запросов. Подробнее о работе с конструктором см. раздел Конструктор запросов к базе событий. Строить запросы можно по любому полю таблицы. Ниже приведено описание возможных значений полей.

Поле	Оператор	Описание
№	равно	точное значение поля
	не равно	любое значение поля, кроме указанного
	меньше	значение поля меньше указанного
	больше	значение поля больше указанного
	содержит	значение поля содержит указанные символы
	не содержит	значение поля не содержит указанные символы
События Длительность Риск	равно	точное значение поля
	не равно	любое значение поля, кроме указанного
	меньше	значение поля меньше указанного

	больше	значение поля больше указанного
	содержит	значение поля содержит указанные символы
	не содержит	значение поля не содержит указанные символы
	пусто	поле не содержит значения
	не пусто	поле содержит какое-либо значение
Имя директивы Статус	равно	выбор значения поля из списка
	не равно	
Дата фиксации Дата начала	равно	точное значение поля
	не равно	любое значение поля, кроме указанного
	меньше	значение поля меньше указанного
	больше	значение поля больше указанного
	между	значение поля лежит в указанном интервале
	пусто	поле не содержит значения
	не пусто	поле содержит какое-либо значение

10.2.3 Карточка инцидента

Для просмотра полной информации об инциденте щелкните по нему левой кнопкой мыши в таблице инцидентов. Откроется карточка инцидента, представленная на Рисунок 120.

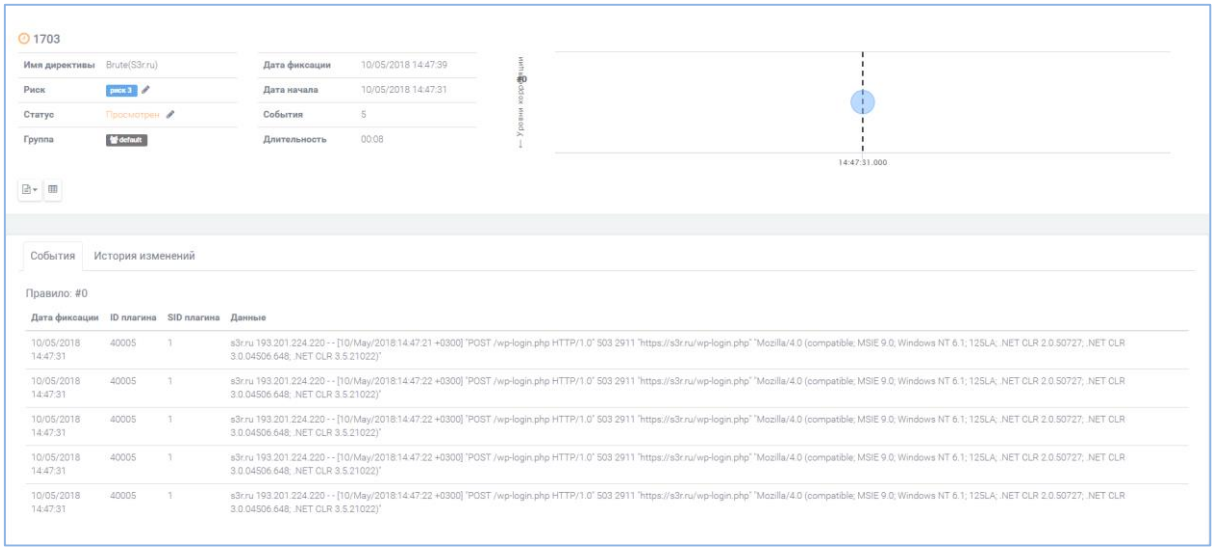


Рисунок 120. Пример карточки инцидента

Карточка инцидента содержит следующие элементы:

- сводную информацию по инциденту;
- список событий инцидента;
- диаграмму распределения во времени событий, составивших инцидент;

- историю изменений статуса, риска и группы реагирования на инцидент, а также комментарии участников группы реагирования.

10.2.3.1 Просмотр событий, составляющих инцидент

События расположены на вкладке **Количество событий**. Они сгруппированы по правилам директивы, в результате работы которой был сформирован инцидент. Все события в блоке с названием **Правило: <*Название правила директивы*>** удовлетворяют критериям указанного правила. Подробная информация о событии доступна в карточке события. Для перехода к карточке события щелкните по нему левой кнопкой мыши.

10.2.3.2 Диаграмма событий инцидента

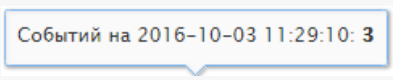
Диаграмма событий инцидента позволяет отследить распределение во времени событий, сформировавших инцидент. Левая граница временного отрезка соответствует дате поступления события, удовлетворяющего правилу верхнего (нулевого) уровня, правая граница соответствует дате поступления последнего события, необходимого для формирования инцидента. Дата поступления события верхнего (нулевого) уровня и дата поступления первого события из правила следующего уровня на временной оси выделены вертикальными пунктирными линиями. Радиус круга на графике пропорционален количеству событий, поступивших в указанный период.

10.2.3.2.1 Информационные сообщения

10.2.3.2.1.1 Количество событий

При наведении курсора мыши на круг, соответствующий интересующему периоду времени, на диаграмме событий инцидента отображается всплывающее информационное сообщение. Сообщение содержит количество зафиксированных в ПК «Комрад» в этот период времени событий, удовлетворяющих одному или нескольким правилам директивы, работа которой привела к формированию инцидента.

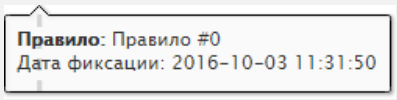
Пример информационного сообщения:



10.2.3.2.1.2 Сведения о первом событии правила

При наведении курсора мыши на вертикальную пунктирную линию на диаграмме событий инцидента отображается всплывающее информационное сообщение. Сообщение содержит информацию о названии правила и дате поступления первого события, удовлетворяющего критерию правила.

Пример информационного сообщения:



10.2.3.2.2 Работа с диаграммой событий

10.2.3.2.2.1 Уточнение запроса

Предусмотрена возможность уточнения временных интервалов для отображения событий на диаграмме событий инцидента. Для уточнения запроса выполните следующие действия:

1. Выберите дату и время начала и окончания интересующего периода времени.
2. Нажмите и удерживайте левую кнопку мыши на области диаграммы, соответствующей дате начала интересующего периода.
3. Не отпуская левую кнопку мыши, переместите курсор в область, соответствующую дате окончания интересующего периода.
4. Отпустите кнопку мыши.

В результате будет построена диаграмма распределения событий инцидента в уточненный период времени. В выборке событий будут только те события, которые соответствуют уточненному интервалу.

10.2.3.2.2.2 Отмена уточнения

Для возвращения к первоначальной (неуточненной) диаграмме событий нажмите кнопку **Сбросить** в правой верхней части диаграммы.

10.2.3.3 История изменений

Все изменения в атрибутах инцидента, а также комментарии участников группы реагирования на инциденты информационной безопасности доступны на вкладке **История изменений** (Рисунок 121).

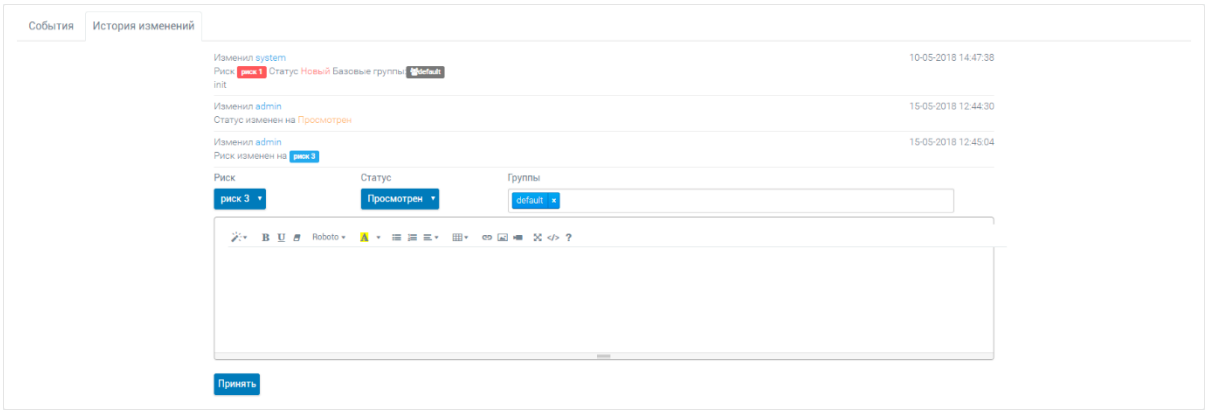


Рисунок 121. История изменений

10.2.4 Работа с инцидентами

Изменение атрибутов инцидента производится на вкладке **История изменений** (Рисунок 121). На данной вкладке предусмотрена также возможность внесения текстовых комментариев. Для изменения атрибутов инцидента выполните следующие действия:

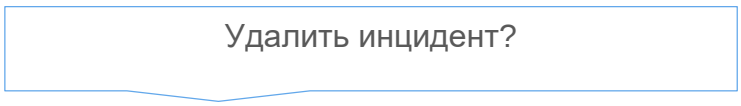
1. Перейдите на вкладку **История изменений**.
2. Задайте необходимое значение риска в выпадающем меню **Риск**.
3. Задайте статус в выпадающем меню **Статус**.
4. Определите список участников группы реагирования на инцидент в блоке **Группы**.
5. Если необходимо оставить примечание, внесите текстовый комментарий.
6. Нажмите кнопку **Принять**.

Все внесенные изменения отобразятся в карточке инцидента.

10.2.5 Удаление инцидента

Для удаления инцидента выполните следующие действия:

1. Выберите инцидент, который необходимо удалить.
2. Нажмите кнопку **Удалить** в строке выбранного инцидента.
3. В открывшемся диалоговом окне в ответ на вопрос



нажмите кнопку **ОК** для подтверждения и кнопку **Отмена** для отмены удаления.

10.2.6 Отчет по инцидентам

10.2.6.1 Сводный отчет по всем инцидентам

Для экспорта отчета по инцидентам выполните следующие действия:

1. Осуществите выборку необходимых инцидентов (см. раздел Поиск по инцидентам).
2. Нажмите кнопку:
   -  для экспорта сведений об инцидентах из выборки в формате CSV;

-  для экспорта сведений об инцидентах из выборки в формате PDF.

Отчет об инцидентах в формате PDF включает:

- титульный лист с указанием даты и времени генерации отчета;
- запрос, по которому была осуществлена выборка инцидентов;
- диаграмму «Типы инцидентов», отражающую распределение инцидентов выборки по директивам корреляции;
- диаграмму «Статусы инцидентов», отражающую состояния инцидентов выборки (новые, просмотренные, закрытые);
- диаграмму «Дата фиксации инцидентов», отражающую распределение инцидентов выборки во времени.

10.2.6.2 Отчет по отдельному инциденту

Для экспорта отчета по отдельному инциденту выполните следующие действия:

1. Перейдите в карточку инцидента.
2. Для экспорта отчета в формате CSV нажмите кнопку  .
3. Для экспорта отчета в формате PDF выберите в выпадающем меню  :

   3.1. Пункт **История изменений**, если историю изменений атрибутов инцидента и комментарии необходимо включить в отчет.

   3.2. Пункт **Последовательность событий**, если события, составляющие инцидент, необходимо включить в отчет, и укажите необходимые поля события.

   3.3. Пункт **График** для включения в отчет диаграммы событий инцидента.
4. Нажмите кнопку **Создать** для экспорта отчета на свой ПК.

11Аналитика

В данной главе содержатся сведения о работе с пунктом меню **Аналитика**, который включает следующие разделы:

- **Визуализатор событий** представляет собой средство для визуального моделирования любого множества событий и позволяет эффективно выявлять взаимосвязи между событиями и расследовать инциденты ИБ;
- **База фактов** позволяет управлять запросами к базе фактов и строить диаграммы по выборкам данных, соответствующих запросам.

11.1 Визуализатор событий

Рабочее пространство визуализатора событий может быть разделено на следующие рабочие области:

- временной отрезок;
- граф визуализации;
- фильтр визуализируемых событий.

11.1.1 Граф визуализации

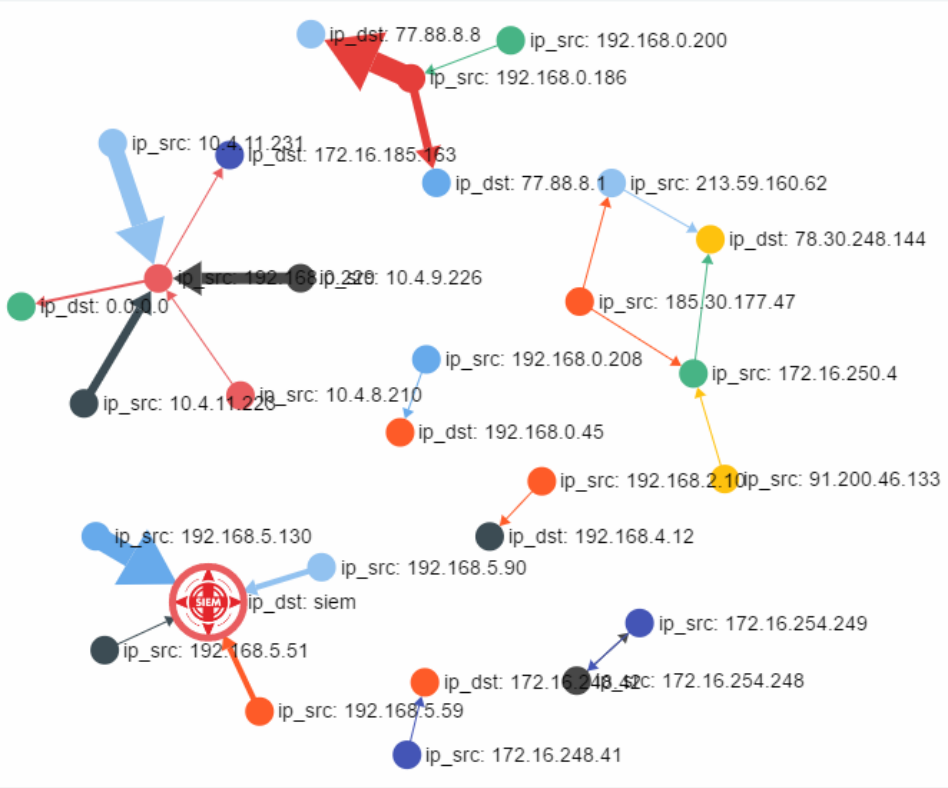


Рисунок 122. Пример графа визуализации

Граф визуализации представляет собой множество помеченных вершин и соединяющих их дуг. Вершины могут быть двух типов:

- источник: вершина, из которой исходит дуга;
- назначение: вершина, в которую входит дуга.

Метка вершины с типом «источник» («назначение») принимает значение поля события, заданного в настройке **Поле источника** (**Поле назначения**). Любая дуга в графе имеет направление от вершины типа «источник» к вершине типа «назначение». Толщина дуги пропорциональна количеству событий с соответствующими вершинам значениями полей.

11.1.2 Фильтр визуализируемых событий

Данный фильтр позволяет настроить отображение событий безопасности, которые необходимо визуализировать. Для настройки фильтра выполните следующие действия:

1. Создайте запрос на выборку событий. Запрос создается средствами Конструктора запросов. Подробнее о работе с конструктором запросов см. в разделе Поиск по событиям.
2. Укажите поле источника. Данное поле будет использовано для подписи вершин графа типа «источник».
3. Укажите поле назначения. Данное поле будет использовано для подписи вершин графа типа «назначение».
4. Укажите, сколько событий нужно задействовать. Указанное количество событий выборки будет использовано при построении графа визуализации.
5. Нажмите кнопку **Обновить**.

11.1.3 Временной отрезок

Средство визуального задания границ периода времени (Рисунок 123). События, зафиксированные в указанный период времени, будут использованы при построении графа визуализации. Начало и конец временной шкалы соответствуют дате первого и последнего событий в выборке, заданной на этапе фильтрации визуализируемых событий. Для сужения временных границ нажмите и удерживайте точку на временной шкале, соответствующую дате начала (дате окончания) шкалы. Не отпуская левую кнопку мыши, переместите курсор в область, соответствующую дате начала (дате окончания) интересующего периода. Отпустите кнопку мыши.

Рисунок 123. Временной отрезок

Граф будет изменяться «на лету» в процессе всего перемещения курсора мыши.

11.2 База фактов

11.2.1 Просмотр списка запросов

Список запросов к базе фактов отображается в левой части страницы (Рисунок 124).

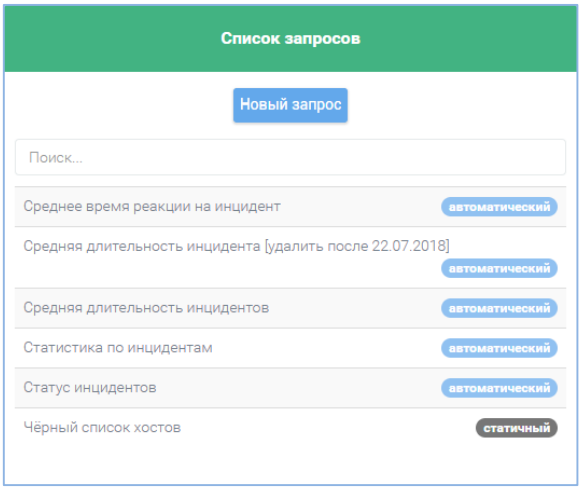


Рисунок 124. Список запросов

Название каждого запроса сопровождается меткой «статичный» или «автоматический», значение меток приведено ниже.

Тип запроса	**Описание**
Автоматический	данные формируются на основе SQL-запроса к базе данных ПК «Комрад»
Статичный	данные формируются на основе загруженного администратором файла в формате CSV

Для поиска по списку запросов введите его имя или часть имени в строку поиска, расположенную в верхней части списка.

11.2.2 Рабочая область запроса

Для просмотра подробной информации по запросу щелкните по нему левой кнопкой мыши в списке запросов, откроется карточка запроса (Рисунок 125).

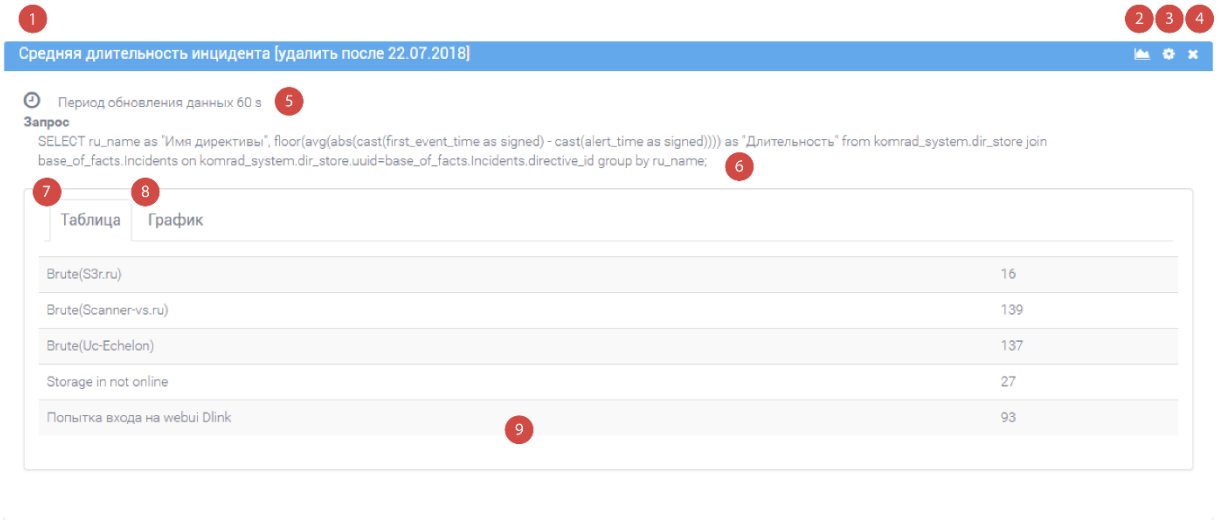


Рисунок 125. Рабочая область запроса

Рабочая область запроса содержит следующие элементы:

1) название запроса;
2) кнопка выбора типа графика;
3) кнопка вызова окна редактирования запроса;
4) кнопка удаления запроса;
5) период обновления данных (для автоматического запроса);
6) SQL-запрос (для автоматического запроса);
7) вкладка с данными;
8) вкладка с графиком;
9) результат выполнения запроса (выборка данных).

Чтобы посмотреть график запроса, перейдите на вкладку «График» (Рисунок 126).

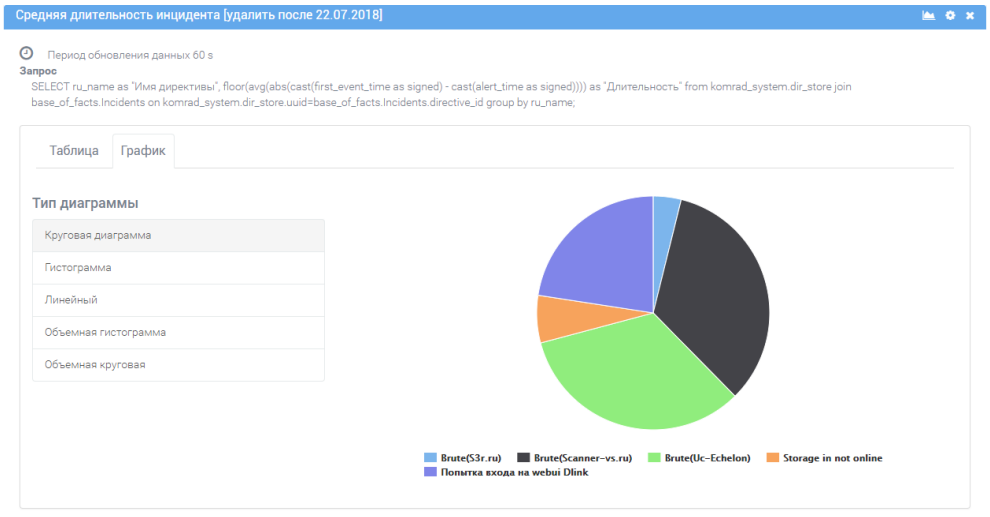


Рисунок 126. График запроса

Выберите тип графика для отображения из списка или при нажатии на кнопку  .

11.2.3 Создание нового запроса

Для создания нового запроса к базе фактов выполните следующие действия:

1. Нажмите кнопку **Новый запрос** (Рисунок 124).
2. **Данные события**:
   а) укажите имя запроса;
   б) выберите тип запроса;
   в) для перехода к следующему шагу нажмите кнопку **Далее**, для отмены создания запроса нажмите кнопку **Отмена**.
3. **Запрос***:* Если на предыдущем шаге выбран тип запроса Автоматический, то:
   а) введите SQL-запрос на выборку данных, конец запроса сопровождается символом «;» (точка с запятой);
   б) укажите период обновления данных;
   в) при необходимости предварительного просмотра результата выполнения запроса нажмите кнопку **Выполнить** (результат выполнения запроса отобразится в поле **Результат**).
4. **Запрос***:* Если на предыдущем шаге выбран тип запроса Импорт из CSV, то нажмите кнопку **Загрузить файл** для загрузки файла в формате CSV (данные из загруженного файла отобразятся в окне).
5. Для завершения создания запроса нажмите кнопку **Создать**, для возврата к предыдущему шагу нажмите кнопку **Назад**, для отмены создания виджета нажмите кнопку **Отмена**.

11.2.4 Примеры автоматических запросов

11.2.4.1 Статистика по инцидентам информационной безопасности

Рассмотрим пример создания автоматического запроса к базе фактов для получения данных по количеству инцидентов разных типов.

1. Создайте новый запрос с именем «Статистика по инцидентам», выбрав тип запроса Автоматический.
2. В качестве SQL-запроса на выборку данных укажите следующий запрос:

```
SELECT ru_name, COUNT(*) as Count FROM base_of_facts.Incidents JOIN
komrad_system.dir_store WHERE directive_id = uuid group by
directive_id order by Count desc;
```

В результате будет получено распределение инцидентов ИБ по типам.

3. При необходимости создайте виджет (см. Создание нового виджета), указав в качестве источника данных базу фактов. В качестве запроса укажите созданный запрос «Статистика по инцидентам».

11.2.4.2 Статистика по статусам инцидентов информационной безопасности

Рассмотрим пример создания автоматического запроса к базе фактов для получения данных по количеству инцидентов с разными статусами.

1. Создайте новый запрос с именем «Статистика по статусам инцидентов», выбрав тип запроса Автоматический.
2. В качестве SQL-запроса на выборку данных укажите следующий запрос:

```
SELECT case when status=0 then "Открыто" when status=1 then
"Просмотрено" when status=2 then "Закрыто" end as status, count(*)
FROM base_of_facts.Incidents group by status;
```

В результате будет получено распределение статусов инцидентов информационной безопасности.

3. При необходимости создайте виджет (см. Создание нового виджета), указав в качестве источника данных базу фактов. В качестве запроса укажите созданный запрос «Статистика по статусам инцидентов».

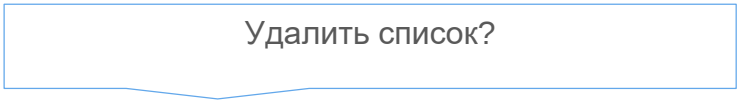
11.2.5 Редактирование запроса

Для редактирования нажмите кнопку  в правом верхнем углу запроса (Рисунок 125). Работа с интерфейсом подробно описана в разделе Создание нового запроса.

11.2.6 Удаление запроса

Для удаления запроса к базе фактов выполните следующие действия:

1. Выберите запрос, который необходимо удалить.
2. Нажмите кнопку  в правом верхнем углу запроса (Рисунок 125).
3. В открывшемся диалоговом окне в ответ на вопрос



нажмите кнопку **Удалить** для подтверждения и кнопку **Отмена** для отмены удаления.

12Мониторинг доступности

В данной главе содержатся сведения о работе с пунктом меню **Мониторинг доступности**, который включает следующие разделы:

- **Доступность** предназначен для контроля безотказного функционирования технических средств, обнаружения и локализации отказов;
- **Карта** предназначен для управления картами, отображающими доступность активов и сервисов.

12.1 Карта

Возможно создание трех типов объектов: карты, вложенной карты и автокарты

12.1.1 Управление картами

12.1.1.1 Просмотр списка карт

В разделе **Открыть > Обзор** отображаются все имеющиеся в системе карты и статус доступности их объектов (Рисунок 127). При наведении курсора мыши на пиктограмму состояния отобразится детализированная информация о доступности.

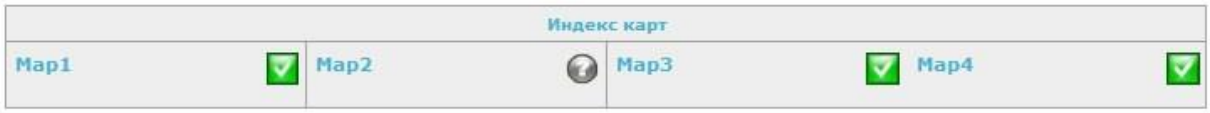


Рисунок 127. Обзор состояния карт

12.1.1.2 Создание новой карты

Для создания новой карты выполните следующие действия:

1. Выберите пункт меню **Настройки > Управление картами**.
2. В разделе **Создать карту** (Рисунок 128) введите название карты, набор значков карты (big, dot, medium, small) и фон.

Название карты необходимо вводить латинскими буквами без пробелов.

В ПК «Комрад» предустановлены фоновые изображения MapKOMRAD-civil.png и MapKOMRAD-MO.png.

3. Для завершения процедуры создания карты нажмите кнопку **Создать**, для отмены создания карты закройте окно.

Созданная карта отобразится в текущем окне.

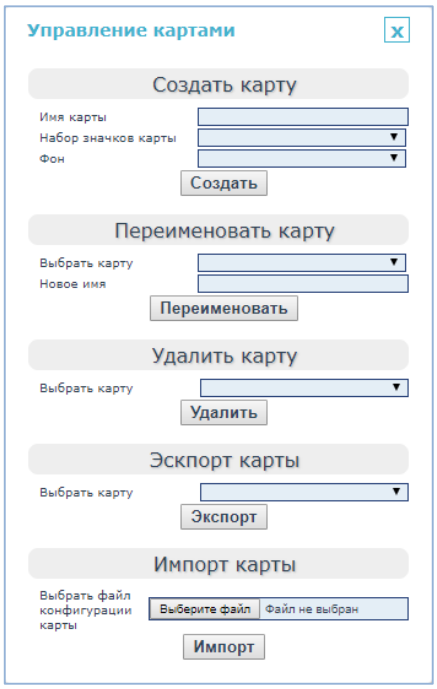


Рисунок 128. Окно «Управление картами»

12.1.1.3 Редактирование названия карты

Для изменения названия карты выполните следующие действия:

1. Выберите пункт меню **Настройки > Управление картами**.
2. В разделе **Переименовать карту** (Рисунок 128) выберите карту, которую необходимо переименовать, и укажите новое название.
3. Для завершения процедуры редактирования нажмите кнопку **Переименовать**, для отмены закройте окно.

12.1.1.4 Удаление карты

Для удаления карты выполните следующие действия:

1. Выберите пункт меню **Настройки > Управление картами**.
2. В разделе **Удалить карту** (Рисунок 128) выберите карту, которую необходимо удалить.
3. Для завершения процедуры удаления нажмите кнопку **Удалить**, для отмены закройте окно.

12.1.1.5 Экспорт карты

Для экспорта карты выполните следующие действия:

1. Выберите пункт меню **Настройки > Управление картами**.
2. В разделе **Экспорт карты** (Рисунок 128) выберите карту, которую необходимо экспортировать.

3. Для завершения процедуры экспорта нажмите кнопку **Экспорт**, для отмены закройте окно.

Карта сохранится локально с расширением *.cfg*. Открыв документ в текстовом редакторе, можно поменять конфигурацию.

12.1.1.6 Импорт карты

Для импорта карты выполните следующие действия:

1. Выберите пункт меню **Настройки > Управление картами**.
2. В разделе **Импорт карты** (Рисунок 128) выберите локально сохраненную карту в формате cfg.
3. Для завершения процедуры импорта нажмите кнопку **Импорт**, для отмены закройте окно.

Название импортируемой карты не должно содержать пробелов.

Пример карты в формате cfg

```
define global {
object_id=0
map_image=MapKOMRAD-MO.png
iconset=std_medium
}

define map {
object_id=29b26d
map_name=schm1
x=219
y=372
}

define map {
object_id=bbb992
map_name=schm1
x=119
y=527
}
```

12.1.1.7 Добавление объекта на карту

Для добавления объекта на карту выполните следующие действия:

1. Выберите карту, на которую необходимо добавить объект.
2. Выберите пункт меню **Редактировать карту > Добавить значок...** .

3. Выберите тип объекта, который необходимо добавить.
4. Поместите курсор в точку на карте, куда необходимо добавить объект.
5. В появившемся меню настройте параметры объекта.
6. Для завершения процедуры добавления объекта нажмите кнопку **Сохранить**, для отмены добавления объекта закройте окно.

12.1.1.8 Просмотр объектов на карте

При наведении курсора мыши на объект на карте появляется всплывающее меню (hover menu), которое включено по умолчанию (Рисунок 129). Данное меню отображает детализированную информацию по каждому объекту. Содержание меню может быть изменено при изменении шаблонов для меню. Также возможно отключение отображения данного меню.

Сервис (Последнее обновление состояния: 2015-02-06 13:06:25)	
Имя узла	localhost (localhost)
имя сервиса	SSH
Итоговое состояние	OK
Итоговый вывод	SSH OK - OpenSSH_6.0p1 Debian-4+deb7u2 (protocol 2.0)
Последняя проверка	2015-02-05 21:41:37
Следующая проверка	2015-02-05 21:46:37
Последнее изменения состояния	2015-02-05 18:00:42

Рисунок 129. Всплывающее меню для узла

12.1.1.9 Перемещение объектов на карте

Для перемещения объекта на карте выполните следующие действия:

1. Выберите карту, на которой необходимо изменить расположение объектов.
2. Выберите пункт меню **Редактировать карту > Прикрепить/ Переместить все объекты**; на панели меню отобразится сообщение «Включен режим редактирования».
3. Переместите объекты на карте так, как это необходимо.
4. Для выхода из режима редактирования карты повторите действия п.2.

12.1.1.10 Состояния объектов на карте

В зависимости от типа отображаемых пиктограмм на карте (std_big, std_medium, std_small, std_dot) они имеют следующие возможные статусы:

-  узел доступен;
-  узел недоступен;

-  проверка доступности узла еще не запускалась;
-  сервис доступен или имеет нормальные значения;
-  сервис недоступен или для сервиса превышено пороговое значение состояния CRITICAL (например, объем оставшегося пространства на жестком диске);
-  проверка сервиса еще не запускалась;
-  для сервиса превышено пороговое значение состояния WARNING (например, объем оставшегося пространства на жестком диске).

12.1.1.11 Работа с вложенными картами

В качестве объекта на карту можно добавить другую карту, для этого выполните следующие действия:

1. Выберите карту, на которую необходимо добавить другую карту в качестве объекта.
2. Выберите пункт меню **Редактировать карту > Добавить значок > Карта**.

Дальнейшие действия аналогичны действиям, перечисленным в пункте Добавление объекта на карту.

12.1.1.12 Работа с автокартами

На автокарте объекты размещаются автоматически, начиная с корневого узла, при этом корневым узлом выступает виртуальный узел, обозначающий ПК «Комрад».

12.1.1.12.1 Создание автокарты

Для создания автокарты выполните следующие действия:

1. Выберите пункт меню **Настройки > Управление картами**.
2. Создайте карту (см. пункт Создание новой карты).
3. Выберите пункт меню **Редактировать карту > Настройка карты**.
4. Отметьте поле **sources**.
5. В появившемся текстовом поле введите *automap* (Рисунок 130).

Рисунок 130. Создание автокарты

5. Для завершения процедуры создания автокарты нажмите кнопку **Сохранить**, для отмены создания карты закройте окно.

Созданная карта отобразится в текущем окне. Пример автокарты представлен на Рисунок 131.

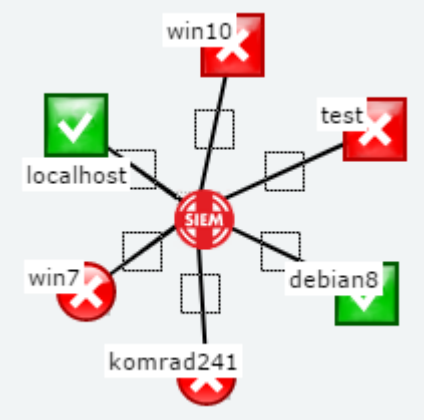


Рисунок 131. Пример автокарты

12.1.1.12.2 Экспорт автокарты в статическую карту

Для экспорта карты в статическую карту выполните следующие действия:

1. Выберите пункт меню **Действия > Экспорт в статическую карту**.
2. Задайте имя новой карты.
3. Для завершения процедуры экспорта в статическую карту нажмите кнопку **Сохранить**, для отмены экспорта карты закройте окно.

12.1.2 Управление фонами

12.1.2.1 Создание нового изображения

Для создания нового изображения выполните следующие действия:

1. Выберите пункт меню **Настройки > Управление фонами**.
2. В разделе **Создать фоновое изображение** (Рисунок 132) введите название фона, настройте цвет, используя палитру, или указав его HTML-код, укажите размеры изображения.

Название фона необходимо вводить латинскими буквами без пробелов.

3. Для завершения процедуры создания фона нажмите кнопку **Создать**, для отмены создания фона закройте окно.

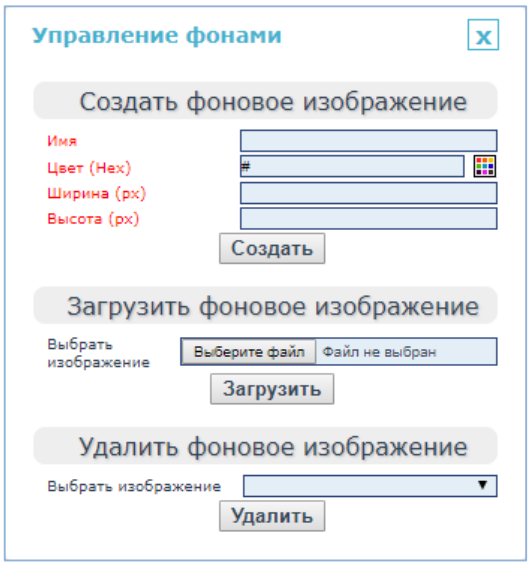


Рисунок 132. Управление фонами

12.1.2.2 Импорт фонового изображения

Для импорта фонового изображения выполните следующие действия:

1. Выберите пункт меню **Настройки > Управление фонами**.
2. В разделе **Загрузить фоновое изображение** (Рисунок 132) выберите локально сохраненное изображение.
3. Для завершения процедуры импорта нажмите кнопку **Загрузить**, для отмены закройте окно.

12.1.2.3 Удаление фонового изображения

Для удаления фонового изображения выполните следующие действия:

1. Выберите пункт меню **Настройки > Управление фонами**.
2. В разделе **Удалить фоновое изображение** (Рисунок 132) выберите фон, который необходимо удалить.
3. Для завершения процедуры удаления нажмите кнопку **Удалить**, для отмены закройте окно.

12.2 Доступность

Доступность активов и их сервисов проверяется каждые 90 секунд. Для проверки модуль мониторинга доступности использует плагины — небольшие программы, предназначенные для мониторинга доступности одного сервиса.

Плагин	Описание
check_udp	проверка, запущен ли сервис и отвечает ли на UDP-подключения

check_tcp	проверка, запущен ли сервис и отвечает ли на TCP-подключения
check_ssh	для проверки возможности подключения по протоколу SSH
check_http	для проверки возможности подключения по протоколу HTTP
check_https	для проверки возможности подключения по протоколу HTTPS
check_smtp	для проверки возможности подключения по протоколу SMTP
Ping	для проверки доступности удаленных узлов

Подключение плагинов для каждого из активов осуществляется на странице **Активы > Управление активами**.

12.2.1 Список полей таблицы доступности

Поле	**Описание**
Host	имя актива
Service	список сервисов актива, доступность которых контролируется в данный момент
Status	результат проверки доступности
Last Check	дата и время последней проверки
Duration	время, в течение которого актив или сервис находится в текущем состоянии
Attempt	число попыток обращения модуля мониторинга доступности к активу или сервису до получения состояния OK; отображается в формате *x*/4, где *x* — текущее число попыток, 4 — максимальное число попыток
Status Information	подробная информация по состоянию актива или сервиса

12.2.2 Состояния доступности сервисов

Состояние	**Описание**
OK	сервис работает в штатном режиме
CRITICAL	критическое состояние сервиса
WARNING	предупредительный сигнал о том, что у сервиса могут быть проблемы
UNKNOWN	не удалось получить статус (например, в результате внутренней ошибки)
PENDING	ожидается выполнение проверки

13Администрирование

В данной главе содержатся сведения о работе с пунктом меню **Администрирование**, который включает следующие разделы:

- **Пользователи** предназначен для управления учетными записями пользователей;
- **Компоненты** предназначен для активации/деактивации узлов, а также просмотра информации о состоянии серверов;
- **Хранилище событий** предназначен для управления модулем ротации;
- **Настройка источников** предназначен для настройки источников на передачу событий ИБ, фильтрации этих событий, а также для управления режимом работы плагинов.

13.1 Пользователи

Каждому пользователю должна быть назначена роль. Роль представляет собой именованный набор правил разграничения доступа, которые назначаются пользователю с присвоением ему роли. Объединение пользователей в группы необходимо для передачи расследования инцидента группе реагирования на инцидент информационной безопасности.

13.1.1 Вкладка Пользователи

На Рисунок 133 представлена вкладка **Пользователи**.

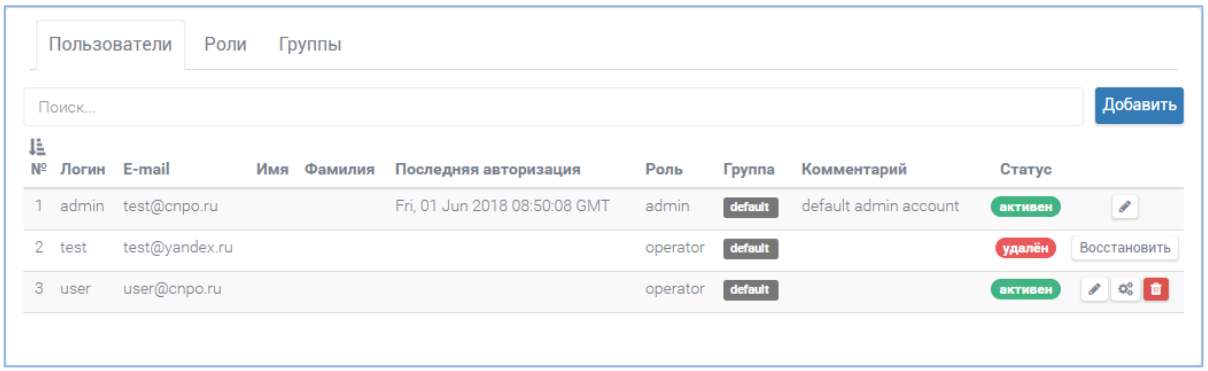


Рисунок 133. Вкладка "Пользователи"

13.1.1.1 Просмотр пользователей

13.1.1.1.1 Список полей таблицы пользователей

Поле	**Описание**
№	числовой идентификатор пользователя
Логин	идентификатор пользователя для входа в систему
E-mail	адрес электронной почты пользователя
Имя	имя пользователя
Фамилия	фамилия пользователя
Последняя авторизация	дата и время последнего входа в систему
Роль	название роли, которая назначена пользователю
Группа	группа реагирования на инцидент ИБ, в которую входит пользователь
Комментарий	комментарий администратора, является необязательным параметром

Статус	если пользователь удален, то ему присваивается статус **Удален**, в противном случае пользователь имеет статус **Активен**

13.1.1.1.2 Рабочие элементы

-  переход к редактированию атрибутов пользователя;
-  переход к редактированию прав доступа пользователей к пунктам меню;
-  удаление пользователя;
- **Восстановить** восстановление удаленного пользователя;
- **Добавить** переход к созданию нового пользователя;
- **Поиск...** строка ввода для поиска пользователя по ключевому слову/части слова.

13.1.1.2 Создание нового пользователя

На Рисунок 134 представлено диалоговое окно создания нового пользователя.

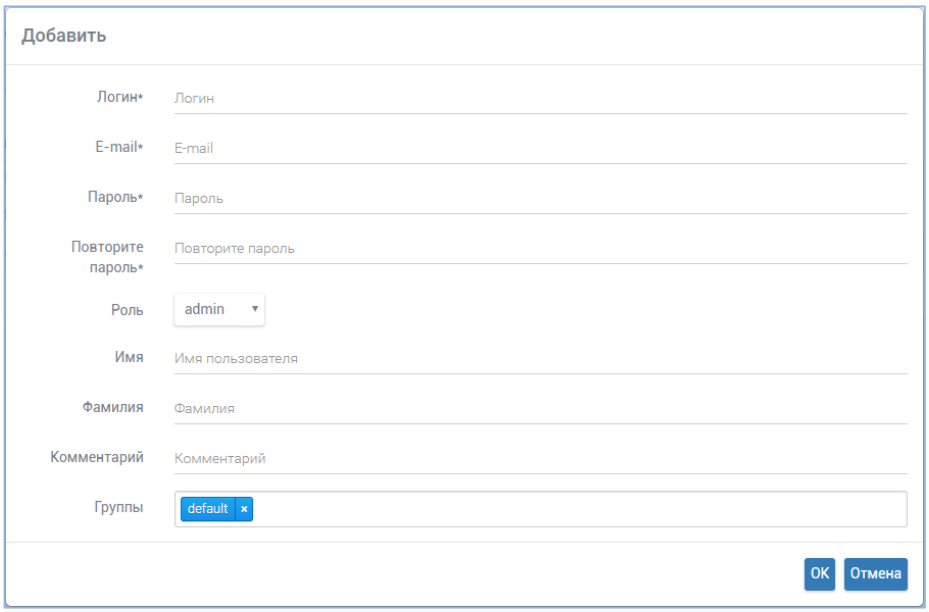


Рисунок 134. Создание нового пользователя

Для создания нового пользователя выполните следующие действия:

1. Нажмите кнопку **Добавить** в правой верхней части страницы (Рисунок 133).
2. Заполните атрибуты пользователя.
3. Для завершения создания пользователя нажмите кнопку **ОК**, для отмены создания пользователя нажмите кнопку **Отмена**.

13.1.1.3 Редактирование учетной записи пользователя

Для изменения учетной записи пользователя выполните следующие действия:

1. Выберите пользователя, учетную запись которого необходимо изменить (Рисунок 133).
2. Нажмите кнопку  .
3. Отредактируйте необходимые данные.
4. Для завершения редактирования учетной записи нажмите кнопку **ОК**, для отмены внесенных изменений нажмите кнопку **Отмена**.

13.1.1.4 Редактирование прав доступа пользователя к пунктам меню

Для изменения прав доступа пользователя к пунктам меню выполните следующие действия:

1. Выберите пользователя, права доступа которого необходимо изменить (Рисунок 133).
2. Нажмите кнопку  .
3. Задайте необходимые права доступа к пунктам меню.

Категория	**Описание**
Нет доступа	пользователь не имеет доступа к пункту меню
Чтение	пользователь имеет доступ к пункту меню и может просматривать соответствующую страницу
Запись	пользователь может вносить изменения на странице (создавать/ редактировать/ удалять/ изменять статус и т.п.)

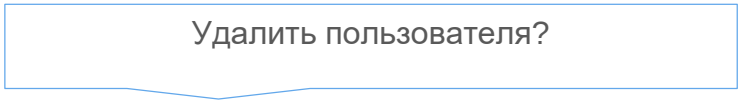
4. Для завершения редактирования прав доступа нажмите кнопку **ОК**, для отмены внесенных изменений нажмите кнопку **Отмена**.

Индивидуальные настройки прав доступа пользователя перекрывают настройки прав, задаваемые присвоенной ему ролью.

13.1.1.5 Удаление пользователя

Для удаления пользователя выполните следующие действия:

1. Выберите пользователя, учетную запись которого необходимо удалить (Рисунок 133).
2. Нажмите кнопку  в строке выбранного пользователя.
3. В открывшемся диалоговом окне в ответ на вопрос



нажмите кнопку **ОК** для подтверждения или кнопку **Отмена** для отмены удаления.

13.1.1.6 Восстановление пользователя

Для восстановления ранее удаленного пользователя нажмите кнопку **Восстановить** напротив его учетной записи (Рисунок 133). После завершения процедуры восстановления статус пользователя будет изменен на **Активен**.

13.1.2 Вкладка Роли

13.1.2.1 Просмотр ролей

На Рисунок 135 представлена вкладка **Роль**.

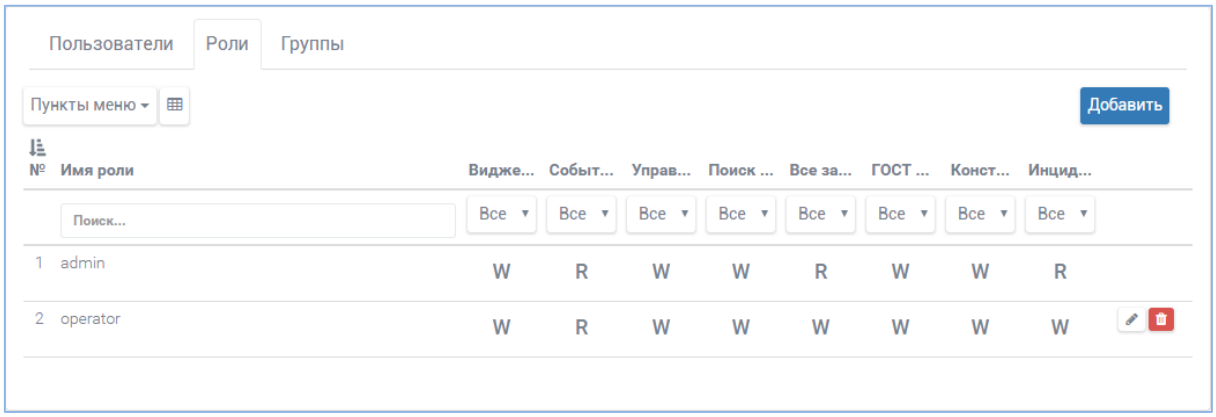


Рисунок 135. Вкладка "Роль"

По строкам таблицы на вкладке **Роли** перечислены наименования ролей, по столбцам — пункты меню. На пересечении строки и столбца отображено условное обозначение категории прав доступа.

Категория	**Условное обозначение**
Нет доступа	N/A
Чтение	R
Запись	W

Пункты меню (столбцы) для отображения можно варьировать в выпадающем списке **Пункты меню**.

13.1.2.1.1 Фильтрация ролей

Роли можно отфильтровать по категориям прав доступа к пунктам меню. Для этого в таблице ролей выберите столбец, соответствующий интересующему пункту меню, и укажите значение фильтра.

Фильтр	Описание
All	отображать все роли
N/A	отображать роли с категорией «Нет доступа» для данного пункта меню
R	отображать роли с категорией «Чтение» для данного пункта меню
RW	отображать роли с категорией «Запись» или «Чтение» для данного пункта меню
W	отображать роли с категорией «Запись» для данного пункта меню

13.1.2.1.2 Рабочие элементы

-  переход к редактированию категорий прав доступа;
-  удаление роли;
-  экспорт списка ролей в формате CSV;
- **Пункты меню** выпадающий список пунктов меню, позволяющий отобразить/скрыть настройки доступа для пунктов меню;
- **Добавить** переход к созданию новой роли;
- **Поиск...** строка ввода для поиска роли по ключевому слову/части слова.

13.1.2.2 Создание новой роли

Для создания новой роли выполните следующие действия:

1. Нажмите кнопку **Добавить** в правой верхней части страницы (Рисунок 135).
2. Введите название новой роли.
3. Назначьте категории прав доступа к пунктам меню.
4. Для завершения создания роли нажмите кнопку **ОК**, для отмены создания роли нажмите кнопку **Отмена**.

13.1.2.3 Редактирование роли

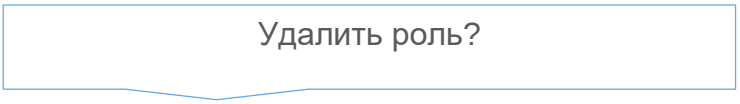
Для редактирования роли выполните следующие действия:

1. Выберите роль, которую необходимо изменить (Рисунок 135).
2. Нажмите кнопку  .
3. Отредактируйте необходимые данные.
4. Для завершения редактирования роли нажмите кнопку **ОК**, для отмены внесенных изменений нажмите кнопку **Отмена**.

13.1.2.4 Удаление роли

Для удаления роли выполните следующие действия:

1. Выберите роль, которую необходимо удалить (Рисунок 135).
2. Нажмите кнопку  в строке выбранной роли.
3. В открывшемся диалоговом окне в ответ на вопрос



нажмите кнопку **ОК** для подтверждения и кнопку **Отмена** для отмены удаления.

13.1.3 Вкладка Группы

13.1.3.1 Просмотр групп

13.1.3.1.1 Список полей таблицы групп

На Рисунок 136 представлена вкладка Группы.

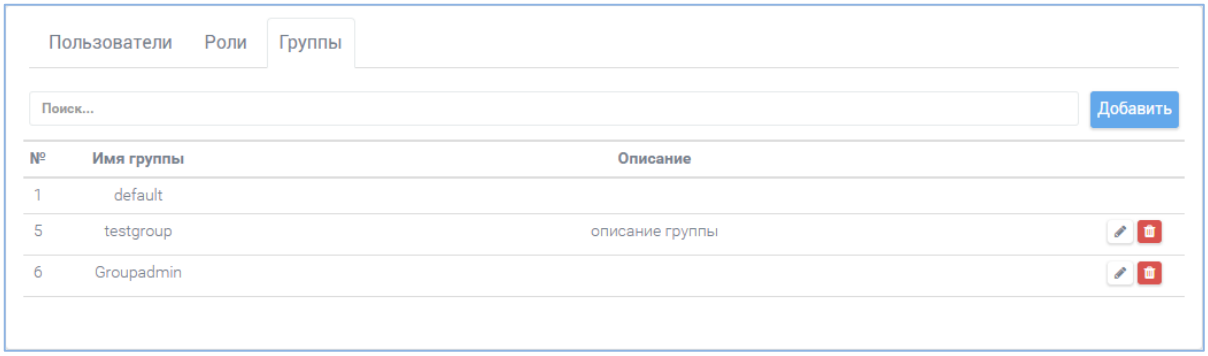


Рисунок 136. Вкладка "Группы"

Поле	Описание
№	числовой идентификатор пользователя
Имя группы	название группы
Описание	комментарий администратора, является необязательным параметром

13.1.3.1.2 Рабочие элементы

-  переход к редактированию группы;
-  удаление группы;
- **Добавить** переход к созданию новой группы;
- **Поиск...** строка ввода для поиска группы по ключевому слову/части слова.

13.1.3.2 Создание новой группы

Для создания новой группы выполните следующие действия:

1. Нажмите кнопку **Добавить** в правой верхней части страницы (Рисунок 136).
2. Введите название новой группы.
3. При необходимости добавьте описание группы.
4. Для завершения создания группы нажмите кнопку **ОК**, для отмены создания группы нажмите кнопку **Отмена**.

13.1.3.3 Редактирование группы

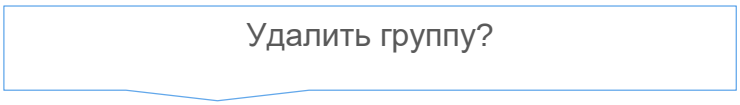
Для редактирования группы выполните следующие действия:

1. Выберите группу, которую необходимо изменить (Рисунок 136).
2. Нажмите кнопку  .
3. Отредактируйте необходимые данные.
4. Для завершения редактирования группы нажмите кнопку **ОК**, для отмены внесенных изменений нажмите кнопку **Отмена**.

13.1.3.4 Удаление группы

Для удаления группы выполните следующие действия:

1. Выберите группу, которую необходимо удалить (Рисунок 136).
2. Нажмите кнопку  в строке выбранной группы.
3. В открывшемся диалоговом окне в ответ на вопрос



нажмите кнопку **ОК** для подтверждения и кнопку **Отмена** для отмены удаления.

13.2 Компоненты

Раздел **Компоненты** предназначен для активации/деактивации узлов, установленных в системе ПК «Комрад», а также для просмотра сведений о состоянии узлов (Рисунок 137).

Рисунок 137. Пример схемы узлов в системе ПК «Комрад»

Процедура активации/деактивации узлов подробно описана в разделе Активация.

13.2.1 Просмотр состояния сервера

Для просмотра информации о состоянии узла щелкните левой кнопкой мыши по необходимому узлу на схеме (Рисунок 137). Система осуществит переход на страницу **Состояние сервера**, которая состоит из следующих вкладок:

- **Данные**, содержащая виджеты, отображающие основную информацию о состоянии данного узла;
- **Сервисы**, содержащая таблицу подключенных сервисов.

13.3 Хранилище событий

Страница **Хранилище событий** предоставляет интерфейс для управления модулем ротации (Рисунок 138). Модуль ротации базы данных событий безопасности предназначен для контроля размера дискового пространства, занимаемого событиями ИБ. Все события ИБ распределяются по каталогам: каждый каталог содержит события за период 24 часа (с 00:00:00 до 23:59:59). Каталог характеризуется состоянием, в котором он находится. От состояния зависят операции, доступные администратору для работы с событиями каталога. Управление состояниями автоматизировано и определяется правилами ротации.

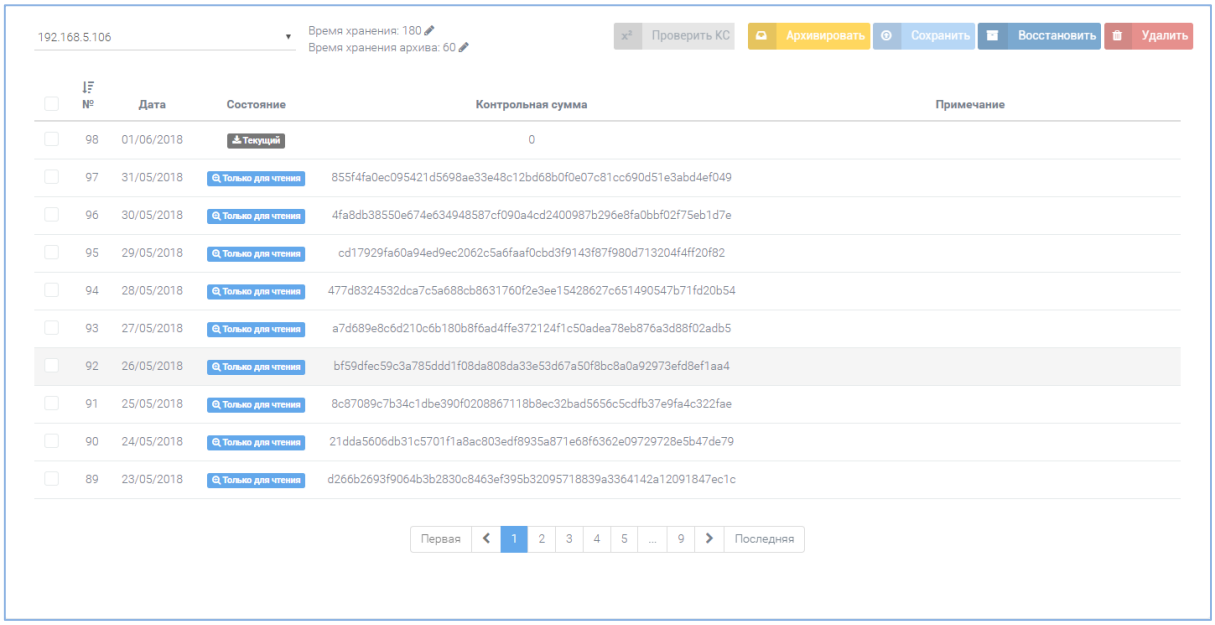


Рисунок 138. Страница "Хранилище событий"

13.3.1 Состояния каталогов

Состояние	**Описание**
Текущий	текущий каталог для записи и чтения событий
Только для чтения	каталог доступен только для чтения, время хранения определяется администратором
Архив	архив недоступен для записи и чтения, время хранения определяется администратором
Сохранен для чтения	каталог доступен только для чтения, время хранения не ограничено
Сохраненный архив	каталог недоступен для записи и чтения, время хранения не ограничено
Удален	каталог отсутствует (удален)

Состояние	Запись событий	Поиск	Удаление (администратором)	Удаление (подсистемой ротации)
Текущий	+	+	–	–
Только для чтения	–	+	–	+[1]
Архив	–	–	–	+
Сохранен для чтения	–	+	+	–
Сохраненный архив	–	–	+	–
Удален	–	–	–	–

13.3.2 Правила ротации

Схема переходов состояний каталогов под управлением модуля ротации приведена на рисунке 139. Администратор может изменять состояния каталогов. Схема управления состояниями каталогов приведена на рисунке 140.

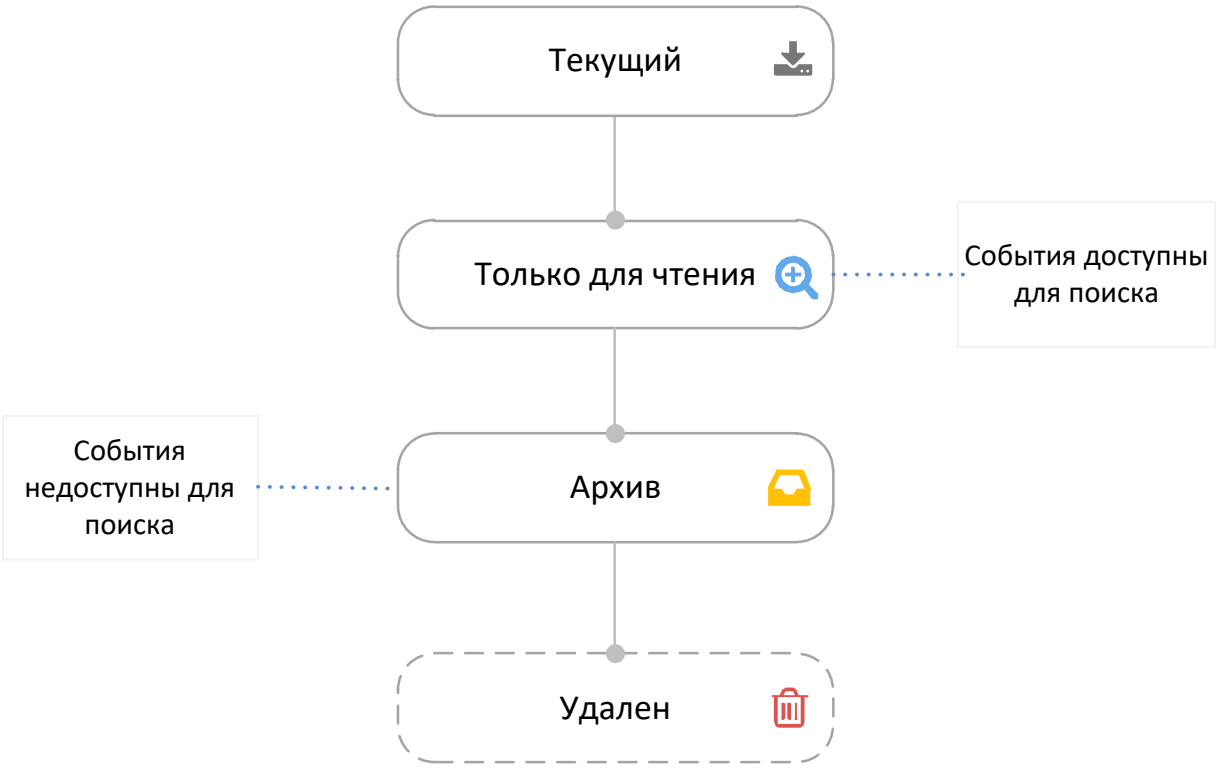


Рисунок 139. Переходы состояний каталогов, определяемые работой модуля ротации

[1] Только если время хранения архива равно 0 дней.

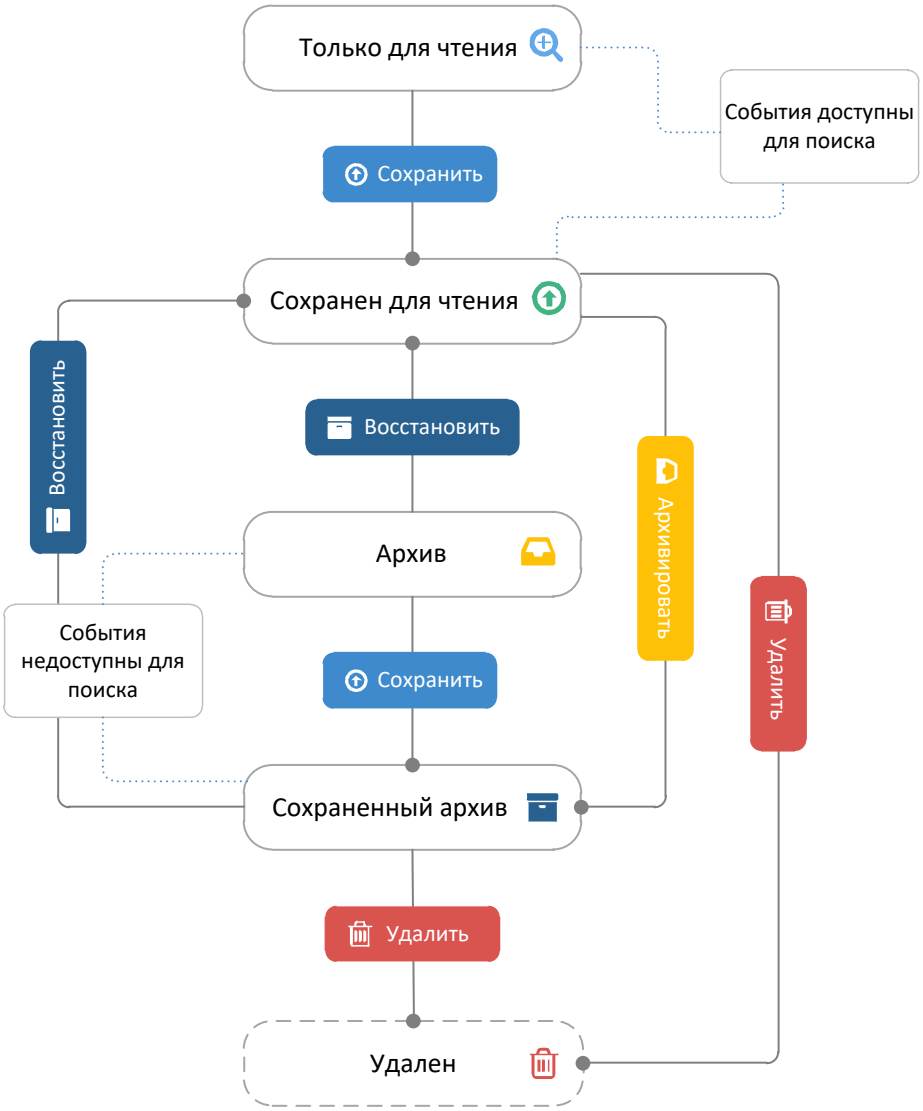


Рисунок 140. Возможные действия администратора по управлению состояниями каталогов

13.3.2.1 Состояние «Текущий»

Каталог с данными состоянием создается подсистемой ротации при первом старте и далее ежедневно в промежуток времени 04:00-04:05.

13.3.2.2 Переход каталога в состояние «Только для чтения»

Переход осуществляется из состояния «Текущий» ежедневно в промежуток времени 04:00-04:05.

13.3.2.3 Переход каталога в состояние «Архив»

Если время хранения каталога «Только для чтения» истекло, подсистема ротации в промежуток времени 04:00-04:05 создаст задачу на перевод данного каталога в состояние «Архив». Смена состояния произойдет только

после того, как архивация будет успешно завершена. Длительность архивации зависит от многих факторов и может длиться несколько часов.

13.3.2.4 Переход в состояние «Сохранен для чтения»

Переход каталога в данное состояние возможен из состояний «Только для чтения», «Архив», «Сохраненный архив», осуществляется по команде администратора.

13.3.2.5 Переход в состояние «Сохраненный архив»

Переход каталога в данное состояние возможен из состояний «Архив» и «Сохранен для чтения», осуществляется по команде администратора.

13.3.2.6 Переход в состояние «Удален»

Каталог переходит в состояние «Удален»:

- из состояния «Архив», если истекло время хранения архива;
- из состояний «Сохранен для чтения» и «Сохраненный архив» по команде администратора.

13.3.3 Информация о каталогах

Поле	**Описание**
№	порядковый номер каталога в хранилище
Дата	дата создания каталога
Состояние	текущее состояние каталога
Контрольная сумма	контрольная сумма каталога
Примечание	текстовый комментарий

13.3.4 Настройка времени хранения

Время хранения (в сутках) каталогов в состояниях «Только для чтения» и «Архив» указано в левом верхнем углу страницы в параметрах **Время хранения** и **Время хранения архива** соответственно.

Для настройки периода хранения каталога в состоянии «Только для чтения» и «Архив» выполните следующие действия:

1. Нажмите кнопку .
2. Укажите необходимое количество дней хранения.
3. Нажмите кнопку для сохранения изменений и кнопку для отмены изменений.

13.3.5 Изменение состояния каталога

Администратор может изменить состояние любого каталога, за исключением текущего. Для этого выполните следующие действия:

1. Выберите каталоги, состояние которых необходимо изменить.
2. Нажмите кнопку с состоянием, в которое необходимо перевести выбранные каталоги (**Архивировать**, **Сохранить**, **Восстановить** или **Удалить**). Подробнее о состояниях см. раздел Правила ротации.

13.3.6 Контроль целостности

Для контроля целостности каталогов фиксируется его эталонная контрольная сумма. Для верификации контрольной суммы каталогов выполните следующие действия:

1. Выберите каталоги, контрольные суммы которых необходимо сравнить с эталонными значениями.
2. Нажмите кнопку **Проверить КС**.
3. Результат проверки целостности отразится напротив эталонных контрольных сумм:
   - расчет контрольной суммы еще не завершен, необходимо подождать;
   - рассчитанная контрольная сумма совпала с эталонной, целостность каталога не нарушена;
   - рассчитанная контрольная сумма не совпала с эталонной, целостность каталога нарушена.

Контроль целостности осуществляется в соответствии с алгоритмом ГОСТ 34.11-2012 (256 бит).

13.4 Настройка источников

13.4.1 Вкладка Коллекторы

Вкладка **Коллекторы** предназначена для настройки параметров источников сбора событий ИБ.

Ниже представлен список плагинов сбора, осуществляющих сбор событий ИБ, а также соответствующие им типы сбора событий.

Плагины сбора	Тип сбора событий
Syslog (UDP)	Пассивный
Syslog (TCP)	Пассивный
NetFlow	Пассивный
FTP	Активный
SFTP	Активный
Базы данных	Активный
SNMP	Активный
SSH	Активный
WMI	Активный

Плагины сбора, осуществляющие **пассивный** сбор событий ИБ, работают в режиме сенсора. Данные плагины не требуют настройки. Для остальных необходима настройка источников сбора (см. разделы Источники, Задачи).

13.4.1.1 Выбор коллектора

В левом верхнем углу страницы предусмотрена возможность выбора коллектора для настройки параметров источников сбора событий ИБ (Рисунок 141).

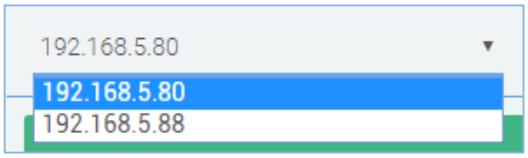


Рисунок 141. Выбор коллектора

13.4.1.2 Статусы плагинов сбора

Каждый плагин сбора находится в одном из двух возможных состояний (Рисунок 142):

- включен: плагин сбора осуществляет сбор событий ИБ в соответствии с правилами плагина;
- выключен: плагин сбора не осуществляет сбор событий ИБ.

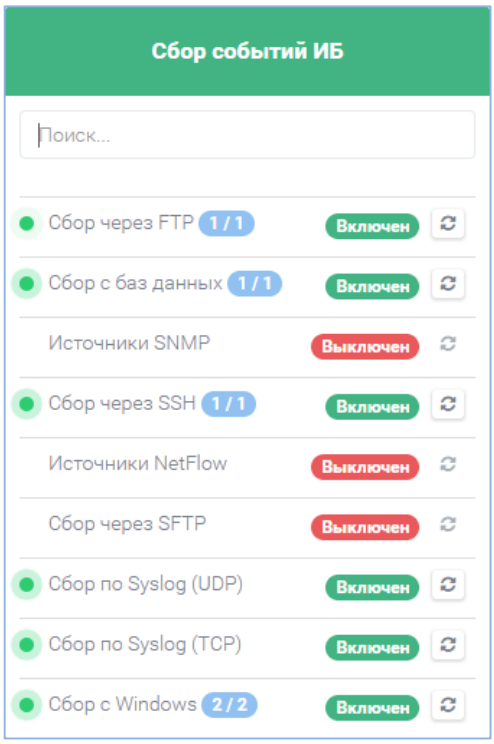


Рисунок 142. Список плагинов сбора

Индикатор, обозначающий успешно выполненный сбор событий ИБ в заданный интервал времени;
индикатор, обозначающий ошибку при сборе событий ИБ в заданный интервал времени.

13.4.1.3 Изменение статуса плагина сбора

Администратор может изменить статус любого плагина сбора. Для этого выполните следующие действия:

1. Выберите плагин, статус которого необходимо изменить (Рисунок 142).
2. Нажмите на его статус:

- Включен — для отключения плагина;
- Выключен — для включения плагина.

13.4.1.4 Перезагрузка плагина сбора

Для перезагрузки плагина сбора выберите необходимый из списка (Рисунок 142) и нажмите кнопку  в его строке.

Статус выбранного плагина должен быть в состоянии **Включен**.

13.4.1.5 Панель настроек

На панели настроек для плагинов сбора, осуществляющих **активный** сбор событий ИБ, кнопка позволяет задать интервал перезапуска (в секундах) завершившихся задач. Для плагинов сбора, осуществляющих **пассивный** сбор ИБ, данная кнопка предназначена для изменения порта.

13.4.1.6.1 Настройки маппинга

Поле Extension представляет собой набор пар типа «ключ=значение», разделенных пробелом. Соответствие ключей полям нормализации ПК «Комрад» задается в диалоговом окне **Настройки маппинга** (Рисунок 143), которое открывается при нажатии на кнопку {...} на панели настроек плагинов сбора. Полный список полей нормализации ПК «Комрад» приведен в Приложении А.

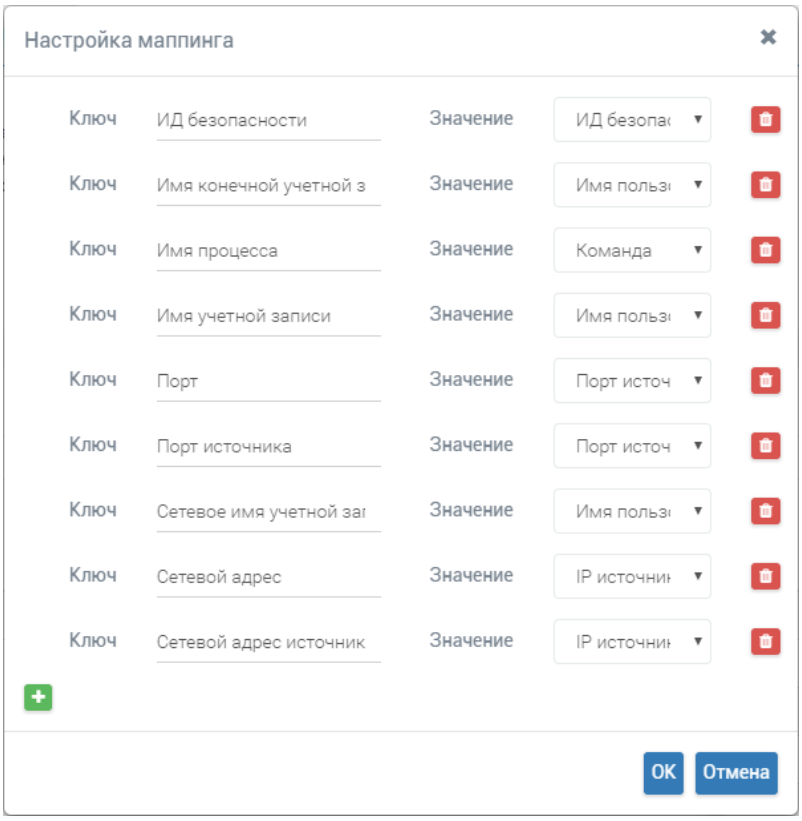


Рисунок 143. Диалоговое окно "Настройки маппинга"

В случае отсутствия полей различные вендоры вкладывают различное значение в данные нестандартизированные поля. В связи с этим в диалоговом

окне **Настройки маппинга** есть возможность задавать пару типа «ключ=значение». Для этого выполните следующие действия:

1. Нажмите кнопку {...}.
2. В открывшемся диалоговом окне нажмите .
3. В новой строке введите название ключа и выберите его значение из выпадающего списка.
4. Для сохранения нажмите кнопку **ОК**, для отмены действия нажмите кнопку **Отмена**.

Для удаления пары типа «ключ=значение» нажмите в строке выбранной пары в диалоговом окне **Настройки маппинга**.

13.4.1.6 Источники

Блок **Источники** предназначен для подключения источников для сбора событий безопасности ИБ в систему ПК «Комрад».

13.4.1.6.1 Информация об источниках

Администратору доступна следующая информация об источниках (Рисунок 144).

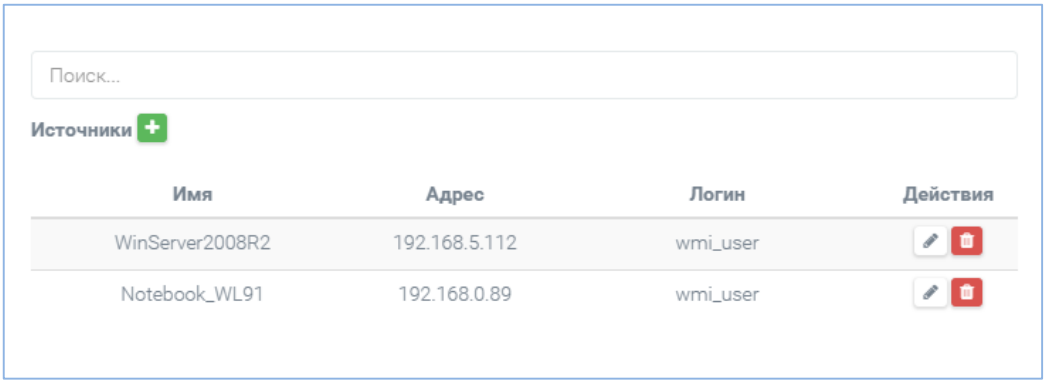


Рисунок 144. Источники событий безопасности

Поле	Описание
Имя	Название источника
Адрес	IP-адрес источника
Логин	Логин источника

Список источников можно отфильтровать по любому из полей. Для этого щелкните по заголовку соответствующего столбца.

13.4.1.6.2 Рабочие элементы

- переход к редактированию параметров источника;

-  удаление источника;
- **Поиск...** строка ввода для поиска источников.

13.4.1.6.3 Добавление источника

Для добавления источника сбора событий ИБ выполните следующие действия:

1. Нажмите  (Рисунок 144).
2. В открывшемся диалоговом окне заполните параметры источника.

В зависимости от выбранного плагина сбора параметры источника могут изменяться.

3. Для завершения добавления нажмите кнопку **ОК**, для отмены нажмите кнопку **Отмена**.

Добавленный источник отобразится в списке, представленном на Рисунок 144.

13.4.1.6.4 Редактирование источника

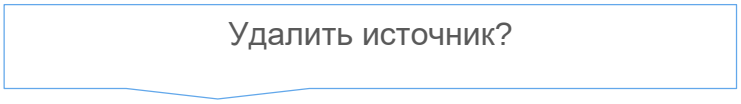
Для редактирования параметров источника выполните следующие действия:

1. Выберите источник, параметры которого необходимо изменить (Рисунок 144).
2. Нажмите кнопку  в строке выбранного источника.
3. Отредактируйте необходимые параметры.
4. Для завершения редактирования параметров источника нажмите кнопку **ОК**, для отмены внесенных изменений нажмите кнопку **Отмена**.

13.4.1.6.5 Удаление источника

Для удаления источника выполните следующие действия:

1. Выберите источник, который необходимо удалить (Рисунок 144).
2. Нажмите кнопку  в строке выбранного источника.
3. В открывшемся диалоговом окне в ответ на вопрос



нажмите кнопку **Удалить** для подтверждения или кнопку **Отмена** для отмены удаления.

13.4.1.7 Задачи

Блок **Задачи** позволяет создавать задачи на сбор событий ИБ с доступных источников.

13.4.1.7.1 Информация о задачах

Администратору доступна следующая информация о задачах (Рисунок 145).

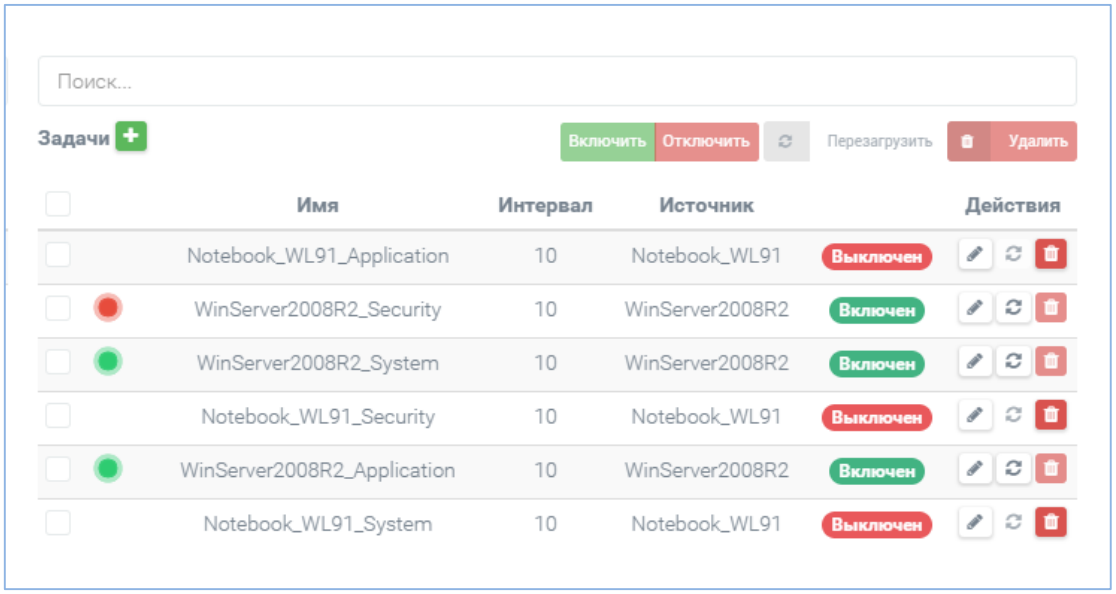


Рисунок 145. Задачи

Индикатор, обозначающий успешно выполненную задачу в заданный интервал времени;
индикатор, обозначающий ошибку при выполнении задачи в заданный интервал времени.

Поле	Описание
Имя	Название задачи
Интервал	Интервал сбора событий (сек)
Источник	Имя источника
Статус	Состояние задачи (включена/выключена)

Список задач можно отфильтровать по любому из полей. Для этого щелкните по заголовку соответствующего столбца.

13.4.1.7.2 Рабочие элементы

-  переход к редактированию задачи;
-  удаление задачи;

-  перезагрузка задачи;
- **Поиск...** строка ввода для поиск задач.

13.4.1.7.3 Создание задачи

Для создания новой задачи выполните следующие действия:

1. Нажмите кнопку  (Рисунок 145).
2. В открывшемся диалоговом окне заполните поля.
3. В поле **Источники** выберите источники из выпадающего списка, добавленные ранее (см. раздел Добавление источника).
   При необходимости есть возможность добавления всех источников, для этого нажмите кнопку **Выбрать все**, чтобы отменить действие нажмите кнопку **Сброс**.
4. Для завершения создания задачи нажмите кнопку **ОК**, для отмены создания нажмите кнопку **Отмена**.

Созданная задача отобразится в списке, представленном на Рисунок 145.

13.4.1.7.4 Редактирование задачи

Для редактирования задачи выполните следующие действия:

1. Выберите задачу, которую необходимо отредактировать (Рисунок 145).
2. Нажмите кнопку  в строке выбранной задачи.
3. Отредактируйте необходимые параметры.
4. Для завершения редактирования нажмите кнопку **ОК**, для отмены внесенных изменений нажмите кнопку **Отмена**.

13.4.1.7.5 Статусы задач

Каждая задача находится в одном из двух возможных состояний (Рисунок 145):

- включена: сбор событий ИБ происходит согласно параметрам задачи;
- выключена: сбор событий ИБ не происходит согласно параметрам задачи.

13.4.1.7.6 Изменение статуса задачи

Администратор может изменить статус любой задачи. Для этого выполните следующие действия:

1. Выберите задачи, статус которых необходимо изменить, установив флажки напротив.

Статус выбранных задач должен быть одинаковым.

2. Нажмите кнопку **Включить (Отключить)**.

Если требуется изменить статус одной задачи, достаточно щелкнуть по статусу и дождаться его обновления.

13.4.1.7.7 Перезагрузка задачи

Для перезагрузки задачи выполните следующие действия:

1. Выберите задачи, которые необходимо перезагрузить, установив флажки напротив (Рисунок 145).

Статус выбранных задач должен быть в состоянии **Включен**.

2. Нажмите кнопку **Перезагрузить**.

Если требуется перезагрузить одну задачу, достаточно щелкнуть на кнопку в строке выбранной задачи.

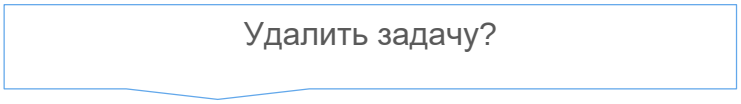
13.4.1.7.8 Удаление задачи

Для удаления задачи выполните следующие действия:

1. Выберите задачи, которые необходимо удалить, установив флажки напротив (Рисунок 145).

Статус выбранных задач должен быть в состоянии **Выключен** (см. раздел Изменение статуса задачи).

2. Нажмите кнопку **Удалить**.
3. В открывшемся диалоговом окне в ответ на вопрос



нажмите кнопку **Удалить** для подтверждения или кнопку **Отмена** для отмены удаления.

Если требуется удалить одну задачу, достаточно щелкнуть на кнопку в строке выбранной задачи.

13.4.2 Вкладка Фильтрация

Вкладка **Фильтрация** предназначена для фильтрации событий ИБ, поступающих из источников событий в систему ПК «Комрад».

13.4.2.1 Статусы фильтров

Каждый фильтр находится в одном из двух возможных состояний (Рисунок 146):

- включен: фильтрация событий ИБ происходит согласно правилам фильтра;
- выключен: фильтрация событий ИБ не происходит согласно правилам фильтра.

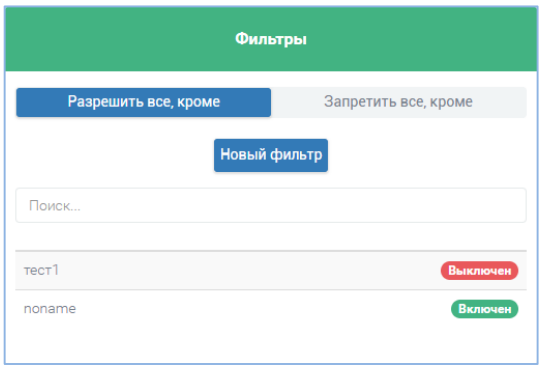


Рисунок 146. Список фильтров

13.4.2.2 Управление фильтрами

Фильтрация событий ИБ происходит по одному из двух возможных правил:

- **Разрешить все, кроме**: фильтрация событий ИБ происходит только по правилам фильтров, имеющих статус **Выключен**;
- **Запретить все, кроме**: фильтрация событий ИБ происходит только по правилам фильтров, имеющих статус **Включен**.

Для включения правила нажмите кнопку **Разрешить все, кроме (Запретить все, кроме)**(Рисунок 146).

13.4.2.3 Изменение статуса фильтра

Администратор может изменить статус любого фильтра. Для этого проделайте следующие действия:

1. Выберите фильтр, статус которого необходимо изменить.
2. Нажмите на его статус:

- Включен для отключения фильтра;
- Выключен для включения фильтра.

13.4.2.4 Создание нового фильтра

Для создания нового фильтра выполните следующие действия:

1. Нажмите кнопку **Новый фильтр** (Рисунок 146).
2. В открывшемся диалоговом окне введите название фильтра.
3. Для подтверждения создания фильтра нажмите кнопку **ОК**, для отмены действия нажмите кнопку **Отмена**; созданный фильтр отобразится в списке, представленном на Рисунок 146.
4. Нажмите левой кнопкой мыши на созданный фильтр.
5. С помощью инструментария конструктора запросов (см. раздел Поиск по событиям) создайте запрос на выборку событий.
6. Для сохранения параметров запроса нажмите кнопку **Сохранить**.

13.4.2.5 Редактирование фильтра

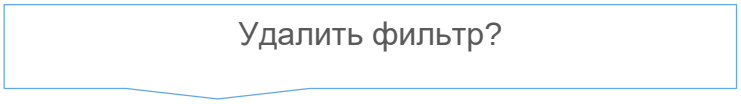
Для редактирования параметров фильтра выполните следующие действия:

1. Выберите фильтр из списка, который необходимо отредактировать, нажав на него левой кнопкой мыши (Рисунок 146).
2. Отредактируйте параметры запроса (см. раздел Поиск по событиям).
3. Для сохранения внесенных изменений нажмите кнопку **Сохранить**.

13.4.2.6 Удаление фильтра

Для удаления фильтра выполните следующие действия:

1. Выберите фильтр из списка, который необходимо удалить, нажав на него левой кнопкой мыши (Рисунок 146).
2. Нажмите кнопку **Удалить**.
3. В открывшемся диалоговом окне в ответ на вопрос



нажмите кнопку **Удалить** для подтверждения или кнопку **Отмена** для отмены удаления.

13.4.3 Вкладка Плагины

Вкладка **Плагины** предназначена для управления режимом работы плагинов. Плагин представляет собой группу правил для обработки событий. Каждый плагин включает в себя подгруппы правил.

13.4.3.1 Информация о плагинах

Администратору доступна следующая информация о плагинах.

Поле	Описание
ID плагина	идентификатор плагина
Статус	состояние плагина (включен/выключен)
Имя плагина	название плагина
Описание плагина	дополнительная информация

Список плагинов можно отфильтровать по любому из полей. Для этого щелкните по заголовку соответствующего столбца.

13.4.3.2 Статусы плагинов

Каждый плагин находится в одном из двух возможных состояний:

- включен: модуль обработки событий обрабатывает события в соответствии с инструкциями плагина;
- выключен: модуль обработки событий не осуществляет обработку событий в соответствии с правилами плагина.

Все активные (включенные) плагины располагаются в верхней части общего списка плагинов.

13.4.3.3 Изменение статуса плагина

Администратор может изменить статус любого плагина. Для этого проделайте следующие действия:

1. Выберите плагины, статус которых необходимо изменить.
2. Нажмите кнопку **Включить** (**Отключить**).

Если требуется изменить статус одного плагина, достаточно щелкнуть по статусу и дождаться его обновления.

13.4.3.4 Поиск плагинов

Полнотекстовый поиск плагина возможен по полям ID плагина, Имя плагина и Описание плагина. Для осуществления поиска введите данные в строку поиска и нажмите `Enter`.

Рисунок 147. Строка поиска плагинов

13.4.3.5 Информация о подгруппах правил плагина

Для просмотра информации о подгруппах правил плагина щелкните по его имени левой кнопкой мыши. Администратору доступна следующая информация о подгруппах правил плагина.

Поле	**Описание**
SID плагина	идентификатор подгруппы правил
Описание	информация о типах событий, которые обрабатываются данной подгруппой

14Выход из системы

Для выхода из системы необходимо нажать кнопку в левой нижней части веб-интерфейса и подтвердите действие, нажав кнопку **Да** в диалоговом окне (Рисунок 148).

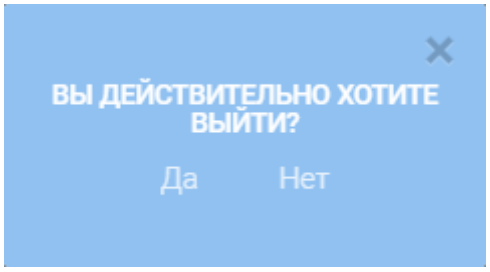


Рисунок 148. Диалоговое окно подтверждения выхода из системы

15Сообщения администратору

В данной главе содержатся сведения о сообщениях, которые администратор может получить в ходе работы с ПК «Комрад».

15.1 Ошибка входа в систему

При ошибке ввода имени пользователи или пароля в окне авторизации (Рисунок 78) администратор получает сообщение (Рисунок 149). Необходимо убедиться в корректности вводимых данных.

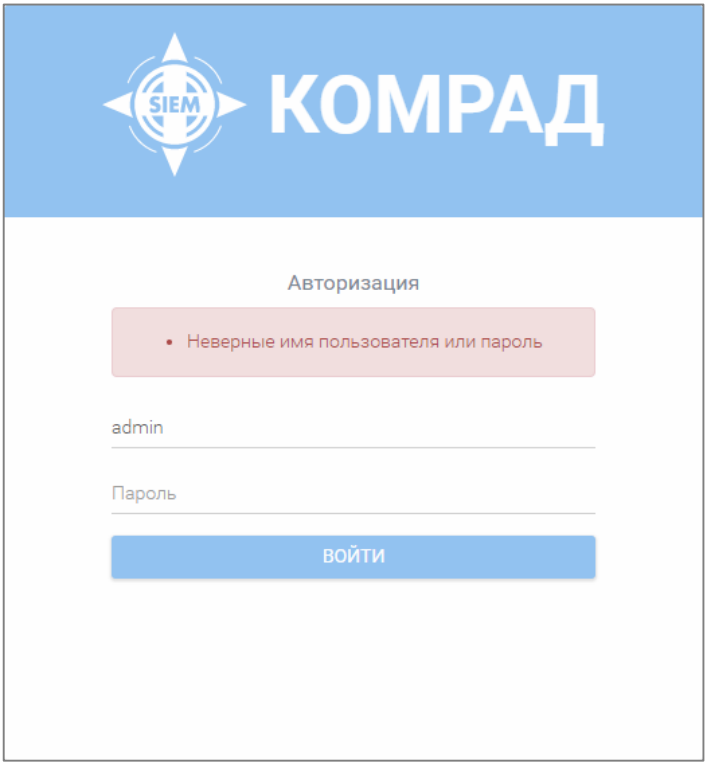


Рисунок 149. Сообщение об ошибке авторизации

15.2 Работа с виджетами

15.2.1 Заполнение обязательных полей

Если при создании/редактировании виджета поля, отмеченные символом *, остаются незаполненными, администратор получает сообщение о необходимости их заполнения (Рисунок 150).

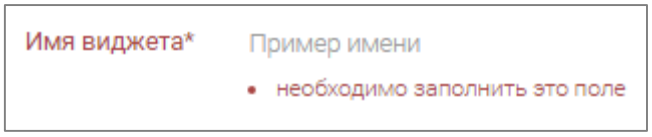


Рисунок 150. Пример сообщения о необходимости заполнения поля

15.2.1 Минимальные значения периода и длительности

Минимальные значения периода и длительности диаграммы виджета составляют 5 секунд. Если при создании/редактировании виджета администратор назначает значения периода и/или длительности менее 5 секунд, ПК «Комрад» выдает сообщение об ошибке (Рисунок 151).

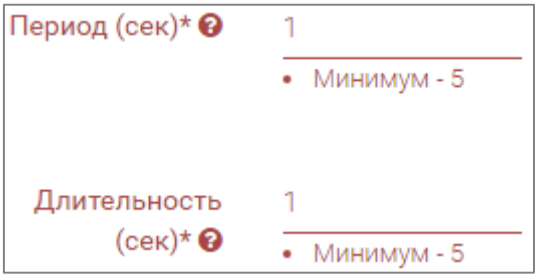


Рисунок 151. Сообщение о некорректном значении периода и длительности

15.2.2 Длительность меньше периода

Значение длительности диаграммы виджета не должно быть меньше значения периода. В противном случае администратор получит сообщение об ошибке (Рисунок 152).

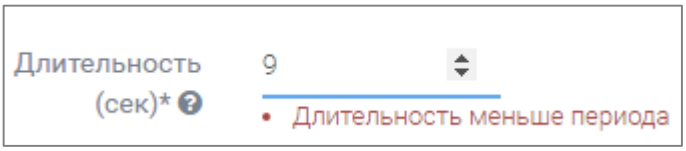


Рисунок 152. Сообщение о некорректном значении длительности

15.2.3 Удаление виджета

При попытке удалить виджет администратор получает предупреждающее сообщение (Рисунок 153). Администратор может отменить удаление виджета, нажав кнопку **Отмена**, либо подтвердить удаление, нажав кнопку **Удалить**.

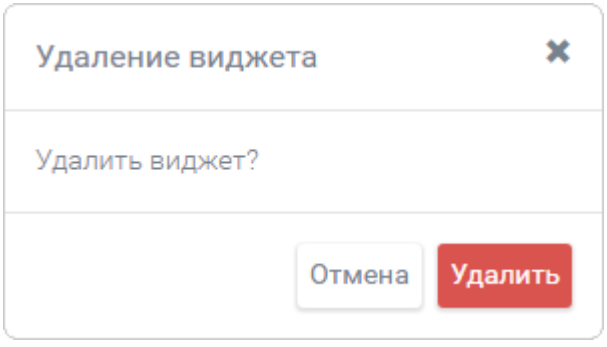


Рисунок 153.Сообщение об удалении виджета

15.2.4 Удаление панели виджетов

При попытке удалить панель виджетов администратор получает предупреждающее сообщение (Рисунок 154). Администратор может отменить удаление панели, нажав кнопку **Отмена**, либо подтвердить удаление, нажав кнопку **Удалить**.

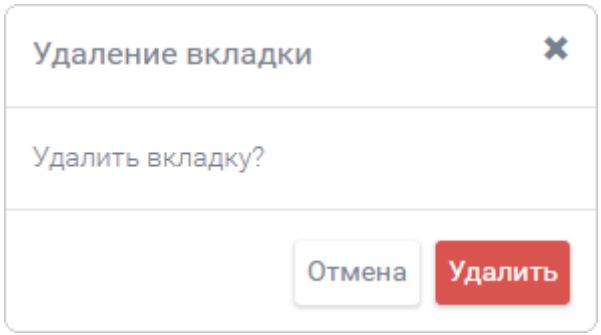


Рисунок 154.Сообщение об удалении панели

15.3 Работа с запросами к базе данных событий безопасности

15.3.1 Сохранение запроса

При сохранении запроса к базе данных событий безопасности администратор получает всплывающее уведомление (Рисунок 155). Ошибка при сохранении запроса возникает, если администратор пытается сохранить запрос с названием, которое уже зарегистрировано для ранее сохраненного запроса.

а) б)

Рисунок 155. Сообщение о сохранении запроса:
а) — успешном; б) — неуспешном

15.3.2 Ошибка при построении запроса

Если запрос к базе данных событий безопасности в конструкторе запросов содержит ошибку, администратор получает сообщение «Ошибка при построении запроса», поля конструктора запросов подсвечены красным цветом (Рисунок 156).

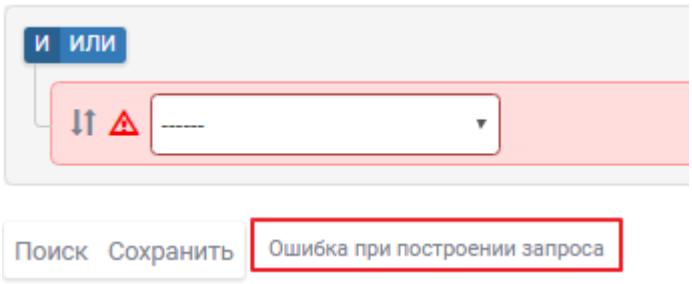


Рисунок 156. Сообщение об ошибке при построении запроса к базе данных событий безопасности

15.3.3 Удаление запроса

При попытке удалить запрос администратор получает предупреждающее сообщение (Рисунок 157). Администратор может отменить удаление запроса, нажав кнопку **Отмена**, либо подтвердить удаление, нажав кнопку **Удалить**.

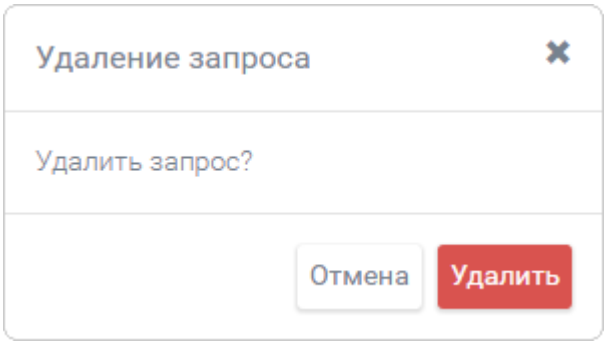


Рисунок 157. Сообщение об удалении запроса

15.3.4 Нет данных

При попытке сгруппировать события по полю, которое отсутствует во всех событиях выборки, администратор получает сообщение о том, что необходимых данных нет на сервере (Рисунок 158).

Рисунок 158. Сообщение об отсутствии данных

15.3.5 Некорректный период автообновления

При попытке задать период обновления менее 30 секунд администратор получает сообщение о некорректных параметрах обновления (Рисунок 159).

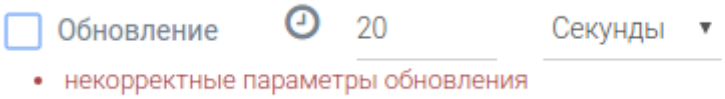


Рисунок 159. Сообщение о некорректном периоде обновления

15.4 Работа с директивами корреляции

15.4.1 Несохраненные изменения

При внесении изменений в директиву корреляции в момент перехода к просмотру другой директивы администратор получает предупреждающее сообщение о возможной потере несохраненных изменений (Рисунок 160). Администратор может вернуться к директиве, нажав кнопку **Отмена**, либо подтвердить переход к другой директиве, нажав кнопку **ОК**.

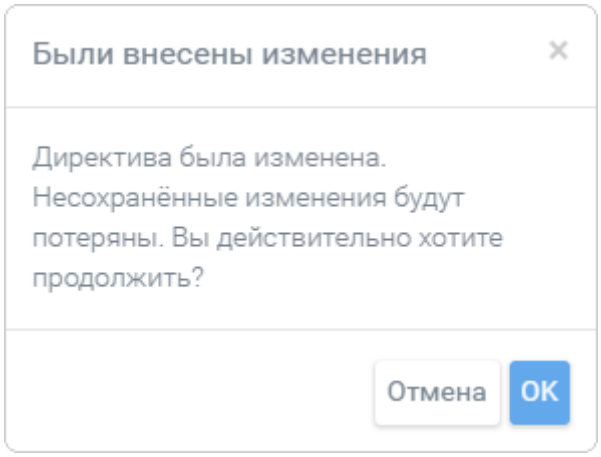


Рисунок 160. Сообщение о возможной потере несохраненных изменений

15.4.2 Удаление правила корреляции

При попытке удалить правило директивы корреляции администратор получает предупреждающее сообщение (Рисунок 161). Администратор может отменить удаление правила, нажав кнопку **Отмена**, либо подтвердить удаление, нажав кнопку **Удалить**.

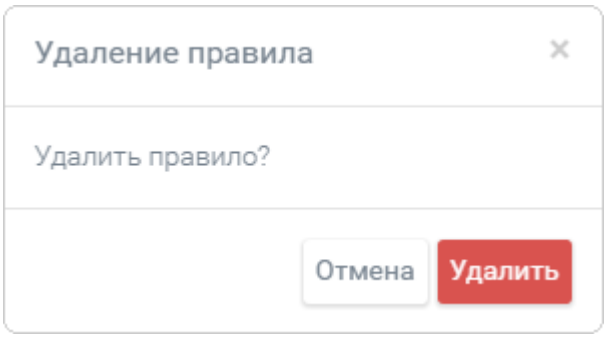


Рисунок 161. Сообщение об удалении правила директивы корреляции

15.4.3 Выбор каталога для директивы/ подкаталога

Перед созданием директивы/ подкаталога директив администратор должен выбрать один из существующих каталогов (Рисунок 162).

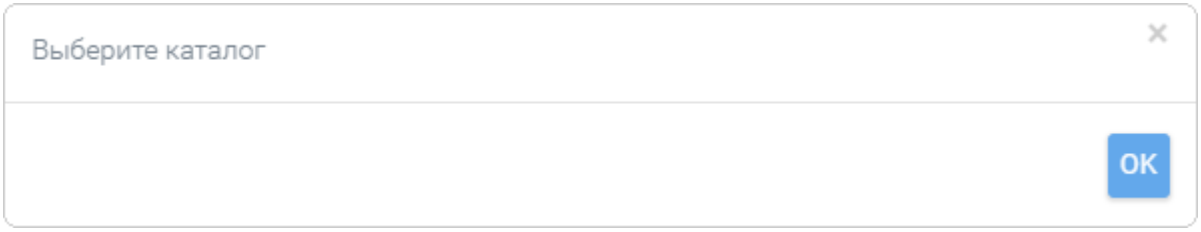


Рисунок 162. Сообщение о необходимости выбрать каталог для создания директивы/ подкаталога

15.4.4 Создание директивы корреляции с пустым именем

При попытке создания директивы корреляции с пустым именем администратор получает сообщение о том, что пустые имена не могут быть использованы (Рисунок 163).

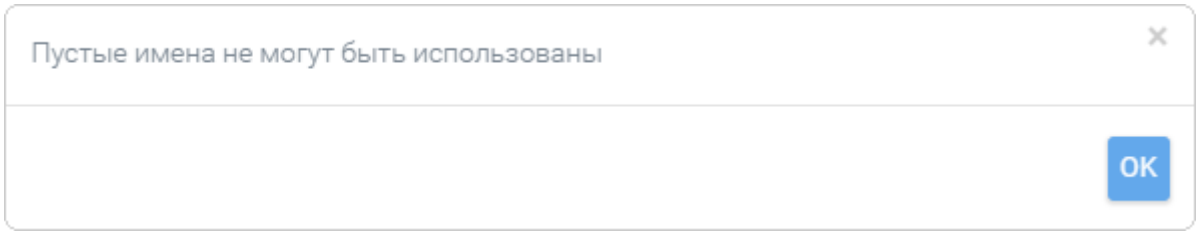


Рисунок 163. Сообщение о запрете на пустые имена

15.4.5 Удаление директивы корреляции

При попытке удалить директиву корреляции администратор получает предупреждающее сообщение (Рисунок 164). Администратор может отменить

удаление директивы, нажав кнопку **Отмена**, либо подтвердить удаление, нажав кнопку **Удалить**.

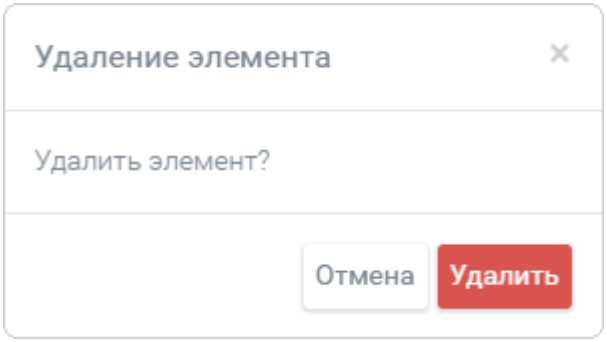


Рисунок 164. Сообщение об удалении директивы корреляции

15.4.6 Удаление каталога директив

При попытке удалить каталог с директивами корреляции администратор получает предупреждающее сообщение (Рисунок 165). Администратор может отменить удаление каталога, нажав кнопку **Отмена**, либо подтвердить удаление, нажав кнопку **Удалить**.

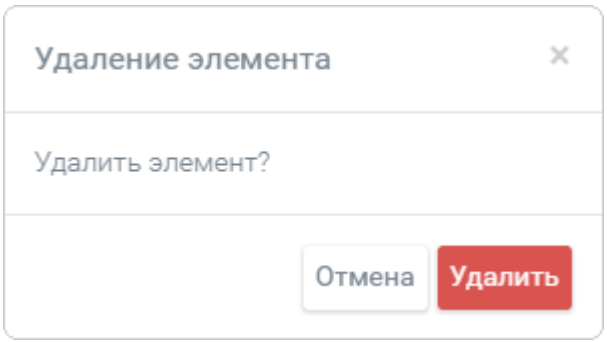


Рисунок 165. Сообщение об удалении каталога директив

15.4.7 Удаление непустого каталога директив

Удаление каталогов, в которых присутствуют директивы корреляции, невозможно. При попытке удалить непустой каталог администратор получает сообщение о том, что данное действие запрещено (Рисунок 166).

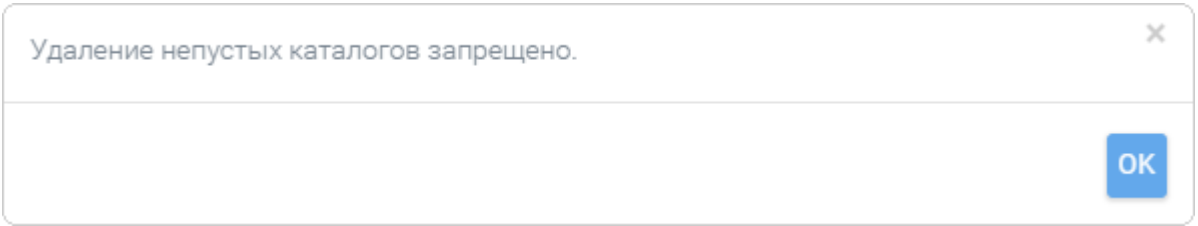


Рисунок 166. Сообщение о запрете удаления непустых каталогов

15.5 Работа с инцидентами

15.5.1 Уведомление о новом инциденте

При обнаружении нового инцидента информационной безопасности администратор получает сообщение (Рисунок 167).

Рисунок 167. Пример сообщения о новом инциденте

15.5.2 Уведомление о количестве инцидентов в статусе «Новый»

При входе в систему администратор получает сообщение об общем количестве инцидентов в статусе «Новый» (Рисунок 168).

Рисунок 168. Пример сообщения о количестве новых инцидентов

15.5.3 Удаление инцидента

При попытке удалить инцидент информационной безопасности администратор получает предупреждающее сообщение (Рисунок 169). Администратор может отменить удаление инцидента, нажав кнопку **Отмена**, либо подтвердить удаление, нажав кнопку **Удалить**.

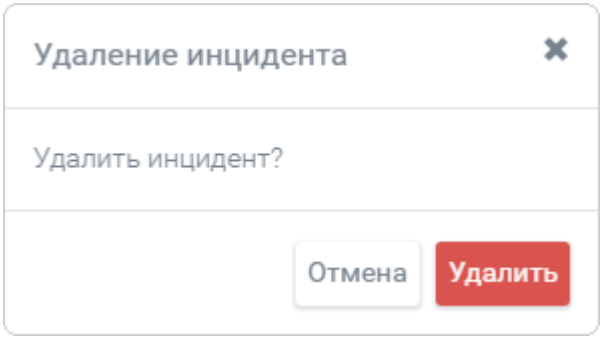


Рисунок 169. Сообщение об удалении инцидента

15.6 Работа с пользователями, ролями и группами

15.6.1 Заполнение обязательных полей

Если при создании/редактировании пользователя поля, отмеченные символом *, остаются незаполненными, администратор получает сообщение о необходимости их заполнения (Рисунок 170).

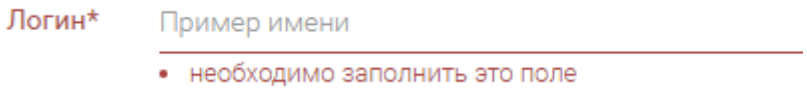


Рисунок 170. Пример сообщения о необходимости заполнения поля

15.6.2 Попытка создать пользователя с существующим логином

При попытке создать пользователя с логином, который уже занят, администратор получает предупреждающее сообщение (Рисунок 171).

Рисунок 171. Пример сообщения о невозможности использовать занятый логин

15.6.3 Удаление пользователя/роли/группы

При попытке удалить пользователя, роль или группу администратор получает предупреждающее сообщение (Рисунок 172). Администратор может отменить удаление, нажав кнопку **Отмена**, либо подтвердить удаление, нажав кнопку **Удалить**.

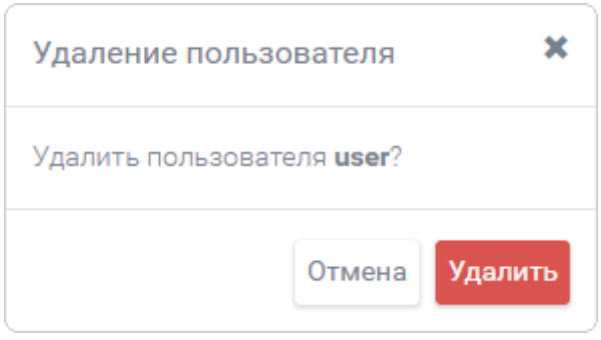


Рисунок 172. Сообщение об удалении пользователя

15.7 Работа с хранилищем событий

При попытке удалить каталог событий ИБ администратор получает предупреждающее сообщение (Рисунок 173). Администратор может отменить удаление каталога, нажав кнопку **Отмена**, либо подтвердить удаление, нажав кнопку **Удалить**.

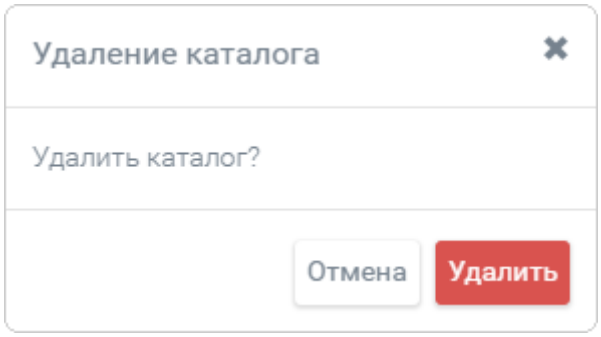


Рисунок 173. Сообщение об удалении каталога событий информационной безопасности

15.8 Работа со строкой поиска

При отсутствии данных, удовлетворяющих критериям поиска, администратор получает сообщение о том, что по его запросу ничего не найдено (Рисунок 174).

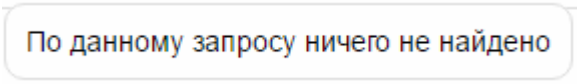


Рисунок 174. Сообщение об отсутствии информации по запросу

16Интерфейс командной строки

В данной главе содержатся сведения о работе с интерфейсом командной строки. Интерфейс командной строки предназначен для обеспечения администратора безопасности функциями управления системой и предоставления данных об ошибках и сбоях компонентов ПК «Комрад».

Интерфейс командной строки, помимо управления компонентами ПК «Комрад», позволяет просматривать журналы, которые находятся в каталоге **/var/log** в виде отдельных текстовых файлов.

Доступ осуществляется под учетной записью **admin**, пароль задается на этапе установки программы. Далее представлены команды, доступные пользователю admin из интерфейса командной строки.

16.1 Запуск оболочки командной строки

После загрузки системы появится окно (Рисунок 175), где необходимо ввести логин **admin** и пароль пользователя admin, заданный на этапе установки.

Рисунок 175. Окно входа в систему

После успешной авторизации администратор видит приветственное сообщение (Рисунок 176).

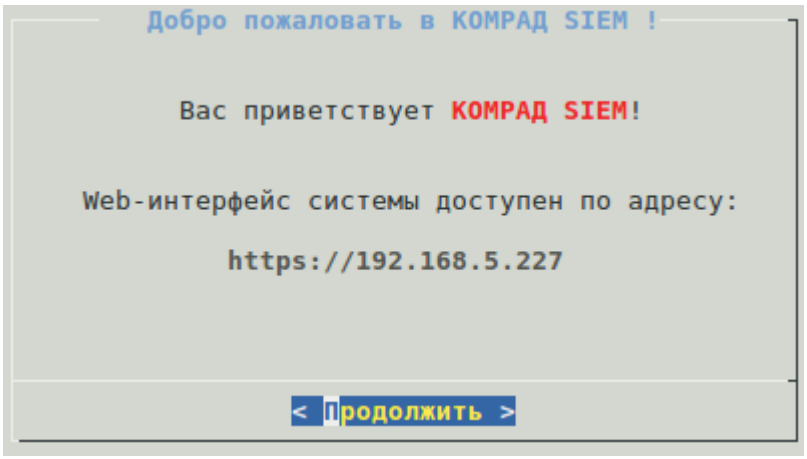


Рисунок 176. Окно входа в систему

Для продолжения работы нажмите **Продолжить**.

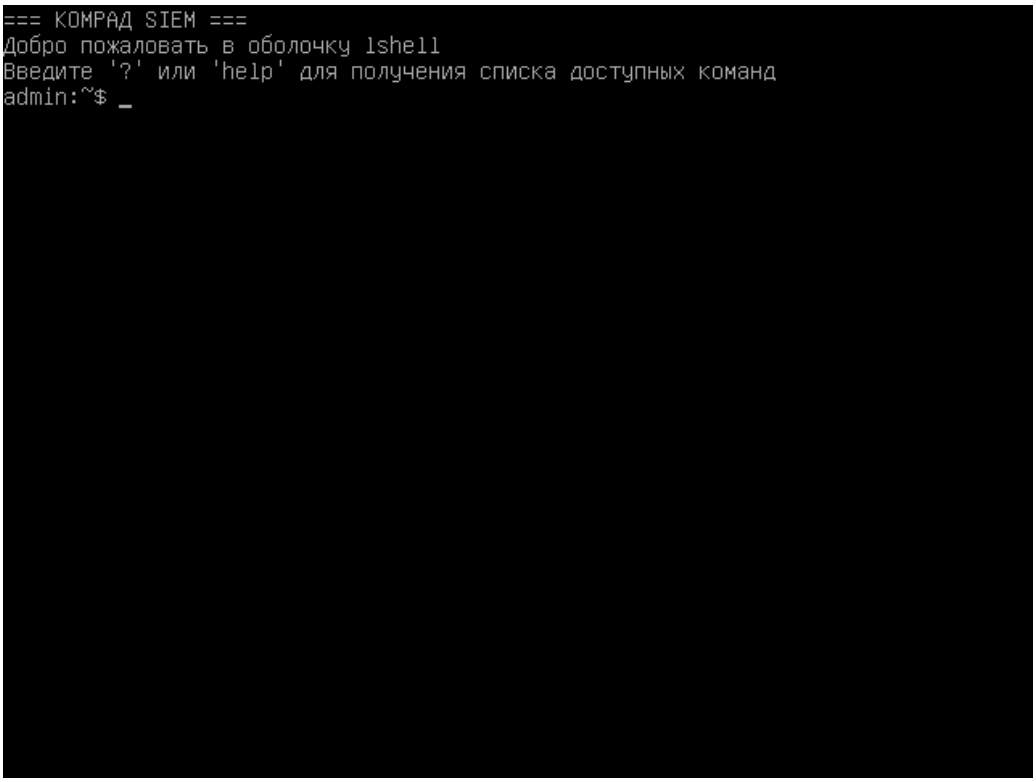


Рисунок 177. Оболочка lshell

Введите команду **jailbreak** и подтвердите выход из безопасного режима, нажав **Да** (Рисунок 178).

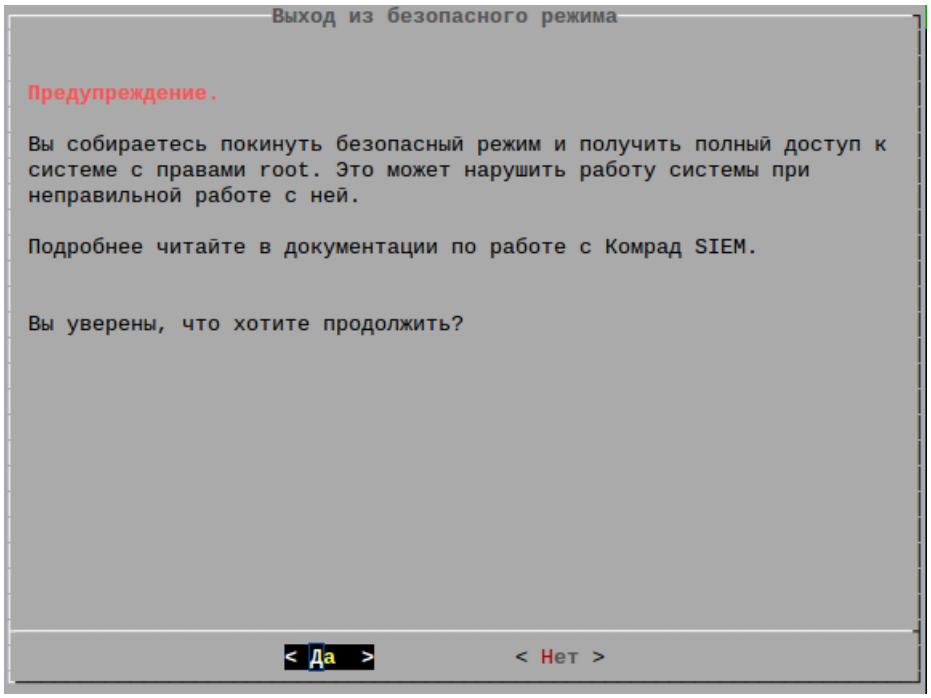


Рисунок 178. Выход из безопасного режима

Ниже приведен список команд, доступных пользователю admin.

16.2 Команды, не требующие повышения привилегий

Ниже представлены перечни команд и утилит, доступные пользователю admin без повышения привилегий.

При использовании команд и утилит, отмеченных символом «*», с повышенными привилегиями объекты файловой системы доступны с правами root.

16.2.1 Базовые операции на файловой системе

Команда/Утилита	Описание
cp	команда для копирования файлов
find*	команда для поиска файлов (например, `find ./ -name file`)
ls*, ll*	команда вывода списка файлов в каталоге, указанном в параметре, 'll' = 'ls -l'
md5sum	утилита для подсчета хэш-кода файла по алгоритму MD5
mkdir	команда для создания каталога
mv	команда перемещения объектов файловой системы
pwd	команда вывода текущего каталога

16.2.2 Обработка текста

Команда/Утилита	Описание
awk, sed	потоковые текстовые редакторы
cat*	команда для вывода содержимого файлов, указанных в качестве параметра
echo	передача текста на стандартный вывод
grep	утилита для поиска подстроки в файле/потоке
less*	постраничный просмотр текстовых файлов
nano, vim	текстовые редакторы
tail*	команда для просмотра последних строк файла

16.2.3 Операции над архивами

Утилита	Описание
bzip2, gzip	утилиты для сжатия файлов и их распаковки (*.bz2, *.gz соответственно)

tar	утилита для управления архивами (создание архивов файлов и каталогов, в том числе сжатых, и их распаковка)
zcat*, zless*	утилиты для просмотра сжатых алгоритмом gzip текстовых файлов без их распаковки

16.2.4 Настройка учетной записи

Команда	**Описание**
passwd	команда для смены пароля пользователя admin для доступа к интерфейсу командной строки
jailbreak	выход в командную оболочку bash

16.2.5 Работа с сетевыми ресурсами

Утилита	**Описание**
mysql	консольный клиент для подключения к серверу базы фактов (СУБД MySQL), не требует параметров при доступе к локальному серверу
mysqldump	утилита для копирования содержимого баз данных MySQL
scp	утилита для передачи файлов между машины по сети (используется защищенный протокол SSH)
ssh	инструмент удаленного доступа к узлам по протоколу SSH
wget	утилита для скачивания документов с удаленных веб-ресурсов

16.2.6 Диагностика системы

Команда/Утилита	**Описание**
date	команда для получения и изменения настроек времени (для изменения необходимо повышение привилегий)
df*	утилита для получения сведений об утилизации носителей (в первую очередь, дисков)
du*	утилита для вычисления занимаемого объектом файловой системы дискового пространства
free*	команда для вывода данных об утилизации виртуальной памяти системы (ОЗУ+swap)
htop*	top с улучшенной визуализацией и корректной поддержкой многоядерных систем

lsof*	утилита для анализа используемых процессами файлов и устройств
ps*	утилита выводит список процессов, соответствующих параметрам
top*	программа для вывода информации о нагрузке на вычислительные ресурсы со стороны тех или иных процессов
tree	утилита для визуализации структуры каталога
uname	команда для вывода информации об узле: имя узла, версия ядра, версия базового дистрибутива
who	команда для вывода информации о запущенных оболочках

16.2.7 Диагностика сетевых подключений

Команда/Утилита	**Описание**
arp	вывод ARP-таблицы
ifconfig	команда для вывода текущего состояния и параметров сетевых интерфейсов узла, в качестве параметров можно указать конкретный интерфейс
netstat*	команда для вывода текущих сетевых подключений и их статусов
nmap*	программа для сетевого анализа
ping	утилита для проверки доступности удаленного ресурса по протоколу ICMP
route	вывод IP-маршрутов

16.3 Команды, доступные после повышения привилегий

Ниже представлены перечни команд и утилит, доступные пользователю admin после повышения привилегий.

16.3.1 Диагностика системы

Команда/Утилита	**Описание**
viewlog	команда для просмотра некоторых лог-файлов

16.3.2 Настройка системы

Команда/Утилита	**Описание**

date	команда установки системного времени
dpkg	пакетный менеджер
mount	команда для монтирования съемных носителей
reboot	команда перезагрузки ПК «Комрад»
service	утилита для управления службами
umount	команда для извлечения съемных носителей
web-reset-pass	команда сброса пароля пользователя admin для доступа к веб-интерфейсу

16.3.3 Настройка сетевых подключений

Утилита	**Описание**
arp	инструмент для управления ARP-таблицей
ifdown, ifup	команды отключения/включения сетевого адаптера
interface	команда настройки сетевых интерфейсов
route	утилита для управления таблицей маршрутизации
tcpdump	программа для прослушивания сетевого интерфейса

16.3.4 Подсистема мониторинга доступности

Утилита	**Описание**
check_nagios_conf	вывод результата проверки корректности конфигурации модуля доступности

Перейти к содержанию ↑

Приложение А. Поля нормализации ПК «Комрад»

Поле нормализации	Имя в интерфейсе ПК «Комрад»
timestamp_event	Дата генерации
data	Данные
plugin_id	ID плагина
plugin_sid	SID плагина
proto	Протокол
ip_src	IP источника
ip_dst	IP назначения
port_src	Порт источника
port_dst	Порт назначения
host_src	Имя источника
host_dst	Имя назначения
mac_src	MAC источника
mac_dst	MAC назначения
filename	Имя файла
username	Имя пользователя
device	Устройство
http_method	HTTP метод
http_request_url	HTTP запрос
http_status_code	HTTP код возврата
http_url	HTTP ресурс
user_agent	HTTP клиент
geo_src_city	GeoIP город источника
geo_dst_city	GeoIP город назначения
geo_src_country_name	GeoIP страна источника
geo_dst_country_name	GeoIP страна назначения
assoi_object_type	АССОИ тип объекта
assoi_object_name	АССОИ имя объекта
assoi_initiator	АССОИ инициатор
assoi_event	АССОИ событие
text_test	Тест токенов
cgtwname	Имя шлюза
cgtwtype	Тип шлюза
comdesc	Описание команды
qstname	Имя запроса
iname	Имя сетевого интерфейса
role	Роль пользователя
rnm	Название фильтра
status	Статус операции
tdirection	Направление трафика
dvc	Адрес шлюза

Поле нормализации	Имя в интерфейсе ПК «Комрад»
device_id	ID устройства
cef_severity	CEF значимость
cef_device_vendor	CEF вендор
cef_device_product	CEF продукт
cef_device_version	CEF версия продукта
ef_device_event_class_id	CEF ID события
cef_event_name	CEF описание
cef_extension	CEF сообщение
wmi_ComputerName	WMI имя компьютера
wmi_Logfile	WMI журнал
wmi_Message	WMI сообщение
wmi_Type	WMI тип (строка)
wmi_CategoryString	WMI категория (строка)
wmi_SourceName	WMI имя источника
wmi_EventType	WMI тип события
wmi_RecordNumber	WMI номер записи
wmi_EventIdentifier	WMI идентификатор
wmi_Category	WMI категория
wmi_EventCode	WMI код события
wmi_ErrorReason	WMI причина ошибки
home_dir	Домашняя директоря
cmd	Команда
act	Действие
tty	Терминал
shell	Интерпретатор
user_id	ID пользователя
group_id	ID группы
group_name	Имя группы
msg	Сообщение
category	Категория события
service	Сервис
alert_level	Уровень тревоги
rule_id	ID правила
log_location	Файл журнала
IDSClass	Класс СОВ
IDSGroup	Группа СОВ
CVEID	Номер CVE
ExternalRef	Адресс ссылки
IDSTags	Имя тэга
deviceFacility	Тип атаки
peername	Имя узла
cssid	CSSID шлюза

Поле нормализации	Имя в интерфейсе ПК «Комрад»
WMI_sec_id	WMI идентификатор безопасности
code	Событие
kav_message	KAV сообщение
result	Результат операции
cgtw_name	Имя шлюза
rule_group	ID группы правил
packet_length	Длина пакета
rule_pri	Приоритет правила
classification	Классификация
priority	Приоритет
reason	Причина

Приложение Б. Установка агента OSSEC

Б.1 Операционные системы семейства Linux

Для установки агента OSSEC на источник событий с ОС Linux выполните следующие действия.

1. Скачайте и распакуйте архив с агентом OSSEC:

```
wget -U ossec http://www.ossec.net/files/ossec-hids-2.8.1.tar.gz
tar -zxf ossec-hids-2.8.1.tar.gz
```

2. Перейдите в распакованный каталог:

```
cd ossec-hids-2.8.1
```

3. Отредактируйте файл **~/ossec-hids-2.8.1/active-response/host-deny.sh**, убрав пробелы перед переменными:

```
TMP_FILE=`mktemp /var/ossec/ossec-hosts.XXXXXXXXXX`
TMP_FILE="/var/ossec/ossec-hosts.`cat /dev/urandom | tr -dc 'a-zA-Z0-9' | fold -w 32 | head -1 `"
```

4. Для запуска процесса установки следует выполнить в интерфейсе командной строки следующую команду:

```
/bin/bash ./install.sh
```

5. После запуска процесса установки появится предложение ввести необходимые данные для установки.

Вопрос	**Ответ**
Выбрать язык работы, например, русский	ru
Какой тип установки Вы выбираете (сервер, агент, локальный или помощь)?	агент
Укажите куда установить OSSEC HIDS [/var/ossec]	/var/ossec
Какой IP адрес (Hostname) у Вашего OSSEC HIDS сервера?	IP-адрес ПК «Комрад»
Запустить сервис проверки целостности системы? (д/н) [д]	д
Активировать сервис обнаружения руткитов? (д/н) [д]	д
Включить систему активного реагирования? (д/н) [д]	д

6. Для продолжения установки нажмите `Enter`.

АО «НПО «Эшелон»
Адрес: 107023, г. Москва, ул. Электрозаводская, д. 24
Тел.: 8 (495) 223-23-92, , 8 (800) 100-05-02
Веб-сайт: www.npo-echelon.ru
По вопросам приобретения: sales@cnpo.ru
Техническая консультация: support.siem@cnpo.ru