Закрытое акционерное общество «Научно-производственное Объединение «Эшелон»

**УТВЕРЖДЕНО**
НПЭШ.60010-03 91 01-ЛУ

# ПРОГРАММНЫЙ КОМПЛЕКС «KOMRAD Enterprise SIEM»

## Руководство администратора

## НПЭШ.60010-03 91 01

**Листов 222**

| Инв.№подл. | Подп. и дата | Взам.инв.№ | Инв.№ дубл. | Подп. и дата |
|---|---|---|---|---|
| | | | | |

2015

# АННОТАЦИЯ

Настоящий документ представляет собойруководство администратора программного комплекса «KOMRAD Enterprise SIEM» (далее — ПК «КОМРАД» или система),предназначенного для фиксации, сбора, хранения, обработки и анализа событий информационной безопасности (ИБ) сконечных устройств и систем ИТ-инфраструктуры в автоматическом режиме.

В настоящем документе содержатся сведения о назначении и архитектуре ПК «КОМРАД», а также описание функциональных обязанностей администратора по управлению системой, настройке подсистем, эксплуатации и масштабированию системы.

В приложении приводятся требования по настройке источников событий для их корректной работы и обеспечения выполнения системой своих целевых функций.

# СОДЕРЖАНИЕ

1. Общие сведения о программном комплексе ..... 10
1.1. Наименование программного комплекса ..... 10
1.2. Назначение и функции программного комплекса ..... 10
1.3. Требования к уровню подготовки администратора ..... 11
1.4. Обеспечение безопасности ПК ..... 11
1.5. Обязанности администратора ПК ..... 11
2. Структура Программного комплекса ..... 12
2.1. Перечень подсистем программного комплекса ..... 14
2.1.1. Источники событий ..... 14
2.1.2. Средства сбора и передачи информации ..... 16
2.1.2.1. Сбор и передача данных с помощью собственных средств, устройств и систем (безагентный способ) ..... 17
2.1.2.2. Сбор и передача данных с помощью агентов ..... 18
2.1.2.3. Сбор и передача данных с помощью сенсорных запросов 19
2.1.3. Ядро ПК «КОМРАД» ..... 19
2.1.3.1. Сенсор с плагинами ..... 19
2.1.3.2. Модуль корреляции ..... 20
2.1.3.3. Система управления базой данных ..... 22
2.1.3.4. Веб-интерфейс ПК «КОМРАД» ..... 22
2.1.3.5. Интерфейс командной строки ..... 23
2.2. Взаимодействие компонентов системы ..... 24
2.3. Взаимодействие ПК с другими объектами ИТ-инфраструктуры ..... 25
3. Установка программного комплекса ..... 27
3.1. Требования к программно-техническому обеспечению ..... 27
3.2. Установка программного комплекса на сервер ..... 30
3.3. Этапы внедрения ПК «КОМРАД» ..... 43

4. Предварительная настройка Программного комплекса ..... 45
4.1. Настройка модулей ПК «КОМРАД» ..... 45
4.1.1. Настройка плагинов ПК «КОМРАД» ..... 45
4.2. Настройка источников событий ..... 46
4.2.1. Настройка мониторинга доступности для источников событий 46
4.2.2. Проверка настройки агентов UNIX-систем и устройств ..... 50
4.3. Настройка сбора данных из журналов с помощью rsyslog ..... 50
5. Работа с программным комплексом ..... 53
5.1. Обзор доступных интерфейсов ..... 53
5.1.1. Интерфейс командной строки ..... 53
5.1.2. Веб-интерфейс ПК «КОМРАД» ..... 72
5.2. Функции администратора безопасности ..... 74
5.2.1. Вход/выход из веб-интерфейса ПК КОМРАД ..... 74
5.2.2. Работа с директивами корреляции ..... 76
5.2.2.1. Добавление директивы корреляции ..... 77
5.2.2.2. Редактирование пользовательской директивы ..... 88
5.2.2.3. Удаление правила/директивы ..... 88
5.2.3. Мониторинг событий безопасности ..... 88
5.2.4. Оценка уровня обеспечения безопасности системы ..... 97
5.2.5. Обработка инцидентов безопасности ..... 98
5.2.6. База знаний ПК ..... 107
5.2.7. Управление учётными записями пользователей ..... 110
5.2.7.1. Таблица зарегистрированных пользователей ..... 110
5.2.7.2. Добавление учётных записей пользователей ..... 111
5.2.7.3. Изменение учётных записей пользователей ..... 113
5.2.7.4. Удаление учётных записей пользователей ..... 114
5.2.7.5. Копирование учётных записей пользователей ..... 114
5.2.8. Управление активами ..... 114

5.2.8.1. Хосты ..... 115
5.2.8.2. Группы хостов ..... 119
5.2.8.3. Сети ..... 121
5.2.8.4. Порты ..... 123
5.2.8.5. Группы портов ..... 124
5.2.8.6. Редактирование правил Rsyslog ..... 125
5.2.8.7. Инвентаризация OCS ..... 126
5.2.9. Создание отчётов ..... 131
5.3. Дополнительные возможности при работе с ПК ..... 135
5.3.1. Настройка отображения статистической информации ..... 135
5.3.2. Настройка механизма уведомлений ..... 140
5.3.2.1. Отправка электронных писем о новых тревогах ..... 140
5.3.2.2. Настройка оповещений о новых заданиях на обработку инцидентов безопасности ..... 143
5.3.3. Контроль соответствия ..... 144
5.3.4. Отслеживание трафика сети ..... 147
5.3.5. Карта мониторинга доступности ..... 151
5.3.6. Конфигурирование настроек сервера и сенсора ..... 160
5.3.7. Выявление и анализ уязвимостей системы ..... 165
5.3.8. Настройка параметров хранения событий безопасности ..... 169
5.3.9. Резервное копирование системы ..... 170
ПРИЛОЖЕНИЕ А ..... 173
ПРИЛОЖЕНИЕ Б ..... 174
ПРИЛОЖЕНИЕ В ..... 214
ПРИЛОЖЕНИЕ Г ..... 215
ПРИЛОЖЕНИЕ Д ..... 218

# ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

IDS — IntrusionDetectionSystem (Система Обнаружения Вторжений);

SIEM — SecurityInformationandEventManagement (система управления информацией о безопасности и событиях безопасности);

SSH — Secure Shell (безопасная оболочка);

БД — база данных;

ИБ — информационная безопасность;

ИС — источник события

ИТ — информационные технологии;

ЛВС — локальная вычислительная сеть.

МЭ — межсетевой экран;

НСД — несанкционированный доступ;

ОС — операционная система;

ПК — программный комплекс;

ПО — программное обеспечение;

СОВ — система обнаружения вторжений;

СУБД — система управления базами данных.

# ОПРЕДЕЛЕНИЯ

**MySQL** —свободная система управленияреляционными базами данных.

**Nagios** —программа мониторинга компьютерных систем и сетей, предназначенная для наблюдения, контроля состояния вычислительных узлов и служб, оповещающая администратора в том случае, если какие-то из служб прекращают (или возобновляют) свою работу.

**Nginx** — веб-сервер и почтовый прокси-сервер, работающий на Unix-подобных операционных системах.

**OSSEC** (Open Source SECurity) — хостовая система обнаружения вторжений (HIDS).

**OSSIM**— программное средство, предназначенное для инспектирования и выявления уязвимостей в сети, обнаружения и предотвращения вторжений, оперативного оповещения пользователей и других инструментов.

**SIEM** (Security Information and Event Management) — система управления информацией о безопасности и событиях безопасности.

**Snare** (System iNtrusion Analysis and Reporting Environment) — сервис, который предоставляет удалённое слежение, передачу информации в режиме реального времени.

**SSHd** — демон, входящий в состав OpenSSH и предоставляющий защищённый доступ к ресурсам.

**Syslog** — стандарт отправки и регистрации сообщений о происходящих в системе событиях, то есть создания логов, использующийся в компьютерных сетях, работающих по протоколу IP.

**Агент —**программное обеспечение, устанавливаемое на операционную систему Linux или Windows, позволяющее осуществлять сбор данных с источника событий.

**Администратор** — выделенный персонал, в обязанности которого входит выполнение технологических функций по обслуживанию ПК«КОМРАД» и осуществление мониторинга ИБ с помощью системы.

**База знаний**— набор рекомендаций и справочных материалов по инцидентам и событиям информационной безопасности.

**Демон** — компьютерная программа в системах класса UNIX, запускаемая самой системой и работающая в фоновом режиме без прямого взаимодействия с пользователем.

**Директива корреляции** — набор логических правил позволяющих осуществлять сравнение параметров событий информационной безопасности, а также их количества и частоты с заданными показателями для выявления инцидентов информационной безопасности.

**Инцидент информационной безопасности** — изменение параметров состояния конечного устройства или системы, превышающее заданные граничные показатели и представляющее угрозу безопасности ИТ-инфраструктуры.

**Источник события(актив, средство)**— конечное устройство или система, на котором фиксируется изменение контролируемых параметров (возникновение событий информационной безопасности).

**Корреляция данных** — сравнение параметров данных о событиях информационной безопасности с заданными граничными показателями для выявления инцидентов информационной безопасности.

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

**Плагин** — программный модуль, динамически подключаемыйк сенсору ядра ПК «КОМРАД», реализованный в виде конфигурационных файлов с набором инструкций, в соответствии с которыми данные от источников событий обрабатываются и передаются на дальнейшую обработку.

**Портал** — типовой веб-портал: веб-сервер, интерпретатор программного кода, система управления базами данных, дополнительные сервисы (планировщик, кэширование, поиск), общесистемные сервисы (электронная почта, DNS, NTP).

**Сенсор**— программный модуль ядра ПК «КОМРАД», агрегирующий, нормализующий и передающий данные о событиях ИБ на дальнейшую обработку.

**Событие информационной безопасности** — изменение параметров состояния конечного устройства или системы, данные о котором вносятся в системный журнал устройства или системы.

# 1. ОБЩИЕ СВЕДЕНИЯ О ПРОГРАММНОМ КОМПЛЕКСЕ

## 1.1. Наименование программного комплекса

Программный комплекс мониторинга событий и инцидентов информационной безопасности «KOMRAD Enterprise SIEM».

Условное обозначение —ПК «КОМРАД».

## 1.2. Назначениеи функции программного комплекса

ПК «КОМРАД» предназначен для автоматизации мониторинга событий и обнаружения инцидентов информационной безопасности, а также для обеспечения эффективной работы сотрудников отдела информационной безопасности.

Объектами автоматизации являются основные объекты ИТ-инфраструктуры, к которым относятся:

- системы и средства защиты информации;
- общесистемное ПО;
- программно-технические устройства центра обработки данных;
- информационные системы (например, порталы в сети Интернет);
- телекоммуникационное и серверное оборудование.

ПК «КОМРАД» реализует следующие основные функции:

- фиксация данных о событиях ИБ на источниках событий;
- сбор, фильтрация и передача на сервер данных о событиях ИБ;
- получение, агрегация, нормализация и хранение поступающих данных;
- автоматическая корреляция нормализованных данных о событиях ИБ;
- выявление инцидентов ИБ;
- контроль устранения инцидентов ИБ;
- организация мониторинга доступности узлов и служб;
- генерация отчетов различных типов на основе хранимых на сервере данных.

Также ПК «КОМРАД» предоставляет администратору системы возможность управлять:

- директивами корреляции с целью выявления более широкого спектра угроз;
- данными об обнаруженных инцидентах безопасности;
- механизмом заявок с целью устранения конкретных инцидентов ИБ конкретным исполнителем.

## 1.3. Требования к уровню подготовки администратора

Для корректного управления системой администратор должен обладать навыками работы с системами подобного типа, владеть понятийным аппаратом, понимать принципы работы SIEM-систем и входящих в них компонентов, а также предварительно ознакомиться снастоящим Руководством иинойэксплуатационной документацией

## 1.4. Обеспечение безопасности ПК

Сервер ПК «КОМРАД» должен размещаться в контролируемой административной зоне (например, в центре обработки данных с пропускным режимом) в оборудованной замком телекоммуникационной стойке. Штатным средством защиты от НСД является механизм авторизации по заданной паре «логин/пароль».

## 1.5. Обязанности администратора ПК

Основными обязанностями администратора являются:

- установка, модернизация, настройка и наблюдение за работоспособностью системного и базового программного обеспечения ПК «КОМРАД» в соответствии с настоящим Руководством;
- управление списком пользователей системы (в том числе распределение прав доступа и назначение ролей);
- отслеживание своевременного исполнения заявок на обработку инцидентов безопасности;
- администрирование баз данных и СУБД MySQL;
- резервное копирование и восстановление данных.

# 2. СТРУКТУРА ПРОГРАММНОГО КОМПЛЕКСА

ПК «КОМРАД» организован по иерархическому принципу. Структурная схема ПК «КОМРАД» представлена на Рисунке 1.

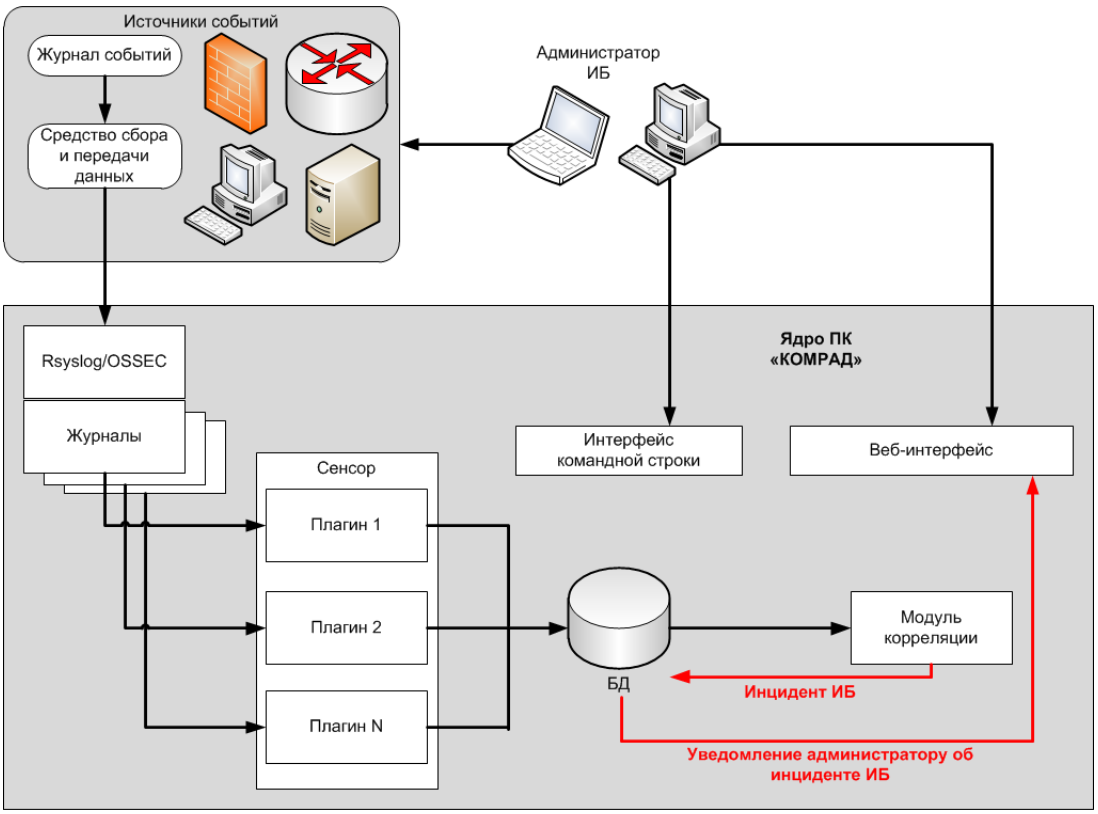



Рисунок 1 – Структурная схема ПК «КОМРАД»

При возникновении событий ИБ на конечных устройствах или системах данные об этом записываются в журналы состояния соответствующих объектов ИТ-инфраструктуры и в режиме времени, близком к реальному, отправляются на сервер ПК «КОМРАД» агентами, собственными средствами конечных устройстви систем или по запросу от сенсора(SQL, WMI, и т.д.).

Сервер ПК «КОМРАД» принимает данные, агрегирует и записывает их в журналы в соответствии с типом источника событий с помощью утилиты rsyslog. Сенсор обрабатывает журналы в соответствии с логикой плагинов, обеспечивающих поддержку работы с конечными устройствами и системами различных типов, после чего нормализованные данные поступают в БД ПК «КОМРАД», где каждому событию ИБ присваивается персональный идентификатор. После этого выполняется обработка данных модулем корреляции в соответствии с заранее определёнными пра-

вилами корреляции и политиками, на основании которых выявляются инциденты ИБ.

Уведомление о выявленных инцидентах ИБ передаётся средствами веб-интерфейса администратору безопасности.

Нормализованные события ИБ, данные об инцидентах ИБ и информация о настройках системы хранятся в реляционной базе данных.

Взаимодействие администратора безопасности с ядром ПК «КОМРАД» осуществляется с использованием веб-интерфейсаи интерфейса командной строки.

## 2.1. Перечень подсистем программного комплекса

### 2.1.1. Источники событий

Источниками событий для ПК «КОМРАД» являются объекты ИТ-инфраструктуры (конечные устройства и системы), в состав которых могут входить:

- серверы и рабочие станции под управлением операционной системы (ОС) Linux, в том числе требующие дополнительных настроек веб-серверы (nginx, Apache), почтовые серверыи СУБД (MySQL, Oracle);
- серверы и рабочие станции под управлением ОС Windows (Windows-системы), в том числе домен ActiveDirectory;
- база данных журнала действий администраторов и пользователей;
- активное сетевое оборудование;
- межсетевые экраны;
- системы обнаружения вторжений (СОВ) /IntrusionDetectionSystem (IDS);
- средства мониторинга состояния антивирусной безопасности ИТ-инфраструктуры;
- средства мониторинга, контроля доступа и защиты от несанкционированного доступа (НСД) к ИТ-инфраструктуре;
- средство мониторинга, контроля доступа к базам данных(например, MySQLProxy).

ПК «КОМРАД» обеспечивает сбор, обработку и анализ данных о событиях ИБ от источников событий, точный состав и количество которых определяются по фактическому состоянию ИТ-инфраструктуры на этапе технического проектирования конкретного проекта.

Фиксация событий информационной безопасности на объектах ИТ-инфраструктуры производится в журналах событий конечных устройств и систем (Таблицы 1, 2), откуда с помощью средств сбора и передачи информации данные передаются в ядро ПК «КОМРАД».

Таблица 1. Перечень журналов событий объектов ИТ-инфраструктуры

| **Тип устройства или системы** | **Средство сбора и передачи информации** | **Источник информации или список журналов** |
|---|---|---|
| Windows-системы | Агент Snare | Журналы**EventLog**:<br>**Security** (событиябезопасности, генерируемыесистемойаудитабезопасностиОСWindows)<br>**System** (событияприложенийислужб) |
| Active Directory | Агент Snare | Журнал**EventLog**:<br>**Security** (событиябезопасности, генерируемыесистемойаудитабезопасностидомена ОС Windows) |
| UNIX-системы | Агент OSSEC | См. таблицу 2 |
| Веб-серверы | Агент OSSEC | См.таблицу 2 |
| Почтовый сервер | Агент OSSEC | См.таблицу 2 |
| MySQL Proxy | Собственные средства | Данные журнала передаются в ядро ПК «КОМРАД» собственными средствами сервера данного приложения |
| СУБД MySQL | Агент OSSEC | См. таблицу 2 |
| База данных журнала действий пользователей на портале | Запросы от сенсора | Журнал формируется средствами программного обеспечения Портала, данные хранятся в БД MySQL |
| База данных журнала действий администраторов на портале | Запросы от сенсора | Журнал формируется средствами программного обеспечения Портала, данные хранятся в БД MySQL |
| Активное сетевое оборудование | Собственные средства | Данные журнала передаются в ядро ПК «КОМРАД» собственными средствами сервера данного приложения |
| Межсетевой экран | Собственные средства | Данные журнала передаются в ядро ПК «КОМРАД» собственными средствами сервера данного приложения |
| Средство обнаружения вторжений | Собственные средства | Данные журнала передаются в ядро ПК «КОМРАД» собственными средствами сервера данного приложения |
| Средство мониторинга, контроля доступа и защиты от НСД | Собственные средства | Данные журнала передаются в ядро ПК «КОМРАД» собственными средствами сервера данного приложения |
| Средство мониторинга антивирусной безопасности | Запросы от сенсора | Журнал формируется средствами ПО Kaspersky Security Center. Хранится в БД MSSQL |

Таблица 2. Журналы событий UNIX-систем

| Расположение журнала | Назначение журнала |
|---|---|
| /var/log/messages | Журнал сообщений ядра и журнальных записей системных программ |
| /var/log/secure | Журнал аутентификации UNIX-системы |
| /var/log/syslog | Основной системный журнал (сообщения служб и других программ, работающих в системе) |
| /var/log/yum.log | Журнал системы управления пакетами YUM |
| /var/log/maillog | Журнал сервиса электронной почты |
| /var/log/httpd/error_log | Журнал ошибок сервиса httpd (веб-сервер) |
| /var/log/httpd/access_log | Журнал сервиса httpd (веб-сервер) |
| /var/log/nginx/access.log | Журнал сервиса nginx (веб-сервер) |
| /var/log/nginx/error.log | Журнал ошибок сервиса nginx (веб-сервер) |
| /var/log/audit/audit.log | Журнал службы audit (информацияо модификации и удалении файлов) |
| /var/log/inotify.log | Журнал inotify-tools (информацияо модификации и удалении файлов) |
| /var/log/mysql/mysql.log | Журнал СУБД MySQL |
| /var/log/ntp.log | Журнал службы NTP (сетевая синхронизация времени) |
| /var/log/php/php-fpm.log | Журнал сервера Php-fpmj, обеспечивающего взаимодействие веб-сервера и приложения |
| /var/log/stunnel/stunnel.log | Журнал службы stunnel (шифрование сетевых соединений) |

### 2.1.2. Средства сбора и передачи информации

Данные из журналов источников событий собираются и передаются в ядро ПК «КОМРАД» тремя способами:

- с помощью агента;
- с помощью собственных средств конечного устройства или системы (без агента);
- с помощью запроса от сенсора.

Средства сбора и передачи информации в зависимости от способа работы связаны с конкретными типами конечных устройств и систем. В качестве примера можно привести классификацию источников событий типовой информационной системы (Таблица 3).

Таблица 3. Классификация источников событий типовой информационной системы

| **Средство сбора и передачи информации** | **Протокол обмена** | **Тип устройства** |
|---|---|---|
| Агент | Syslog (TCP/UDP 514) | Windows-системы |
| | Syslog (TCP/UDP 514) | Unix-системы |
| | Syslog (TCP/UDP 514) | Почтовый сервер |
| | Syslog (TCP/UDP 514) | Веб-серверы |
| | Syslog (TCP/UDP 514) | СУБД |
| Собственные средства | Syslog (TCP/UDP 514) | Межсетевой экран |
| | Syslog (TCP/UDP 514) | Активное сетевое оборудование (маршрутизаторы) |
| | Syslog (TCP/UDP 514) | СОВ (IDS) |
| | Syslog (TCP/UDP 514) | Журнал аутентификации средств мониторинга, контроля доступа и защиты от несанкционированного доступа к ИТ-инфраструктуре |
| Запросы от сенсора | MySQL (TCP 3306) | Базы данных MySQL |
| | MSSQL (TCP 1433) | Базы данных MSSQL |

#### 2.1.2.1. Сбор и передача данных с помощью собственных средств, устройств и систем (безагентный способ)

Для определённого класса источников событий, к которым могут быть отнесены средства защиты информации и активное сетевое оборудование, IDS,используются собственные средства сбора и передачи данных о событиях ИБ. В этом случае данные поступают в ядро ПК «КОМРАД» непосредственно от конечных устройств и систем. Данные передаются на сенсор с помощью протоколasyslog через порт UDP514.

Подробное описание настройки собственных средств источников событий приведено в соответствующих конечным устройствам и системам пунктах Приложения Б.

### 2.1.2.2. Сбор и передача данных с помощью агентов

Для некоторых типов источников событий альтернативы по передаче данных нет, например, для маршрутизаторов Cisco или для сервера управления Kaspersky (только с помощью собственных средств, т.е. безагентным способом). Но для операционных систем имеется возможность установки агента. Агент позволяет более гибко настраивать фильтрацию событий, а также упрощает управление источниками событий. Кроме того, агент осуществляет ряд других дополнительных функций: кодирование передаваемой информации, оповещение ПК «КОМРАД» об отключении агента.

Агенты представляют собой средство сбора и передачи данных из журналов событий конечных устройств и систем в плагины сенсора для последующей обработки в ядре ПК «КОМРАД» и устанавливаются на источники событий с помощью конфигурационных файлов.Данные передаются на сенсор с помощью протоколаsyslog через порт UDP1514 или 514. Безагентный и агентный способы передачи данных представлены на Рисунке 2.

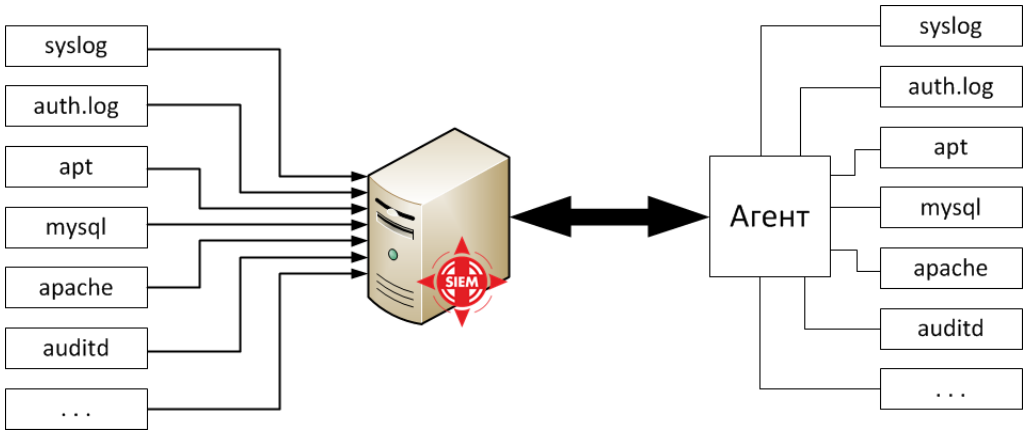



Рисунок 2 – Безагентный и агентный способы передачи данных в ПК «КОМРАД»

Подробное описание процессов установки и настройки агентов на конечных устройствах и системах, а также настройки самих конечных устройств и систем, приведено в соответствующих конкретному агенту пунктах Приложения Б.

#### 2.1.2.3. Сбор и передача данных с помощью сенсорных запросов

При взаимодействии с базами данных ядро ПК «КОМРАД» выполняет периодические запросы о параметрах состояния базы данных в соответствии с настройками соответствующего плагина в сенсоре. При этом на всех БД источников событий, требуется создать пользователя и произвести настройки системы управления базами данных в соответствии с разделами «Требования по настройке СУБД MySQL» и «Требования по настройке СУБД MSSQL» Приложения Б.

Сенсор получает данные от СУБД MySQLобращением по протоколу TCPк порту 3306 (по умолчанию), а от СУБД MSSQLпо протоколу TCPк порту 1433 (по умолчанию).

### 2.1.3. Ядро ПК «КОМРАД»

Ядро ПК «КОМРАД» установлено на сервере ПК «КОМРАД» и реализует основной функционал по обработке данных о событиях ИБ (агрегация, нормализация, корреляция данных и выявление инцидентов ИБ, назначение параметров выявления инцидентов ИБ, в том числе значений достоверности инцидента ИБ, веса конечных устройств и систем, приоритета правил).

В ядре ПК «КОМРАД» можно выделить основные компоненты:

- сенсор с плагинами (может быть вынесен на отдельный сервер);
- модуль корреляции;
- база данных ПК «КОМРАД»(может быть вынесена на отдельный сервер);
- веб-интерфейс;
- интерфейс командной строки.

#### 2.1.3.1. Сенсор с плагинами

Ядро ПК «КОМРАД» принимает данные от средств сбора и передачи информации на сенсор с помощью его плагинов.

Контролируемые события ИБ зависят от настроек соответствующего конкретным конечным устройствам и системам плагина. Каждому типу источника событий соответствует определённый плагин, пример приведен в Таблице 4.

Таблица 4. Пример соответствия плагинов типам источников событий

| **Тип плагинов** | **Тип устройства** |
|---|---|
| OSSEC | Unix-системы |
| | Почтовый сервер |
| | Веб-серверы |
| | СУБД MySQL |
| snare | Windows-системы |
| | Active Directory |
| snort | IDS |
| MySQL | Базы данных MySQL |
| MSSQL | Базы данных MSSQL |
| cisco-asa | Межсетевой экран |
| cisco-router | Активное сетевое оборудование |

Плагины подключаются к сенсору ядра администратором ПК «КОМРАД».

Данные о событиях ИБ, полученные плагинами от соответствующих конечных устройств и систем, агрегируются и нормализуются сенсором, после чего передаются на дальнейшую обработку в модуль корреляции после записи нормализованных данных в базу данных ПК «КОМРАД».

#### 2.1.3.2. Модуль корреляции

Модуль корреляции выполняет автоматический анализ собранных данных и обеспечивает выявление инцидентов ИБ с помощью набора правил корреляции для сравнения зарегистрированных событий ИБ (записей журналов регистрации) с шаблонами распространённых сетевых угроз безопасности.

Выявление инцидентов безопасности обеспечивается с помощью метода, предусматривающего классификацию угроз и проблем безопасности с учётом степени воздействия события на среду, способа атаки и целевых ресурсов. При этом каждому выявленному инциденту ИБ автоматически присваивается уровень значимости на основе заданных значений конфиденциальности, целостности и доступности, определённых для каждого конечного устройства и системы.

Подробные описание и настройки модуля приведены в разделе «Работа с директивами корреляции» настоящего Руководства.

Блок-схема алгоритма работы модуля представлена на Рисунке 3.

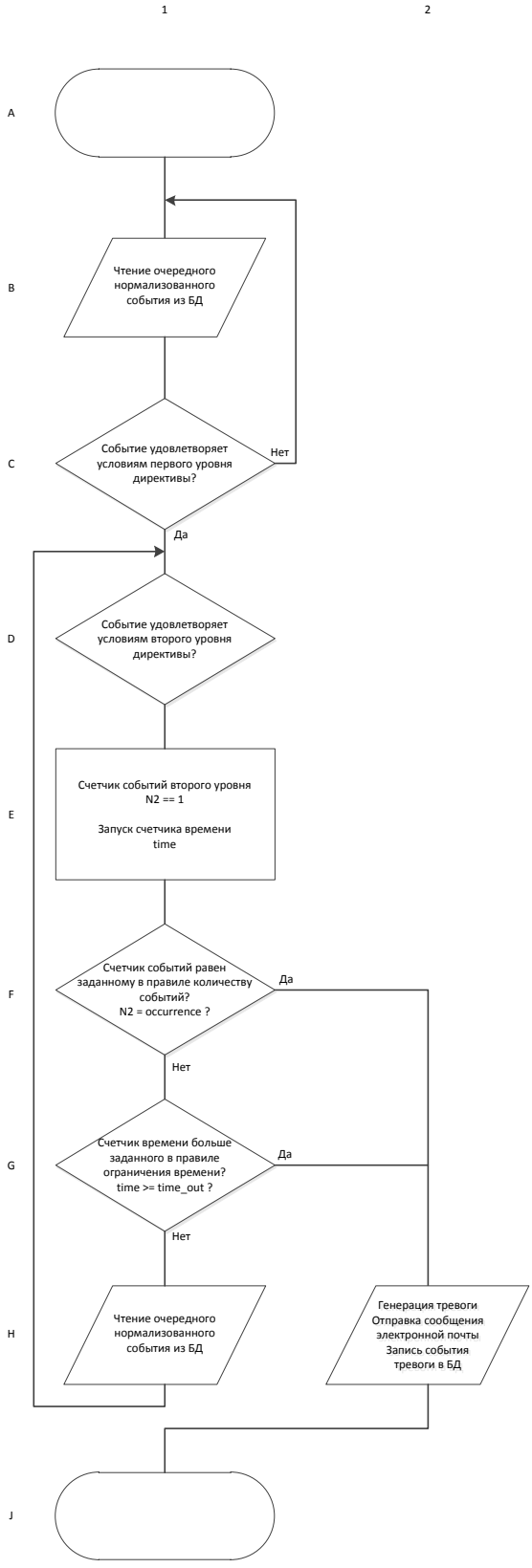



Рисунок 3 – Блок-схема алгоритма работы модуля корреляции

#### 2.1.3.3. Система управления базой данных

Система управления базой данных ПК «КОМРАД» MySQL обеспечивает занесение данных о событиях ИБ в реляционную базу данных, хранение нормализованной информации и позволяет проводить анализ данных, в том числе корреляцию.

При этом СУБД ПК «КОМРАД» решает следующие задачи:

- обеспечение поддержки и сопровождения базы данных ПК «КОМРАД» (проверка состояния, резервное копирование и восстановление, очистка данных об инцидентах ИБ и данных о событиях ИБ);
- управление архивами событий ИБ, в том числе автоматическое удаление устаревших архивов по мере истечения заданного срока их хранения и/или достижения установленного ограничения на использование дискового пространства, отведённого для хранения архивов;
- предоставление возможности управления архивами событий ИБ (создание новых архивов, копирование существующих, просмотр данных в архивах, редактирование параметров архивов).

#### 2.1.3.4. Веб-интерфейс ПК «КОМРАД»

Веб-интерфейс ПК «КОМРАД» предназначен для взаимодействия с системой и предоставляет администратору возможности:

- управления данными о событиях и обнаруженных инцидентахИБ (просмотр информации об инциденте, создание, редактирование, фильтрация, поиск, закрытие, повторное открытие, печать данных об инциденте, экспорт данных об инциденте);
- ведения отчётности о событиях и инцидентах ИБ;
- ведения централизованного перечня конечных устройств и систем, используемых в ходе обработки правил и корреляции данных;
- редактирования параметров конечных устройств и систем;
- управления заявками, необходимыми для устранения инцидентов ИБ (создание, просмотр, фильтрация, изменение приоритета, создание или изменение назначения, добавление примечаний, закрытие);

- разграничения доступа к управлению компонентами ПК между пользователями.

Веб-интерфейс представляет собой оконный интерфейс доступа к управлению компонентами ПК «КОМРАД» (Рисунок 4).

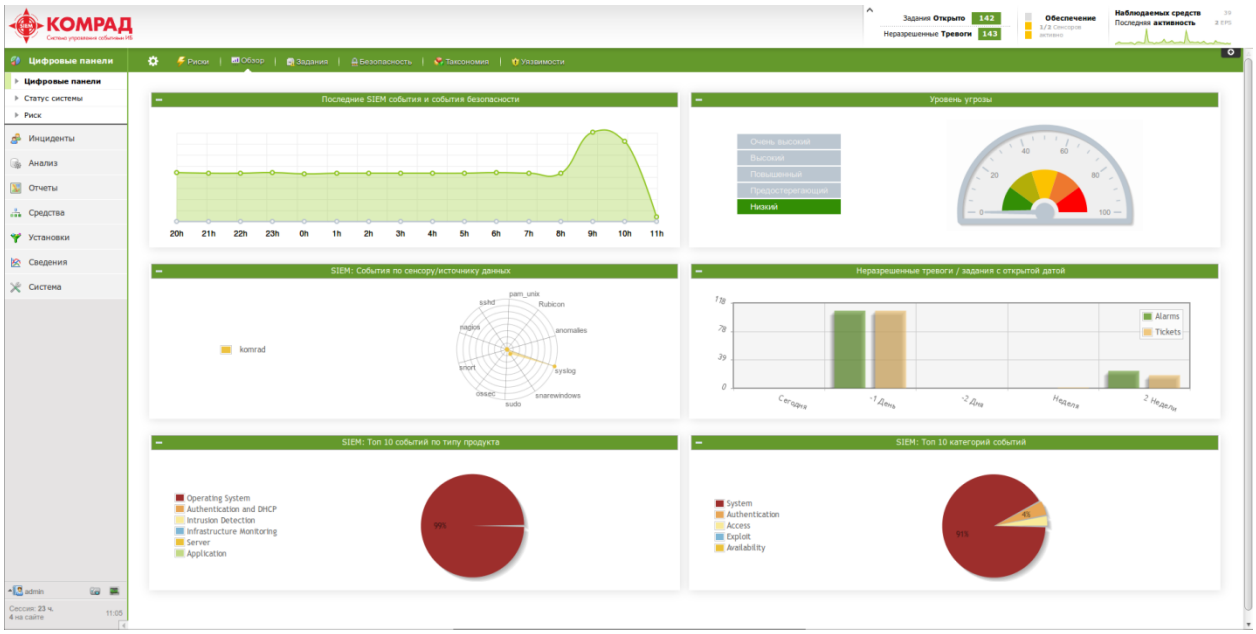



Рисунок 4 – Главное окно веб-интерфейса ПК «КОМРАД»

Подробное описание веб-интерфейса и работы с ним приведено в разделе «Веб-интерфейс ПК «КОМРАД».

### 2.1.3.5. Интерфейс командной строки

Интерфейс командной строки предназначен для обеспечения администратора информационной безопасности функциями управления системой (в том числе плагинами и интерфейсами), и предоставления данных об ошибках и сбоях компонентов ПК «КОМРАД».

Интерфейс командной строки доступен локально, а также удаленно по протоколу SSHчерез порт TCP22(используется по умолчанию).

Более подробно функции и работа интерфейса описаны в разделе «Интерфейс командной строки» настоящего Руководства.

## 2.2. Взаимодействие компонентов системы

Схема информационного обмена между устройствами и программными компонентами ПК «КОМРАД» представлена на Рисунке 5.

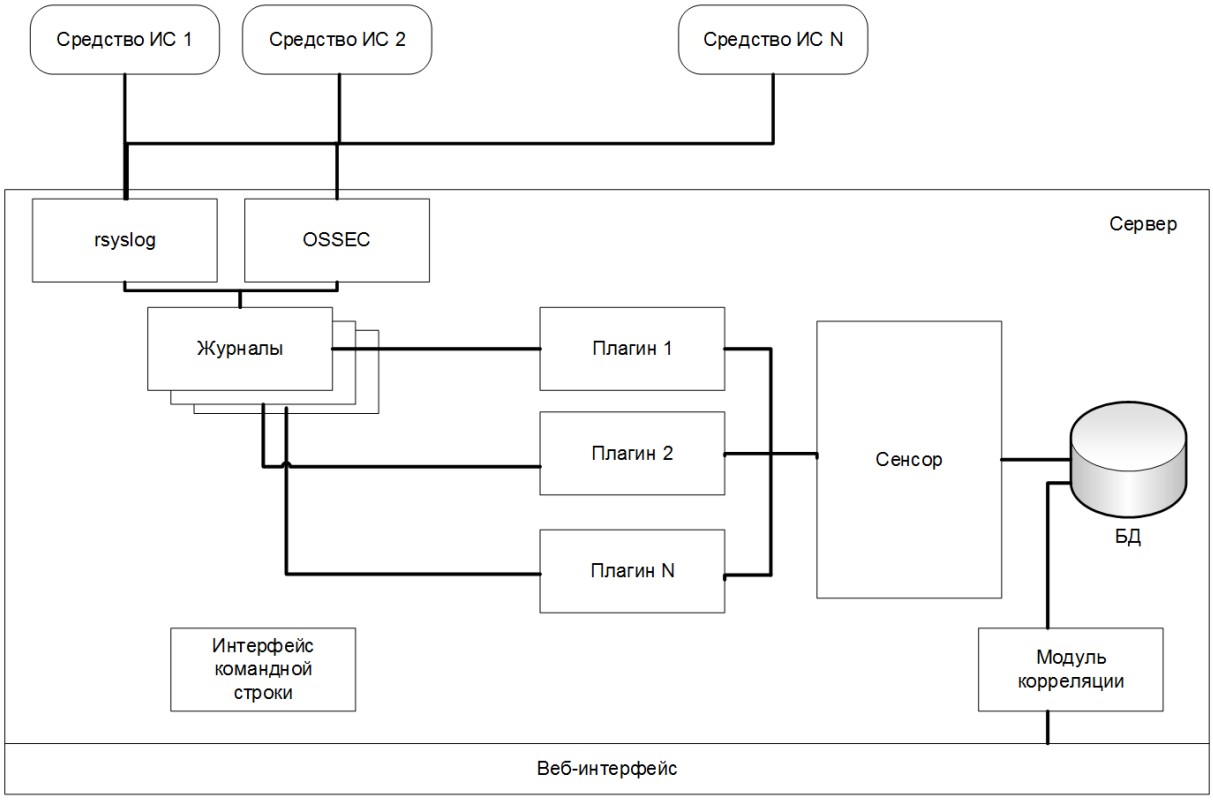



Рисунок 5 – Схема информационного обмена ПК «КОМРАД»

**Примечание**: помимо rsyslog приём данных от источников событий осуществляет OSSEC, который получает данные об определённых событиях с помощью системы фильтрации в соответствии с правилами обработки, описанными в разделе «Настройка фильтрации событий агентомOSSEC» настоящего Руководства.

Ossec-server записывает данные в журнал текущего дня /var/ossec/logs/alerts/<Год>/<месяц>/ossec-alerts-<день>.log. Журнал за текущие сутки доступен по адресу /var/ossec/logs/alerts/alerts.log.

Для информационного обмена между компонентами ПК «КОМРАД» используются стандартные унифицированные протоколы семейства TCP/IP и интерфейсы Ethernet/Fast Ethernet/GigabitEthernet.

Подробная схема информационного взаимодействия компонентов системы представлена на Рисунке 6.

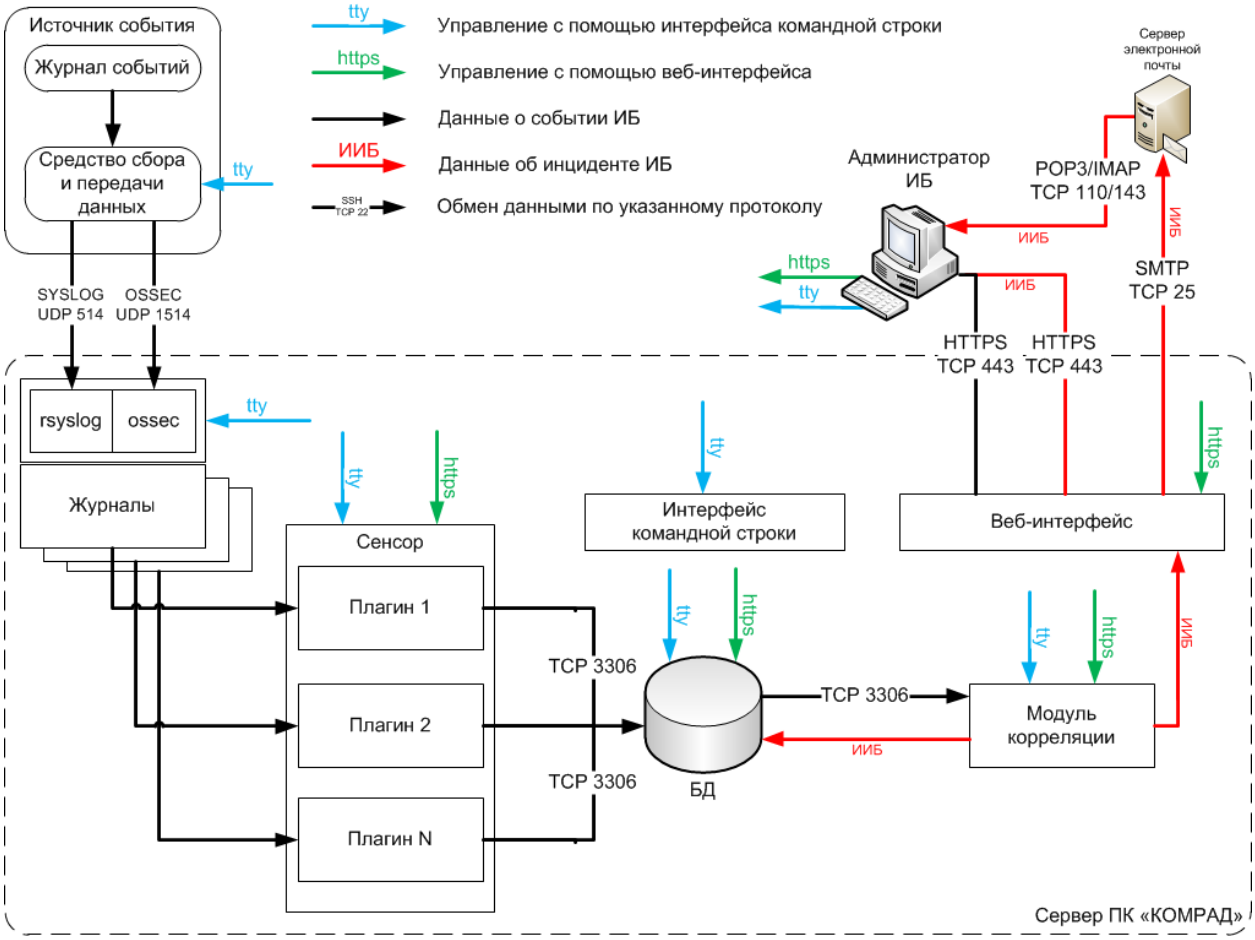



Рисунок 6 – Взаимодействие компонентов ПК «КОМРАД»

Матрица информационного взаимодействия ПК «КОМРАД» с указанием протоколов и портов, через которые осуществляется обмен данными, в том числе взаимодействие оператора и администратора ПК «КОМРАД» с компонентами системы, приведена в Приложении А.

## 2.3. Взаимодействие ПК с другими объектами ИТ-инфраструктуры

ПК «КОМРАД» функционирует параллельно с другими объектами ИТ-инфраструктуры и не оказывает деструктивного воздействия на их работу.

ПК «КОМРАД» имеет возможность интеграции со средствами анализа защищенности, что позволяет расширить функционал сканирования уязвимостей. Описа-

ние настроек интеграции ПК «КОМРАД» с САЗ «Сканер-ВС» приведено в Приложении Д настоящего Руководства.

# 3. УСТАНОВКА ПРОГРАММНОГО КОМПЛЕКСА

Установка ПК «КОМРАД» начинается с развёртывания на сервере образа ПК «КОМРАД». После этого производится копирование конфигурационных файлов для источников событий и компонентов ядра ПК «КОМРАД», ихпервичная настройка с помощью интерфейса командной строки, а также настройка объектов ИТ-инфраструктуры для взаимодействия с ПК «КОМРАД».

## 3.1. Требования к программно-техническому обеспечению

При установке ПК «КОМРАД» необходимо выполнение минимальных системных требований к серверу ПК «КОМРАД», на который устанавливаются компоненты системы (Таблица 5).

Таблица 5 – Минимальные требования к техническому обеспечению сервера ПК «КОМРАД» на 100 источников событий

| Элемент | Минимальное значение |
|---|---|
| Процессор | Intel Xeon |
| Количество ядер процессора | 4 |
| Сетевой интерфейс | Fast Ethernet |
| Оперативная память | 8 Гб |
| Жёсткий диск | 500 Гб |
| RAID контроллер | Поддержка RAID 10 |
| HDD | SAS/SATA 10000 rpm |

Допускается установка ПК «КОМРАД» на виртуальную машину гипервизора KVM или VMware. При этом сервер виртуальной машины должен соответствовать минимальным требованиям, представленным в Таблице 6.

Таблица 6 – Минимальные требования к параметрам сервера виртуальной машины ПК «КОМРАД» на 100 источников событий

| **Элемент** | **Минимальное значение** |
|---|---|
| Процессор | 1 |
| Количество ядер процессора | 4 |
| Сетевой интерфейс | Fast Ehternet |
| Оперативная память | 8 Гб |
| Жёсткий диск | 500 Гб |

**Примечание:** сервер и сенсоры ПК «КОМРАД» для больших сетей ( >200 узлов) не рекомендуется размещать на виртуальных машинах.Минимальные системные требования к техническому обеспечению сенсора ПК «КОМРАД» для приема от 200 источников событий представлены в Таблице 7.

Таблица 7 – Минимальные требования к техническому обеспечению сенсора ПК «КОМРАД» для обеспечения приема от 200 источников событий.

| **Элемент** | **Минимальное значение** |
|---|---|
| Процессор | Intel Xeon |
| Количество ядер процессора | 8 |
| Сетевой интерфейс | Gigabit Ethernet |
| Оперативная память | 8 Гб |
| Жёсткий диск | 500 Гб |
| RAID контроллер | Поддержка RAID 10 |
| HDD | SAS/SATA 10000 rpm |

Рекомендуемые системные требования к техническому обеспечению центрального сервера ПК «КОМРАД» 2 уровня для обеспечения работы с сенсорами: от 5 до 50 представлены в Таблице 8.

Таблица 8 – Рекомендуемые требования к техническому обеспечению центрального сервера ПК «КОМРАД» 2 уровня для обеспечения работы с сенсорами: от 5 до 50

| **Элемент** | **Минимальное значение** |
|---|---|
| Процессор | 1 - 4 x Intel Xeon |
| Количество ядер процессора | 8 |
| Сетевой интерфейс | Gigabit Ethernet |
| Оперативная память | 16 - 128 Гб |
| Жёсткий диск (эффективное пространство) | 1 - 10 Тб |
| RAID контроллер | Поддержка RAID 10 |
| HDD | SAS/SATA 10000 rpm |

Рекомендуемые системные требования к техническому обеспечению центрального сервера ПК «КОМРАД» 3 уровня для консолидации и обработки информации об инцидентах с серверов 2 уровня представлены в Таблице 9.

Таблица 9 – Рекомендуемые требования к техническому обеспечению центрального сервера ПК «КОМРАД» 3 уровня

| Элемент | Минимальное значение |
|---|---|
| Процессор | 1 - 4 x Intel Xeon |
| Количество ядер процессора | 8 |
| Сетевой интерфейс | Gigabit Ethernet |
| Оперативная память | 16 - 128 Гб |
| Жёсткий диск (эффективное пространство) | 1 - 10 Тб |
| RAID контроллер | Поддержка RAID 10 |
| HDD | SAS/SATA 10000 rpm |

Для штатной работы с веб-интерфейсом ПК «КОМРАД» требуется установка на рабочую станцию веб-браузера одного из типов, представленных в Таблице 10.

Таблица 10 – Требования к веб-браузеру

| Тип браузера | Минимально допустимая версия | Необходимые настройки |
|---|---|---|
| Google Chrome | Google Chrome 9.0 | - |
| Safari | Safari 5.0.5 | - |
| Mozilla Firefox | Mozilla Firefox 3.0 | - |
| Internet Explorer | Internet Explorer 7.0 | - |
| Opera | Opera 10.5 | - |
| Yandex Browser | Yandex Browser 13.0 | - |

## 3.2. Установка программного комплекса на сервер

Установка ПК «КОМРАД» на сервер заключается в развёртывании образа программного комплекса и выполнения типовых настроек.

1. Для начала установки необходимо запустить образ на сервере, удовлетворяющем требованиямраздела 3.1 настоящего Руководства.

Откроется начальное окно установки (Рисунок 7).

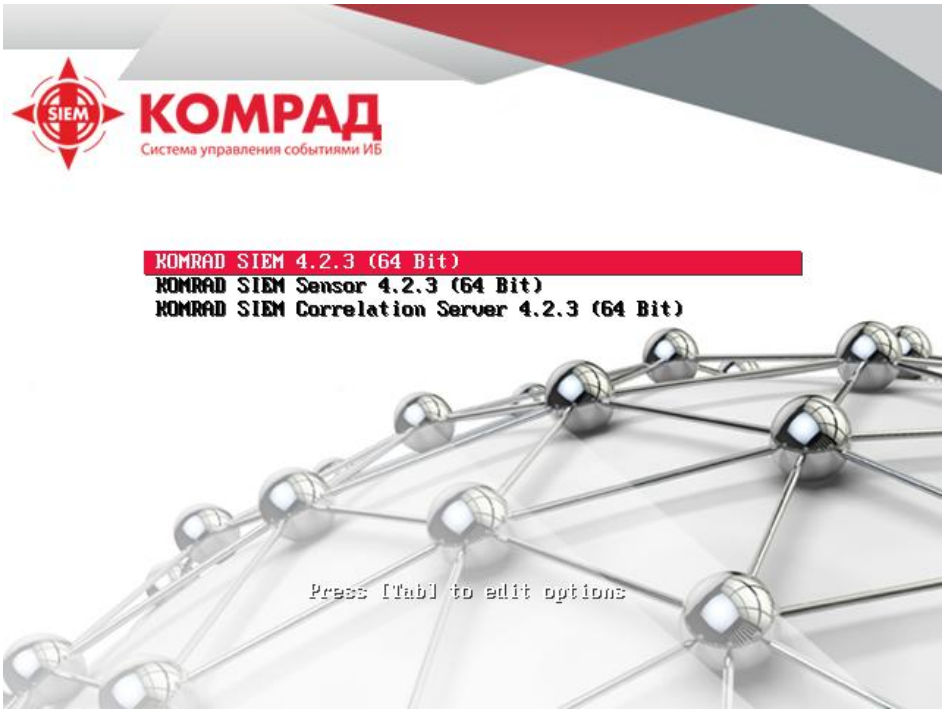



Рисунок 7 – Начальное окно установки ПК «КОМРАД»

Для установки ПК «КОМРАД» необходимо выбрать верхний пункт«**KOMRAD SIEM 4.2.3 (64 Bit)»** и нажатьклавишу «**Enter»**.

**Примечание:** в ходе установки существует возможность сделать снимок экрана, нажав соответствующую кнопку в интерфейсе мастера установки.

2. Следующее окно предлагает выбрать параметры клавиатуры (Рисунок 8). После выбора одного из вариантов необходимо нажать «**Продолжить»**. Затем начнется загрузка компонентов программы установки с компакт-диска (Рисунок 9).

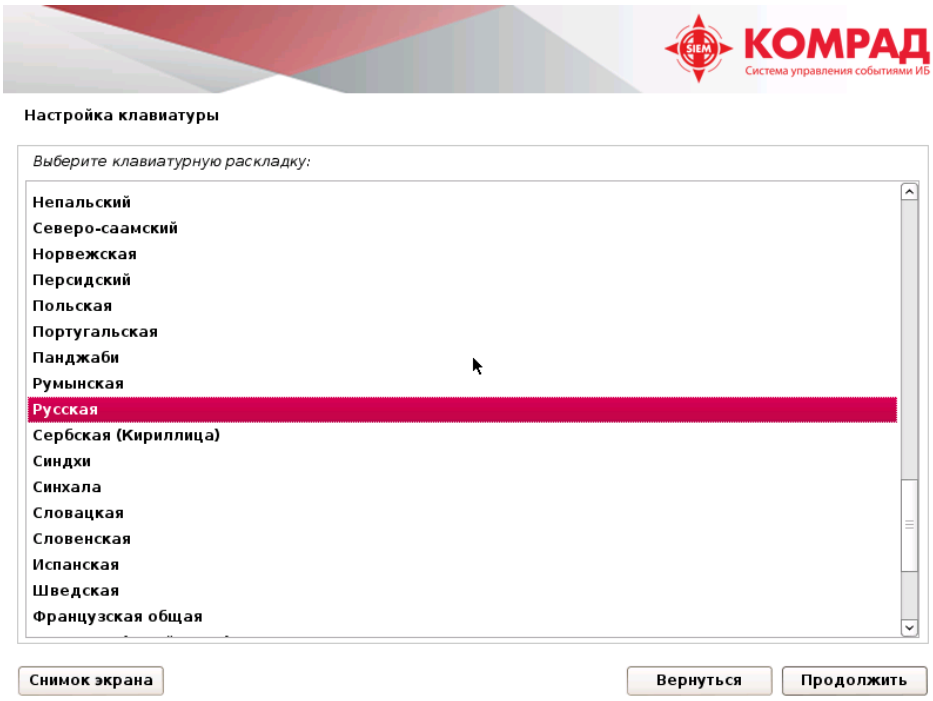



Рисунок 8 – Окно выбора раскладки клавиатуры

Рисунок 9 – Окно загрузки компонентов программы установки

3. Далее предлагается выбор IP-адреса сервера ПК «КОМРАД» (Рисунок 10), маски подсети, IP-адреса шлюза, DNS, назначение имени компьютера. Указать необходимые значения и нажать «**Продолжить**».

Рисунок 10 – Окно ввода IP-адреса сервера ПК «КОМРАД»

4. В следующем окне необходимо задать пароль суперпользователя **root**для доступа к системе по протоколу SSH (Рисунок 11) и нажать «**Продолжить»**.

Рисунок 11 – Окно ввода пароля администратора root

5. Программа установки ПК «КОМРАД» предоставляет возможность самостоятельно выделить разделы на диске. В окне, изображенном на Рисунке 12, выбрать пункт «**Вручную**», нажать «**Продолжить**»

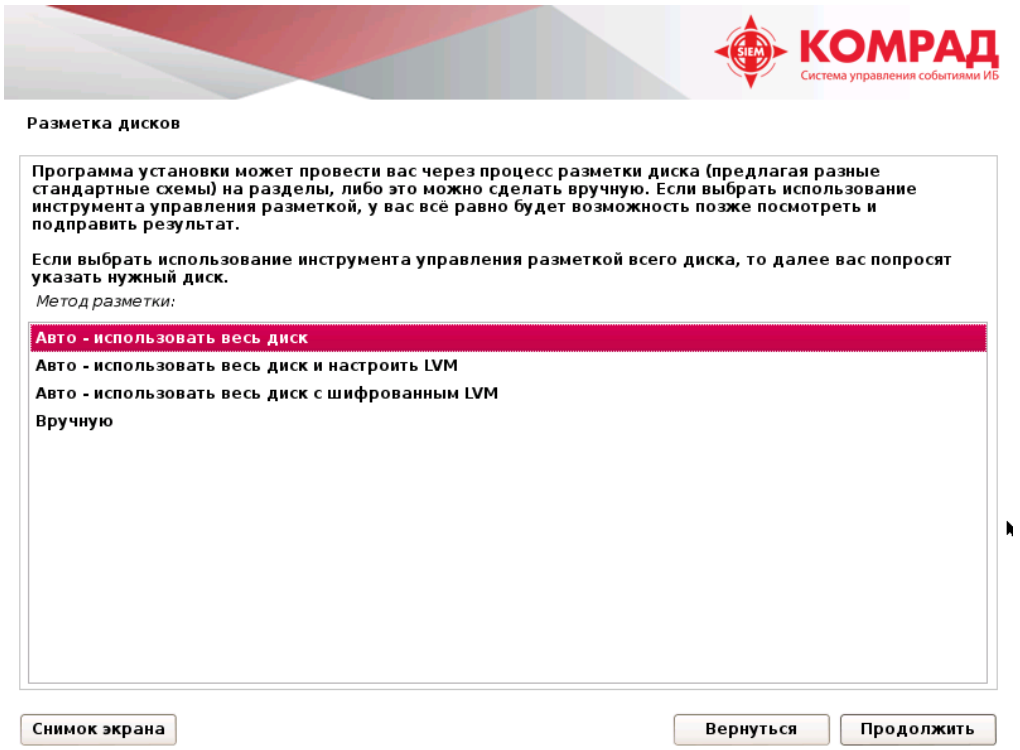



Рисунок 12 – Окно выбора способа разметки диска

**Примечание:** в приведенном списке можно выбрать метод разметки «Авто - использовать весь диск», и тогда процесс разметки будет выполнен автоматически.

6. В следующем окне (Рисунок 13) следует выбрать раздел диска для разметки, нажать «**Продолжить**».

Рисунок 13 – Окно изменения разметки дисков

7. В следующем окне (Рисунок 14) для создания новой таблицы разделов нужно выбрать пункт «**Да**», нажать «**Продолжить**».

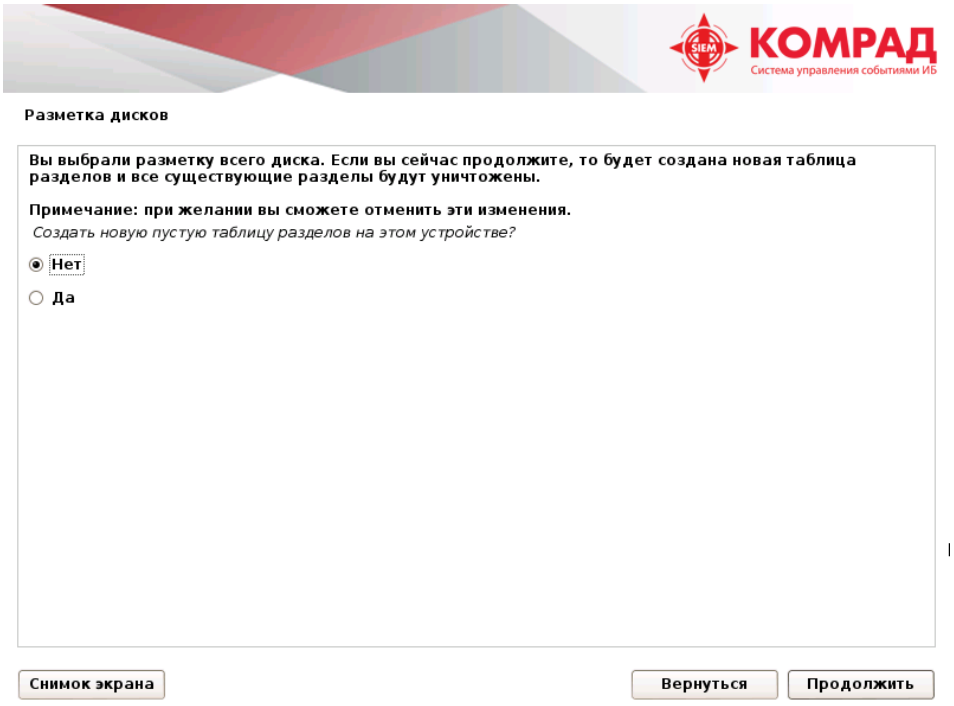



Рисунок 14– Окно изменения разметки дисков

8. Далее необходимо выбратьсвободный раздел диска (Рисунок 15).

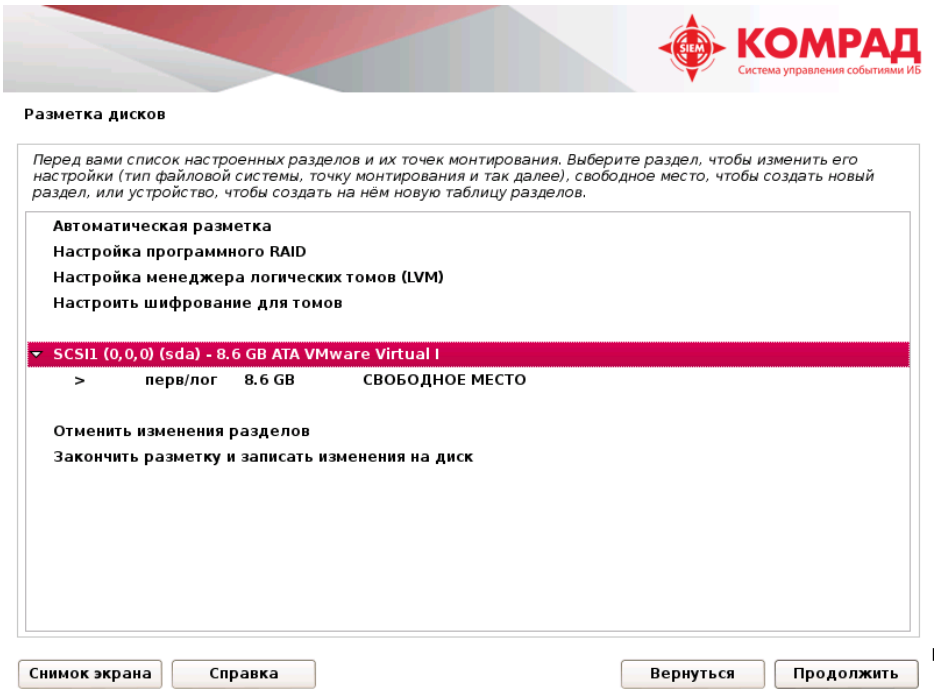



Рисунок 15 – Окно изменения разметки дисков

9. Задать размер для раздела (Рисунок 16), тип нового раздела – «Первичный» (Рисунок 17), местоположение нового раздела – «Начало» (Рисунок 18).

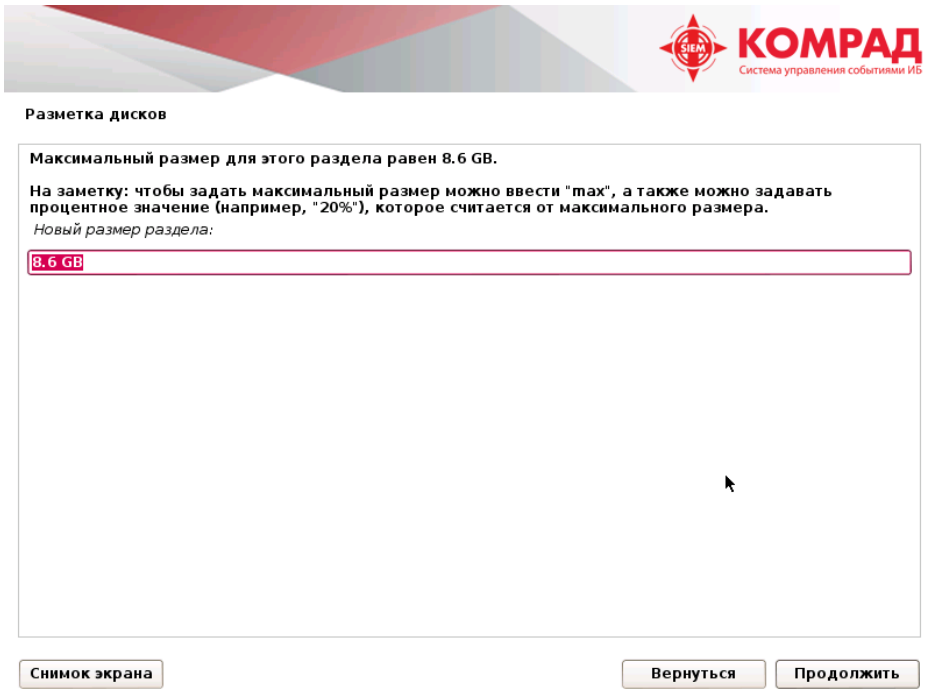



Рисунок 16 – Задание размера раздела

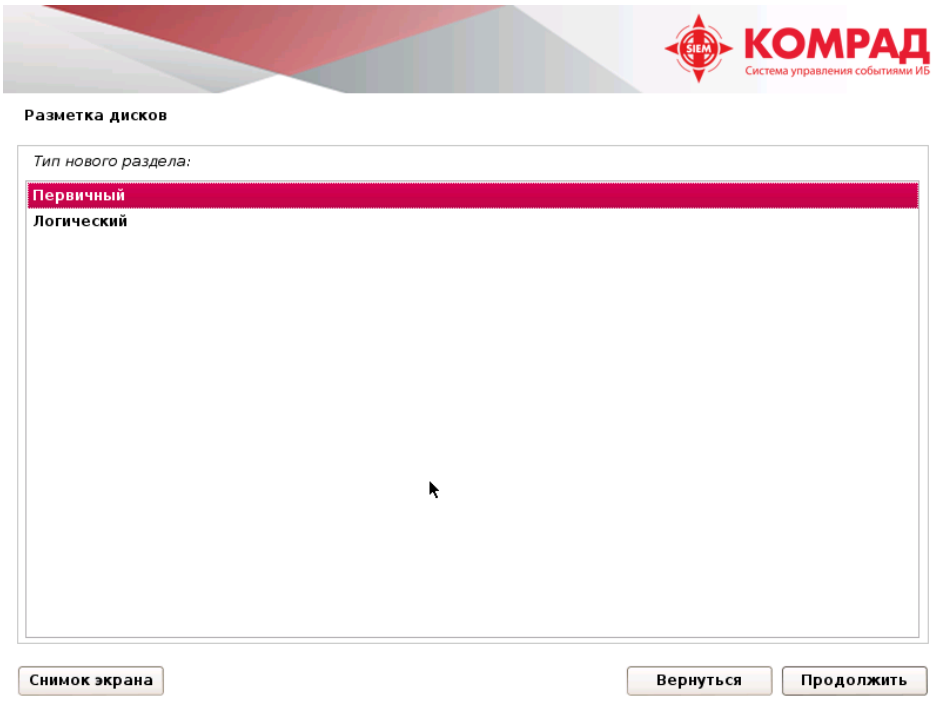



Рисунок 17 – Выбор типа раздела

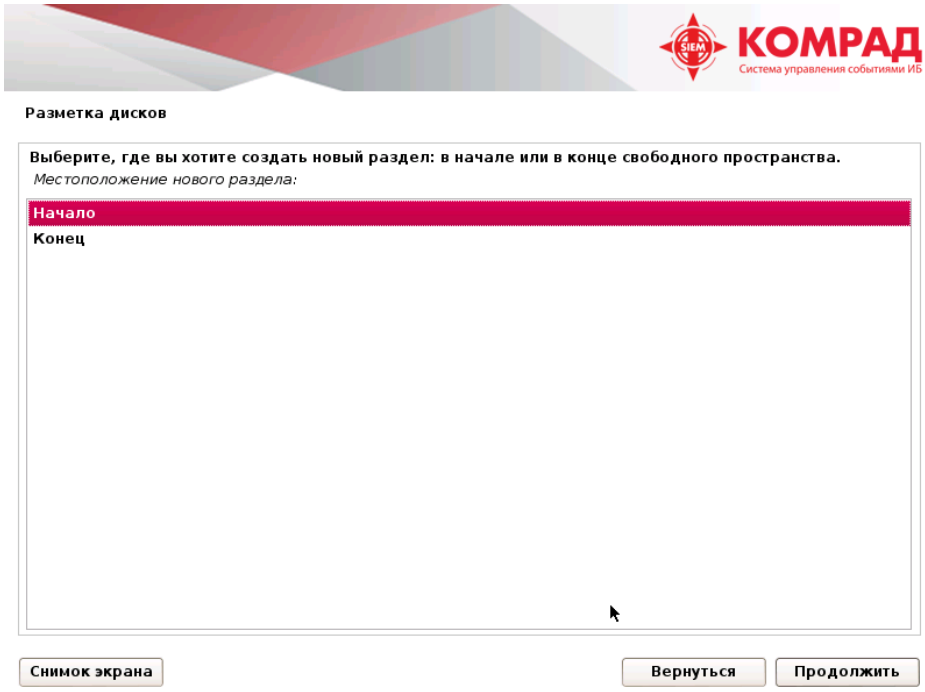



Рисунок 18 – Выбор местоположения нового раздела

10. Далее необходимо изменить точку монтирования для разделов диска (Рисунок 19).

Рисунок 19 – Изменение параметров разметки

Точку монтирования можно выбрать из списка или ввести вручную (Рисунок 20).

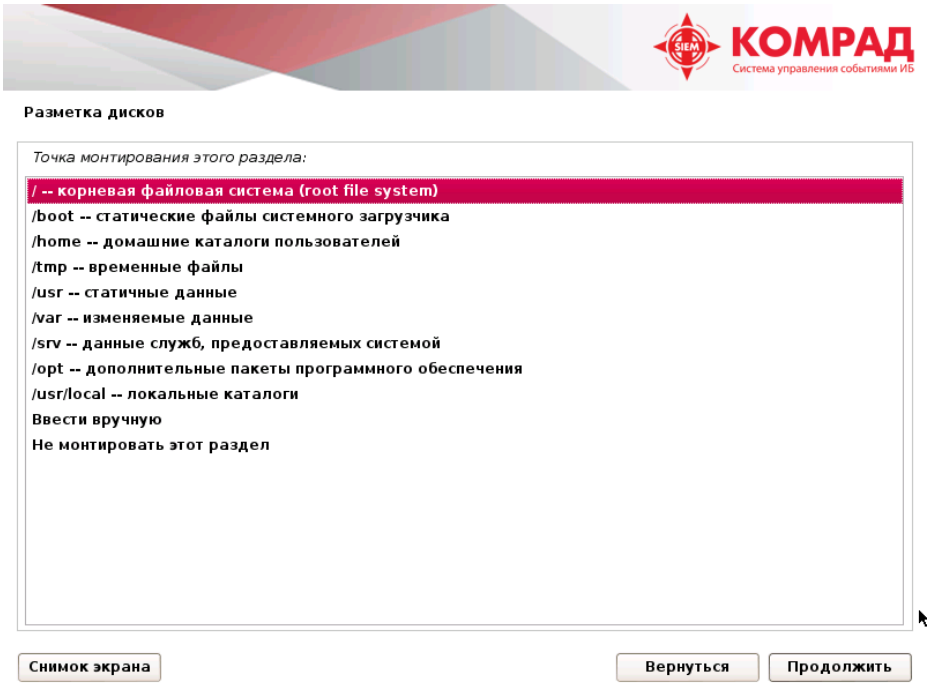



Рисунок 20 – Выбор точки монтирования

Для повышения эффективности работы системы, для обеспечения безопасности обрабатываемых данных, а также в целях снижения рисков нарушения режима

нормального функционирования системы, рекомендуются следующие параметры разбиения диска:

| Точка монтирования | Размер | Файловая система |
|---|---|---|
| / | 10-20% (но не менее 10Гб) | ext4 |
| /var | 10-40% (но не менее 10Гб) | ext4 |
| /var/lib/mysql | 40-80% | ext4 |

После внесения изменений окно разметки дисков должно выглядеть так, как показано на Рисунке 21. Нажать «**Продолжить**».

Рисунок 21 – Настройка разделов диска

11. В следующем окне выбрать «**Нет**» (Рисунок 22), так как раздел подкачки (swap) не требуется.

Рисунок 22 – Окно подтверждения отказа от выбора раздела подкачки

12. Если вся информация о разметки дисков введена верно, то в следующем окне выбрать «**Да**» для записи изменений на диск (Рисунок 23).

Рисунок 23 – Окно подтверждения записи изменений на диск

13. После этого продолжится установка базовой системы (Рисунок 24)

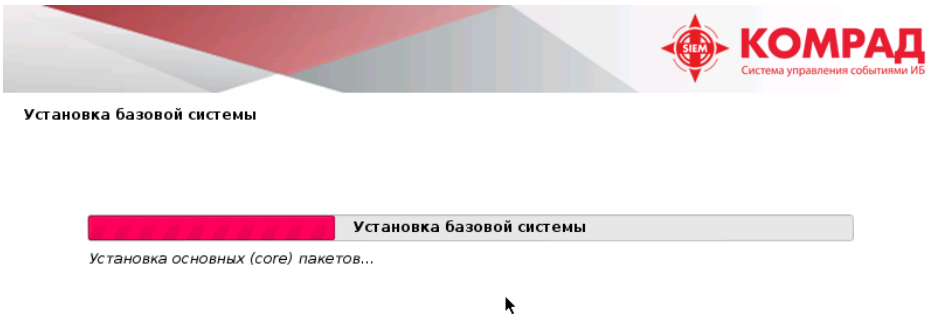



Рисунок 24 – Установка базовой системы

14. По окончании установки система автоматически перезагружается. После перезагрузки необходимо вставить ключ, входящий в комплект поставки, в USB-порт сервера.

15. В случае успешной установки появится экран загрузки системы (Рисунок 25).

Рисунок 25 – Окно загрузки системы

16. После загрузки системы появится окно (Рисунок 26), где необходимо ввести логин **root** и пароль администратора.

Рисунок 26– Окно входа в систему

17. После загрузки следует настроить пользователя веб-интерфейса. Для этого необходимо, используя браузер, войти в веб-интерфейс ПК «КОМРАД». На

открывшейся странице ввести учетные данные администратора ПК «КОМРАД» (Рисунок 27). Вводится имя пользователя, пароль, адрес электронной почты, название компании и географическое местоположение.

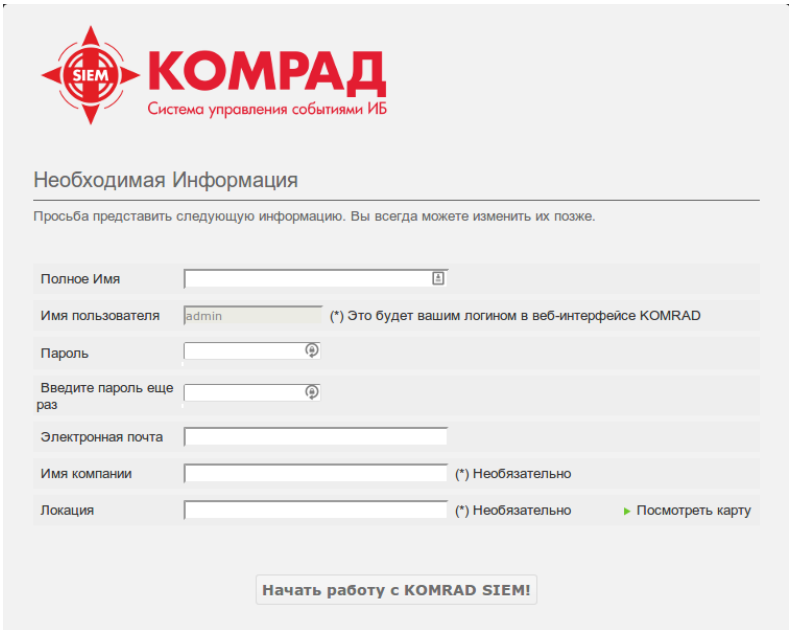



Рисунок 27 – Первичная настройка ПК «КОМРАД»

## 3.3. Этапы внедрения ПК «КОМРАД»

Внедрение ПК «КОМРАД» можно разбить на несколько этапов:

- обследование источников событий (проведение мероприятий по классификации всех компонентов которые будут источниками событий для SIEM-системы, а также выявление методов передачи данных в SIEM-систему. На этом этапе происходит построение списка узлов и СЗИ с подробным перечислением версий продуктов и определения протоколов, по которым события безопасности будут поступать в SIEM-систему. Строится матрица протоколов обмена информации для настройки межсетевых экранов в инфраструктуре ИС.);
- формирование списка узлов для сбора событий ИБ (на основе списка узлов сформированного на предыдущем этапе заполняется база активов сети);
- настройка источников событий (производится настройка самих источников для передачи данных на ПК «КОМРАД», производится установка и настройка агентов или собственных средств передачи событий, открывается доступ к БД событий или средствам удаленного администрирования — WMI, SNMP);

- настройка мониторинга доступности узлов и сервисов (проводится настройка мониторинга доступности узлов и сервисов на них);
- настройка ПК «КОМРАД» на сбор событий безопасности (настраиваются необходимые конфигурационные файлы — rsyslog, logrotate, wmi, smtp-walker, сервис управления агентами, и т.д.);
- подключение плагинов (подключаются необходимые для работы с источниками (или группами источников) плагины);
- анализ поступающих событий (производится анализ для выявления значимых или незначимых событий безопасности);
- настройка фильтров (по результатам анализа на предыдущем этапе производится настройка фильтров для уменьшения количества событий и «отсечения» незначимых событий);
- анализ производительности после применения фильтров и настроек (анализ производительности производится для принятия решения по масштабированию системы или для добавления фильтров, ограничивающих поступление незначимых событий);
- настройка директив корреляции (на основании выявленных значимых событий безопасности, а также имеющихся на предприятии регламентов и моделей угроз и нарушителя формируются директивы корреляции);
- настройка политик и действий (настраиваются политики и действия, сопровождающие выявление инцидентов безопасности, например, оповещение ответственных лиц или заведение задачи в системе разрешения инцидентов);
- формирование рекомендаций по реакции на инцидент;
- наполнение Базы знаний;
- построение схем сети и отчётов (на основании аналитических данных и результатов предыдущих этапов строятся графические схемы сети, настраиваются виджеты и отчёты).

# 4. ПРЕДВАРИТЕЛЬНАЯ НАСТРОЙКАПРОГРАММНОГО КОМПЛЕКСА

## 4.1. Настройка модулей ПК «КОМРАД»

### 4.1.1. Настройка плагинов ПК «КОМРАД»

Для настройки плагинов необходимо подключиться к ПК «КОМРАД» через интерфейс командной строки (непосредственно на сервер или по протоколу SSH) или запустить в интерфейсе командной строки программное обеспечениеПК «КОМРАД» для настройки ядра ПК «КОМРАД» командой:

*# komrad-setup*

Для настройки плагина следует выбрать в отображающемся меню пункт **«1 Конфигурация Сенсора» →«4 Выбор плагинов источников событий»** и в появившемся окне выбрать настраиваемый плагин (Рисунок 28). Выбор плагина (подключение) осуществляется нажатием пробела.

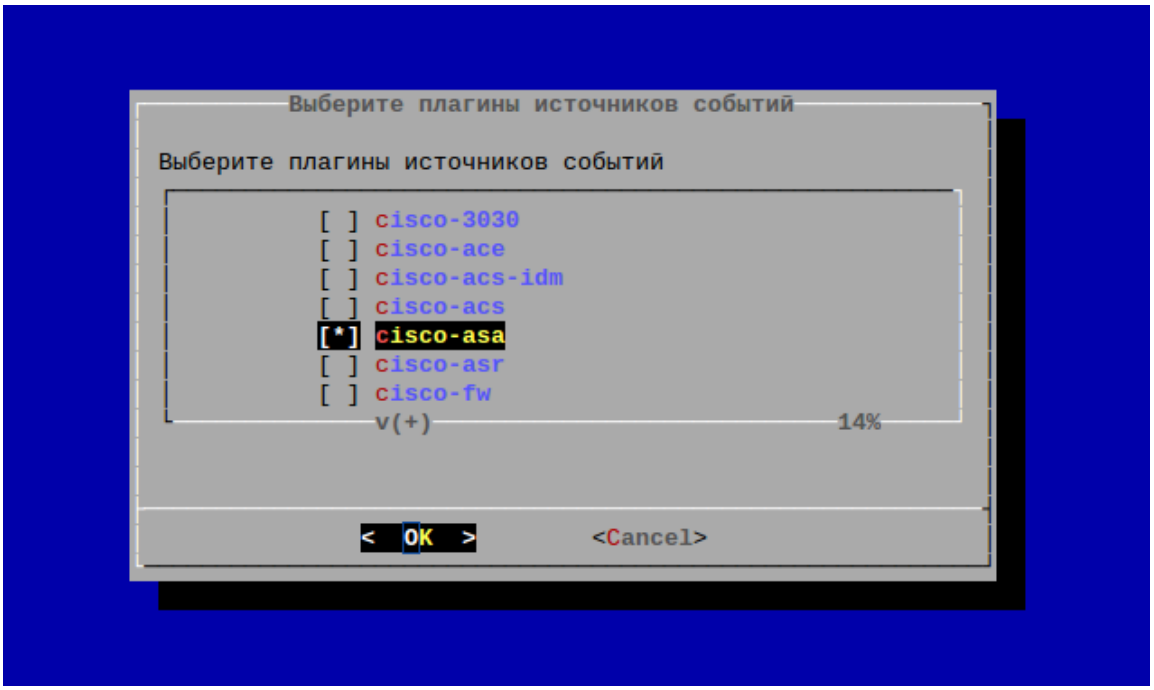



Рисунок 28 – Выбор плагина cisco-asa

**Примечание**: для ускорения поиска необходимого плагина можно нажать на клавишу начальной буквы его названия.

После выбора всех плагинов необходимо в начальном окне выбрать пункт **«5 Сохранить изменения»** и нажать **<Yes>** (Рисунок 29).

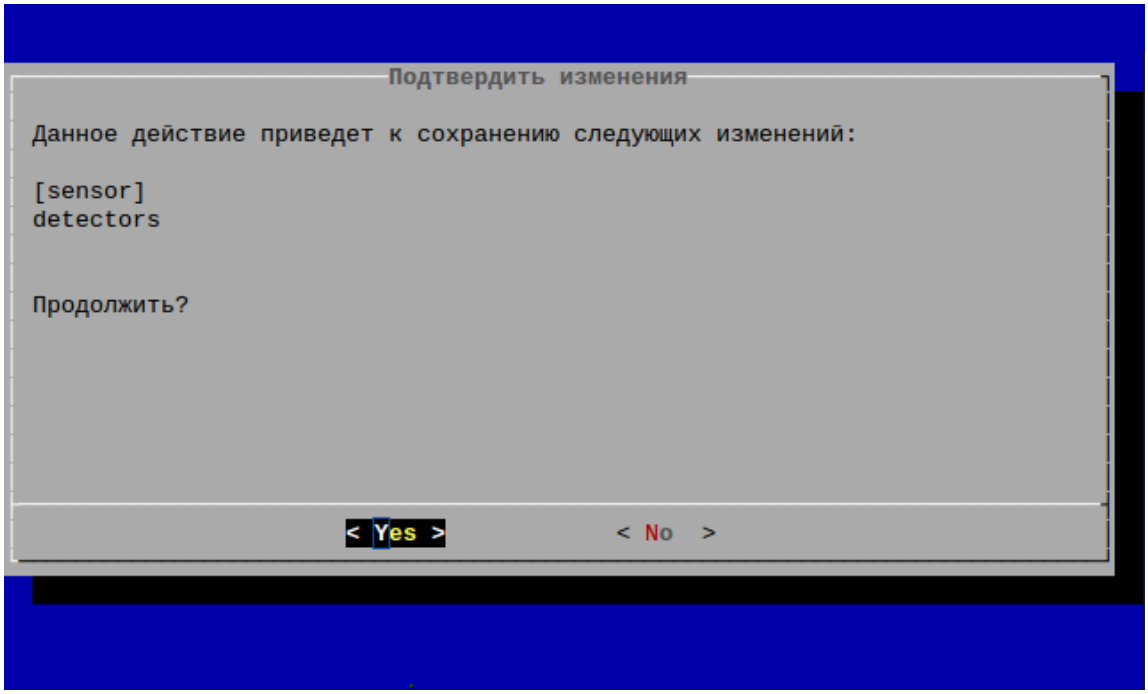



Рисунок 29 – Окно сохранения выбранных плагинов

## 4.2. Настройка источников событий

Для основных типов источников событий подробное описание настроек средств сбора и передачи информации приведено в Приложении Б.

### 4.2.1. Настройка мониторинга доступности для источников событий

Дополнительная настройка в веб-интерфейсе требуется для настройки мониторинга доступности (Рисунок 30).

Для этого необходимо в веб-интерфейсе ПК «КОМРАД» перейти на вкладку «**Средства → Средства**» и в разделе**«Хосты»** убедиться в том, что для всех соответствующих хостов стоит значок ✔ в столбце **Nagios**(мониторинг подключен автоматически).

**Примечание:** механизм добавления источников событий описан в разделе 5.2.8. настоящего руководства.

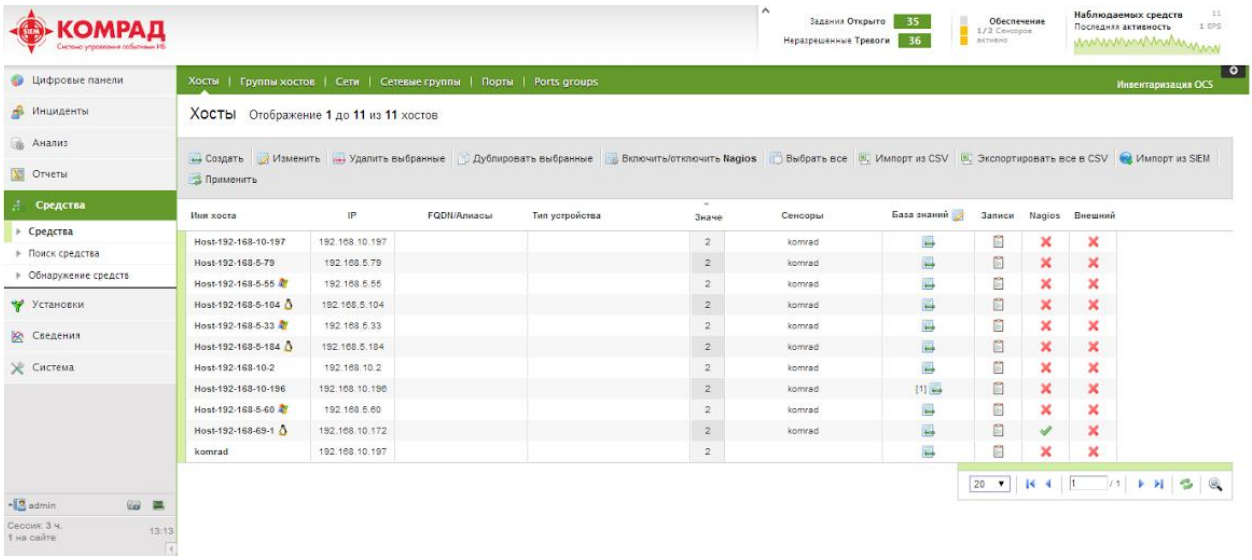



Рисунок 30 – Мониторинг доступности OSSEC-агентов

Для включения мониторинга доступности вручную (если стоит значок ) необходимо выбрать соответствующий объект и в его свойствах поставить галочку в пункте **«Включить nagios»** в подменю «Расширенный вид» → «Варианты сканирования».

В случае отсутствия средства в данном списке следует добавить его вручную. Для этого нажать на кнопку **«Создать»** и в открывшемся окне (Рисунок 31) выбрать подменю «Расширенный вид» (Рисунок 32).

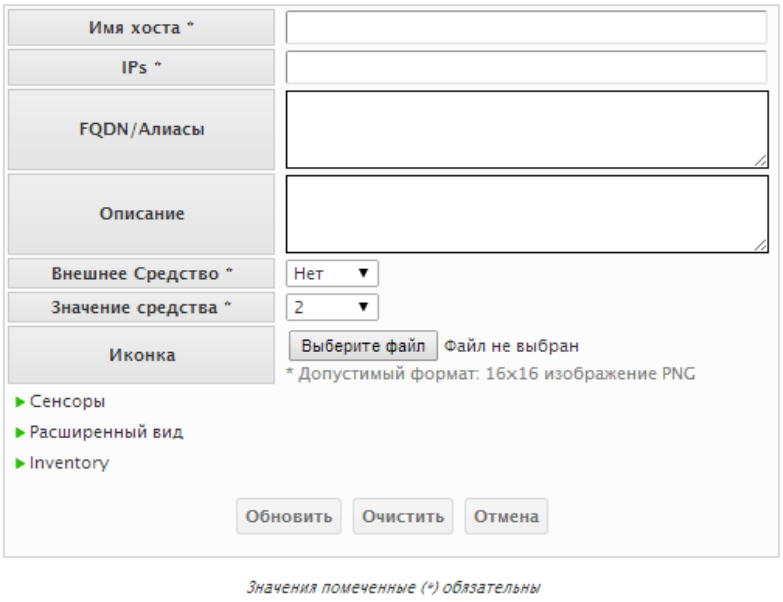



Рисунок 31 – Создание нового хоста

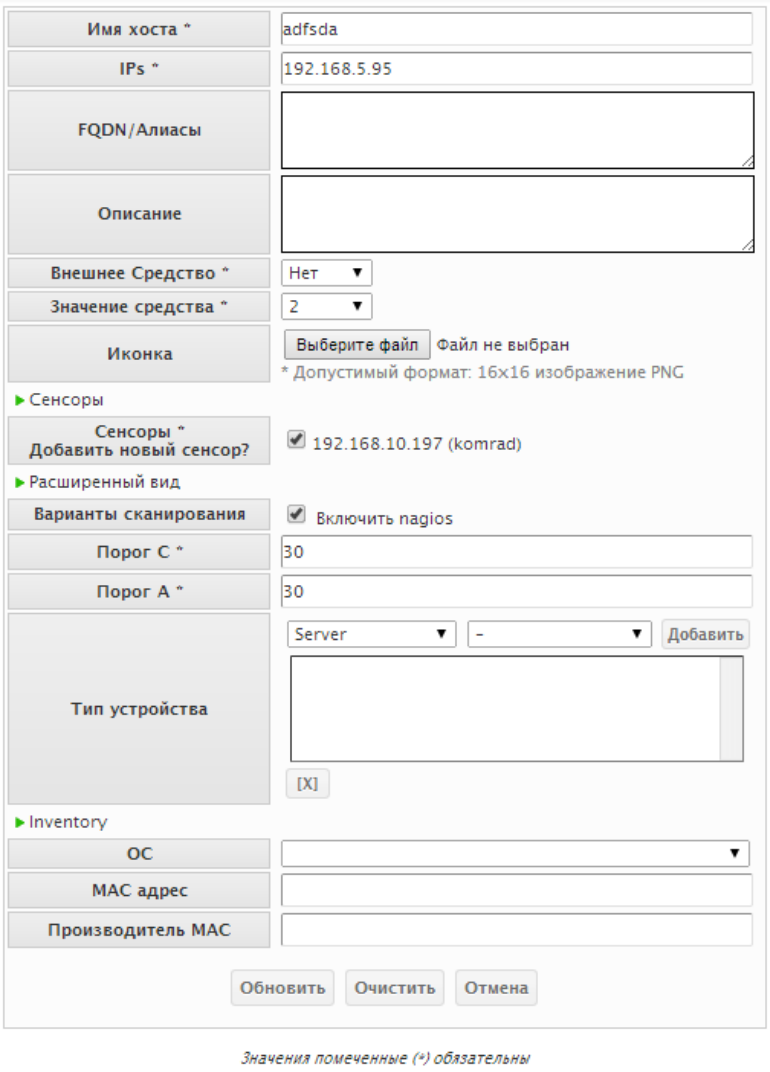



Рисунок 32– Расширенный вид окна «Создание нового хоста»

В расширенном окне необходимо ввести основные данные и поставить галочку в пункте **«Включить nagios»**.

Перейти на вкладку **«Сведения→ Доступность»** и убедиться, что поле хоста подсвечено зеленым цветом (Рисунок 33) (время обновления составляет около 1 минуты). Если поле подсвечено красным цветом, это свидетельствует о недоступности хоста (Рисунок 34).

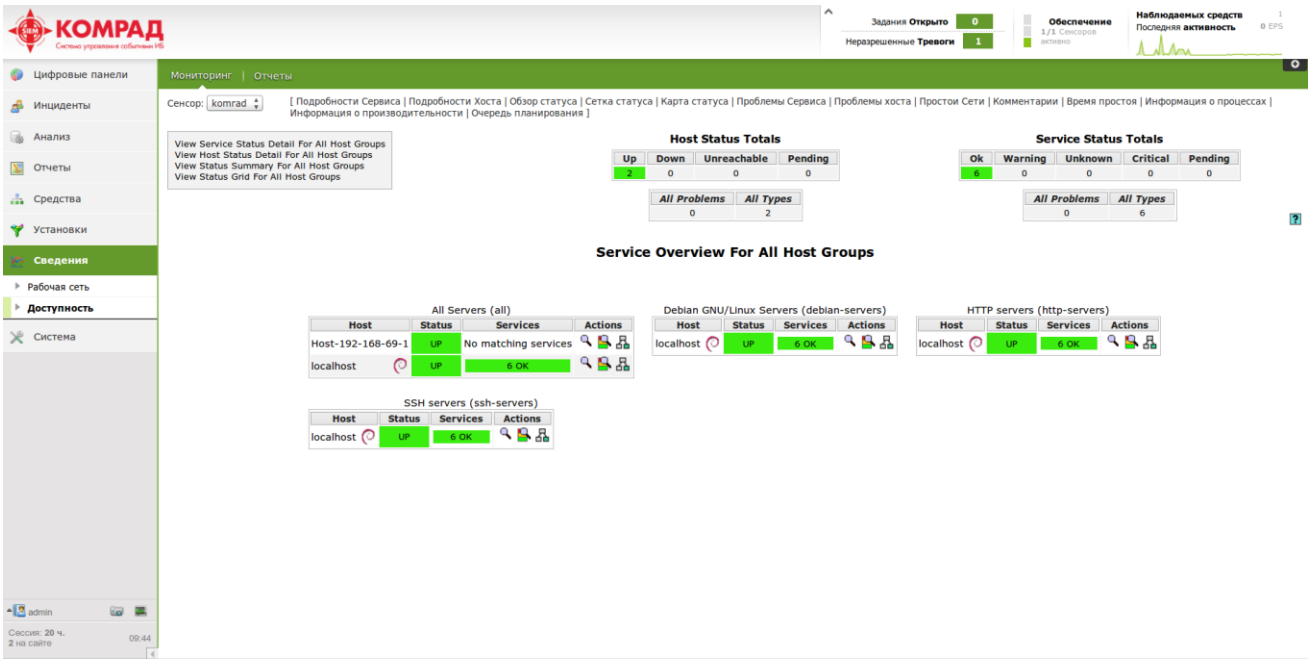



Рисунок 33– Сведения о доступности хоста

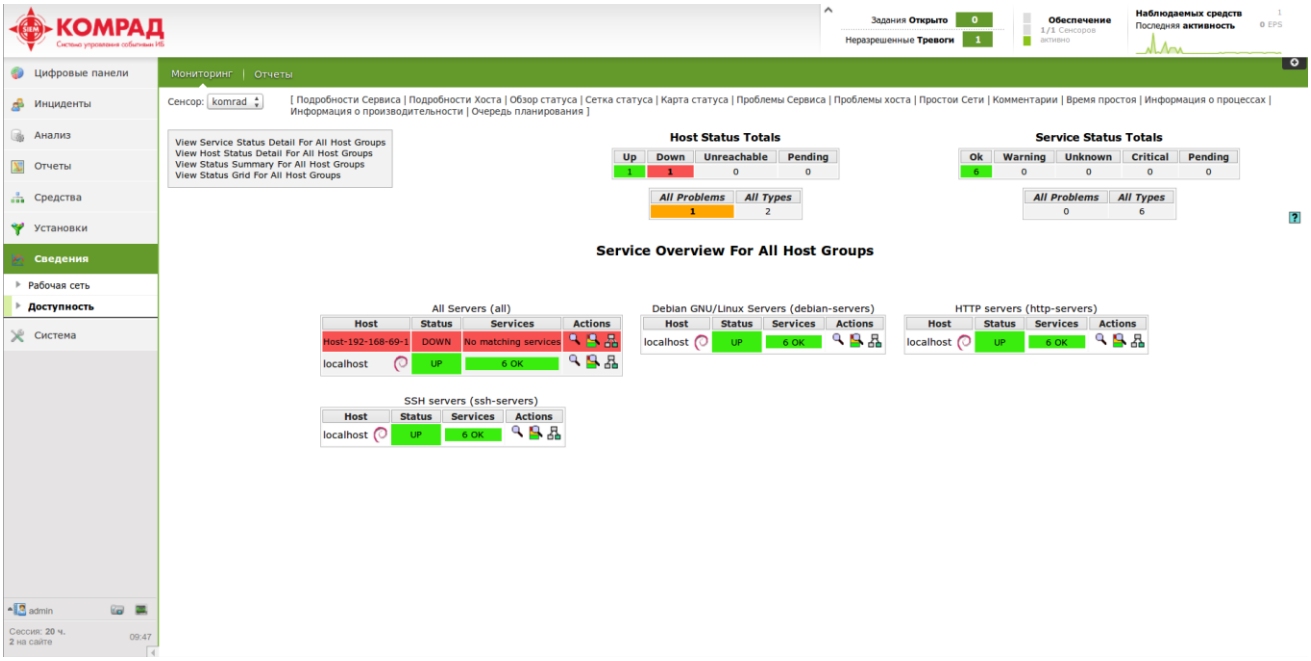



Рисунок 34– Сведения о недоступности хоста

Средства могут быть сгруппированы по признакам, например, автоматически формируются группы средств, входящих в одну IP-подсеть. Средства могут быть объединены в группу для удобства разграничения доступа пользователей к информации о них, а также для удобства написания директив корреляции.

### 4.2.2. Проверка настройки агентов UNIX-систем и устройств

Штатную работу агентовUNIX-систем и устройств можно проверить во вкладке **«Анализ → Обнаружение → «Агенты»** (Рисунок 35).

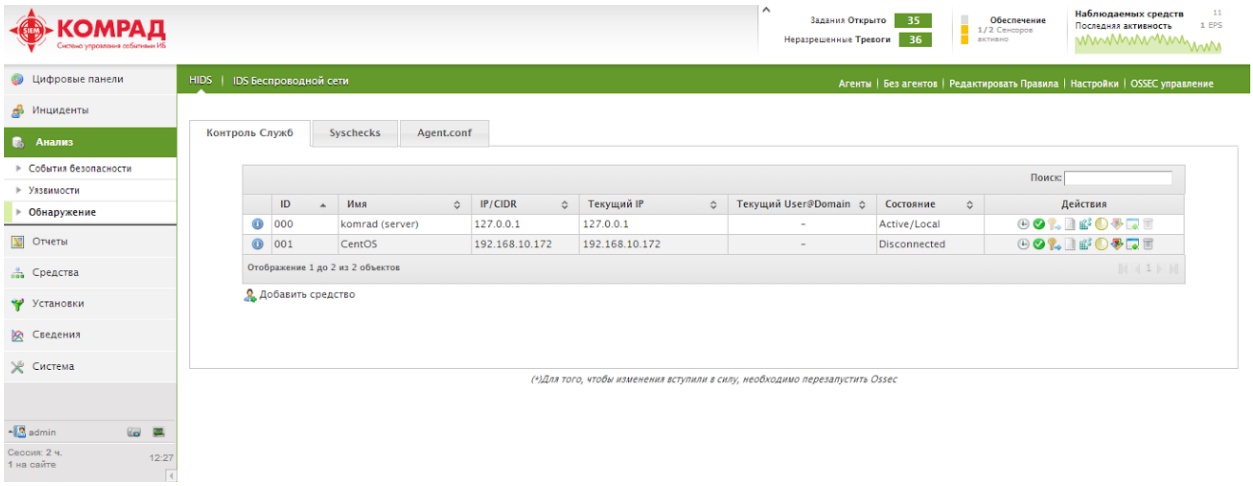



Рисунок 35– Список обнаруженных агентов системы

Можно получить справку, наведя указатель на знак (Рисунок 36).

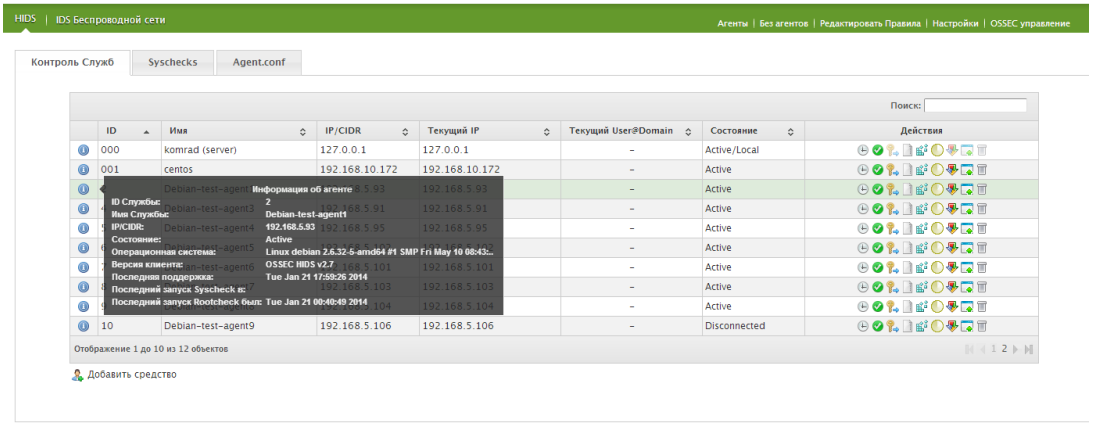



Рисунок 36 – Справочные данные обнаруженного устройства

## 4.3. Настройка сбора данных из журналов с помощью rsyslog

Для настройки источника событий на передачу данных о событиях ИБ из журналов состояния необходимо создать файл **/etc/rsyslog.d/ossim.conf**:

*.* *@192.168.71.8:514*

где 192.168.71.8 — адрес OSSIM-сервера, а *.* — название логов (журналов), которые необходимо отправлять в ядро ПК «КОМРАД» (в данном случае все).

После этого следует перезапустить rsyslog:

*/etc/init.d/rsyslogrestart*

**Примечание**: при необходимостипроверки можно воспользоваться командой logger:

*$ logger«test»*

Результатом будет запись в журнал syslog строки содержащей слово *«test»*.

Необходимо настроитьrsyslog для соответствующих плагинов. Для этого следует перейти во вкладку «**Средства →Средства→ Редактор правил Rsyslog**» в веб интерфейсе ПК «КОМРАД» (Рисунок 37).

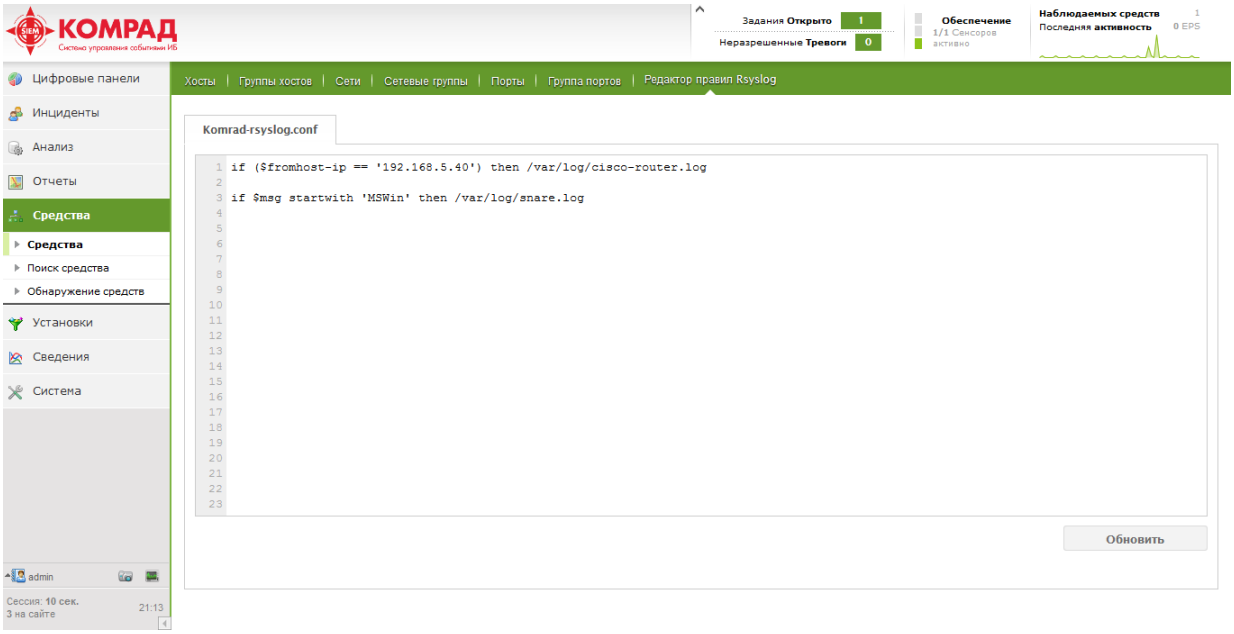



Рисунок 37 – Окно редактора правил Rsyslog

1) В открывшемся окне с помощью языка RainerScript описать правило сортировки сообщений, например:
   а) запись всех syslog-сообщений с хоста 192.168.5.40 в файл /var/log/cisco-router.log:

if ($fromhost-ip == '192.168.5.40') then /var/log/cisco-router.log

   б) запись всех сообщений, содержащих подстроку «MSWin» (для сбора в один файл логов со всех хостов под управлением Windows), в файл /var/log/snare.log:

if $msg startwith 'MSWin' then /var/log/snare.log

2) Нажать кнопку «**Обновить**»

**Примечание**: пути к файлам журналовдля соответствующих плагинов приведены в Приложении В.

# 5. РАБОТА С ПРОГРАММНЫМ КОМПЛЕКСОМ

## 5.1. Обзор доступных интерфейсов

### 5.1.1. Интерфейс командной строки

Интерфейс командной строки предназначен для обеспечения администратора функциями управления системой и предоставления данных об ошибках и сбоях компонентов ПК «КОМРАД».

Для работы с программным комплексом в интерфейсе командной строки необходимо авторизоваться на сервере ПК «КОМРАД» пользователем **root** с паролем, указанным при установке.

Работа с интерфейсом командной строки также доступна по протоколу SSHпо заданному в процессе установки IP-адресу сервера ПК «КОМРАД».

На начальном экране (Рисунок 38) отображаются доступные действия с ПК «КОМРАД» среди которых:

**0Настройки системы**—основные настройки программного комплекса;

**1Конфигурация Сенсора** —меню настройки плагинов;

**2Обслуживание**— меню обслуживания системы, которое включает следующие возможности:

- восстановление базы данных ядра ПК «КОМРАД»;
- сброс пароля доступа к веб-интерфейсу;
- сброс пароля администратора **root**для доступа к системе по SSH;
- перезагрузка сервера ПК «КОМРАД»;
- выключение сервера ПК «КОМРАД»;
- перезапуск ключевых служб сервера.

**3 Средства**— основные средства программного комплекса, среди которых:

- просмотр журналов (как системы, так и отдельных служб);
- утилита htop, отображающая в реальном времени нагрузку на сервер ПК «КОМРАД» и список запущенных процессов;

- утилита netstart, отображающая список активных на момент её запуска сетевых подключений;
- утилита bwm-ng, учитывающая объём трафика на интерфейсах.

**4О системе**— информация о системе;

**5Сохранить изменения**— сохранение внесённых изменений.

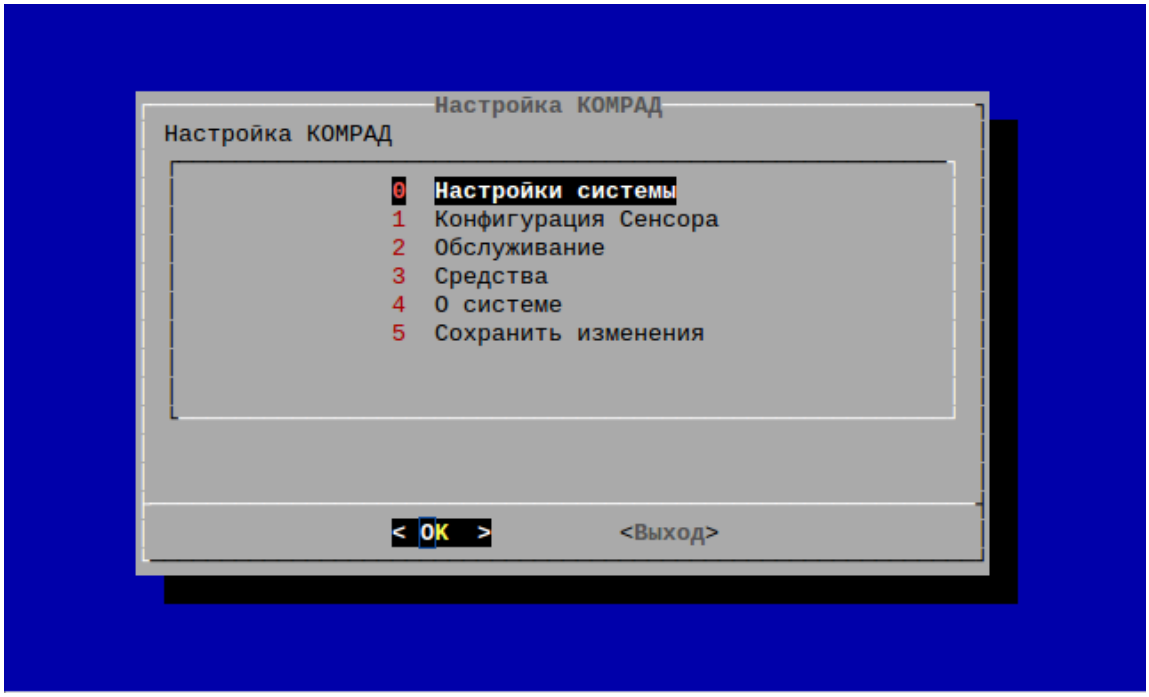



Рисунок 38 – Начальный экран средства настройки ядра ПК «КОМРАД»

Далее представлена подробная структура меню интерфейса командной строки ПК «КОМРАД».

**0. Настройки системы**

**0. Конфигурация сети**

**0. Настройка сетевого интерфейса** (позволяет выбрать основной сетевой интерфейс и указать для него IP-адрес, шлюз и маску подсети).

**1. Сервер службы DNS** (позволяет указать IP-адрес сервера DNS для обеспечения разрешения доменных имён).

**2. KOMRAD Firewall** (включить/выключить собственный межсетевой экран; по умолчанию выключен).

**3. Настройка прокси-сервера** (позволяет настроить подключение к прокси-серверу, если это необходимо).

**4. Сетевой домен** (имя домена, в который помещена машина с ПК «КОМРАД»; не является обязательной настройкой).

**5. Конфигурация VPN** (позволяет настроить сервер VPN, если это необходимо).

**1. Настройка почтового ретранслятора (mail relay)** (позволяет настроить собственного агента почтового ретранслятора для функционирования E-mail оповещений. По умолчанию отключён. При включении необходимо указать: адрес почтового сервера, имя пользователя, пароль, порт SMTP; данные параметры следует уточнять у администратора почтового сервера).

**2. Настройка локализации**

**0. Конфигурация раскладок клавиатуры** (запускает псевдографический интерфейс для настройки пакета console-data, который позволяет изменить настройки раскладок).

**1. Дата и время**

**0. Настройка часового пояса** (запускает псевдографический интерфейс для настройки пакета tzdata, позволяет изменить текущий часовой пояс).

**1. Установить время и дату вручную** (позволяет установить для системы текущие дату и время в формате YY-MM-DD hh:mm:ss).

**2. Конфигурация NTP-сервера** (позволяет указать IP-адрес или имя сервера NTP для получения точного времени).

**3. Настройка имени хоста** (позволяет изменить имя хоста, по умолчанию — «komrad»).

**1. Конфигурация Сенсора**

**0. Выберите интерфейс (смешанный режим)** (позволяет указать сетевой интерфейс, на который будут поступать события безопасности).

**1. Настройка IP-адреса сервера Комрад** (позволяет указать IP-адрес машины, выполняющей роль сервера ПК «КОМРАД»; актуально для сетей с несколькими экземплярами ПК «КОМРАД», используется для создания ихие-

рархии и распределения нагрузки; по умолчанию установлено значение 127.0.0.1).

**2. Настройка IP-адреса Framework Комрад** (позволяет указать IP-адрес машины, на которой функционирует служба «Framework Комрад»; актуально для сетей с несколькими экземплярами ПК «КОМРАД», используется для создания их иерархии и распределения нагрузки; по умолчанию установлено значение 127.0.0.1).

**3. Контролируемые сети** (позволяет указать сети, которые ПК «КОМРАД» считает «домашними»; значение параметра влияет на работу сканеров уязвимостей).

**4. Выберите плагины источников событий** (позволяет включить/отключить обработку событий с помощью плагинов, присутствующих в системе. Отметка о включении плагина ставится пробелом, поиск плагинов по начальной букве — нажатием соответствующей клавиши клавиатуры. После выбора нужных плагинов необходимо в начальном меню выбрать пункт «**Сохранить изменения**», нажать «**YES**»).

**5. Выберите источники netflow** (позволяет указать порт удалённого коллектора «netflow»; по умолчанию установлено значение «Выключено»).

**2. Обслуживание**

**0. Ремонт базы данных** (попытка восстановления повреждённых таблиц штатными средствами сервера MySQL).

**1. Сбросить пароль Администратора web-интерфейса** (указать новый пароль для учётной записи admin, используемой для полного доступа к веб-интерфейсу).

**2. Изменить пароль пользователя root** (указать новый пароль пользователя root для доступа к интерфейсу командной строки).

**3. Выполнить перезагрузку машины** (выполнить команду reboot).

**4. Выключить машину** (выполнить команду halt).

**5. Службы КОМРАД**

**0. Рестарт службы ossim-server**

**1. Рестарт службы ossim-agent**

**2. Рестарт службы ossim-framework**

**3. Рестарт службы IDM**

**4. Рестарт службы СУБД**

**6. Прочие службы**

**0. Рестарт Apache**

**1. Рестарт службы OSSEC**

**2. Рестарт службы Openvas Manager**

**3. Рестарт службы Openvas Scanner**

**4. Рестарт службы Nagios**

**5. Рестарт службы NFSEN**

**6. Рестарт службы NTOP**

**7. Рестарт службы FProbe**

**7. Обновление».**

Пакеты обновлений ПК «КОМРАД» поставляются на электронном носителе в виде файлов с расширением .deb. Для обновления ПК «КОМРАД» необходимо выполнить следующие действия.

1. Подключить носитель, содержащий пакеты обновлений (Рисунок 39), нажать<**Далее**>.

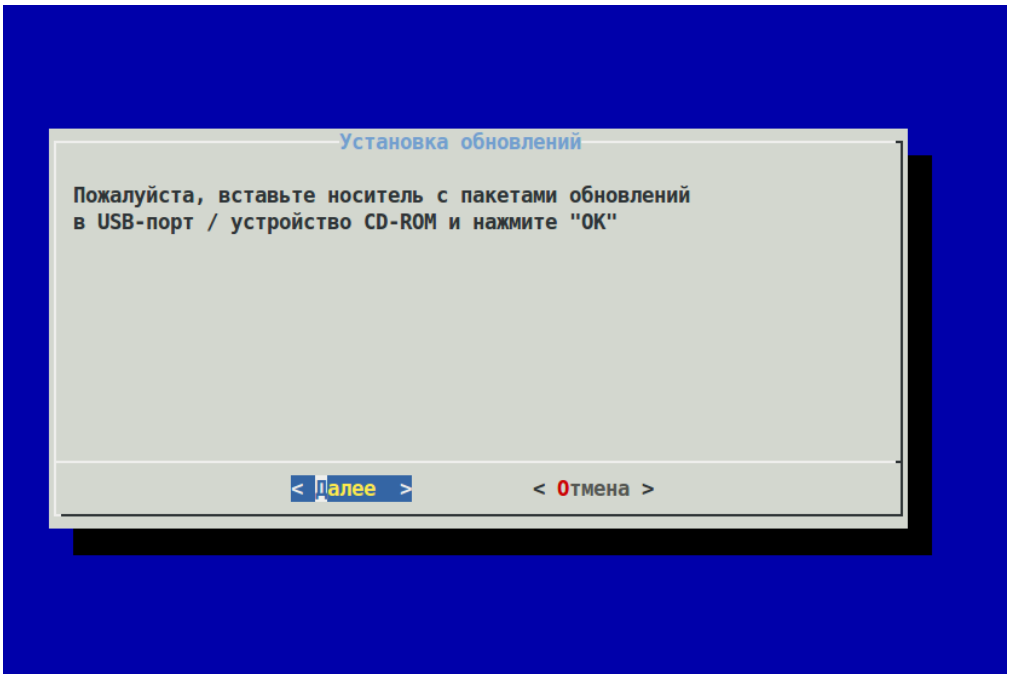



Рисунок 39 – Установка обновлений

Будет выполнен поиск носителя с пакетами обновлений (Рисунок 40) (данная процедура занимает не более 30 секунд). После того, как носитель будет обнаружен, отобразится окно, показанное на Рисунке 41.

**Примечание**: носитель с пакетами обновлений будет автоматически смонтирован в директорию /updates.

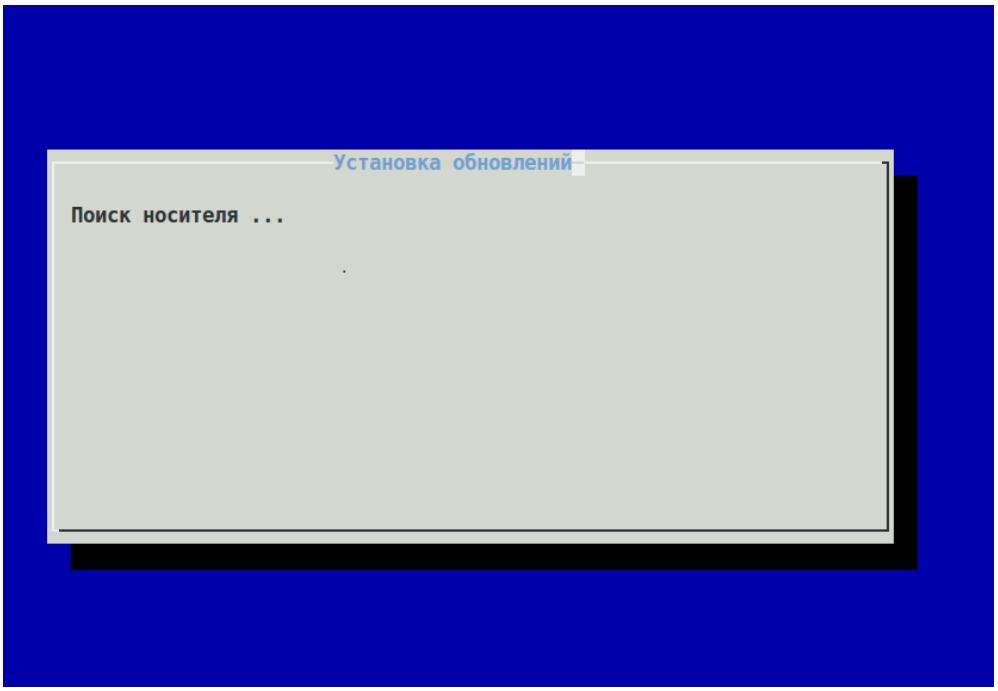



Рисунок 40 – Поиск носителя с пакетами обновлений

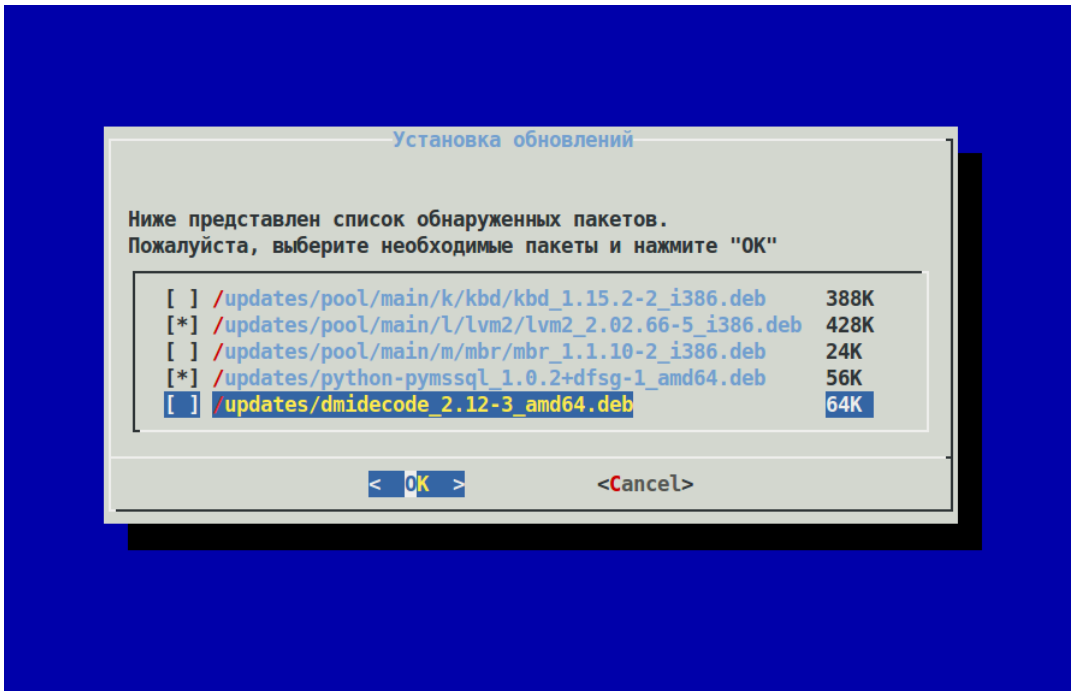



Рисунок 41 – Список пакетов обновлений

2. Из спискавсех доступных обновлений следует выбрать необходимые пакеты для установки. Выбор осуществляется нажатием клавиши «пробел», после выбора нажать <**ОК**>.

**Примечание**: установка пакетов обновлений осуществляется без гарантий удовлетворения зависимостей.

3. После того, как установка пакетов обновлений будет завершена, отобразится соответствующее уведомление (Рисунок 42). По завершении установки носитель следует извлечь.

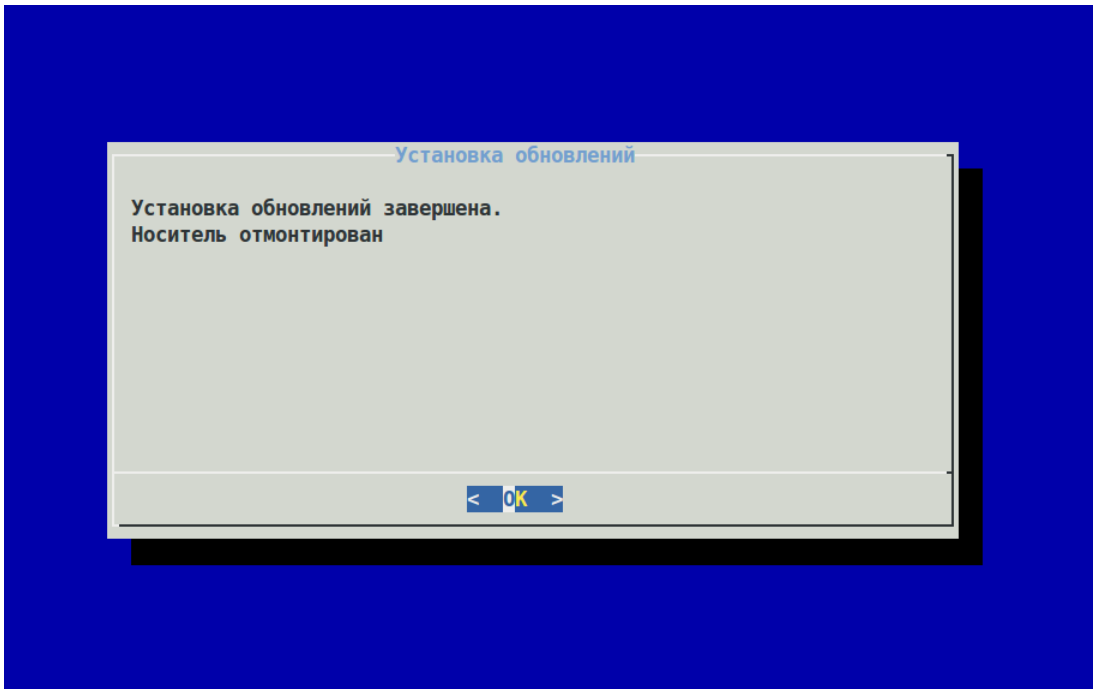



Рисунок 42 – Завершение установки обновлений

**3. Резервное копирование и восстановление**

Механизм резервного копирования и восстановления, встроенный в утилиту komrad-setup, позволяет:

- осуществлять резервное копирование и восстановление критичных для системы конфигурационных файлов (список может быть изменён);
- создавать резервные копии критичных записей в базе данных.

Для выполнения резервного копирования с помощью интерфейса командной строки необходимо из главного меню komrad-setup перейти по пунктам «**Резервное копирование и восстановление**» (Рисунок 43)→«**Резервное копирование и восстановление конфигурационных файлов**» (Рисунок 44)→ «**Создание резервной копии конфигурационных файлов**» (Рисунок 45).

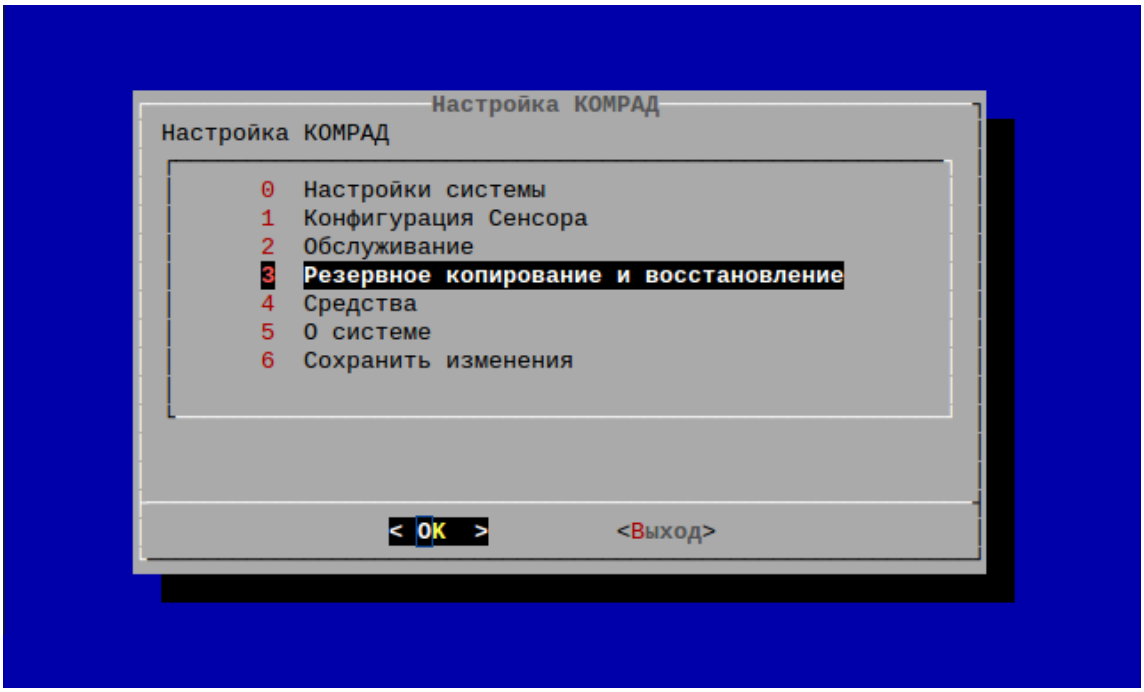



Рисунок 43 – Пункт «Резервное копирование и восстановление»

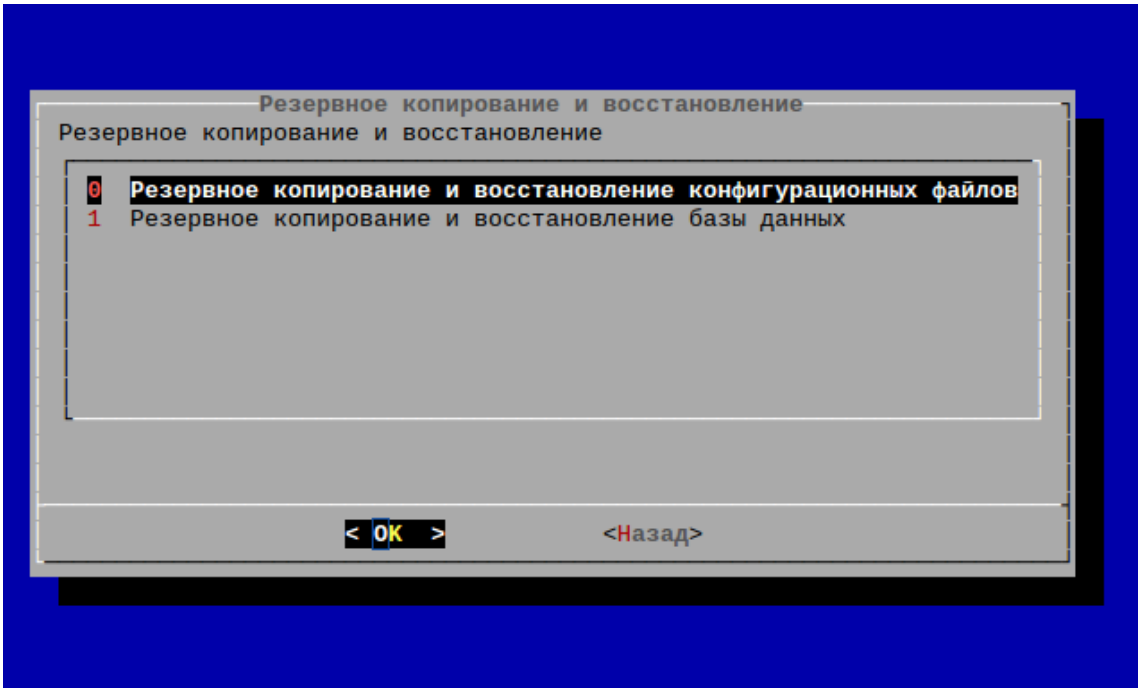



Рисунок 44– Пункт «Резервное копирование и восстановление конфигурационных файлов»

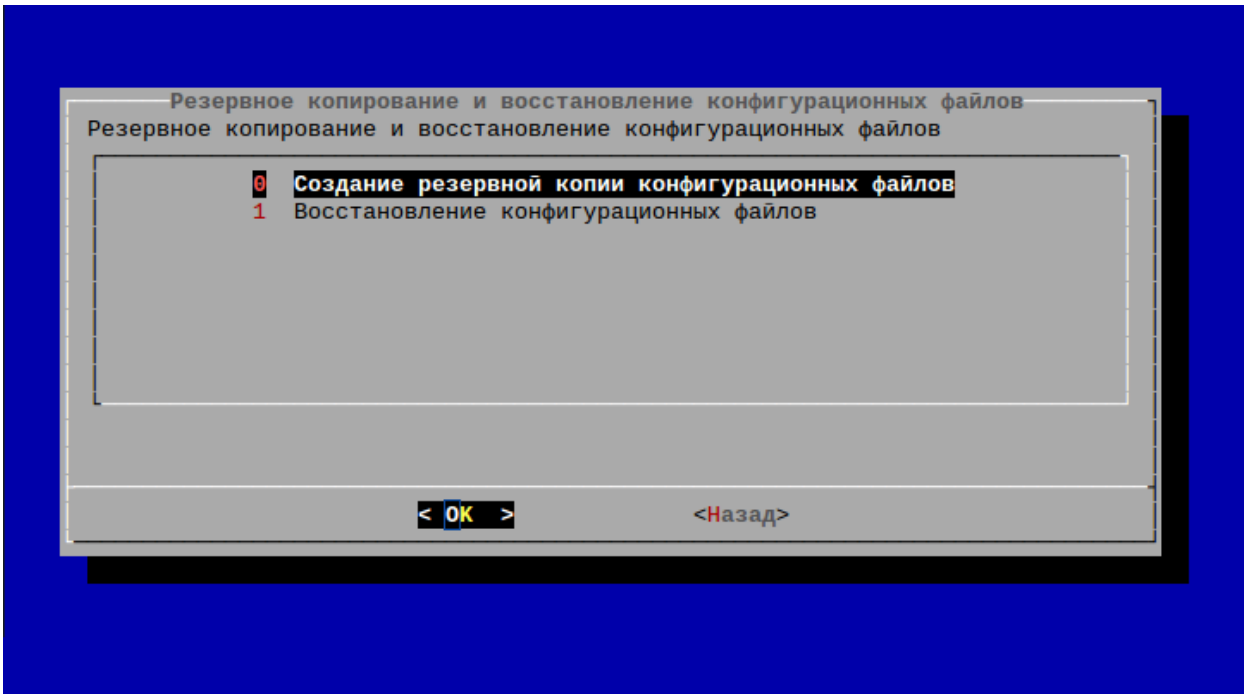



Рисунок 45 – Пункт «Создание резервной копии конфигурационных файлов»

После создания архива появится сообщение с указанием имени нового архива (Рисунок 46).

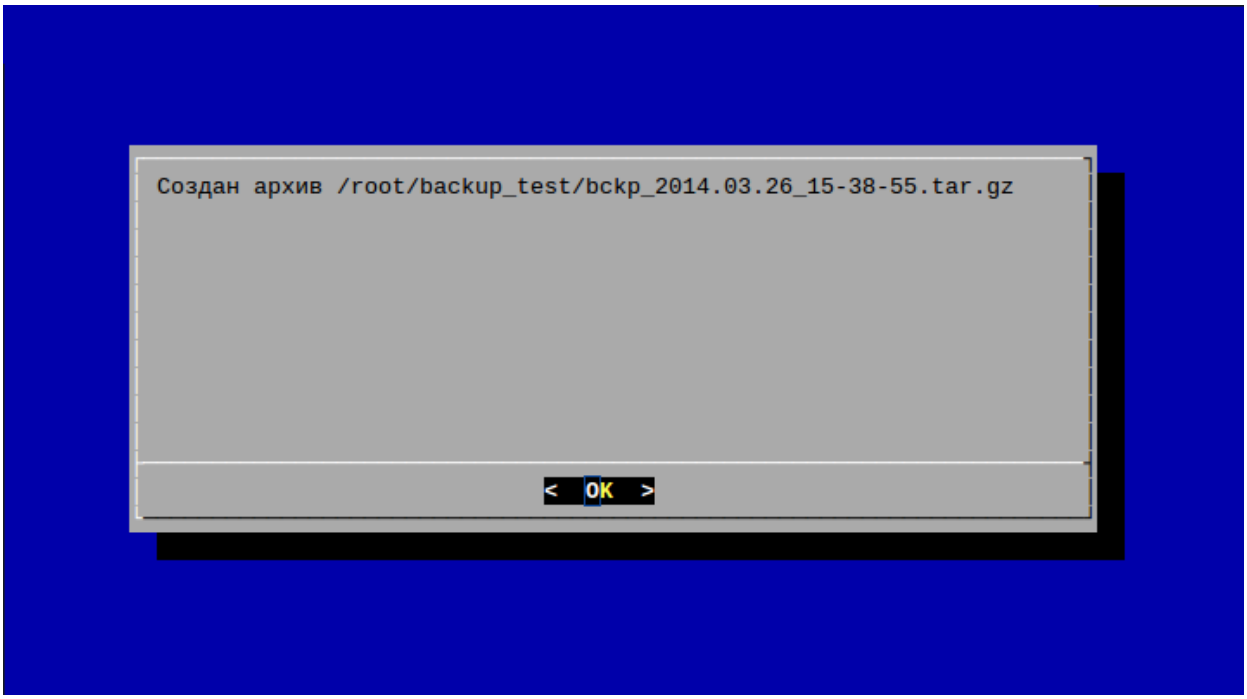



Рисунок 46 – Уведомление о создании нового архива

При этом:

- путь, по которому сохраняется архив, указан явно в тексте скрипта */usr/sbin/komrad_bckp* в значениb переменной SRC (изначально — /var/lib/ossim/backup_conf);

- список файлов и каталогов, подлежащих архивированию, содержится в переменной DIR скрипта */usr/sbin/komrad_bckp* и при необходимости может быть отредактирован.

Изначально он содержит: /var/ossec/etc, /var/ossec/rules, /etc/ossim, /etc/ossim_firewall, /etc/ossim_firewall_ipv6

Для восстановления конфигурационных файлов из архива необходимо из главного меню komrad-setupперейти в меню«**Резервное копирование и восстановление**»→«**Резервное копирование и восстановление конфигурационных файлов**»→«**Восстановление конфигурационных файлов**». Откроется диалог выбора файла (Рисунок 47, стартовый каталог соответствует указанному в переменной SRC). Файл должен быть сжат в формате *.tar.gz.

Для навигации следует использовать на клавиатуре клавиши со стрелками и «**Enter**», для выбора файла — нажать «пробел», для продолжения процедуры восстановления — нажать «**OK**» (соответствующее напоминание выводится при каждом вызове процедуры восстановления конфигурации).

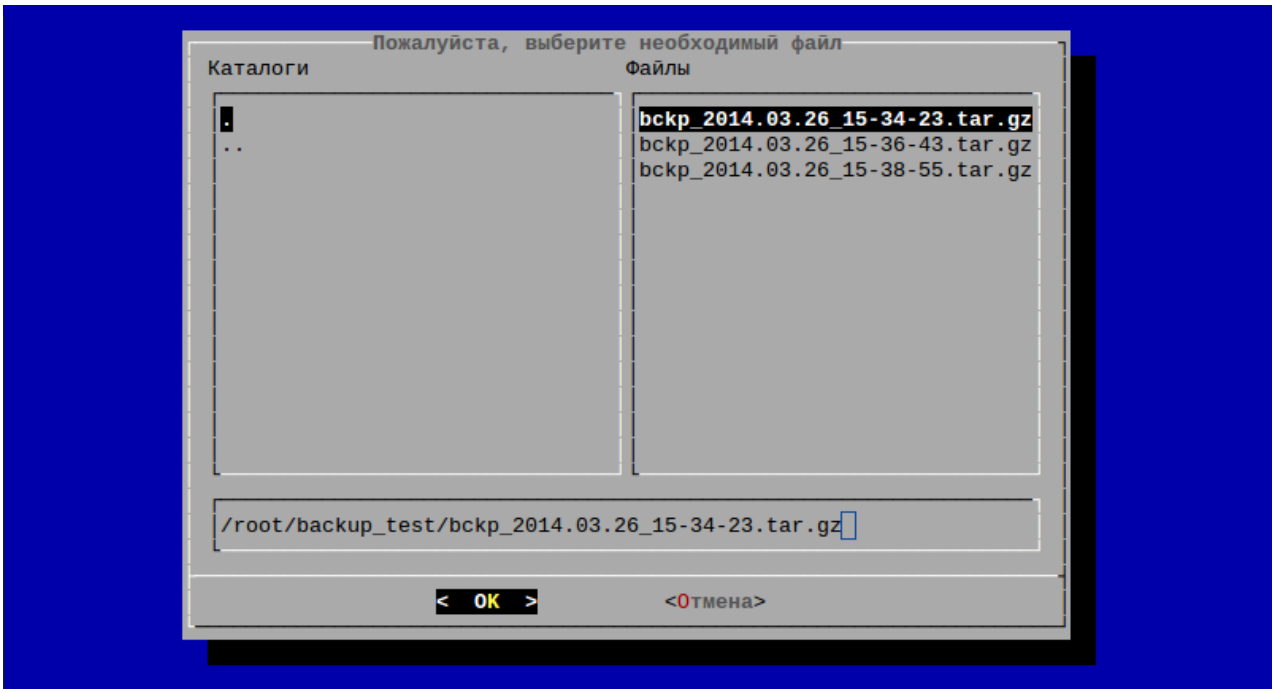



Рисунок 47 – Выбор резервной копии для восстановления

После выбора конкретного файла он распаковывается в директорию, обеспечивающую штатное функционирование системы (например, распакованный из архива каталог */var/ossec/etc*, заменит существующий каталог */var/ossec/etc* вместе со всем содержимым. Текущая конфигурация сохранена не будет (для её сохранения необходимо выполнить действия, приведённые в пункте«Создание архива с конфигурационными файлами»). После успешной распаковки сервисы перезапускаются (автоматически запускается утилита ossim-reconfig).

После этого происходит автоматический возврат к пункту меню «**Резервное копирование и восстановление**»→«**Резервное копирование и восстановление конфигурационных файлов**» утилиты komrad-setup.

Для создания резервной копии базы данных необходимо из главного меню komrad-setup перейти по пунктам «**Резервное копирование и восстановление**»→«**Резервное копирование и восстановление базы данных**»→«**Создание резервной копии базы данных**». Осуществляется резервное копирование БД (Рисунок 48).

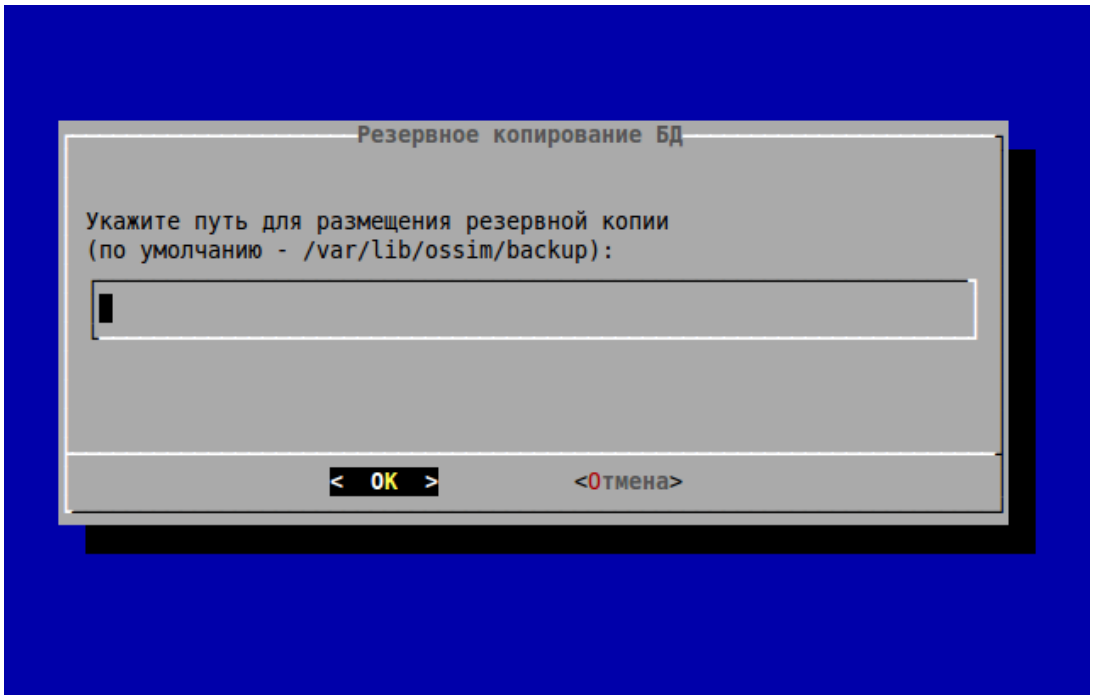



Рисунок 48 – Резервное копирование базы данных

После этого необходимо указать путь к каталогу, вкотором после готовности будет размещён архив (если оставить поле пустым, архив будет сохранён в каталоге */var/lib/ossim/backup*; если указать некорректный путь, архив будет размещён в каталоге */var*), и нажать«**OK**».

Во время созданиярезервной копии будет отображаться сообщение«*Запущен процесс изготовления резервной копии базы данных. Пожалуйста, подождите*».

После завершения создания резервной копии БД появится сообщение, содержащее полный путь к созданному файлу (Рисунок 49). После нажатияподтвержденияпроизойдет возврат к пункту меню «**Резервное копирование и восстановление→Резервное копирование и восстановление базы данных**» утилиты komrad-setup.

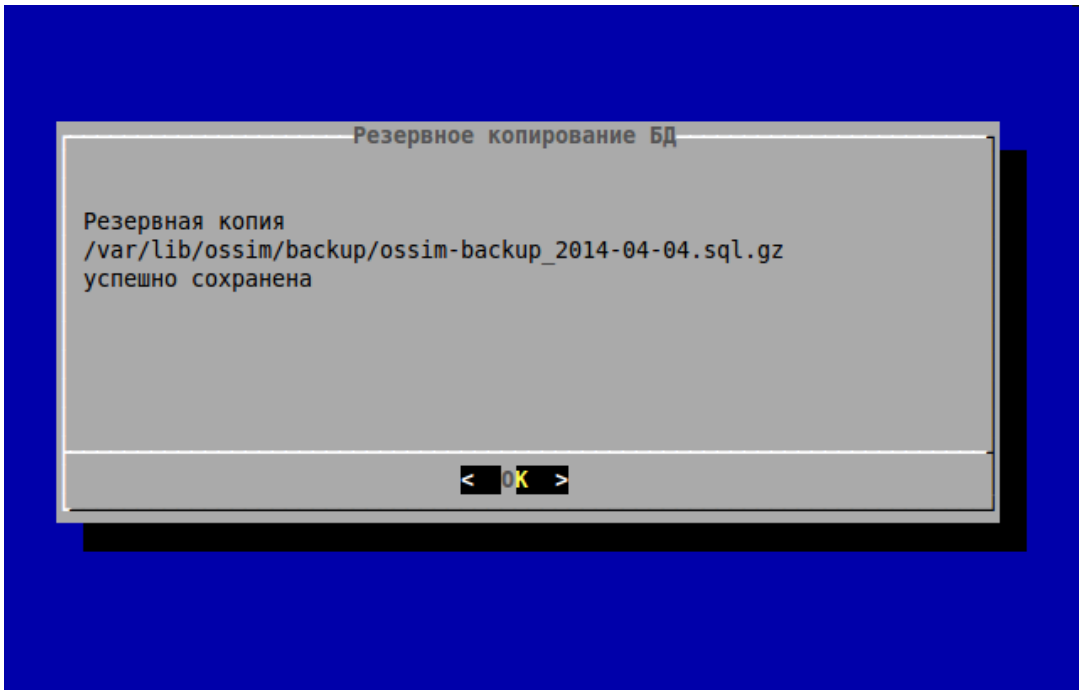



Рисунок 49 – Завершение резервного копирования БД

Для восстановления БД из резервной копии необходимоиз главного меню komrad-setup перейти по пунктам «**Резервное копирование и восстановление**»→«**Резервное копирование и восстановление базы данных**»→«**Восстановление базы данных**».

После этого откроется диалоговое окно для выбора файла (Рисунок 50, стартовый каталог соответствует указанному в переменной SRC; по умолчанию */var/lib/ossim/backup*). Файл должен представлять собой архив базы MySQL, структура которой соответствует структуре базы импорта, сжатой в формате gzip. Для навигации следует использовать клавиши со стрелками и «**Enter**» на клавиатуре, для выбора файла — нажать «пробел», а для продолжения процедуры восстановления нажать «**OK**» (соответствующее напоминание выводится при каждом вызове процедуры восстановления конфигурации).

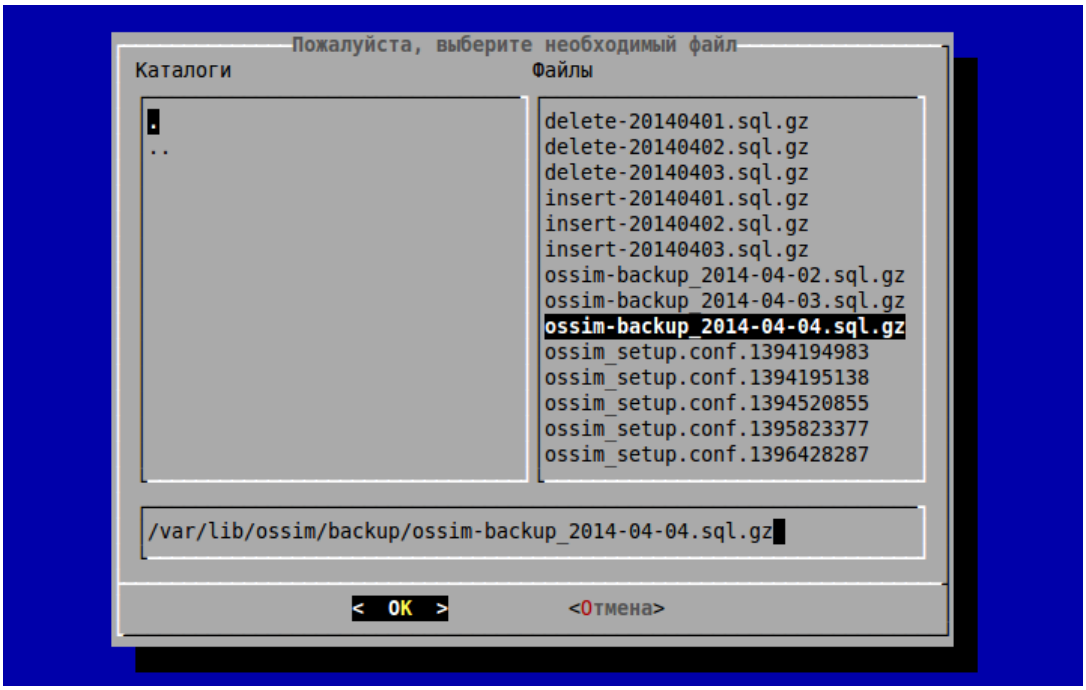



Рисунок 50 – Выбор резервной копии для восстановления

Если выбранная резервная копия не может быть развёрнута (файл не является архивом базы MySQL), или хранящаяся в нём структура БД не соответствует базе, в которую разворачивается файл, то пользователь увидит соответствующее сообщение и будет возвращен к окну выбора файла резервной копии(Рисунок 51):

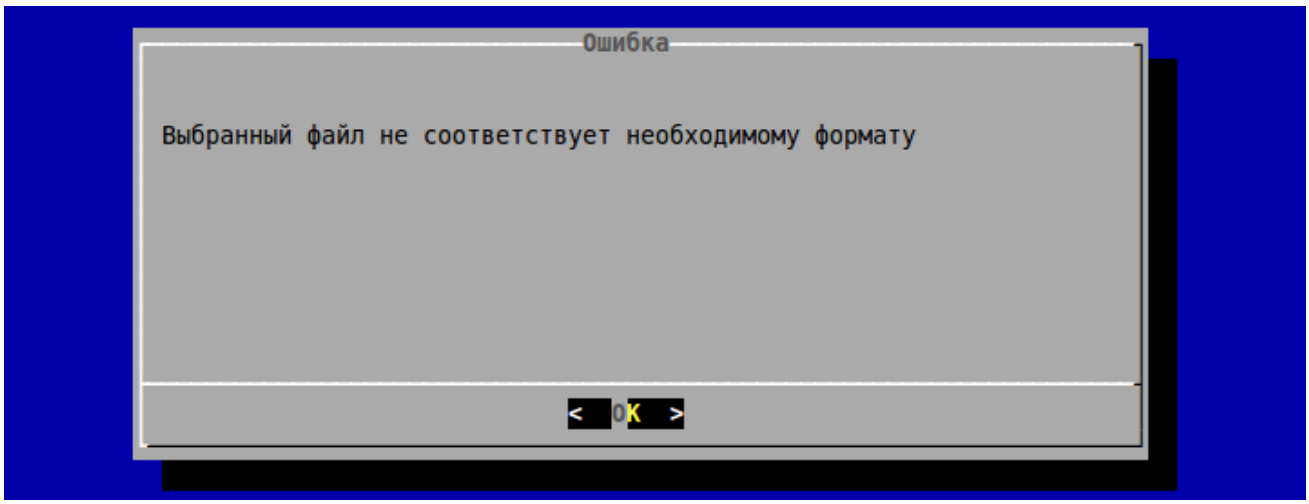



Рисунок 51 – Уведомление о несоответствии формата архива

В случае если архив успешно извлечён и развёрнут, пользователь увидит соответствующее сообщение.

**Примечание**:для того чтобы развернуть резервную копию базы данных, отправляются все запросы, которые содержатся в дампе, в том числе DROP TABLE IF

EXIST. После данной процедуры будут потеряны все данные, добавленные в БД в промежуток времени между текущей датой и временем создания архива.

### 4. Средства

#### 0. Просмотр журналов

При выборе журнала или лога пользователь получает уведомление о том, что выход из режима просмотра лога или журнала осуществляется нажатием «**q**» с подтверждением нажатием на «**Enter**» (Рисунок 52).

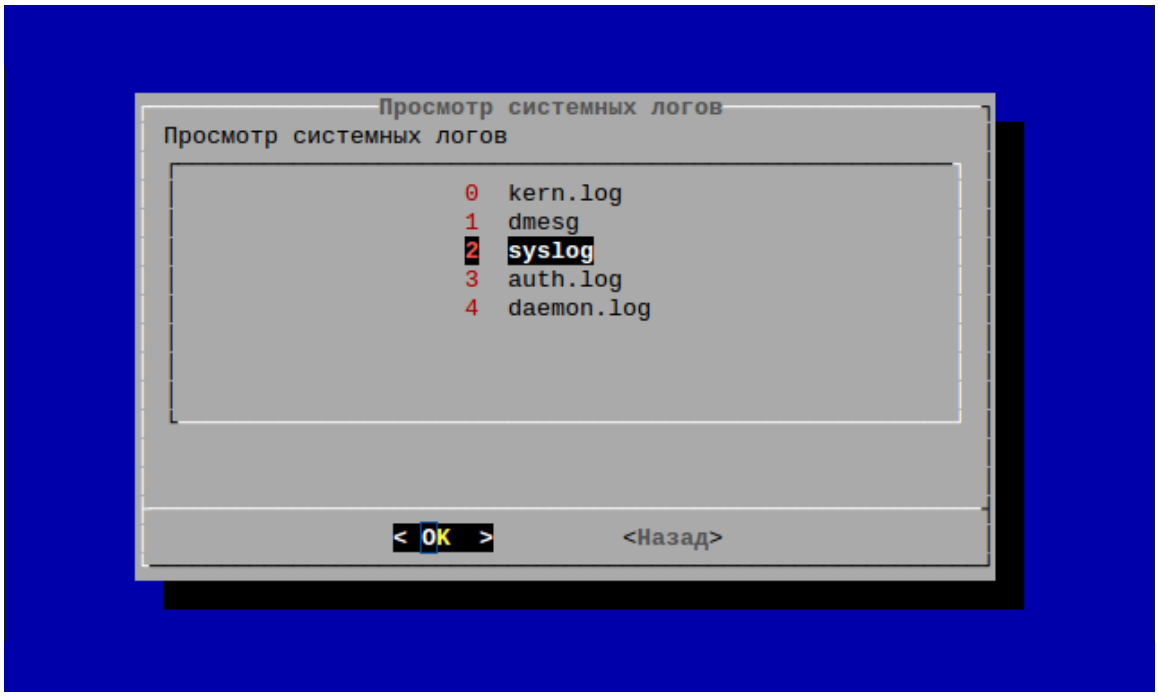



Рисунок 52– Доступ к просмотру журналов и логов ПК «КОМРАД»

Просмотр журнала осуществляется в интерфейсе командной строки (Рисунок 53).

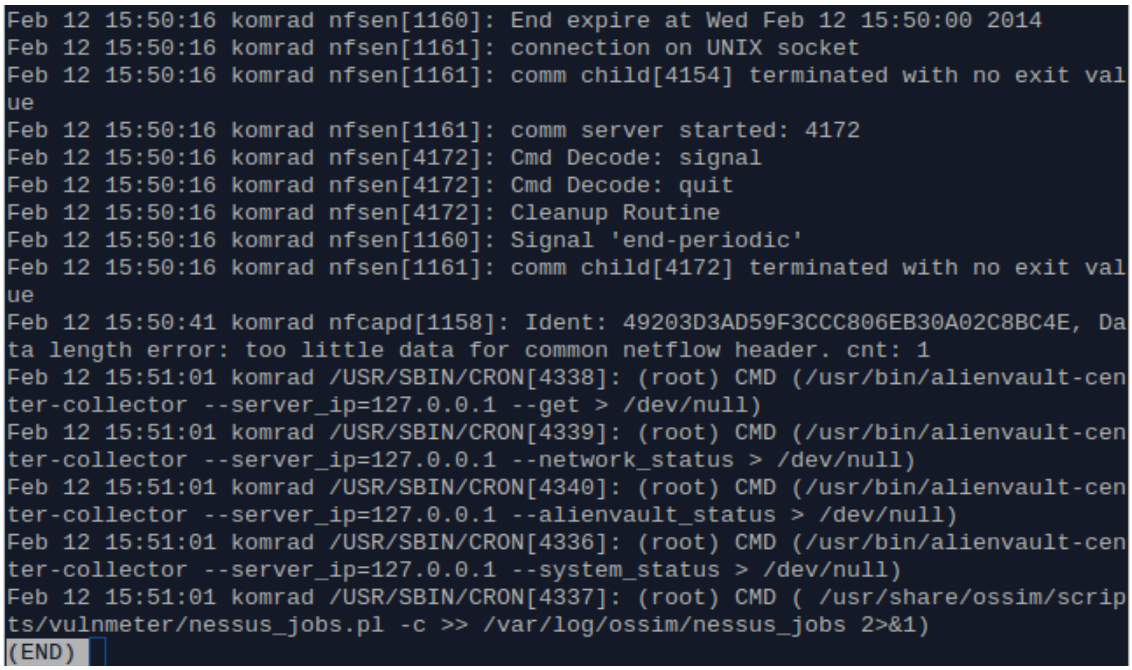



Рисунок 53 – Просмотр журнала в интерфейсе командной строки

Для просмотра доступны следующие журналы:

**0. kern.log** (*/var/log/kern.log*, сообщения от ядра linux).

**1. dmesg** (*/var/log/dmesg*, сообщения об устройствах).

**2. syslog** (/var/log/syslog, обычно содержит все системные сообщения, кроме событий аутентификации).

**3. auth.log** (*/var/log/auth.log*, события аутентификации в системе).

**4. daemon.log** (*/var/log/daemon.log*, сообщения о работе системы и демонов).

**1. Просмотр журналов компонентов Комрад**

**0. Показать лог службы ossim-server** (*/var/log/ossim/server.log*, журнал сервера Комрад).

**1.Показать лог службы ossim-agent** (*/var/log/ossim/agent.log*, журнал получения сенсором сведений о событиях).

**2.Показать лог службы ossim-frameworkd** (*/var/log/ossim/frameworkd.log*, журнал демона ossim-framework).

**3. Показать лог СУБД Комрад** (*/var/log/ossim/mysql.log*, журнал СУБД MySQL).

**1. htop** (средство для мониторинга процессов и использования вычислительных ресурсов системы — CPU, память, обращение к разделу подкачки).

**2. netstat** (средство для мониторинга сетевых соединений).

**3. bwm-ng** (средство для мониторинга сетевого интерфейса, показывает текущие объёмы передаваемых данных).

**5. О системе** (предоставляет справочную информацию о текущей версии ПО и дате установки программного комплекса).

**6. Сохранить изменения** (позволяет записать на диск произведенные в утилите изменения и перезапустить ключевые службы).

Помимо указанных выше команд доступны дополнительные утилиты командной строки. При нажатии «**Выход**»в меню интерфейса командной строки осуществляется выход в оболочку lshell, которая является стандартной для командного интерфейса ПК «КОМРАД». Получить информацию о доступных командах можно, вызвав команду «help».

Команды, доступные в оболочке lshell, можно объединить в несколько категорий:

1) стандартные команды *nix-оболочек:

| | |
|---|---|
| -ls | -less |
| -echo | -zless |
| -cd | -zcat |
| -ll | -uname |
| -cat | -who |
| -modprobe | -date |
| -grep | -pwd |
| -sed | -mkdir |

Справку по использованию указанных команд можно получить, запустив их с ключом *–help*.

2) программы для диагностики *nix-систем:

-htop

-ps

-top

-df

-du

-lsof

-md5sum

3) программы для работы с сетями:

-bwmng

-ping

-tcpdump

-ngrep

-ip

-ifconfig

-ethtool

-netstat

4) сопутствующие задачи:

-tar

-wget

-ssh

-scp

-mysqldump

-nmap

Справку по использованию указанных команд можно получить, запустив их с ключом --*help*

5) управление модулями и компонентами ПК «КОМРАД»:

komrad_bckp — утилита с псевдографическим интерфейсом для создания резервных копий файлов, критичных для работы системы, и восстановления файлов из резервных копий;

komrad_sql_bckp — утилита с псевдографическим интерфейсом для создания резервныхкопий записей, хранящихся в БД;

komrad_sql_unpack — утилита с псевдографическим интерфейсом для восстановления записей, хранящихся в БД, из резервных копий;

ossim-reset-passwd — сброс существующего пароля пользователя веб-интерфейса и назначение нового пароля, сгенерированного случайным образом;

ossim-reconfig — перезапуск всех основных служб системы.

### 5.1.2. Веб-интерфейс ПК «КОМРАД»

Веб-интерфейс представляет собой оконный интерфейс доступа к управлению компонентами ПК «КОМРАД». Окно веб-интерфейса визуально разбито на несколько областей (Рисунок 54):

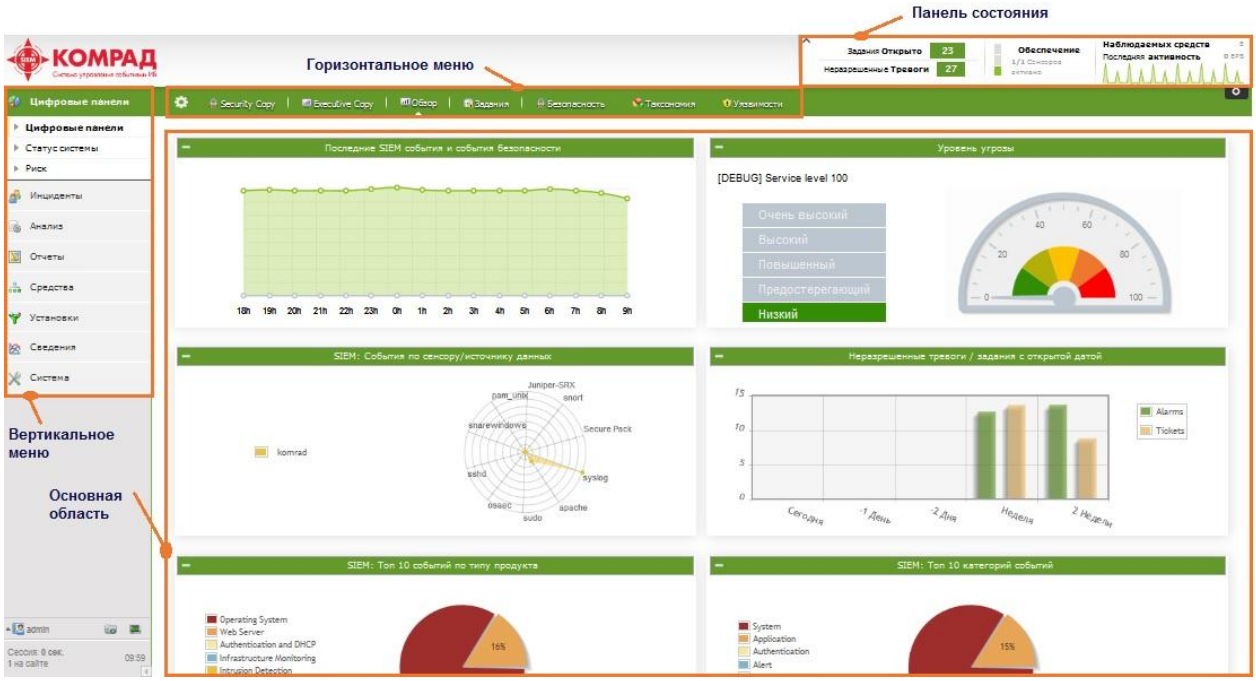



Рисунок 54 – Ключевые области веб-интерфейса ПК «КОМРАД»

**Вертикальное меню**расположено в левой части экрана. Данное меню содержит разделы: «Цифровые панели», «Инциденты», «Анализ», «Отчеты», «Средства», «Установки», «Сведения», «Система». Каждый раздел может содержать набор до-

полнительных вкладок (например, для «Цифровые панели» дополнительными являются вкладки «Статус системы» и «Риск»).

**Горизонтальное меню**расположено в левой верхней части экрана.Данное меню содержит вкладки, уникальные для каждой функции (например, для функции «Цифровые панели» это вкладки «Обзор», «Задания», «Безопасность», «Уязвимости»).

При нажатии на пиктограмму на горизонтальной панели, откроется выпадающее меню (Рисунок 55).

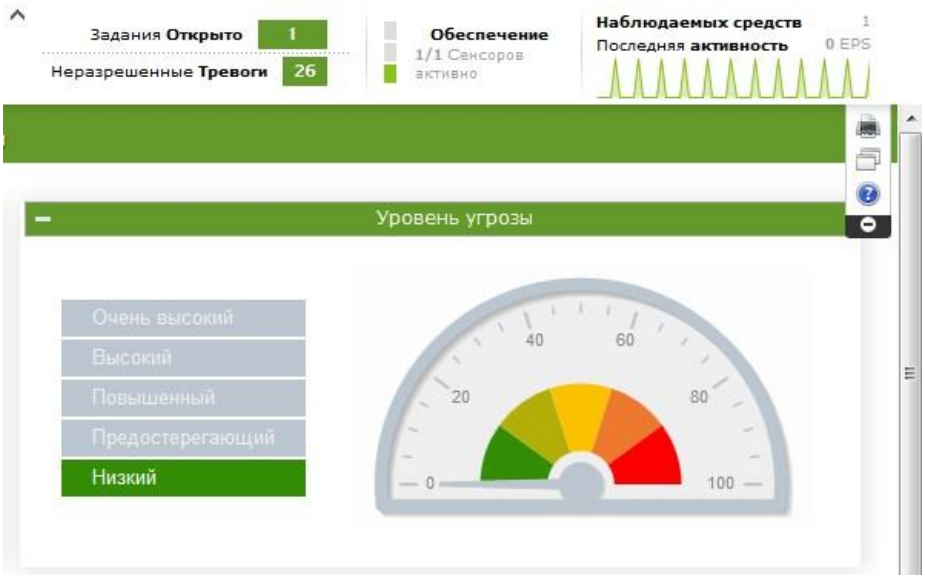



Рисунок 55 – Выпадающее меню на горизонтальной панели

С помощью данного меню возможна отправка на печать текущей страницы, открытие страницы в режиме нового окна и страницы справки.

**Основная область**занимает центральную часть окна. Её вид и содержимое зависят от выбора вкладок и настроек отображения необходимой информации.

**Панель состояния**, расположенная в правой верхней области окна,отображает открытые задания, неразрешённые тревоги, количество активных сенсоров, количество наблюдаемых средств и частоту поступления событий.

## 5.2. Функции администратора безопасности

### 5.2.1. Вход/выход из веб-интерфейса ПК КОМРАД

Для получения доступа к ПК «КОМРАД» с помощью веб-интерфейса необходимо ввести IP-адрес сервера ПК «КОМРАД», заданный при установке, в адресной строке веб-браузера. При обращении к серверу запускается ПК «КОМРАД» и открывается окно авторизации (Рисунок 56).

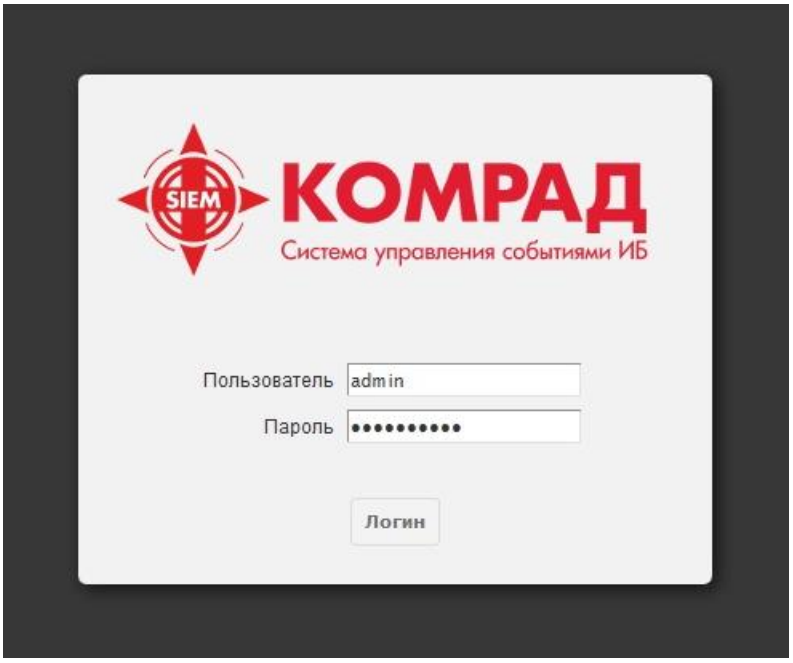



Рисунок 56 – Окно авторизации ПК «КОМРАД»

В случае успешной авторизации открывается вкладка «Цифровые панели» главного окна веб-интерфейса ПК «КОМРАД» (Рисунок 57).

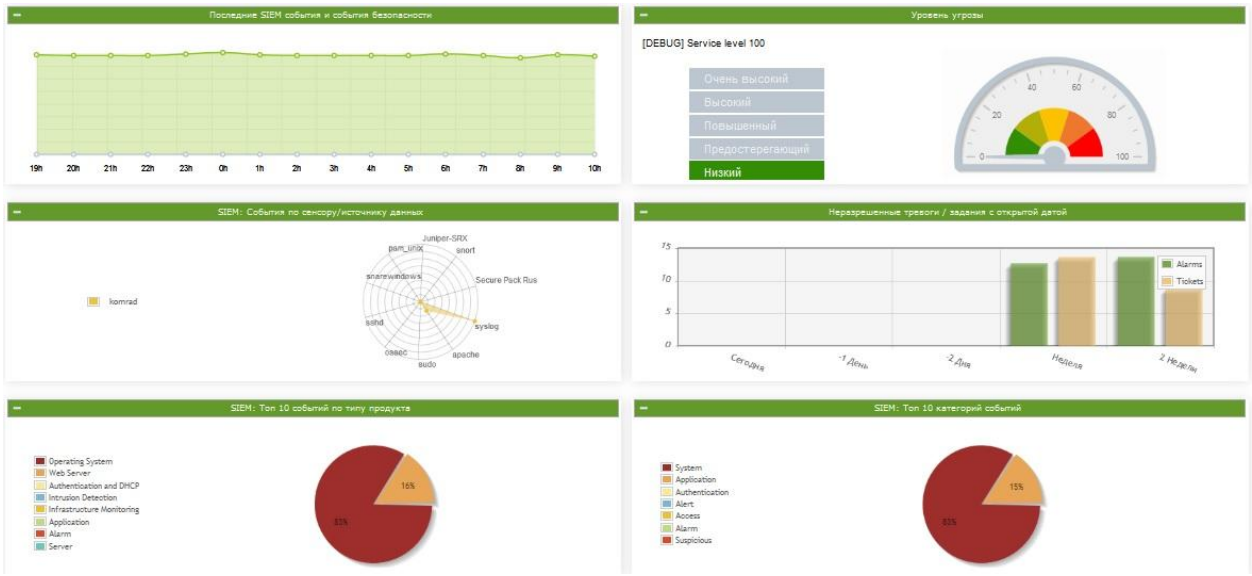



Рисунок 57 – Вкладка «Цифровые панели» главного окна веб-интерфейса ПК «КОМРАД»

Для выхода из веб-интерфейса или смены пользователя необходимо в нижней части вертикального меню нажать на кнопку, отображающую текущего пользователя (Рисунок 58), и выбрать пункт «**Выйти**».

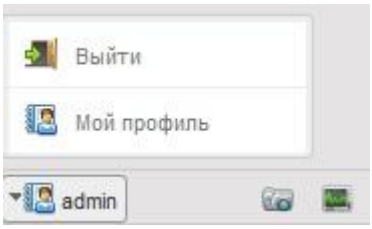



Рисунок 58 – Выход из ПК «КОМРАД»

Помимо возможности выхода из системы, в этой области меню также доступна информация о текущей сессии (Рисунок 59)– длительность текущей сессии и количество пользователей в системе.

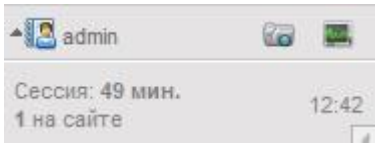



Рисунок 59 – Информация о текущей сессии

### 5.2.2. Работа с директивами корреляции

Для просмотра существующихдиректив корреляции администратор должен зайти в пункт меню **«Установки → Директивы корреляции»** (Рисунок 60).

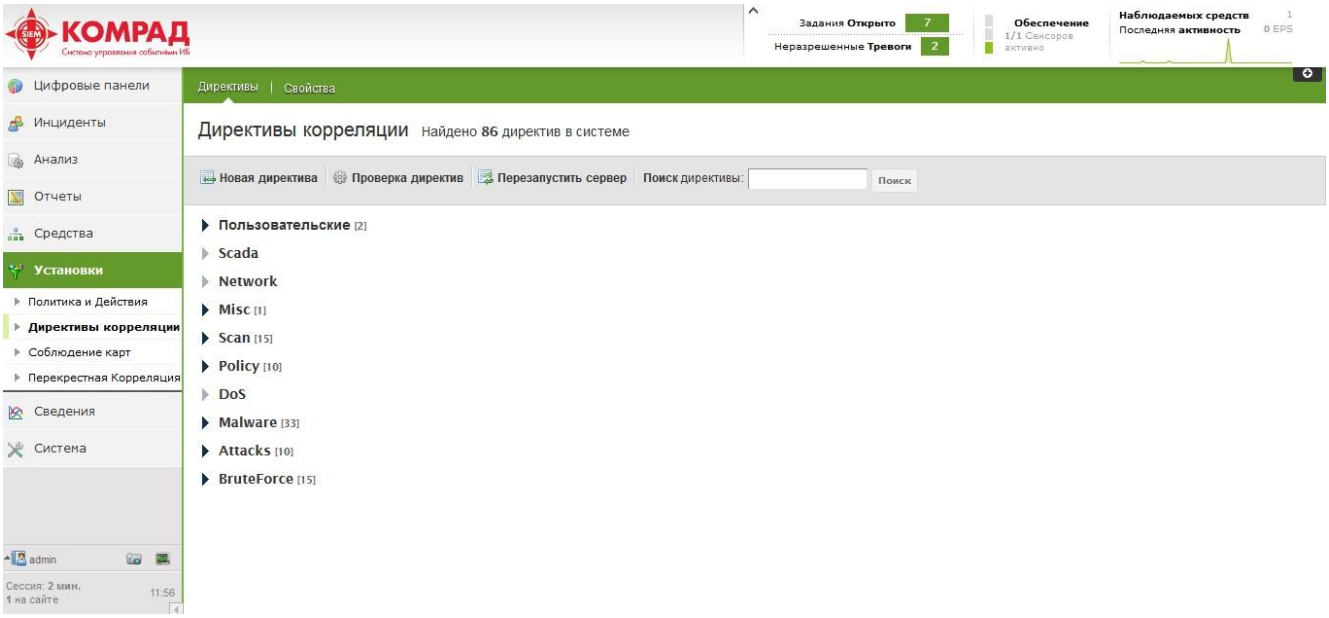



Рисунок 60 – Директивы корреляции ПК «КОМРАД»

В данном окне отображаются все директивы корреляции, действующие в системе, среди которых основным инструментом являются созданные администратором ПК «КОМРАД» **Пользовательские**директивы.

Администратор безопасности может редактировать существующие пользовательские директивы, а также создавать новые во вкладке **«Пользовательские»** (Рисунок 61).

**Примечание:** для редактирования доступны только пользовательские директивы корреляции, встроенные директивы можно только отключать или копировать.

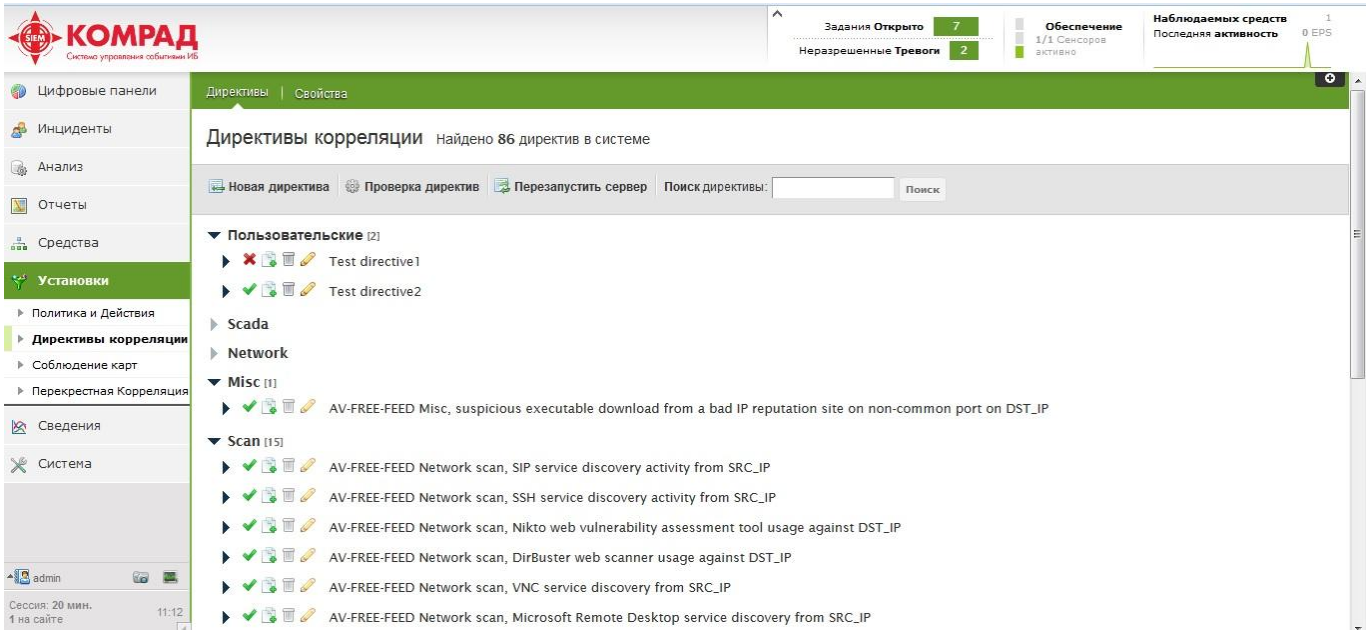



Рисунок 61 – Пользовательские директивы корреляции

В данном списке включенные директивы отмечены знаком «✔», а отключенные — «✖».Для включения/отключения директивы необходимо нажать на данный значок. При этом отобразится соответствующее сообщение (Рисунок 62, Рисунок 63).

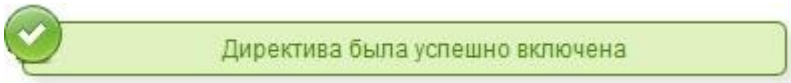



Рисунок 62 – Сообщение о включении директивы

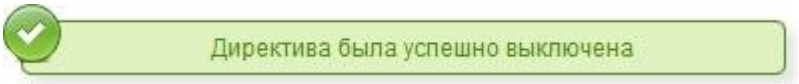



Рисунок 63 – Сообщение о выключении директивы

### 5.2.2.1. Добавление директивы корреляции

Для добавления новой пользовательской директивы корреляции следует нажать на кнопку **«Новая директива»**в окне «Директивы корреляции». В появившемся окне (Рисунок 64) вводится имя новой директивы корреляции и устанавливается её приоритет (0 — низкий, 5 — высокий). После этого необходимо нажать кнопку **«Далее»** для продолжения.

**Примечание:**в любом поле можно использовать следующие ключевые слова, которые в момент исполнения действия будут заменены их реальными значениями(например, «атака на DST_IP» будет отображаться как «атака на 192.168.1.1»):

| Ключевое слово | Значение |
|---|---|
| DATE | Дата |
| PLUGIN_ID | ID плагина |
| PLUGIN_SID | SID плагина |
| RISK | Значение риска |
| PRIORITY | Приоритет |
| RELIABILITY | Надежность |
| SRC_IP_HOSTNAME | Имя узла источника |
| DST_IP_HOSTNAME | Имя узла назначения |
| SRC_IP | IP-адрес источника |
| DST_IP | IP-адрес назначения |
| SRC_PORT | Порт источника |
| DST_PORT | Порт назначения |
| PROTOCOL | Протокол |
| SENSOR | Сенсор |
| BACKLOG | Бэклог |
| EVENT_ID | ID события |
| PLUGIN_NAME | Имя плагина |
| SID_NAME | Имя SID’а |
| USERNAME | Имя пользователя |
| PASSWORD | Пароль |
| FILENAME | Файл |
| USERDATA1 | Данные пользователя 1 |
| USERDATA2 | Данные пользователя 2 |
| USERDATA3 | Данные пользователя 3 |

| | |
|---|---|
| USERDATA4 | Данные пользователя 4 |
| USERDATA5 | Данные пользователя 5 |
| USERDATA6 | Данные пользователя 6 |
| USERDATA7 | Данные пользователя 7 |
| USERDATA8 | Данные пользователя 8 |
| USERDATA9 | Данные пользователя 9 |

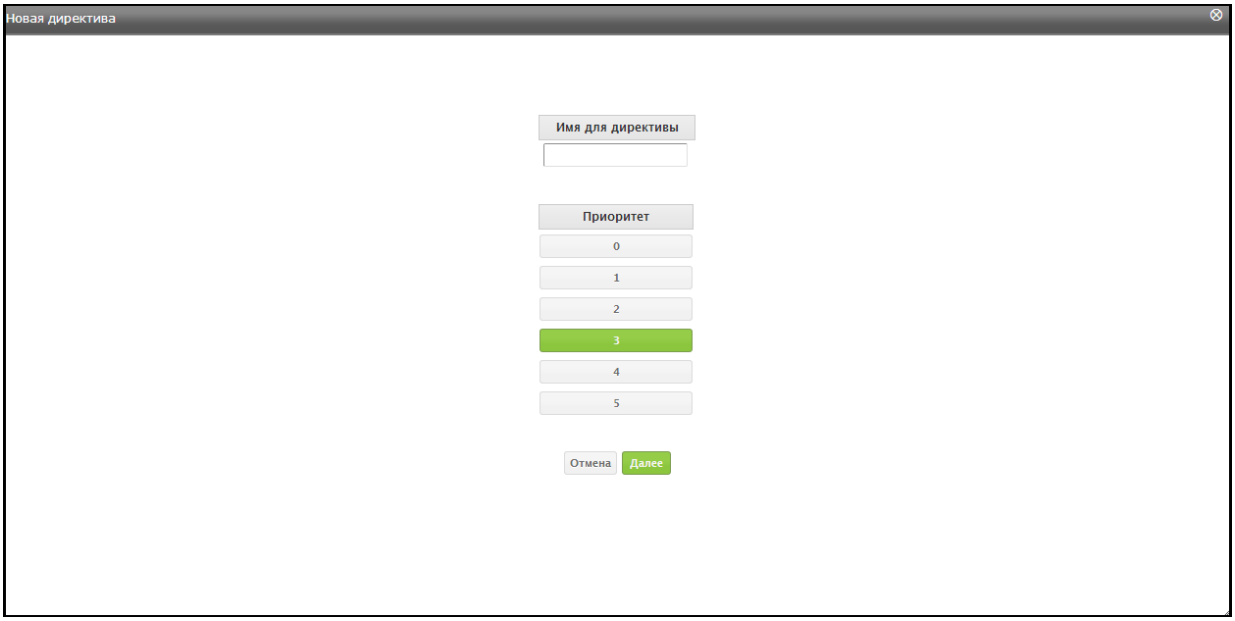



Рисунок 64 – Окно создания новой пользовательской директивы корреляции

В появившемся окне следует ввести имя правила первого уровня (основное правило корреляции) и нажать кнопку **«Далее»**.

В следующем окне необходимо выбрать плагин, который будет фиксировать-определённые события информационной безопасности (Рисунок 65). Выбор можно сделать по конкретному типу источника событий (**Типы Событий**) или с помощью общей классификации конечных устройств и систем (**Таксономия**).

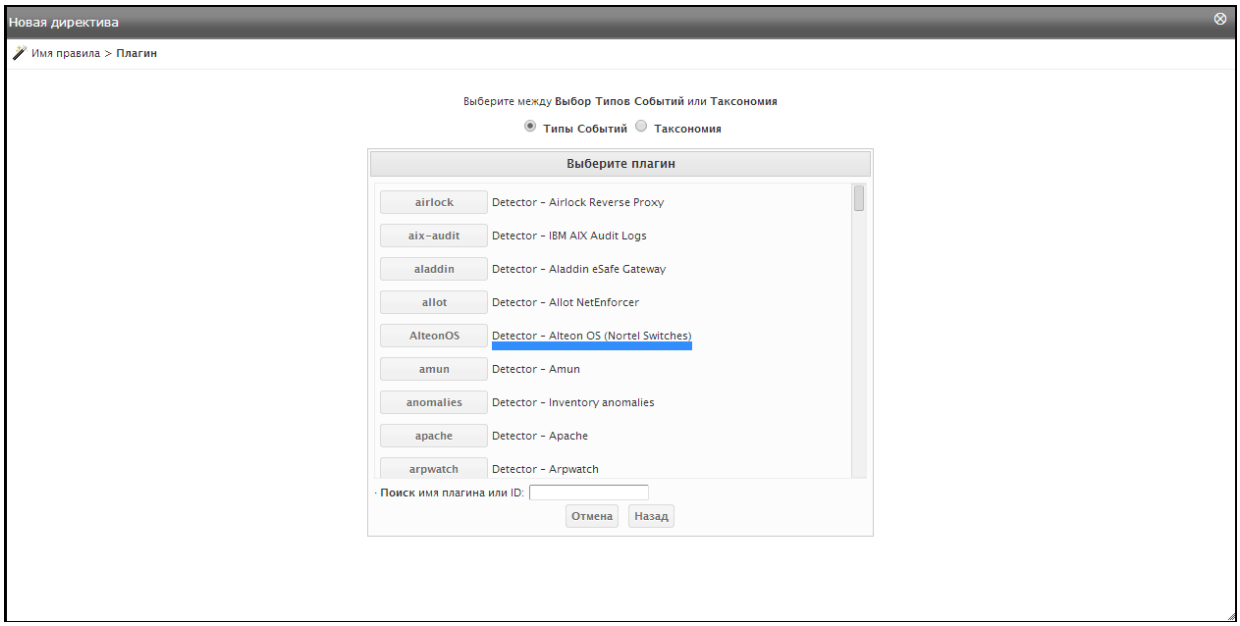



Рисунок 65 – Выбор плагина для новой директивы корреляции

**Примечание:** при необходимости администратор безопасности может воспользоваться строкой поиска в нижней части окна.

В появившемся окне необходимо выбрать для указанного плагина типы детектируемых событий либо из списка соответствующих подтипов событий (**Под-Типы Событий**), либо с помощью классификатора угроз (**Таксономия**).

В случае выбора **«Под-Типов Событий»** появляется окно (Рисунок 66), в левой колонке которого отображаются уже выбранные администратором безопасности типы событий, а в правой –полный список доступных для выбора событийуказанного плагина.

**Примечание**: если администратор не выбрал ни одного значения из правой колонки (левая колонка пустая), считается, что плагин отслеживает все доступные для этого плагина события информационной безопасности.

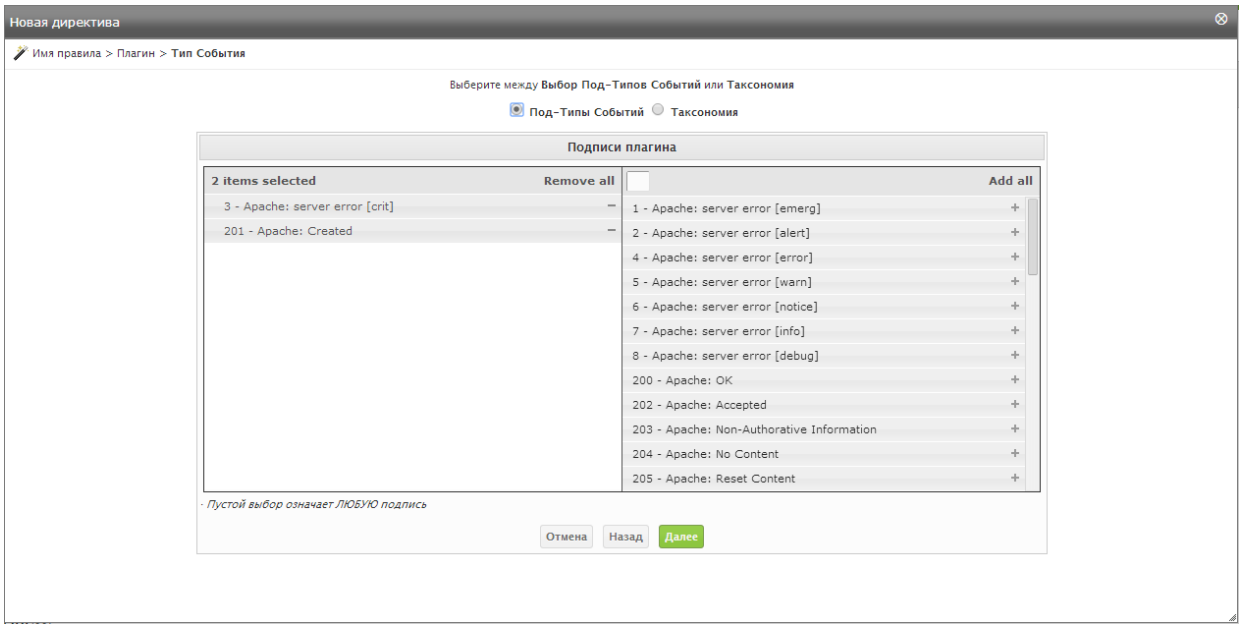



Рисунок 66 – Окно выбора событий плагина

Для перемещения события в левую колонку необходимо нажать на значок **«+»** в строке события в правой колонке. После выбора всех необходимых событий следует нажать кнопку **«Далее»**.

В случае выбора «**Таксономий**» (Рисунок 67) необходимо указать параметры классификации события информационной безопасности (**Категорию** и **Подкатегорию**), после чего нажать **«Next»**.

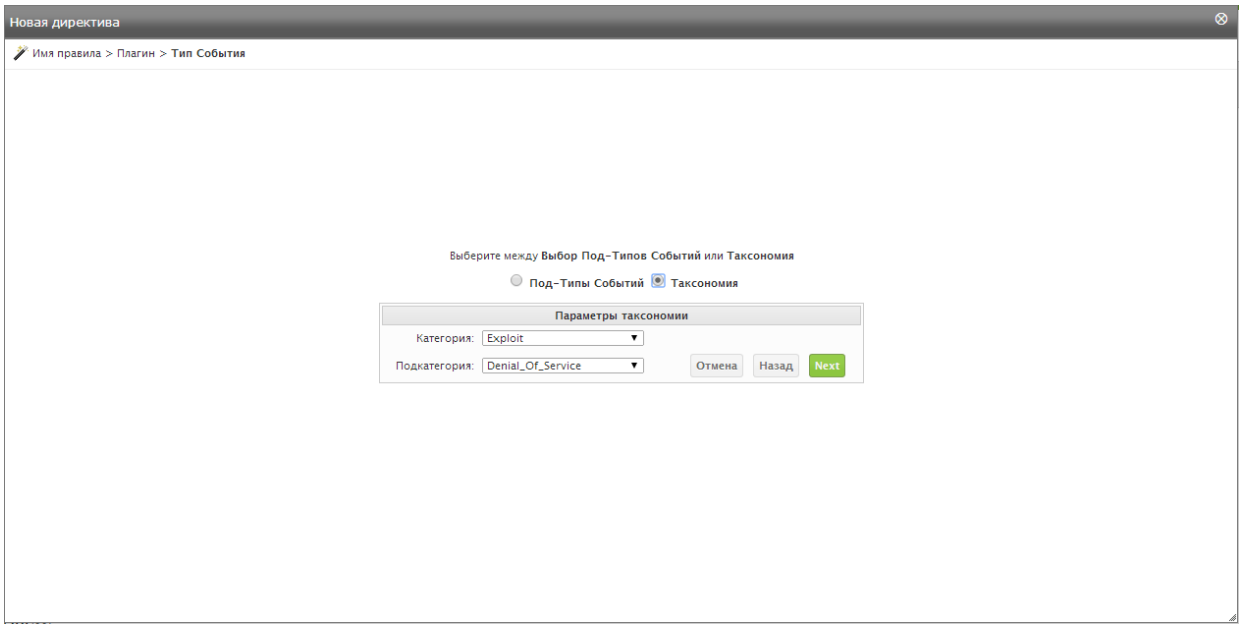



Рисунок 67– Выбор таксономий событий информационной безопасности

В появившемся окне **«Рабочая сеть»** необходимо выбрать источник события и назначения. В качестве источников могут служить хосты, группы, сети и сетевые группы (Рисунок 68).

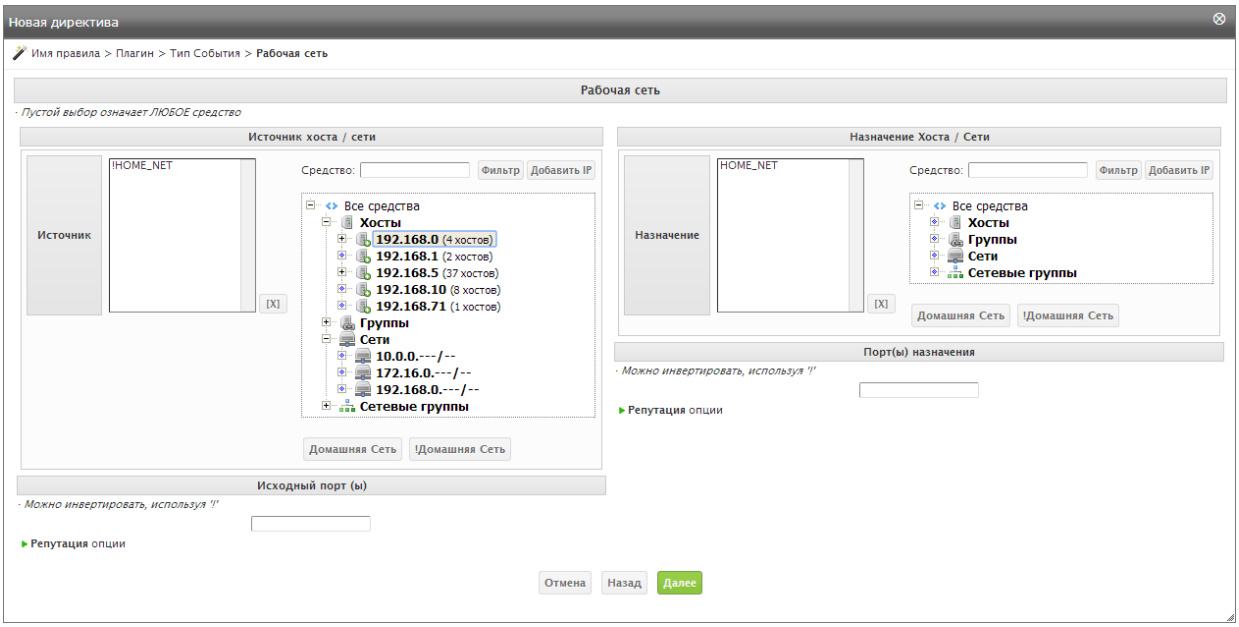



Рисунок 68 – Выбор источника и назначения события

При выборе конкретного средства в подразделе **«Источник хоста / сети»**оно добавится в колонку в левой части окна с надписью **«Источник»**. Если не выбрать ни одного средства, ПК «КОМРАД» будет считать источником любое средство. Существует возможность воспользоваться строкой поиска над деревом выбора средств. Также при необходимости можно указать порт источника событий. Выбор назначения события происходит аналогично выбору источника. После выбора источника и назначения необходимо нажать кнопку **«Далее»**.

**Примечание:** символ **«!»** в строках выбора средства и порта означает инвертирование.

В появившемся окне **«Протокол»** необходимо выбрать протокол, по которому будет приходить событие. Поле **«ANY»**означает любой возможный протокол. После выбора протокола необходимо нажать кнопку **«Далее»** (Рисунок 69).

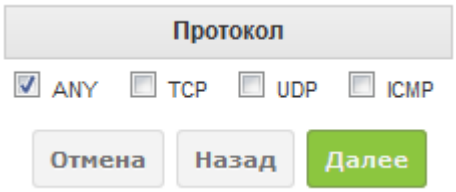



Рисунок 69 – Окно спецификации протокола

В появившемся окне **«Сенсор»** необходимо выбрать сенсор, который будет использоваться для фиксации событий, поступающих от конечных устройств и систем. В левой колонке отображаются уже выбранные сенсоры, в правой — доступные для выбора (Рисунок 70). Для выбора конкретного сенсора необходимо нажать на его имени в правом столбце, после чего он появится в левом.

**Примечание**: если не выбрать ни один сенсор, ПК «КОМРАД» будет считать выбранными все доступные сенсоры.

Для подтверждения выбора необходимо нажать кнопку **«Далее»**.

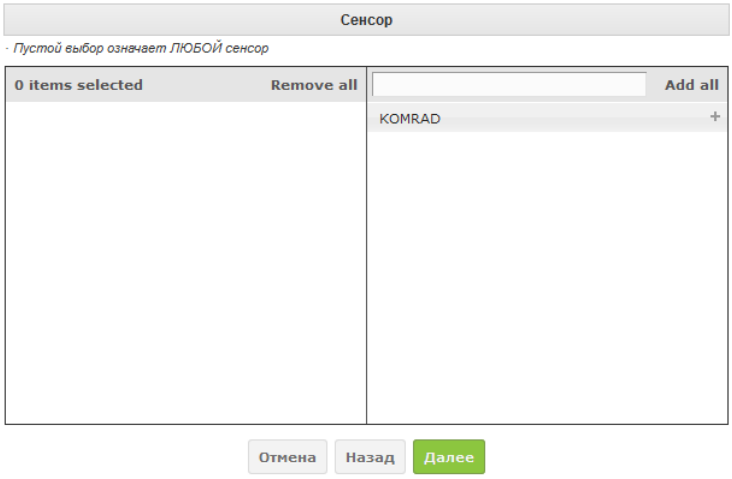



Рисунок 70 – Окно выбора сенсора

В появившемся окне **«Другие»** необходимо нажать кнопку **«Далее»**.

В следующем окне **«Данные пользователя»** при необходимости администратор может выделить дополнительные условия для отдельных полей данных.

После этого необходимо нажать кнопку **«Окончание»**. Если в процессе создания директивы не возникло никаких ошибок, после этого будет повторно показан список пользовательских директив, в котором появится созданное правило (Рисунок **71**).

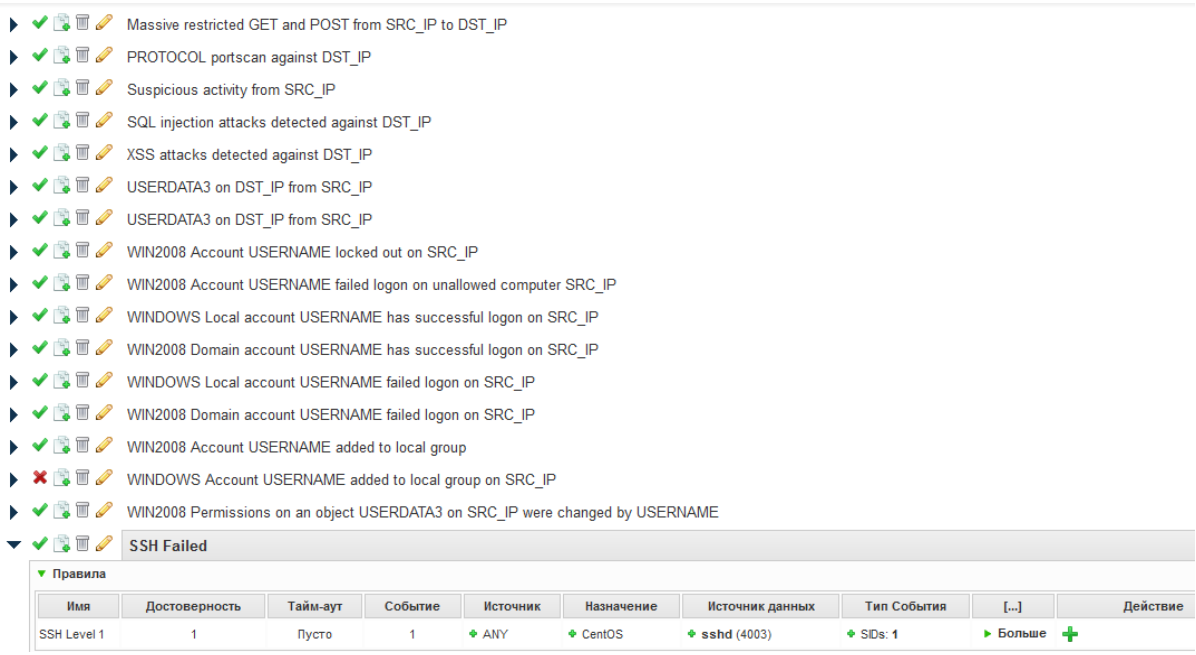



Рисунок 71– Список пользовательских директив после добавления директивы

Также в верхней части списка должна появиться всплывающая надпись, подтверждающая успешное сохранение директивы (Рисунок 72).

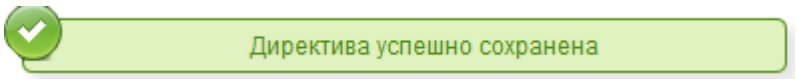



Рисунок 72 – Всплывающее сообщение подтверждения

Для добавления правила второго уровня необходимо щёлкнуть левой кнопкой мыши на созданном правиле и затем нажать на значок ✚ в колонке **«Действие»**. В появившемся окне необходимо ввести имя правила второго уровня и нажать кнопку **«Далее»** (Рисунок 73).

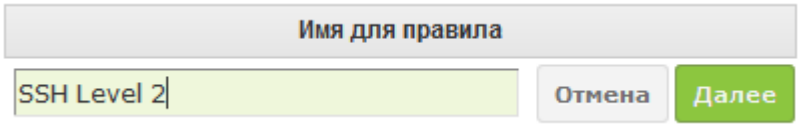



Рисунок 73 – Окно для ввода имени правила

В следующем окне необходимо выбрать плагин, который будет детектировать определённые события.

В окне **«Подпись плагина»** необходимо выбрать типы детектируемых событий. Если необходимо использовать тот же плагин, что и для правила первого уровня, следует нажать кнопку **«Sid плагин из уровня правил1»**. В случае необходимо-

сти использовать все плагины, кроме тех, что использовались для правила первого уровня, следует нажать на кнопку **«!Sid плагин из уровня правил 1»**. После выбора всех необходимых событий нажать кнопку **«Далее».**

В появившемся окне **«Рабочая сеть»** необходимо выбрать источник и назначение события. Существует возможность импортировать настройки из правила первого уровня. Для этого в строке **«Из родительского правила»** колонки **«Источник хоста/сети»** необходимо выбрать **«IP источника с уровня 1»**, а в строке **«Из родительского правила»**колонки **«Назначение хоста/сети»** выбрать **«IP назначения с уровня 1»**. При необходимости можно импортировать порты с первого уровня (Рисунок 74).

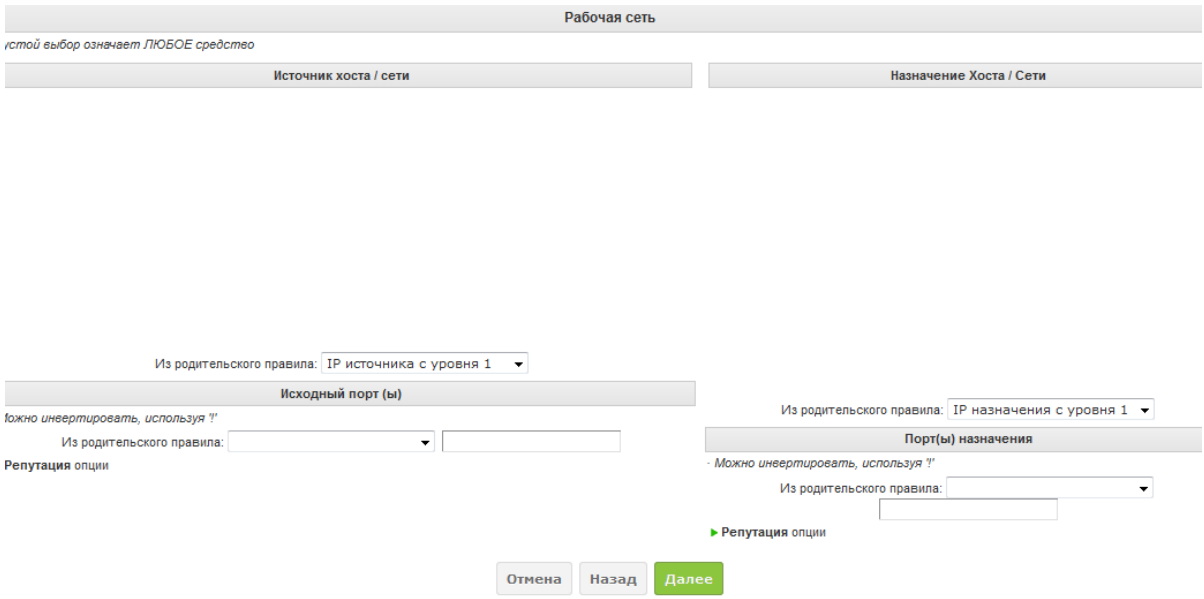



Рисунок 74 – Окно «Рабочая сеть»

После настройки всех параметров директивы необходимо нажать кнопку **«Окончание»** для завершения создания директивы корреляции. При этом можно продолжить настройку директивы с помощью дополнительных условий (для этого следует нажать кнопку **«Далее»**).

В появившемся окне **«Протокол»** необходимо выбрать протокол, по которому будут поступать данные о событии ИБ. Поле **«ANY»**означает любой возможный протокол. Поле **«1-PROTOCOL»**означает выбор протокола из правила первого уровня. После выбора протокола необходимо нажать кнопку **«Далее».**

В появившемся окне **«Вхождение»** следует выбрать количество поступивших

однотипных событий, необходимое для того, чтобы правило сработало.

В следующем окне **«Тайм-аут (секунд)»** необходимо указать время (в секундах), за которое должно произойти выбранное количество событий, чтобы правило сработало.

В окне **«Важные различия»** необходимо нажать кнопку **«None»** (Рисунок 75).

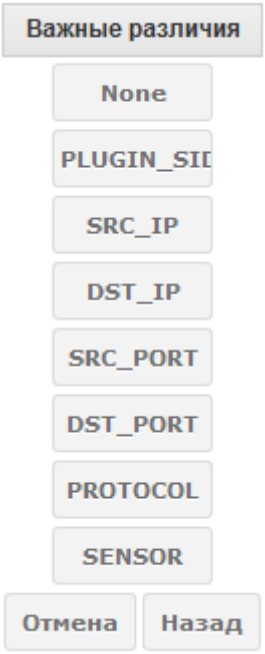



Рисунок 75 – Окно «Важные различия»

В появившемся окне **«Другие»** необходимо нажать кнопку **«Далее»**.

В следующем окне **«Данные пользователя»** администратор ПК «КОМРАД» имеет возможность выделить дополнительные условия для отдельных полей данных. После этого необходимо нажать кнопку **«Окончание»**.

Если в процессе создания правила не возникло никаких ошибок, после этого отображается список пользовательских директив, в котором у созданной директивы появляется правило второго уровня (Рисунок 76).

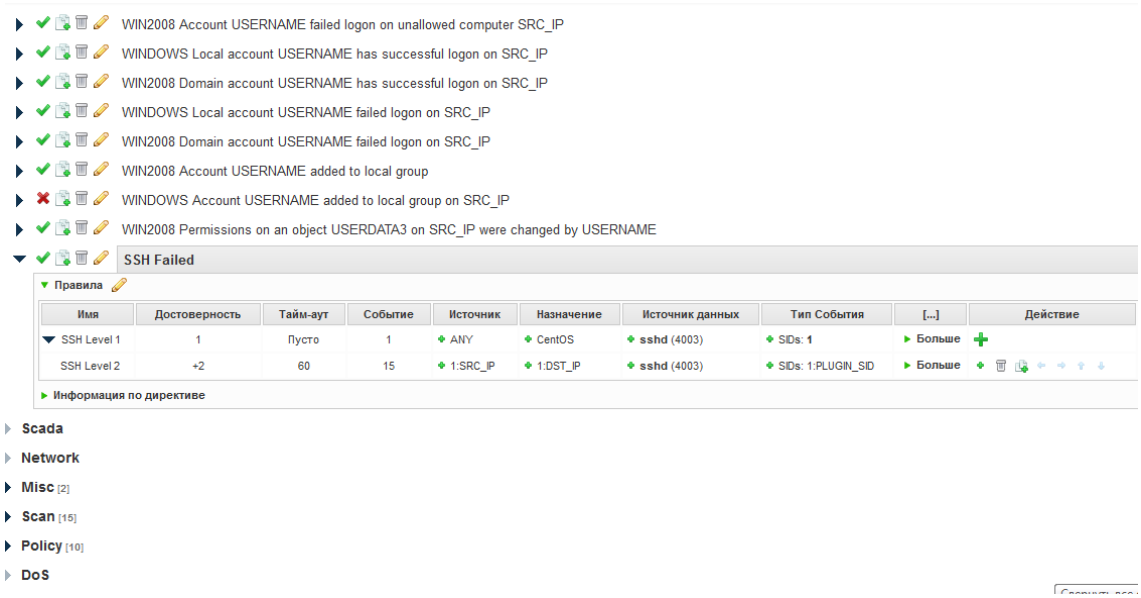



Рисунок 76 – Список пользовательских директив с правилами второго уровня

**Примечание**: при необходимости можно создавать как правила третьего уровня, так и другие правила второго уровня. Максимальное количество уровней для правил не ограничено.

Для создания правила третьего уровня необходимо нажать на значок ✚ напротив правила второго уровня. Для создания другого правила второго уровня необходимо нажать по значку ✚ напротив правила первого уровня. Создание правил всех следующих уровней происходит аналогично созданию правила второго уровня.

Нажатие на пиктограмму приведет к созданию копии правила, при этом все свойства заданные в правиле сохранятся.

Нажатие на пиктограммы и позволяет перемещать правило выше или ниже по списку (перемещение возможно только в пределах одного уровня).

Пиктограммы и позволяют изменять уровень правила.

**Примечание:** копирование, перемещение и сдвиг правила имеющего подправила приведет к изменению всей ветки правил целиком.

После создания директивы и настройки всех правил необходимо нажать на кнопку **«Перезапустить сервер»** над списком директив корреляции.

**Примечание:** нажатие на кнопку **«Перезапустить сервер»** останавливает работу модуля корреляции, поэтому все активные корреляции будут остановлены.

#### 5.2.2.2. Редактирование пользовательской директивы

Для редактирования какого-либо поля директивы корреляции необходимо в списке пользовательских директив нажать на соответствующее поле редактируемой директивы. Значения дополнительных полей доступны при нажатии ссылки **«Больше»** в соответствующем поле.

#### 5.2.2.3. Удаление правила/директивы

Для удаления какого-либо правила/директивы необходимо нажать на значок напротив правила/директивы, которые требуется удалить.

### 5.2.3. Мониторинг событий безопасности

В веб-интерфейсе ПК «КОМРАД» во вкладке **«Анализ → События безопасности»** доступна статистика по всем поступающим данным о событиях ИБ (Рисунок 77).

**Примечание:**нажатие на пиктограмму позволяет создать задание для отдельного события, минуя добавление его в список инцидентов.

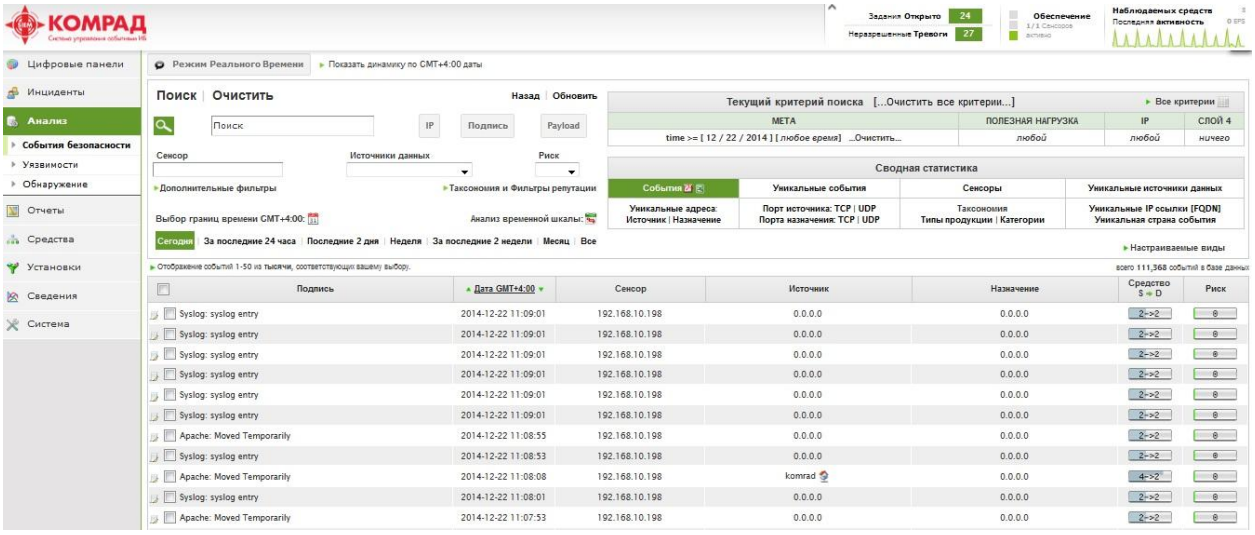



Рисунок 77 – События безопасности

Страница событий безопасности разделена на две части: поле фильтров и поле списокамсобытий.

В *поле фильтров* доступен набор различных режимов фильтрации (Рисунок 78).

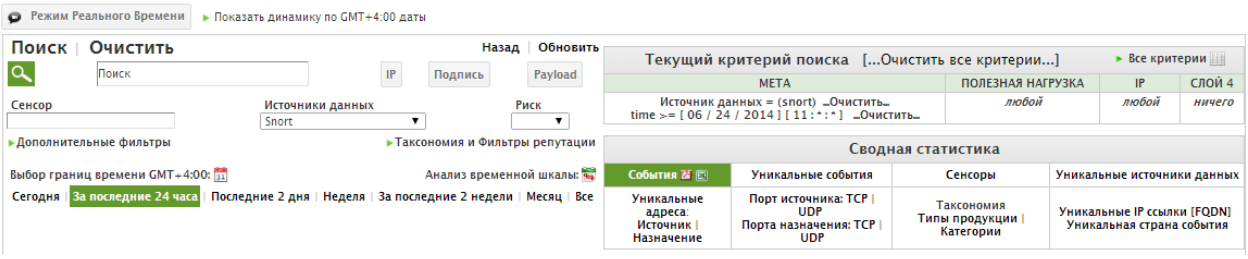



Рисунок 78 – Фильтры событий безопасности

В поле «**Текущий критерий поиска**» доступен список включённых фильтров. Убрать тот или иной фильтр можно нажатием на ссылку «**Очистить**» рядом с фильтром. Сброс всех фильтров осуществляется нажатием на ссылку «**Очистить все критерии**». Более подробно список включенных фильтров отображается при нажатии на ссылку «**Все критерии**» (Рисунок 79).

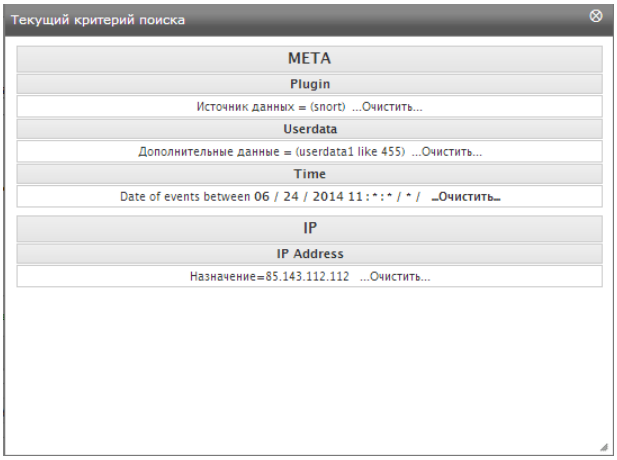



Рисунок 79 – Список включённых фильтров

Нажатие на кнопку «**Поиск**» включает настройку фильтров в режиме «**Мета критериев**» (Рисунок 80).

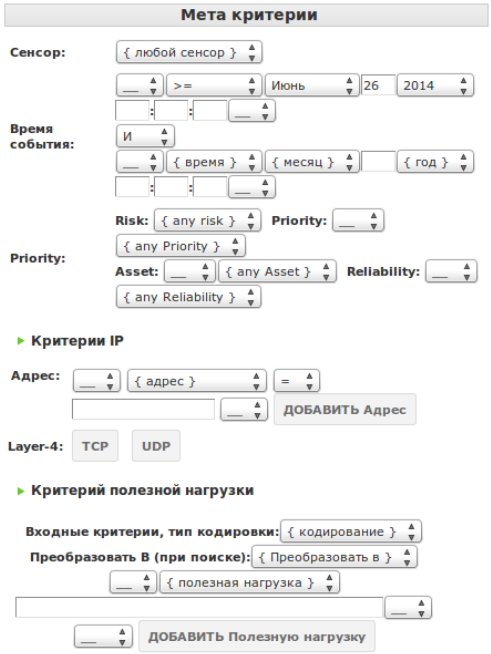



Рисунок 80 – Настройка фильтров в режиме «Мета критериев»

Возможен поиск по заголовку события безопасности. Для этого в строке поиска необходимо ввести часть заголовка (или заголовок целиком) и нажать на кнопку «**Подпись**» или на клавишу «**Enter**»на клавиатуре.

Для поиска по источникам событий необходимо ввести в строку поиска интересующий IP-адрес или имя узла и нажать на кнопку «**IP**», а затем выбрать тип заданного узла (например, «**IP-источник**»).

Нажатие на кнопку «**Назад**» возвращает к фильтру, настроенному ранее.

Нажатие на кнопку «**Обновить**» обновляет таблицу с событиями.

В поле «**Сенсор**» возможен выбор конкретного сенсора, с которого поступили события информационной безопасности.

В поле «**Источники данных**» доступен выпадающий список типов источников данных. При этом для выбора доступны только те источники, события от которых в данный момент присутствуют в базе данных программного комплекса.

Нажатие на ссылку «**Дополнительные фильтры**» вызывает окно поиска по полям событий безопасности отличным от заголовка или IP-адреса (например, по имени пользователя).

Нажатие на пиктограмму календаря «**Выбор границ времени**» позволяет выбрать интервал дат для фильтрации событий. Кроме того, доступны

преднастроенные интервалы времени внизу панели фильтров: *сегодня*, *за последние 24 часа* и т.д. (по умолчанию при нажатии пункта меню «**Анализ**»→«**События безопасности**» отображаются события только за текущий день).

Нажатие на пиктограмму «**Анализ временной шкалы**» приведёт к открытию графического режима отображения событий безопасности на выбранном временном интервале.

На панели фильтров доступны преднастроенные режимы отображения событий безопасности (Рисунок 81). По умолчанию установлен режим отображения «**События**». В каждом режиме доступны отчёты в виде pdf-документа или csv-таблицы, которые выгружаются нажатием на соответствующую пиктограмму рядом с названием режима отображения. Ранее установленные фильтры при выборе режима не сбрасываются.

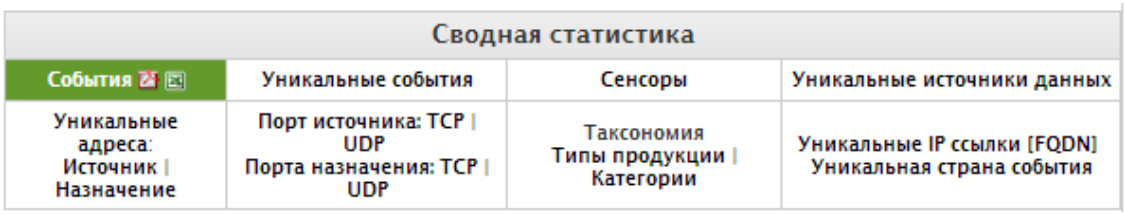



Рисунок 81 – Преднастроенные режимы отображения событий безопасности

НаРисунке82представлен режим отображения «**Уникальные события**». В данном режиме помимо текстовой информации по каждой группе событий представлен график поступления событий такого типа за выбраный период наблюдения.

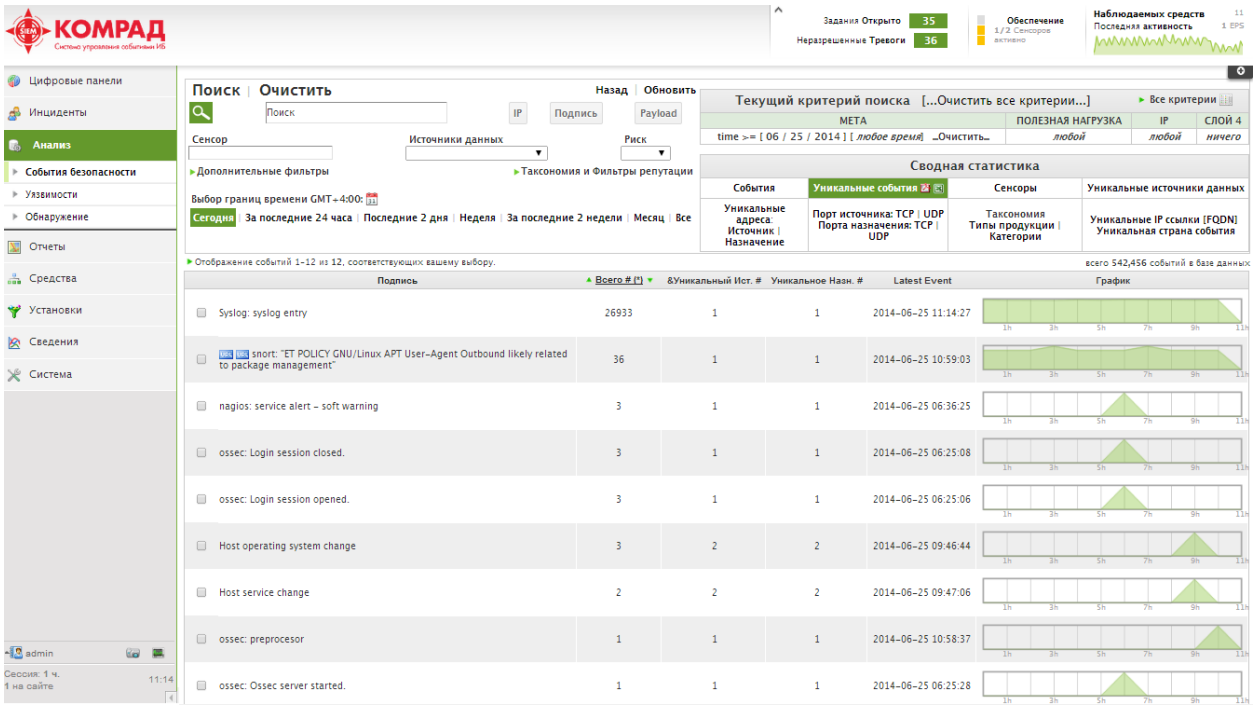



Рисунок 82 – Режим отображения «Уникальные события»

В режиме «События» доступен просмотр поступления событий в реальном времени (Рисунок 83). Для этого над полем фильтров необходимо нажать на кнопку «Режим реального времени». В данном режиме доступна фильтрация отображаемых событий по IP-адресам, TCP/UDP портам, а также по типам источников данных (ссылка «Показать плагины фильтра»).

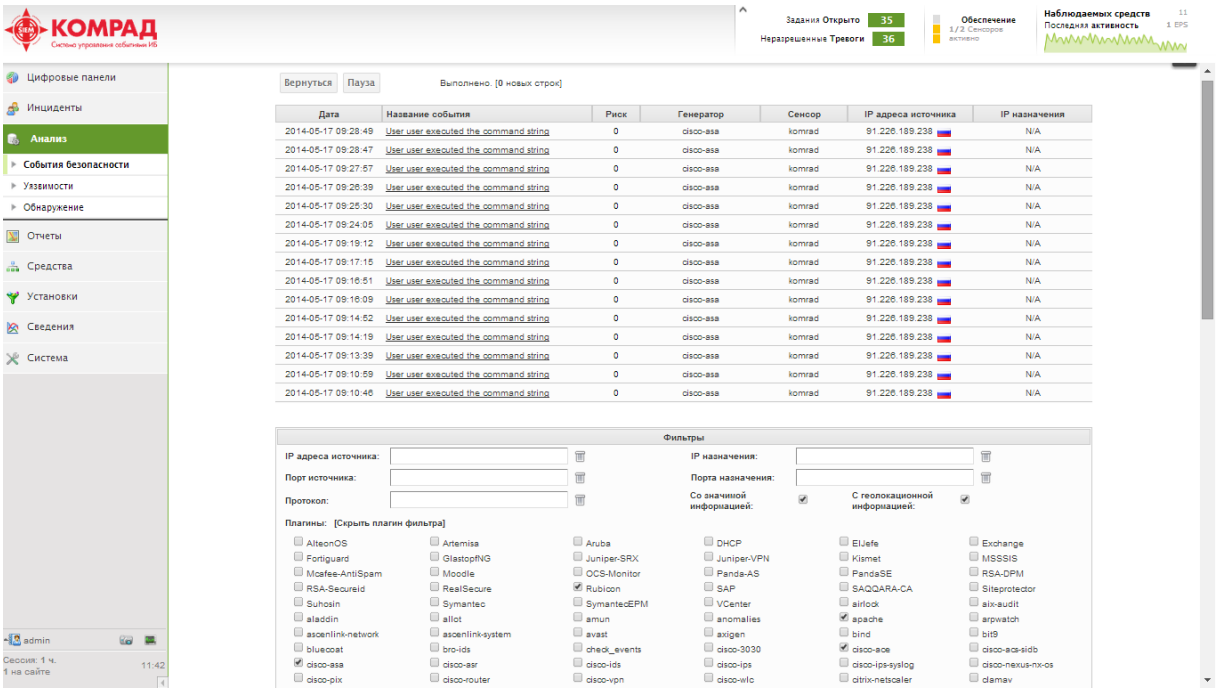



Рисунок 83 – Режим отображения «Режим реального времени»

*Поле событий* содержит информацию о событиях, удовлетворяющих настроенным фильтрам. Структура отображения событий настраивается в пункте «**Настраиваемые виды**» (Рисунок 84) в правой нижней части поля;в данном пункте допускаются: добавление нового вида, удаление старого (пиктограмма), изменение имеющегося (пиктограмма), установка по умолчанию (пиктограмма).

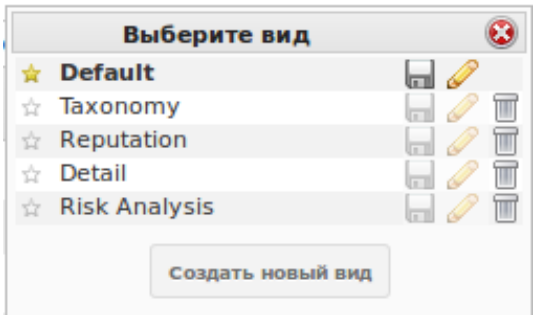



Рисунок 84 – Выбор вида отображения событий безопасности

Нажатие на кнопку «**Создать новый вид**» откроет окно настройки (Рисунок 85), в левом столбце которого расположены отображаемые пункты, в правом столбце — доступные пункты (для разных типов событий некоторые значения в столбцах могут быть пустыми). Нажатие на значок «+» добавит пункт для отображения, нажатие на значок «–» — уберёт его. Нажатие кнопки «**Восстановить по умолчанию**» включит режим редактирования вида по умолчанию. Для

сохранения вида отображения необходимо ввести его имя (латиницей) и нажать кнопку «**Создать**».

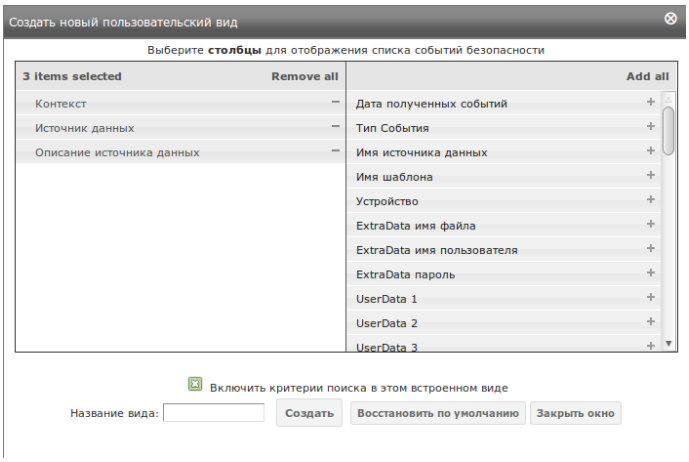



Рисунок 85 – Редактирование вида отображений событий безопасности

Администратор может получить подробную информацию по любому событию, нажав на заголовок события или в поле рядом с заголовком. В первом случае информация о событии откроется в текущем окне (Рисунок 86), во втором — в отдельном окне (Рисунок 87, данный режим позволяет сохранять настройки фильтров отображения списка событий безопасности).

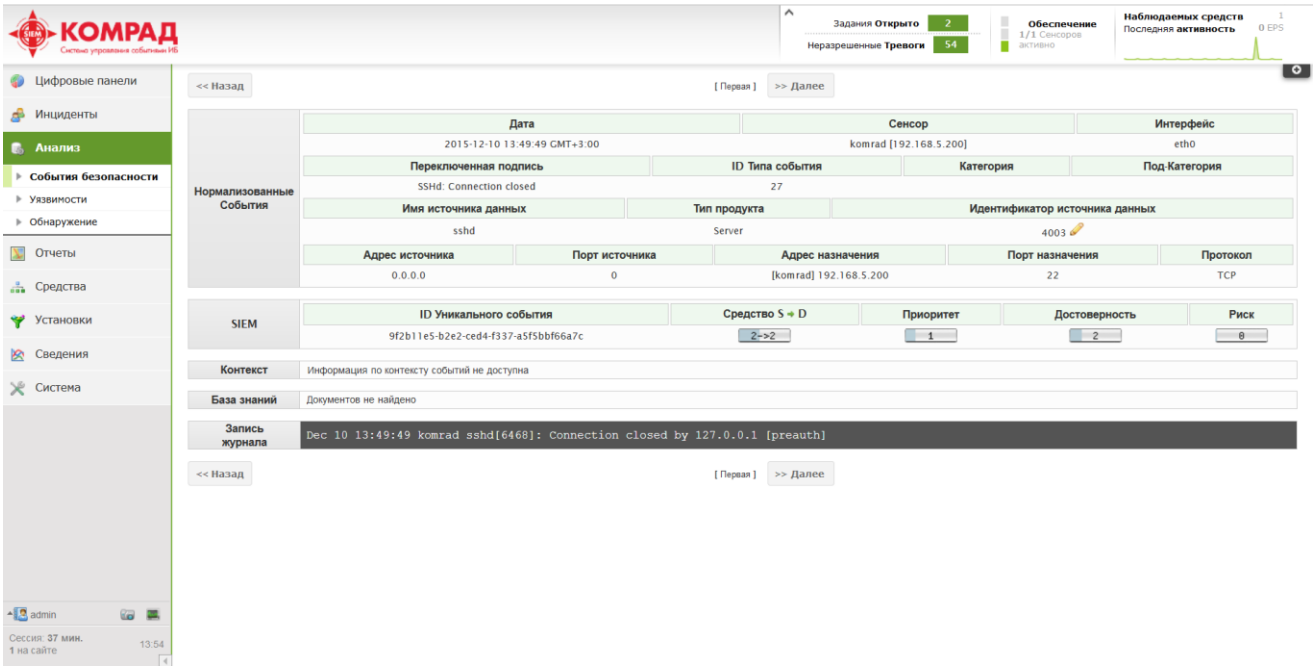



Рисунок 86– Событие безопасности

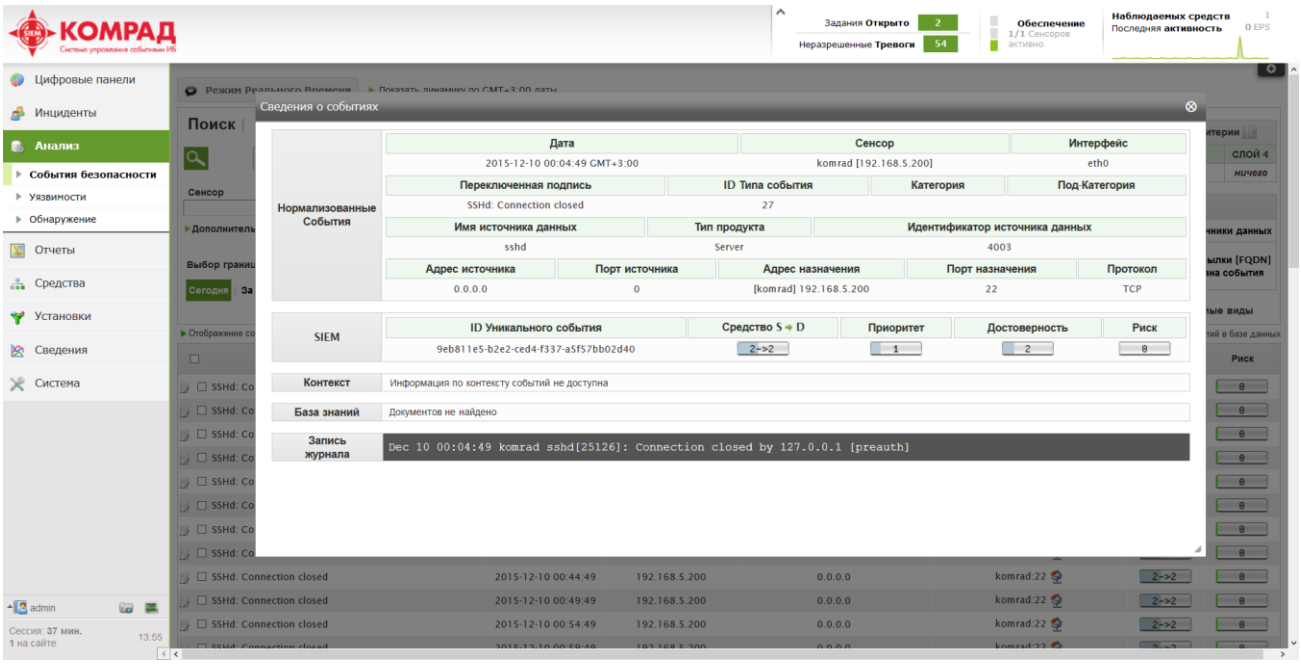



Рисунок 87– Событие безопасности, оконный режим

На странице выбранного события в области «**Нормализованные События**»указаны поля, по которым было нормализовано данное событие. Параметры, по которым производится нормализация данных, представлены в Таблице 11.

Таблица 11 – Параметры нормализации данных в ПК «КОМРАД»

| Поле | Описание | Чем задаются | Пример |
|---|---|---|---|
| id | Уникальный идентификатор события | автоматически | 54cd11e4-b944-225b-5594-61de2d98186a |
| Дата | Дата фиксации события | плагин | 16.10.2014 4:41:33 GMT+4:00 |
| Сенсор | Сенсор, от которого получено событие | автоматически | komrad [192.168.10.198] |
| Устройство | Устройство, от которого получено событие | плагин | CentOS [192.168.10.195] |
| Идентификатор источника данных | Идентификатор плагина | плагин | 4003 |
| ID Типа события | Идентификатор типа события (в плагине) | плагин | 1 |
| Имя источника данных | Название плагина | плагин | sshd |
| Описание источника данных | Описание плагина | плагин | SSHd: Secure Shell daemon |
| Подпись | Подпись события безопасности (плагин: тип события) | плагин | SSHd: Failed password |
| IP ист. | IP-адрес источника | плагин | 122.225.97.103 |
| FQDN IP ист. | Полное доменное имя источника | плагин | mx6.fund123.cn |

| | | | |
|---|---|---|---|
| IP назначения | IP-адрес назначения | плагин | 192.168.10.195 |
| FQDN IP назначения | Полное доменное имя назначения | плагин | centos.test.local |
| L4-proto | Протокол обмена данными | плагин | TCP |
| Порт Ист. | Порт источника | плагин | 15726 |
| Порт назначения | Порт назначения | плагин | 22 |
| Источник | IP-адрес и порт источника | плагин | 122.225.97.103:15726 |
| Назначение | IP-адрес и порт назначения | плагин | 192.168.10.195:22 |
| Контекст | | автоматически | My Company |
| Имя файла | Имя файла, относящегося к событию (например, событие доступа к файлу) | плагин | Empty |
| Имя пользователя | Имя пользователя | плагин | root |
| Пароль | Пароль | плагин | Empty |
| Userdata1 | Дополнительное поле | плагин | Empty |
| Userdata2 | Дополнительное поле | плагин | Empty |
| Userdata3 | Дополнительное поле | плагин | Empty |
| Userdata4 | Дополнительное поле | плагин | Empty |
| Userdata5 | Дополнительное поле | плагин | Empty |
| Userdata6 | Дополнительное поле | плагин | Empty |
| Userdata7 | Дополнительное поле | плагин | Empty |
| Userdata8 | Дополнительное поле | плагин | Empty |
| Userdata9 | Дополнительное поле | плагин | Empty |
| Полезная нагрузка | Ненормализованное событие | плагин | Oct 16 04:41:33 centos sshd[46527]: Failed password for root from 122.225.97.103 port 15726 ssh2 |
| Надежность | Достоверность события | автоматически | 1 |
| Приоритет | Приоритет события | автоматически | 2 |
| Средство SD | Значение средства | автоматически | 2->2 |
| Риск | Риск события | автоматически | 0 |
| IDM: MAC IP источника | MAC-адрес источника (на основании данных системы) | автоматически | Empty |
| IDM MAC IP назначения | MAC-адрес назначения (на основании данных системы) | автоматически | 52:F7:C6:C0:91:80 |
| Реп. Ист. Прио. IP | "статистический" приоритет источника | автоматически | 2 |
| Реп. Назн. Приор. IP | "статистический" приоритет хоста назначения | автоматически | 0 |
| Реп. Ист. Надежн. IP | "статистическая" достоверность источника | автоматически | 3 |
| Реп. Назн. Надежн. IP | "статистическая" достоверность хоста назначения | автоматически | 0 |
| Реп. Ист. Дей.с IP | "статистическая" активность источника | автоматически | Scanning Host |
| Реп. Назн. Дей.с IP | "статистическая" активность хоста назначения | автоматически | Empty |

| | | | |
|---|---|---|---|
| IDM источник | | автоматически | Empty |
| IDM назначения | | автоматически | Empty |
| IDM User@Domain IP Источника | | автоматически | Empty |
| IDM User@Domain IP Назначения | | автоматически | Empty |

В области «**SIEM**»содержатся поля, по которым был произведен расчет риска события.

Стандартная формула расчета риска в ПК «КОМРАД» выглядит следующим образом:

$$\text{Риск} = \left\lfloor \frac{\text{Достоверность} \times \text{Приоритет} \times \text{Актив}}{25} \right\rfloor$$

Актив (значение актива) – определяет значимость актива для инфраструктуры.

Приоритет (приоритет инцидента) определяет степень угрозы состоявшегося инцидента [0..5]. Приоритет задается в директиве единожды и действует на всю директиву целиком.

**Достоверность** (достоверность инцидента) определяет величину, характеризующую вероятность наступления данного инцидента [0..10]. Достоверность задается отдельно для каждого уровня директивы корреляции.

В области «**База знаний**»содержится информация из Базы знаний.

В области «**Запись журнала**» доступен текст выбранного события в ненормализованном виде.

**Примечание:** быстрый переход между событиями безопасности возможен посредством кнопок «**Далее**» / «**Предыдущий**».

### 5.2.4. Оценка уровня обеспечения безопасности системы

Для текущей оценки уровня обеспечения безопасности администратор может воспользоваться вкладкой «**Цифровые панели → Риск**» (Рисунок 88).

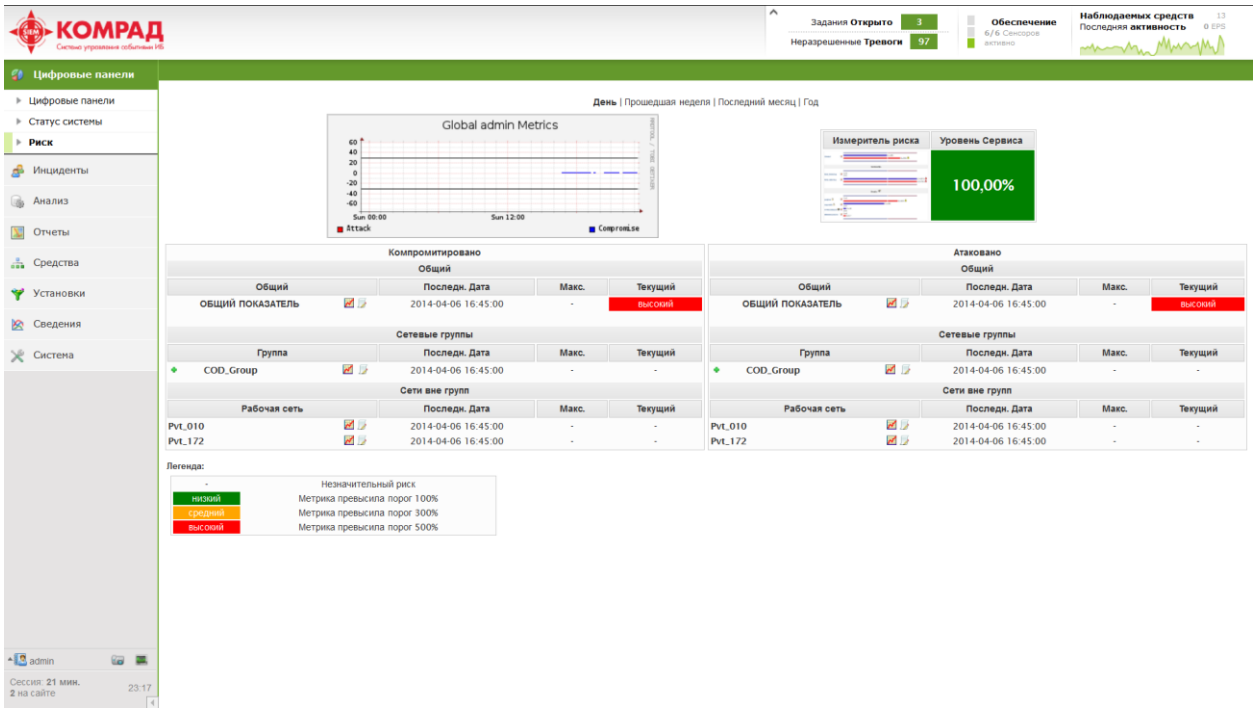



Рисунок 88 – Страница метрик рисков

### 5.2.5. Обработка инцидентов безопасности

Для перехода непосредственно к таблице инцидентов безопасности необходимо перейти в раздел «**Инциденты → Тревоги**» (Рисунок 89).

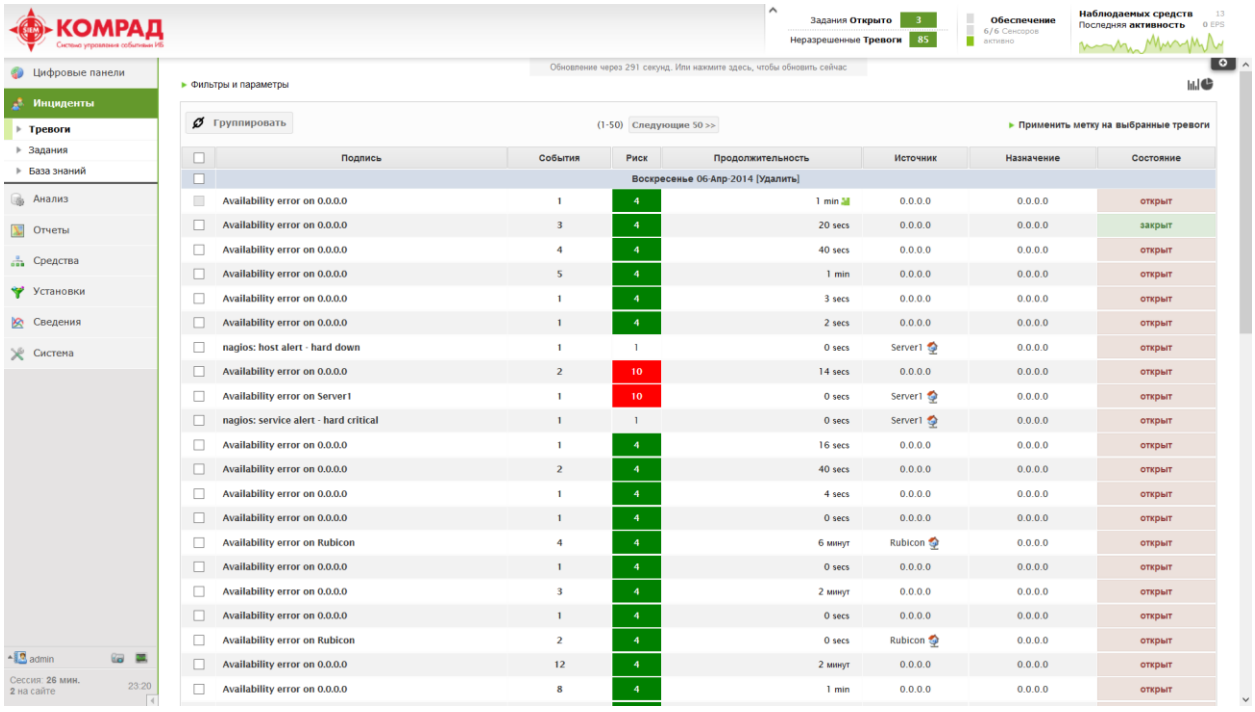



Рисунок 89 – Страница «Тревоги»

Столбцы таблицы имеют следующие заголовки:

- «Подпись» — название инцидента безопасности;

- «События» — количество событий в инциденте;

- «Риск» — значение риска инцидента безопасности (значение от 1 до 10), данное поле заполняется цветом в зависимости от значения, (1,2) — белый, (3,4) — зеленый, (5,6) — жёлтый, (7,8) — оранжевый, (9,10) — красный;

- «Продолжительность» — время между первым и последним событием в инциденте.

**Примечание**: анимированная пиктограмма рядом со значением времени указывает на то, что корреляция событий в инциденте не завершена.

- «Источник» — IP-адрес или имя узла-источника;

- «Назначение» — IP-адрес или имя узла-назначения;

- «Состояние» — статус инцидента безопасности (имеет два значения «открыт» или «закрыт»).

Кнопка Удалить выбранные позволяет удалить инциденты безопасности, помеченные галочкой.

Кнопка Закрыть выбранные позволяет закрыть все инциденты безопасности, помеченные галочкой.

Нажатие на ссылку «Удалить ВСЕ тревоги» приведет к удалению всех инцидентов, хранимых в системе.

Нажатие на ссылку «Фильтры и параметры» приведёт к открытию панели фильтрации таблицы инцидентов безопасности (Рисунок 90).

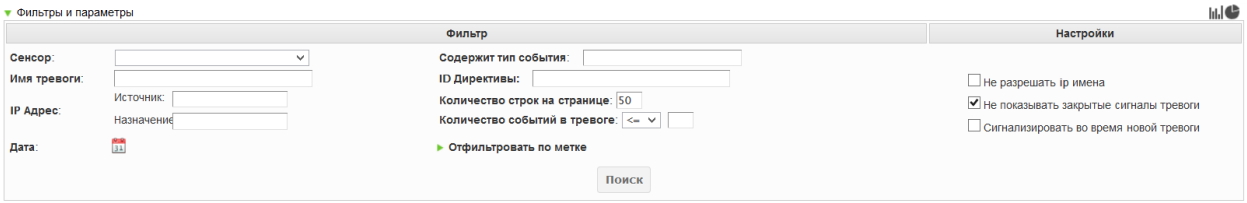



Рисунок 90 – Панель фильтров отображения инцидентов безопасности

В данной панели доступны следующие параметры:

- Сенсор — выбор сенсора, с которого поступил инцидент;

- Имя тревоги — данное поле используется для поиска инцидентов соответствующих вводимому тексту, при этом поиск возможен как по целому названию, так и по части строки названия инцидента;

- IPадрес — в поля «Источник» или «Назначение» вводится IP-адрес для поиска.

**Примечание**: если IP-адрес уже хранится в базе данных системы, возможен его выбор из выпадающего списка.

- Дата — нажатие на пиктограмму приведёт к вызову календаря, в котором можно выбрать интервал дат для отображения;

- Содержит тип события — в данном поле можно задать тип события, который должен присутствовать в отображаемых инцидентах;

- IDдирективы — фильтрация по идентификатору директивы корреляции;

- Количество строк на странице — задаёт отображаемое количество строк на одной странице;

- Количество событий в тревоге — задаёт значение количества событий в инциденте, при этом возможно два режима фильтрации: не менее заданного значения (>=) или не более заданного (<=);

- Отфильтровать по метке — выпадающий список доступных в системе меток для инцидентов безопасности;

- Не разрешать IPимена — включает режим, в котором отображаемые узлы источников и назначения отображаются в виде IP-адресов, а не имён;

- Не показывать закрытые сигналы тревоги — включает режим отображения всех инцидентов, включая закрытые;

- Сигнализировать во время новой тревоги — при включенном режиме фильтрации данная опция позволяет сигнализировать о появлении новых инцидентов безопасности.

После установки все необходимых параметров фильтрации необходимо нажать на кнопку «**Поиск**».

Нажатие на ссылку «**Применить метку на выбранные тревоги**» вызывает выпадающий список (Рисунок 91), который позволяет добавить инцидентам безопасности метку. Нажатие на пункт «Редактировать» в этом списке вызывает окно редактирования меток (Рисунок 92).В данном окне возможно добавление, удаление и изменение меток инцидентов безопасности. Одному инциденту может быть присвоено несколько меток.

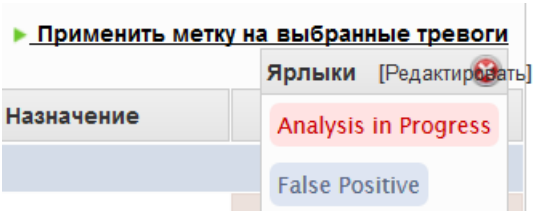



Рисунок 91 – Выбор меток для инцидентов безопасности

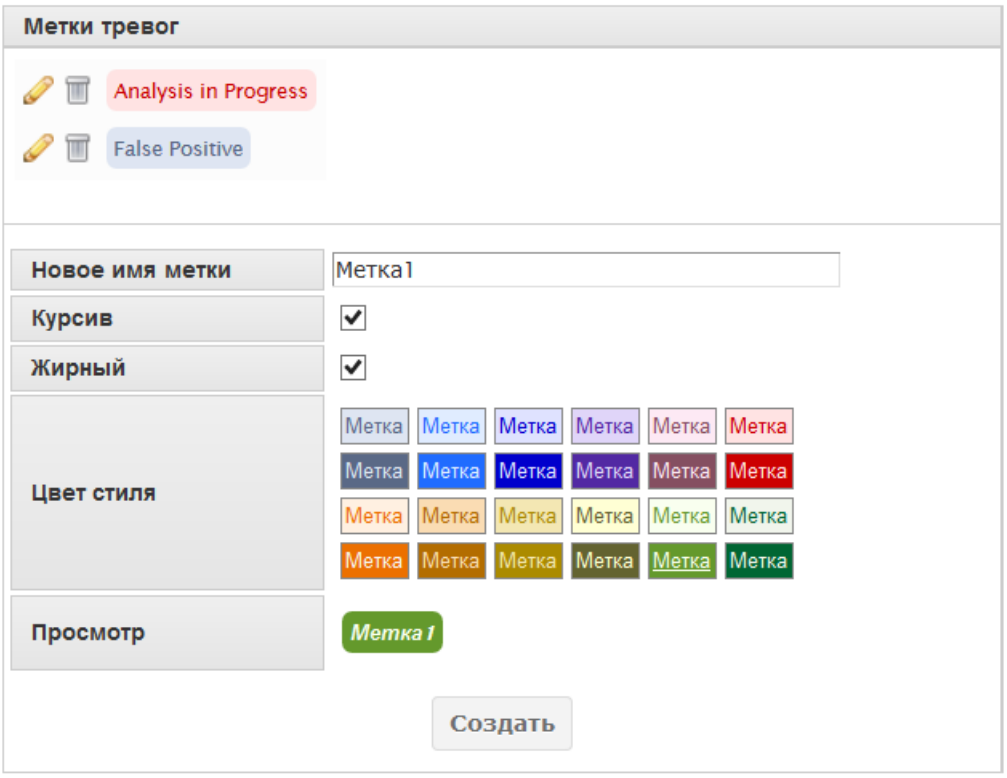



Рисунок 92 – Окно редактирования меток

На странице всех инцидентов содержится кнопка «**Группировать**». Нажатие на данную кнопку приведёт к открытию списка всех инцидентов безопасности, сгруппированных по типу инцидента (Рисунок 93). В данном режиме просмотра на-

против каждого типа инцидентов расположена пиктограмма «+», нажатие на которую позволяет получить список всех инцидентов в группе.

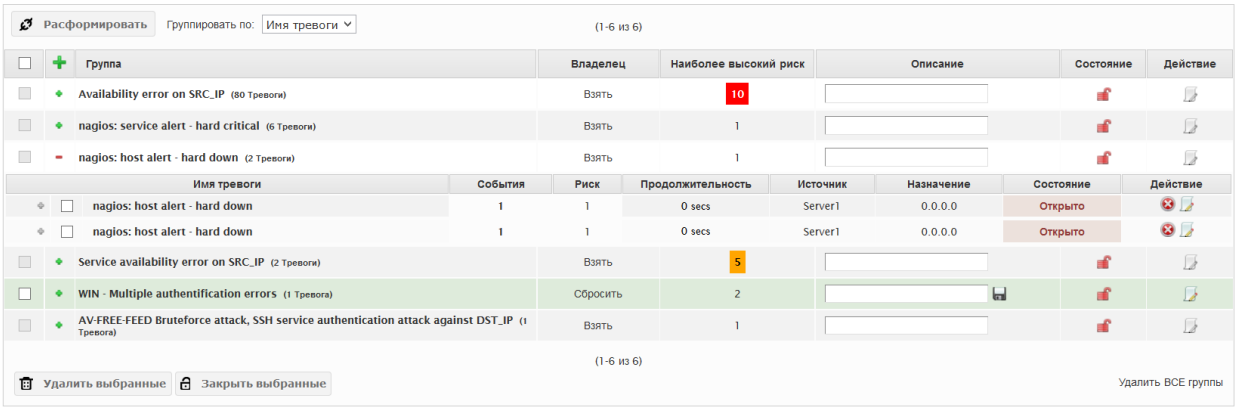



Рисунок 93 – Инциденты безопасности, сгруппированные по типу

Наведение курсора мыши на название инцидента вызывает всплывающее окно с дополнительной информацией об инциденте (Рисунок 94).

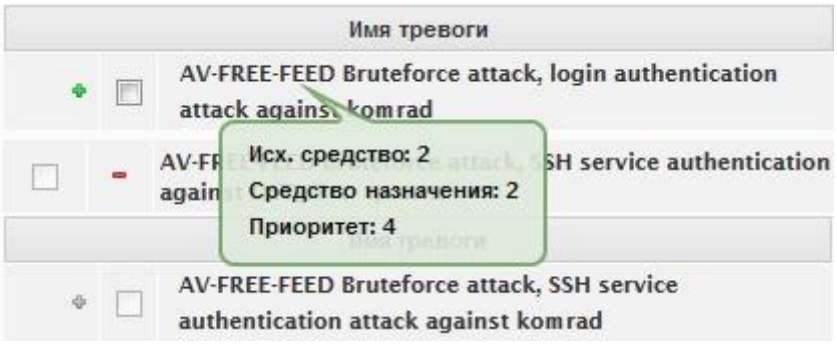
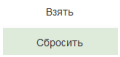
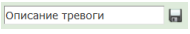



Рисунок 94 – Всплывающее окно



— нажатие на поле в столбце «Владелец» переводит группу инцидентов в одно из двух состояний. Нажатие на поле «**Взять**» позволяет текущему пользователю совершать действия с группой инцидентов. Доступны следующие действия: 

— в данное поле можно добавить описание группы инцидентов, нажатие на пиктограмму дискеты позволяет сохранить внесенное описание;  — нажатие на пиктограмму закрывает группу инцидентов;  — позволяет открыть задание для группы инцидентов или отдельного инцидента;  - позволяет удалить инцидент из системы.

В режиме группировки инцидентов безопасности доступны другие режимы группировки (Рисунок 95), по умолчанию установлен режим группировки по имени инцидента.

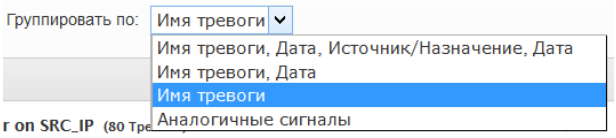



Рисунок 95 – Выпадающий список типа группировки

Кнопка Расформировать переводит страницу в режим обычного списка инцидентов безопасности.

Нажатие на имени инцидента безопасности приведёт к открытию страницы, содержащей информацию по выбранному инциденту (Рисунок 96), где представлен список событий, содержащихся в инциденте.

Нажатие на название события приведёт к открытию всплывающего окна с подробной информацией по этому событию. Зелёным цветом отмечена строка, содержащая информацию о правиле директивы корреляции, сгенерировавшем данный инцидент.

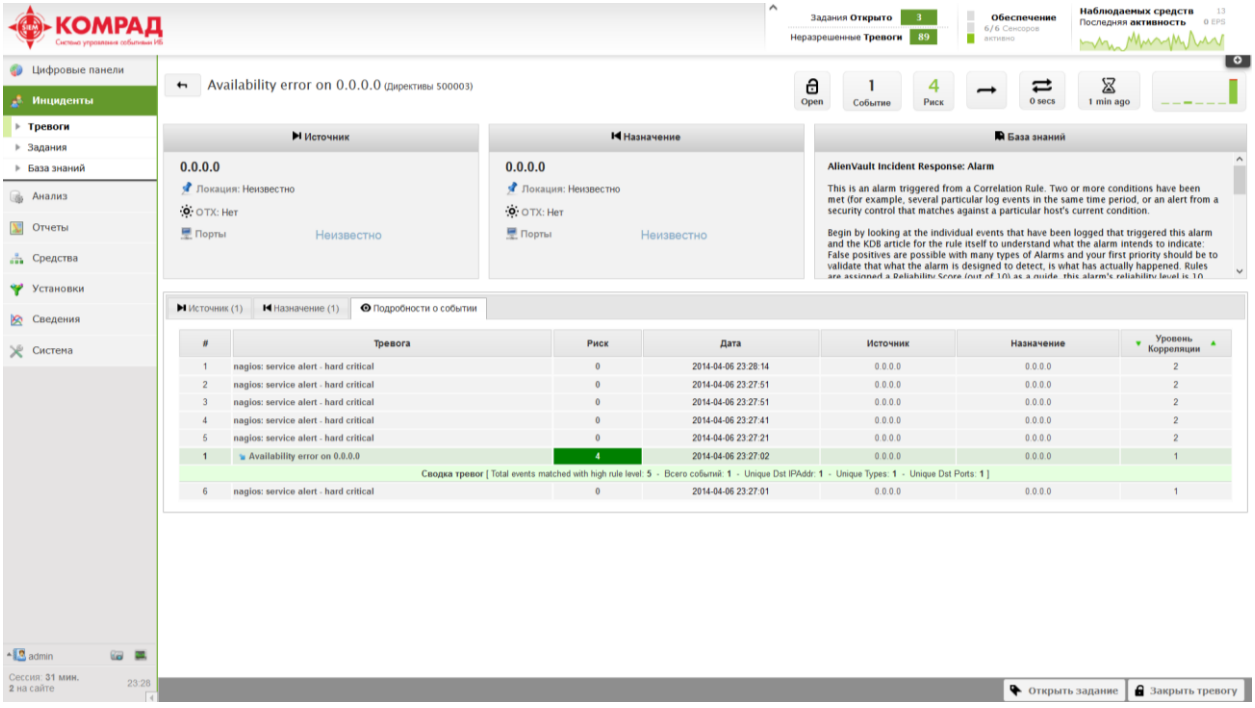



Рисунок 96 – Страница информации по выбранному инциденту

В окне открытого инцидента безопасности в полях «**Источник**» и «**Назначение**» содержится подробная информация об узлах источника и назначения соответственно, вплоть до TCP/UDPпорта.

В поле «**База знаний**» содержится информация о данном типе инцидента, а также рекомендации по его устранению.

Пиктограмма  позволяет вернуться в меню, содержащее все инциденты. В верхнем поле находятся пиктограммы с информацией о данном инциденте:

— статус инцидента, может принимать значение «Open» и «Close»;

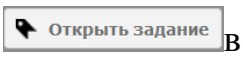
— количество событий в инциденте;

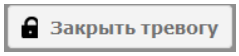
— уровень риска данного инцидента; — тип инцидента, может принимать значения «one-to-one», «one-to-many», «many-to-many»;

— время корреляции данного инцидента;

— время, прошедшее с момента выявления данного инцидента.

В ПК «КОМРАД» реализован механизм заявок на расследование инцидентов безопасности. Администратор с помощью данного механизма может назначать определённые задания конкретным исполнителям, которые должны вести отчётность о ходе выполнения заданий.

Для обработки инцидента или передачи заявки на его обработку другим пользователямадминистратор должен открыть новое задание на обработку инцидента ИБ с помощью кнопки 

в правой нижней части окна инцидента ИБ (Кнопка 

позволяет закрыть тревогу без создания задания на расследование). Задание открывается в новом окне (Рисунок 97), где требуется заполнить все необходимые поля. После нажатия кнопки «**Обновить**» формируется задание (заявка) на обработку инцидента безопасности, которой присваивается свой уникальный номер (ID задания).

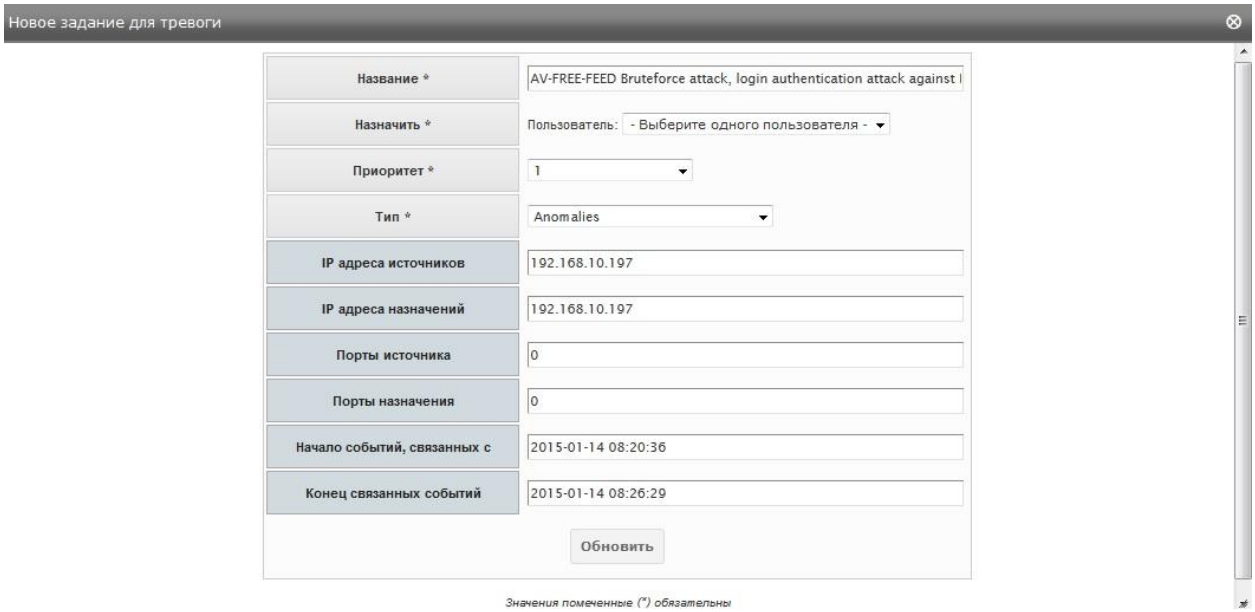



Рисунок 97 – Окно нового задания для тревоги

После заполнения всех обязательных полей (часть полей заполнена автоматически на основе данных об инциденте, но доступна для редактирования) и нажатия кнопки «**Обновить**» будет создана страница нового задания (Рисунок 98).

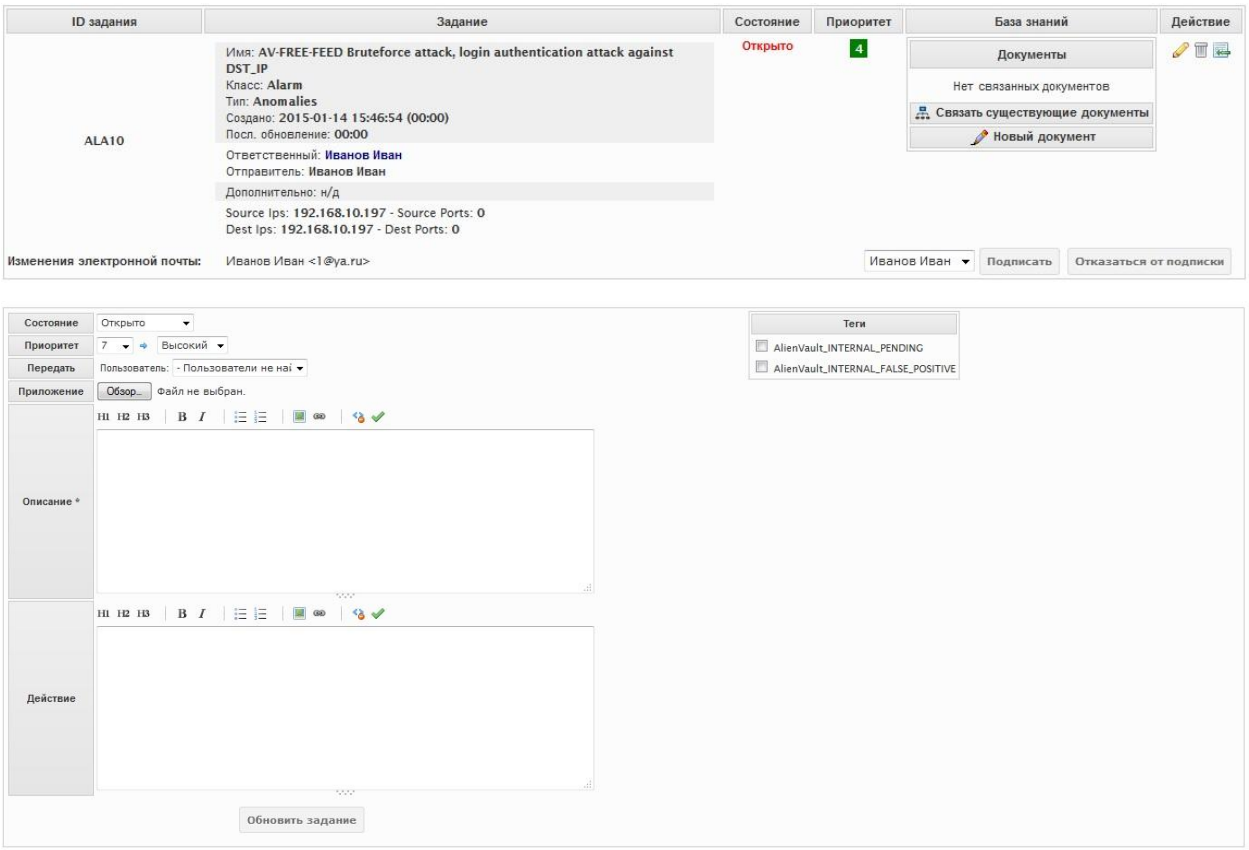



Рисунок 98 – Страница заявки на расследование инцидента безопасности

В поле «**Состояние**» вносится информация о текущей стадии обработки инцидента (Открыто, Назначено, Изучение, Ожидание, Тестирование, Закрыто).

В поле «**Приоритет**» назначается приоритет задания (доступны цифровые значения от 1 до 10 или категории:Низкий, Средний, Высокий).

В поле «**Передать**» производится выбор пользователя, которому назначается задание.

**Примечание**: заданию должен быть назначен хотя бы один пользователь.

Нажатие на кнопку «**Обзор**» в поле «**Приложение**» позволяет добавить к заявке файлы, хранящиеся локально (например, снимки экрана).

В поле «**Описание**» вводится описание шага обработки или иная дополнительная информация (данное поле обязательно к заполнению).

В поле «**Действие**» можно указать действия, произведённые в ходе обработки инцидента.

Кнопка «**Обновить задание**» добавляет новую запись в случае корректного заполнения всех обязательных полей.

Заявка поступит в систему и может отслеживаться во вкладке **«Инциденты → Задания»** (Рисунок 99),где допускается фильтрация заявок по классам, типам, ответственному исполнителю и прочим показателям.

Нажатие на заголовок инцидента в поле «Название» позволяет открыть окно обработки выбранного задания и внесения необходимых изменений.

**Примечание:** новые задания добавляются как вручную, так и автоматически в соответствии с настроенной политикой. Для открытия задания вручную внизу списка заданий из выпадающего списка выберите тип задания (Тревога, Событие, Метрика, Уязвимость, Аномалии) и нажмите кнопку «**Создать**».

**Примечание:** у администратора безопасности есть доступ ко всем без исключения заданиям в ПК «КОМРАД».

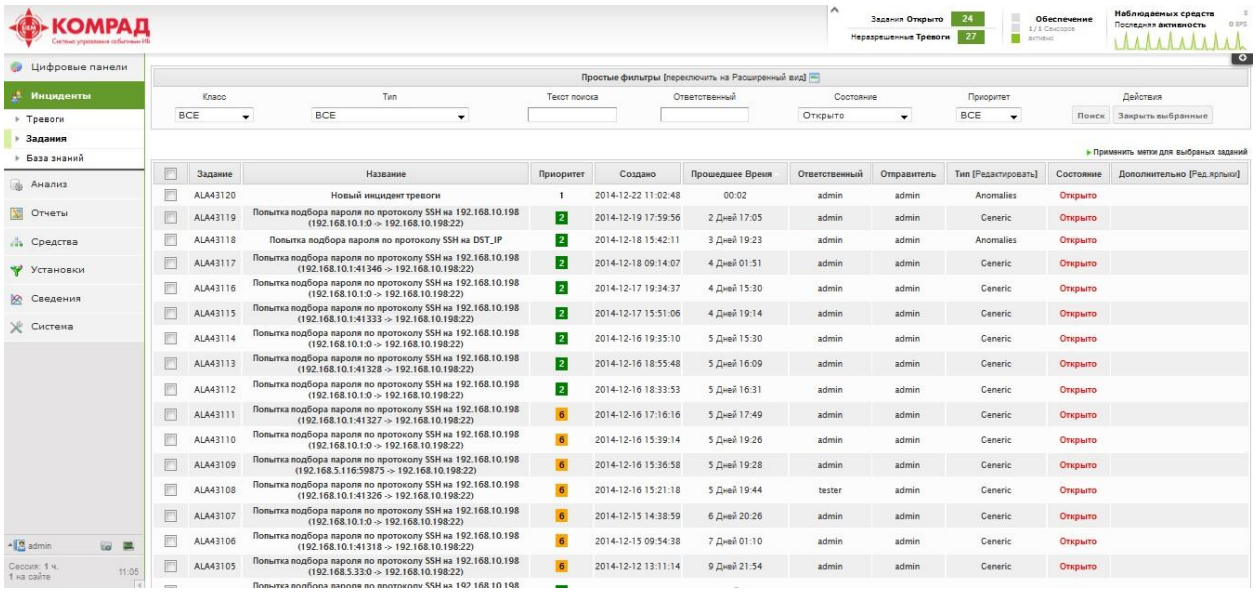



Рисунок 99 – Страница заданий ПК «КОМРАД»

### 5.2.6. База знаний ПК

В разделе «**Инциденты → База знаний**» доступна База знаний по типам инцидентов и событий безопасности (Рисунок 100). Детальный просмотр информации каждой записи возможен при нажатии на соответствующее название (Рисунок 101).

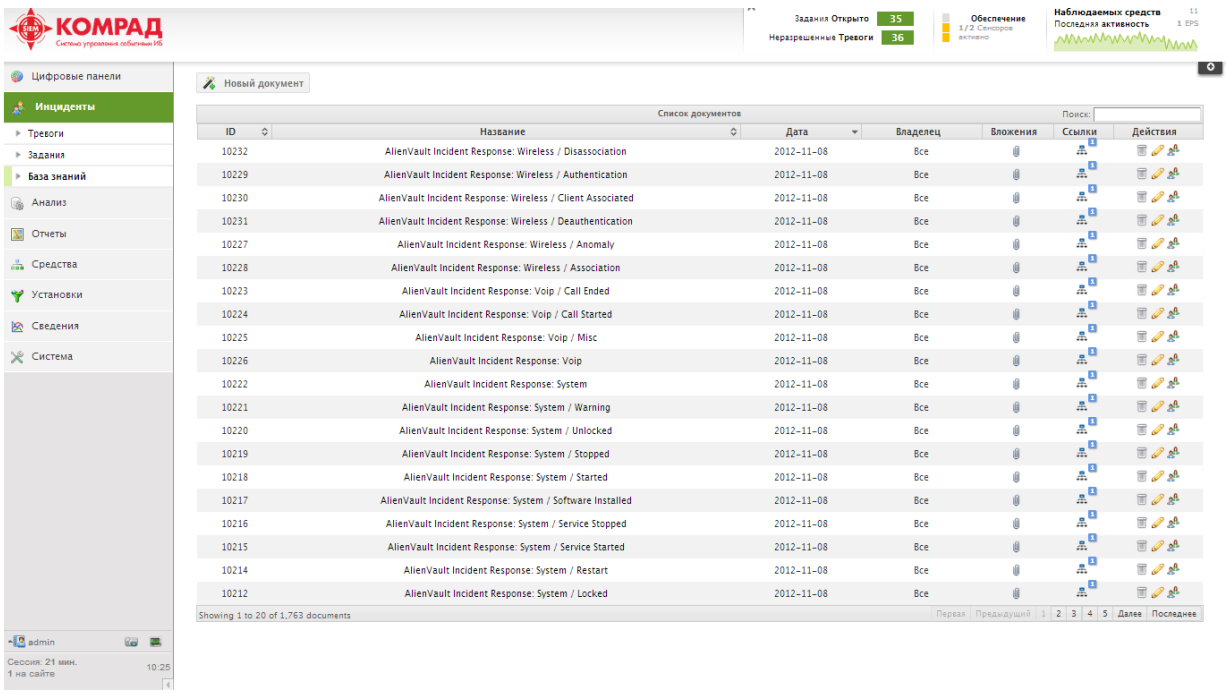



Рисунок 100– База знаний по типам инцидентов и событий безопасности

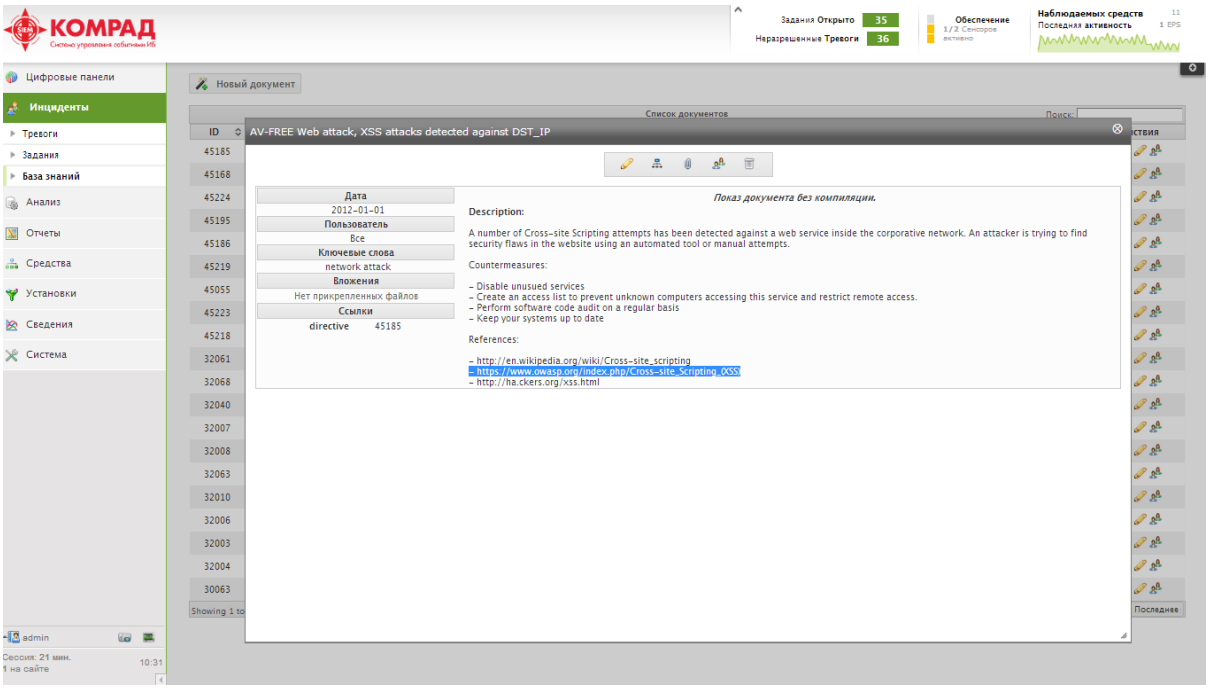



Рисунок 101– Детальная информация по записям в Базе знаний

Возможно добавление новых типов и изменение имеющихся инцидентов, занесённых в Базу знаний (Рисунок 102).

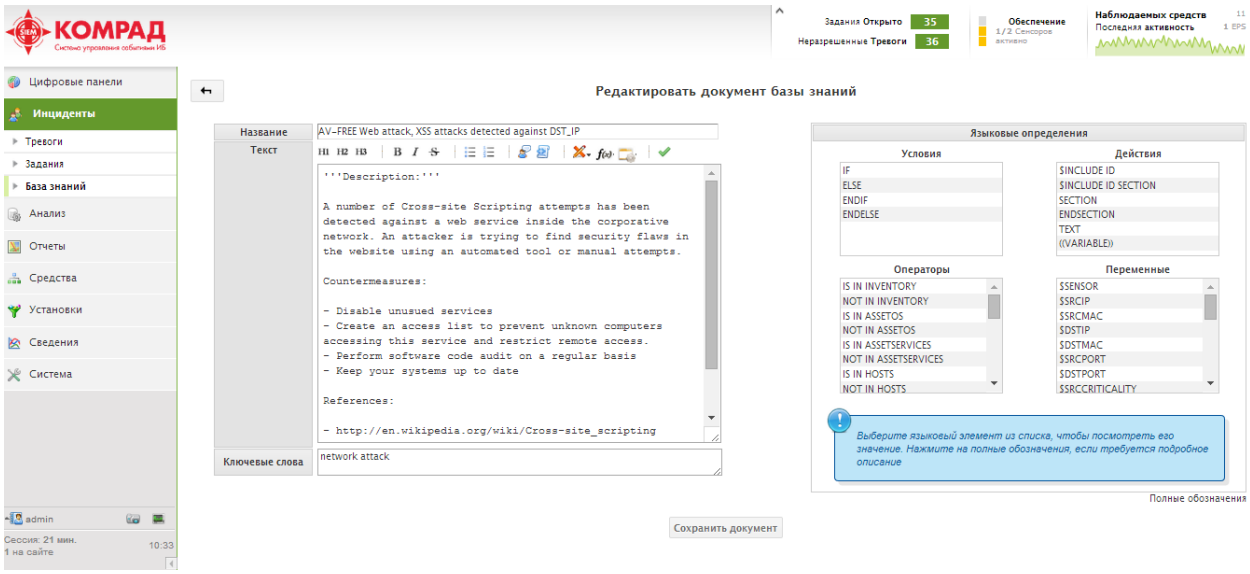



Рисунок 102– Страница редактирования записей в Базе знаний

Редактирование связей записей возможно при нажатии на пиктограмму (Рисунок 103).

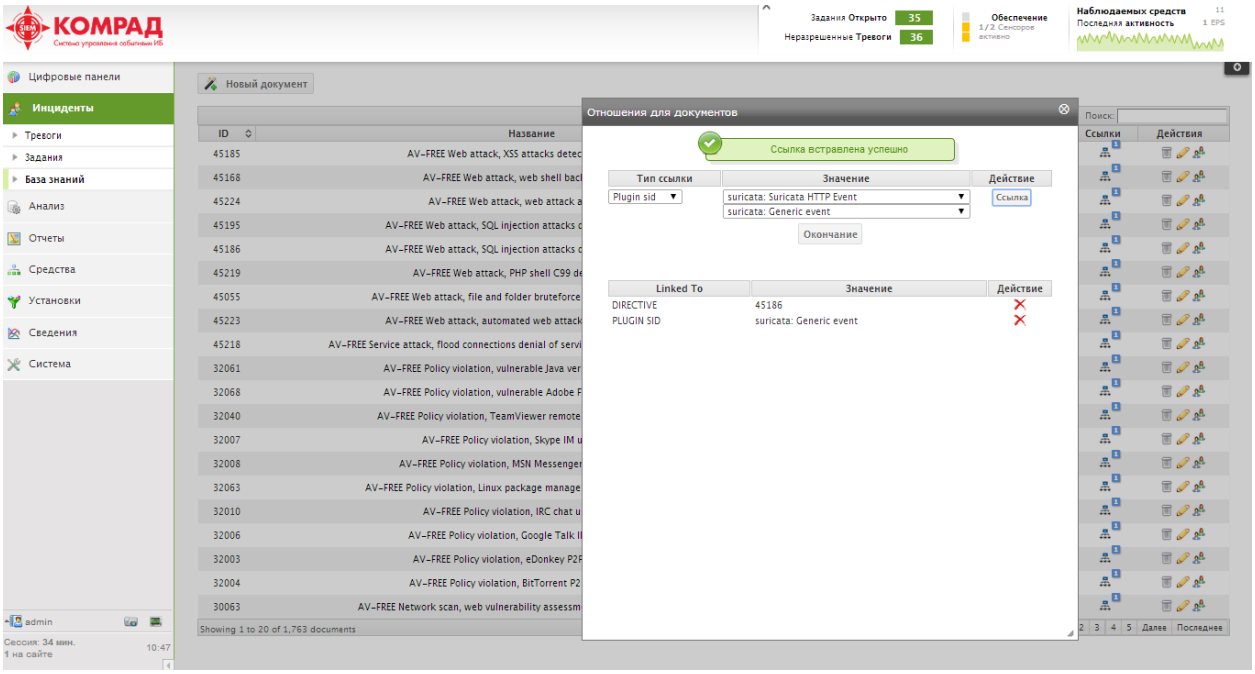



Рисунок 103– Редактирование связей записей в Базе знаний

### 5.2.7. Управление учётными записями пользователей

#### 5.2.7.1. Таблица зарегистрированных пользователей

Для просмотра всех зарегистрированных в ПК «КОМРАД» пользователей системы необходимо зайти в пункт меню «**Система → Пользователи**» (Рисунок 104).

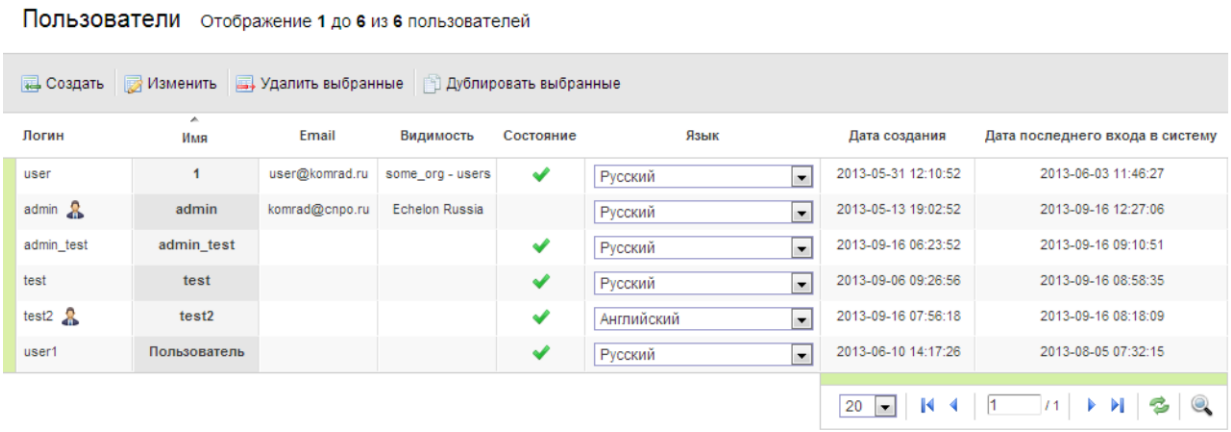



Рисунок 104 – Фрагмент окна просмотра списка зарегистрированных пользователей

Содержащая список всех зарегистрированных пользователей таблица имеет следующие поля:

- **Логин**— идентификатор пользователя в системе.
- **Имя** — реальное имя пользователя, отображаемое в отчётах и статистике, а также при оформлении заявок на обработку инцидентов ИБ.
- **Email**— адрес электронной почты пользователя, на который отправляются уведомления, заявки и отчёты.
- **Видимость** — данные, введённые при регистрации пользователя в поля **Организация** и **Отдел**.
- **Состояние** — текущеесостояние пользователя: доступен (✔) или недоступен (✘).
- **Язык**— выбранный для данного пользователя язык интерфейса ПК (доступные варианты:Chinese simplified, Chinese traditional, Английский, Испанский, Португальский, Русский).
- **Дата создания** — дата создания учётной записи данного пользователя.

- **Дата последнего входа в систему** — дата и время последнего успешного входа данного пользователя в систему.

Под списком зарегистрированных пользователей расположена панель управления, изображённая на Рисунке 105.

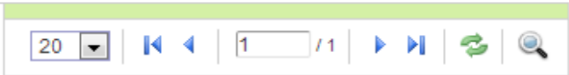



Рисунок 105 – Панель управления списком зарегистрированных пользователей

— количество записей, отображаемых на одной странице (10, 15, 20, 25, 35 и 50 записей на страницу);

— переход на первую страницу списка зарегистрированных пользователей;

— переход на предыдущую страницу;

— текущая страница / общее количество страниц списка;

— переход на следующую страницу;

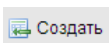
— переход на последнюю страницу списка;

— обновление отображаемой информации;

— поиск по идентификаторам пользователей в системе. При нажатии на данную кнопку открывается меню поиска (Рисунок 106):

Рисунок 106 – Меню поиска пользователей ПК «КОМРАД»

### 5.2.7.2. Добавление учётных записей пользователей

Добавлять новые учётные записи может только пользователь ПК «КОМРАД» с правами администратора. Для этого необходимо в разделе «**Система → Пользователи**» нажать кнопку 

. После этого открывается окносоздания новой учётной записи (Рисунок 107).

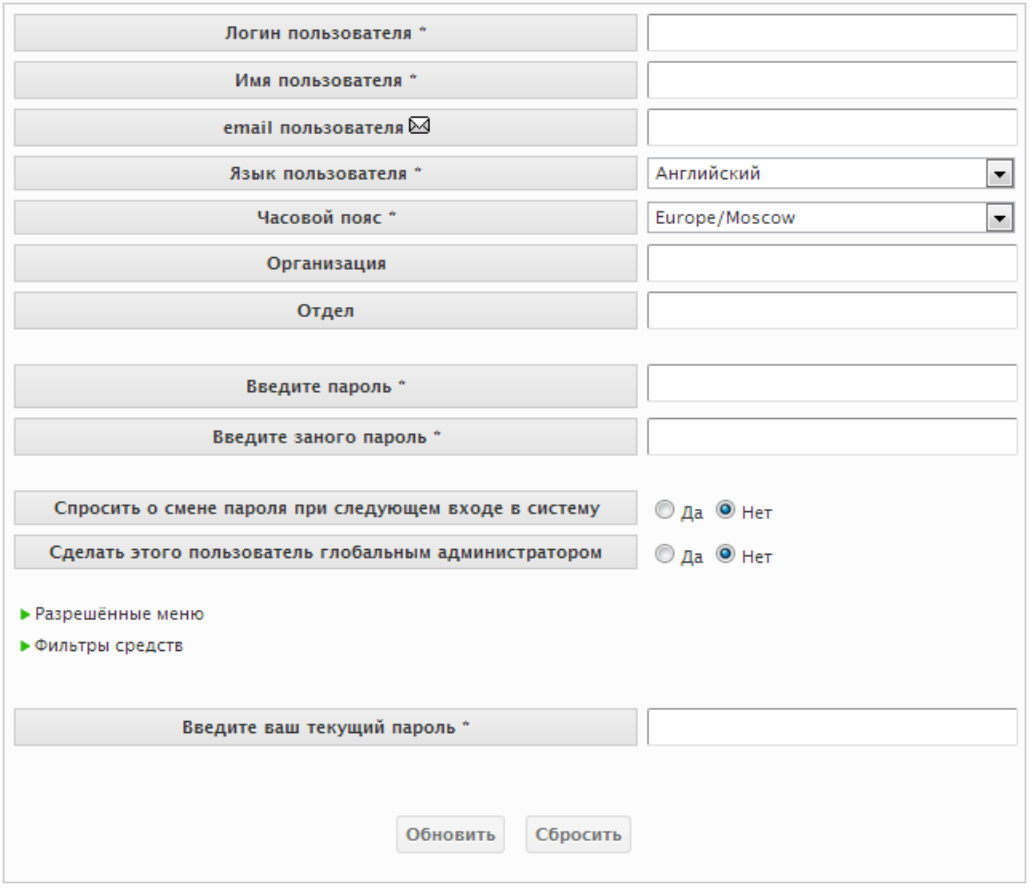



Рисунок 107 – Окно создания нового пользователя системы

В соответствующие поля последовательно вводятся данные нового пользователя системы (логин, имя пользователя, адрес электронной почты, предпочтительный язык интерфейса, часовой пояс, организация иподразделение пользователя), присваивается пароль с указанием необходимости его смены при первом входе пользователя в систему, выполняется выбор роли пользователя (глобальный администратор или нет) и разрешённых к просмотру пунктов меню, а также добавляются источники, мониторинг событий которых сможет осуществлять данный пользователь. (Структура меню веб-интерфейса применительно к указанным ролям приведена в Приложении Г)

После этого администратор вводит свой пароль и нажимает«**Обновить**» для создания новой учётной записи с введёнными данными или «**Сбросить**» при необходимости повторно ввести данные.

**Примечание**: в поле «Разрешённые меню» представлен полный список доступных пользователю меню. Необходимо выбрать только те пункты меню, к которым создаваемому пользователю будет разрешён доступ.

В «Фильтрах средств» приведены все доступные источники событий. Необходимо добавить те источники событий, данные с которых должны быть доступны создаваемому пользователю. По умолчанию данные списки пустые (пользователь не получаетданные об инцидентах ни от одного из источников событий).

При выборе «Да» в пункте «Спросить о смене пароля при следующем входе в систему» при первом успешном входе в систему пользователь с новой учётной записью получает уведомление о необходимости смены пароля (Рисунок 108).

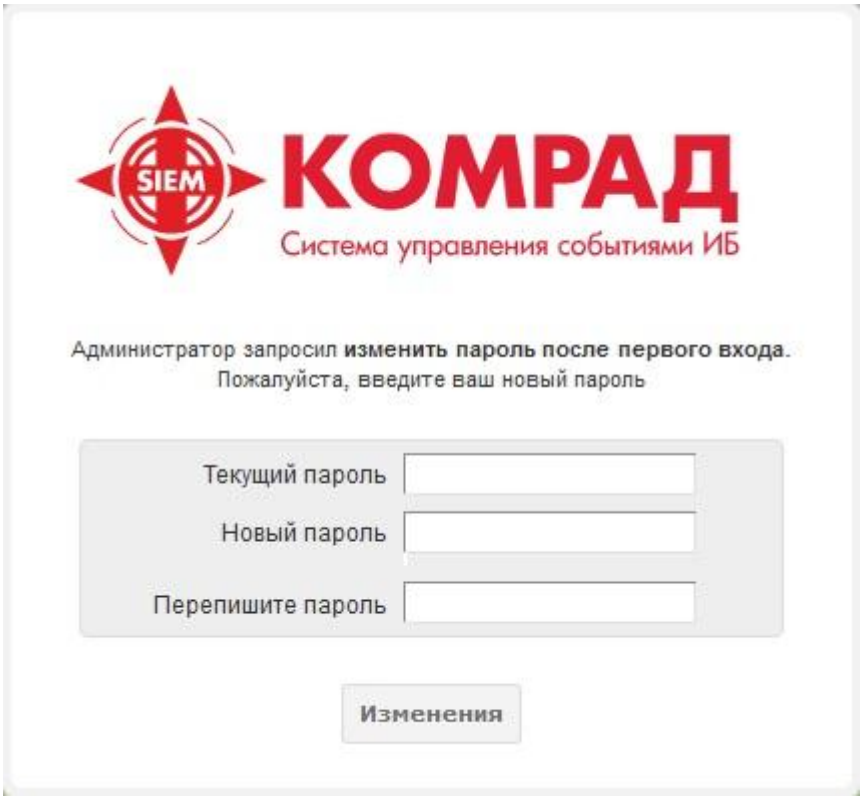
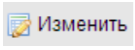



Рисунок 108 – Уведомление о необходимости смены пароля

### 5.2.7.3. Изменение учётных записей пользователей

Администратор может вносить изменения в существующие учётные записи пользователей в окне учётной записи, в котором все поля, за исключением поля **Логин пользователя**, будут доступны для редактирования. Открыть данное окно можно несколькими способами:

- выделить строку учётной записи, в которую необходимо внести изменения, и нажать кнопку 

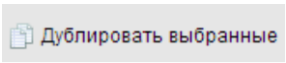
;
- двойным щелчком левой кнопкой мыши по строке учётной записи;
- нажав на имя соответствующего пользователя в столбце «Имя».

#### 5.2.7.4. Удаление учётных записей пользователей

Для удаления учётной записи пользователя администратор в разделе **«Система → Пользователи»** должен выделить строку записи, соответствующую тому пользователю, учётную запись которого следует удалить, и нажать кнопку

. Появится окно с запросом подтверждения действия, в котором необходимо нажать **«ОК»**или **«Отмена»**.

#### 5.2.7.5. Копирование учётных записей пользователей

Для создания копии учётной записи администратор должен выбрать строку копируемой учётной записи в разделе **«Система → Пользователи»**, и нажать кнопку 

. Откроется окно, аналогичное окну, изображенному на Рисунке 107с уже внесенными данными о новом пользователе.

### 5.2.8. Управление активами

Для работы с активами ИТ-инфраструктуры используется вкладка «**Средства →Средства**» (Рисунок 109).

На данной вкладке представлены хосты, сети и порты ИТ-инфраструктуры.

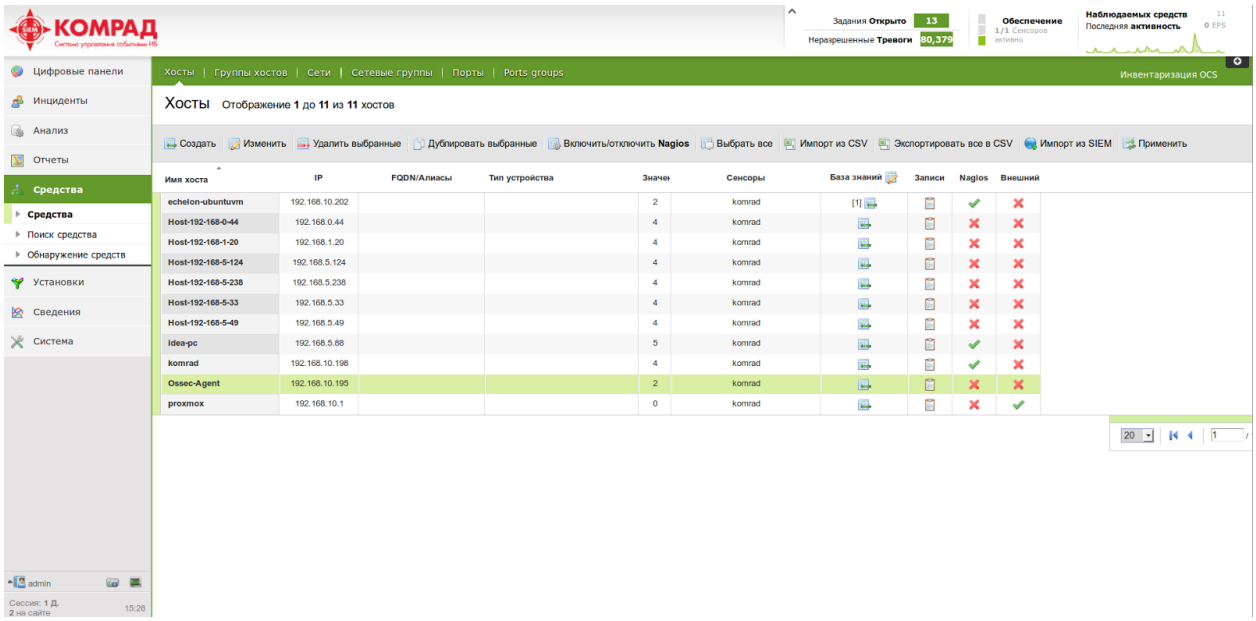



Рисунок 109 – Работа с активами

### 5.2.8.1. Хосты

В разделе «Хосты» доступны следующие действия:

Создать - создание записи о новом узле;

Изменить - изменение имеющейся записи об узле;

Удалить выбранные - удаление выбранных записей (возможен выбор нескольких записей одновременно, последовательным нажатием левой кнопки мыши на каждую запись);

Дублировать выбранные - создание копии записи выбранного узла, при этом необходимо задать новыйIP-адрес, поскольку данное поле в системе должно быть уникальным.

**Примечание:** дублировать можно только один узел, при выборе нескольких узлов копирование будет выполнено только для верхнего в списке.

Включить/отключить **Nagios** - включение или отключение сервиса мониторинга доступности для выбранных узлов. Включение/отключение сервиса происходит в зависимости от состояния указанного в столбце «Nagios», которое может принимать значение ✔ или ✘, поэтому при выборе нескольких записей с разным значением состояния произойдет их переключение на противоположное;

Выбрать все - выбрать все узлы на странице (количество узлов на странице регулируется в правом нижнем углу таблицы);

Импорт из CSV - импорт записей из файла CSV;

Экспортировать все в CSV - экспорт всех имеющихся записей в файл CSV;

Импорт из SIEM - нажатие на эту кнопку заставит систему просканировать базу данных событий безопасности в поисках новых узлов (Рисунок 110) (используются поля «IP источника» и «IP назначения»), новые записи будут добавлены в список с именами вида «Host-<ip addr>»);

Применить - применение совершенных изменений;

- нажатие на данную пиктограмму позволяет привязать к записи об узле информацию из Базы знаний, возможна привязка нескольких записей;

- пиктограмма позволяет добавить произвольную запись для выбранного узла.

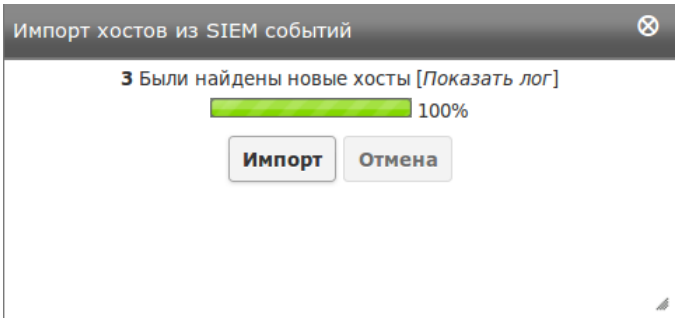



Рисунок 110 – Диалоговое окно импорта списка узлов из событий ИБ

Создание новой записи об узле сети открывает окно, в которое необходимо внести информацию об узле (Рисунок 111).

Возможна привязка узла к определенному сенсору, а также включение сервиса Nagios для мониторинга доступности узла. Узлу могут быть присвоены дополнительные поля: тип устройства, операционная система, MAC-адрес, полное доменное имя (FQDN), произвольное описание. Кроме того, узлу должно быть назначено значение средства (в диапазоне от 0 до 5 в зависимости от критичности ресурса для всей системы в целом) для дальнейшего вычисления риска инцидентов связанных с этим узлом. После заполнения необходимых полей требуется нажать кнопку «**Обновить**». Кнопка «**Очистить**» возвращает содержимое полей к первоначальному виду. Кнопка «**Отменить**» возвращает к списку узлов.

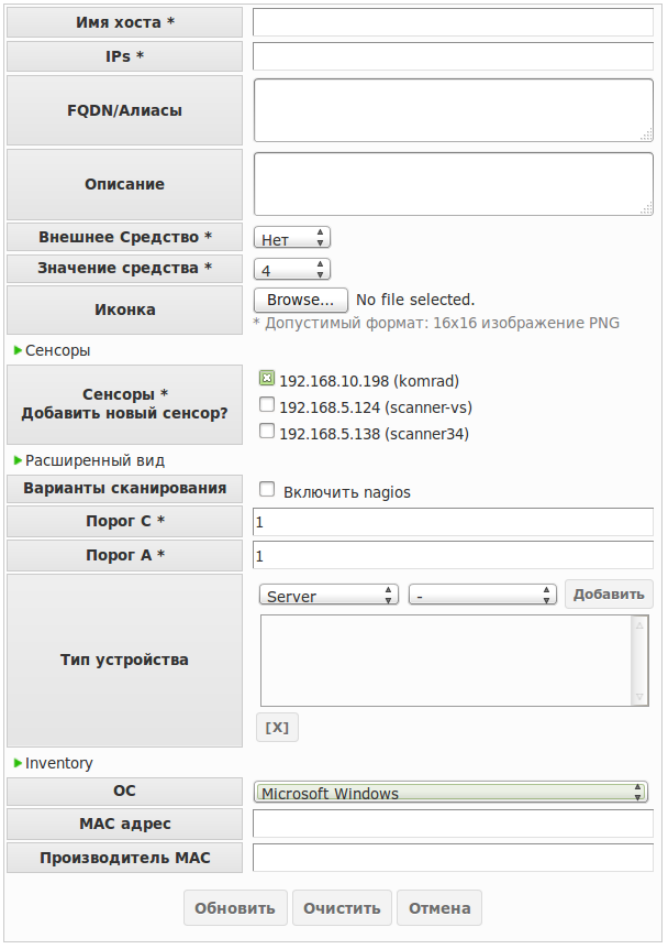



Рисунок 111 – Создание нового узла сети

Нажатие на кнопку «**Изменить**» приводит к открытию диалогового окна с информацией об узле (Рисунок 112). Левая часть окна аналогична окну создания нового узла. Справа расположена информация об узле сети, полученная от системы инвентаризации или сканера узлов.

Сканер узлов может быть запущен принудительно нажатием на кнопку «**Реестр ресурсов [Запустить локальное сканирование ]**», при этом будет просканирован узел и TCP/UDP порты. Полученная в результате сканирования информация будет внесена в запись об узле.

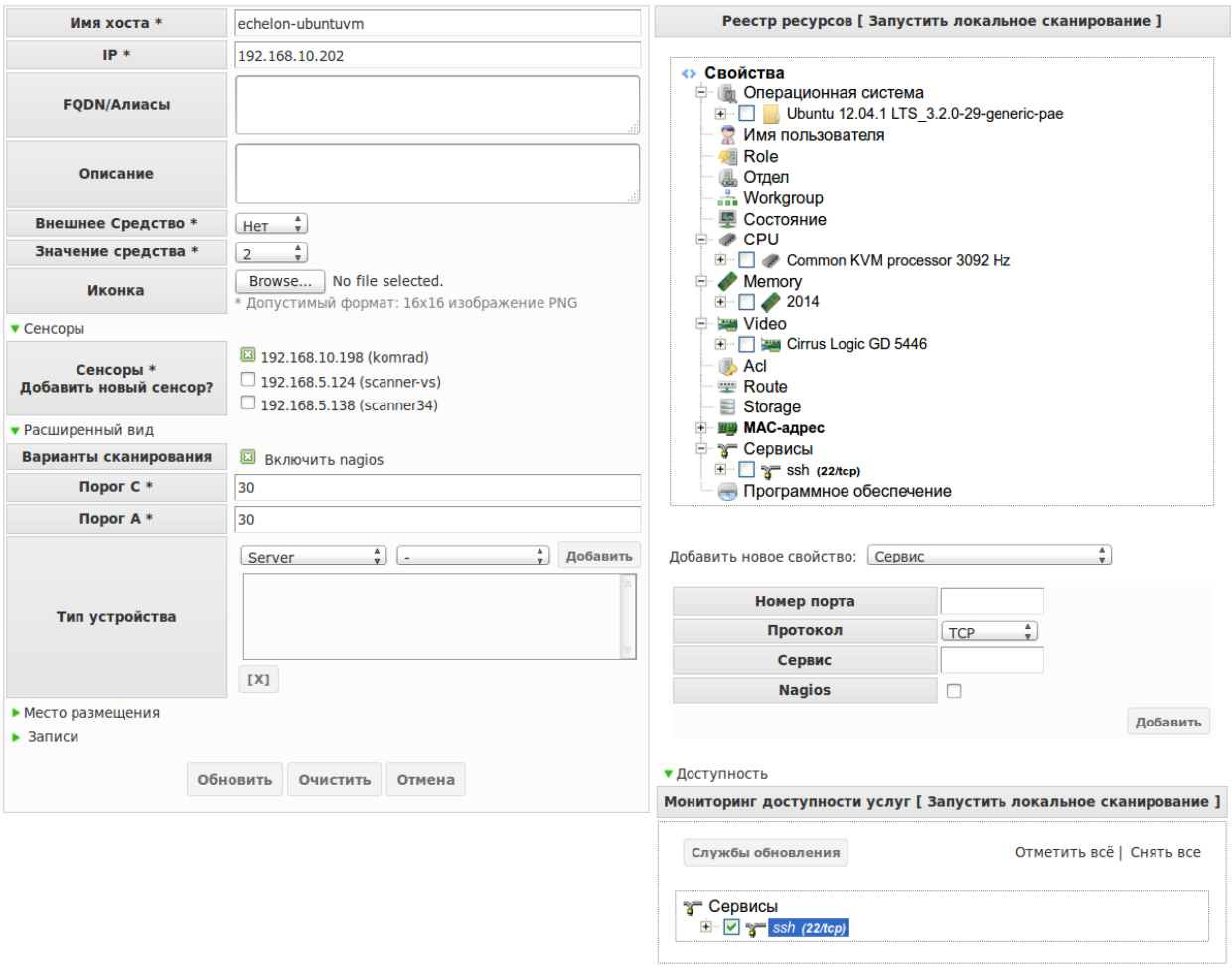



Рисунок 112 – Информация об узле сети

В случае, когда узел имеет открытые TCP/UDP порты, обнаруженные сканированием, возможно включение мониторинга доступности этих портов. Для этого необходимо поставить галочку напротив тех сервисов которые подлежат мониторингу (Рисунок 113).

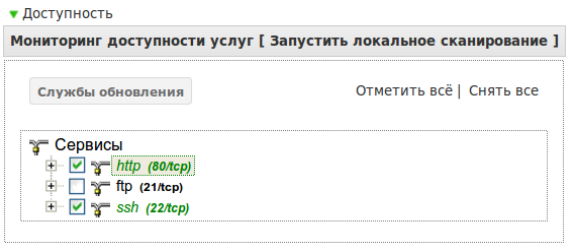



Рисунок 113 – Выбор сервисов узла для мониторинга

Информация о сервисах, программной или аппаратной конфигурации может быть добавлена вручную. Для этого в панели свойств нужно выбрать интересующий пункт, после чего под панелью свойств появится форма для ввода информации (Рисунок 114). После добавления свойства необходимо нажать кнопку «**Обновить**».

Рисунок 114 – Добавление нового свойства

### 5.2.8.2. Группы хостов

На вкладке «Группы хостов» (Рисунок 115) показана таблица со всеми группами узлов сети, хранящимися в БД ПК «КОМРАД». На данной вкладке доступны следующие действия:

Создать - создание новой группы узлов;

Изменить - изменение имеющейся записи о группе узлов;

Удалить выбранные - удаление выбранных записей;

Удалить группу и хосты - удаление выбранных записей групп и узлов, включенных в эту группу;

Включить/отключить Nagios - включение или отключение сервиса мониторинга доступности для выбранных групп. Включение/отключение сервиса происходит в зависимости от состояния указанного в столбце «Nagios», которое может принимать значение ✔ или ✘, поэтому при выборе нескольких записей с разным значением состояния произойдет их переключение на противоположное;

Создать хост-группы по IP геолокации - создание новой группы на основе геолокационных данных об ip-адресе;

- нажатие на данную пиктограмму позволяет привязать к записи о группе информацию из Базы знаний, возможна привязка нескольких записей;

- пиктограмма позволяет добавить произвольную запись для выбранной группы.

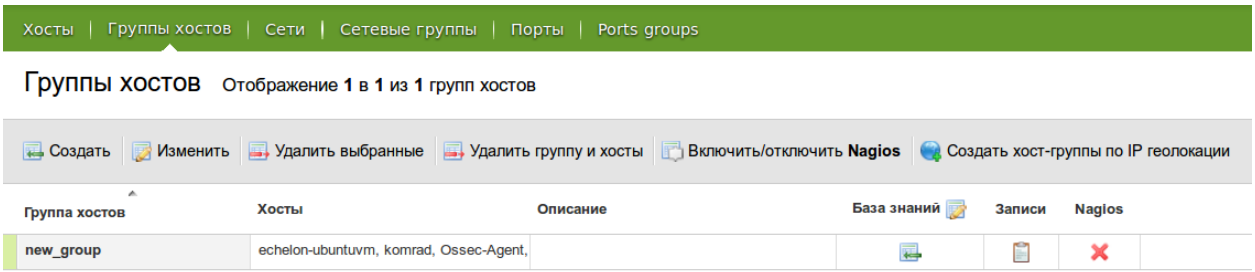



Рисунок 115 – Группы узлов сети

Нажатие на кнопку «**Создать**» открывает диалоговое окно (Рисунок 116), в котором необходимо ввести имя группы и задать узлы, входящие в неё.

Узлы сгруппированы по ряду признаков, например по подсетям, операционным системам. Возможно включение системы мониторинга всей группы (раздел «Расширенный вид», галочка «Включить Nagios для всех узлов в пределах этой группы хостов»). После заполнения всех необходимых полей нужно нажать кнопку «**Обновить**».

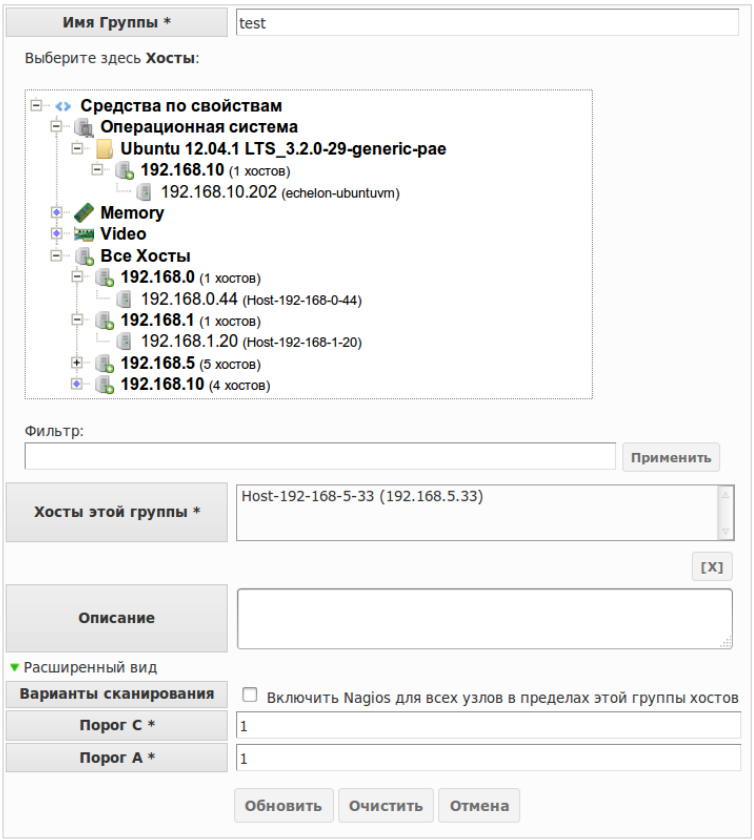



Рисунок 116 – Создание новой группы узлов

### 5.2.8.3. Сети

На Рисунке117представлен список сетей ИТ-инфраструктуры.

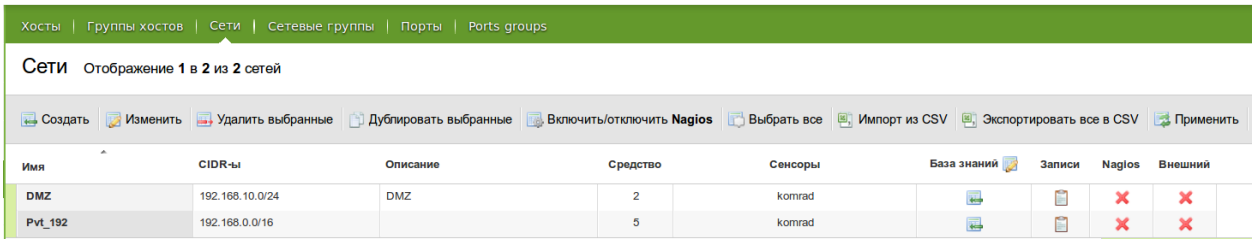



Рисунок 117– Список сетей

Доступны следующие действия:

Создать - создание новой записи о сети;

Изменить - изменение имеющейся записи о сети;

Удалить выбранные - удаление выбранных записей;

Дублировать выбранные - создание копии записи выбранной записи, при этом необходимо задать новый адрес сети;

Включить/отключить Nagios - включение или отключение сервиса мониторинга доступности для выбранных сетей. Включение/отключение сервиса происходит в зависимости от состояния указанного в столбце «Nagios», которое может принимать значение ✔ или ✘, поэтому при выборе нескольких записей с разным значением состояния произойдет их переключение на противоположное;

Выбрать все - выбрать все записи на странице (количество записей на странице регулируется в правом нижнем углу таблицы);

Импорт из CSV - импорт записей из файла CSV;

Экспортировать все в CSV - экспорт всех имеющихся записей в файл CSV;

Применить - применение сделанных изменений;

- нажатие на данную пиктограмму позволяет привязать к записи о сети информацию из Базы знаний, возможна привязка нескольких записей;

- пиктограмма позволяет добавить произвольную запись для выбранной сети.

Нажатие на кнопку «**Создать**» или «**Изменить**» открывает диалоговое окно, представленное на Рисунке 118. Возможно задание следующих параметров: имя се-

ти, адрес сети (CIDR) в формате ip-сети/маска, описание сети, значение актива, сенсор к которому относится данная сеть, также можно включить мониторинг доступности сети. После заполнения необходимых полей требуется нажать кнопку «**Обновить**». Кнопка «**Очистить**» возвращает содержимое полей к первоначальному виду. Кнопка «**Отменить**» возвращает к списку сетей.

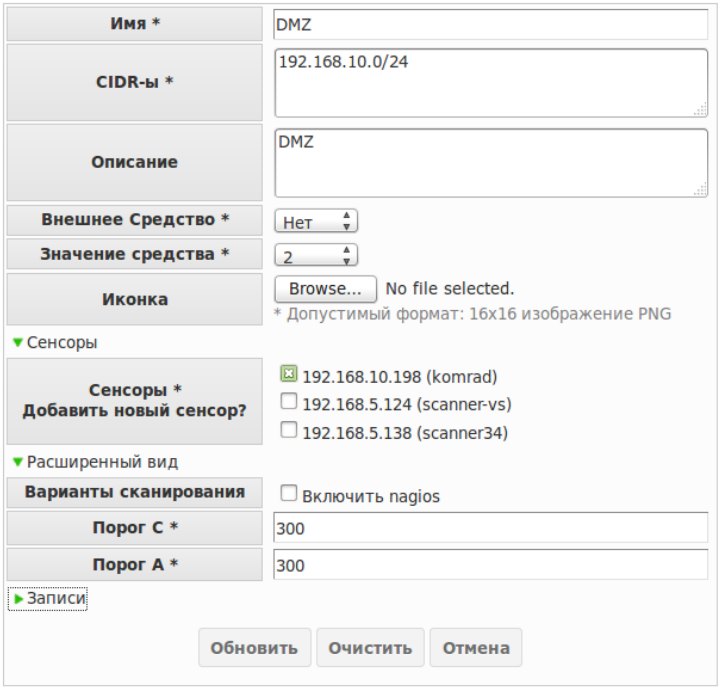



Рисунок 118 – Создание/изменение записи о сети

На Рисунке119представлен список сетевых групп ИТ-инфраструктуры.

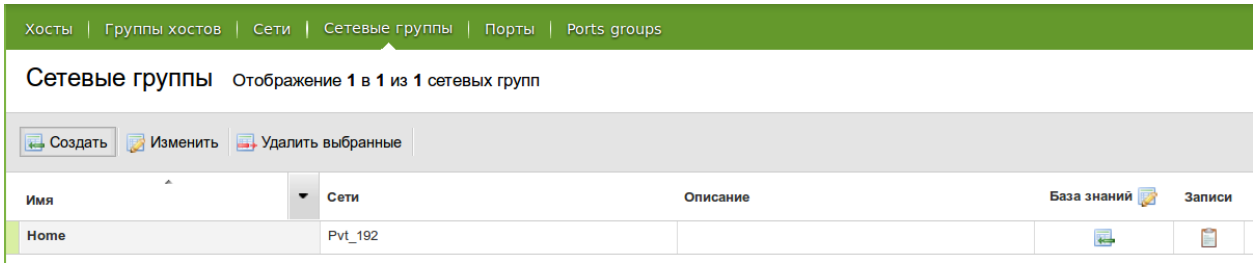



Рисунок 119 – Сетевые группы

Доступны следующие действия:

Создать - создание новой записи о группе сетей;

Изменить - изменение имеющейся записи о группе сетей;

Удалить выбранные - удаление выбранных записей;

- нажатие на данную пиктограмму позволяет привязать к записи о сети информацию из Базы знаний, возможна привязка нескольких записей;

- пиктограмма позволяет добавить произвольную запись для выбранной сети.

Нажатие на кнопку «**Создать**» или «**Изменить**» открывает диалоговое окно, представленное на Рисунке 120. Возможно задание следующих параметров: имя группы, сети, описание группы. После заполнения необходимых полей требуется нажать кнопку «**Обновить**». Кнопка «**Очистить**» возвращает содержимое полей к первоначальному виду. Кнопка «**Отменить**» возвращает к списку групп сетей.

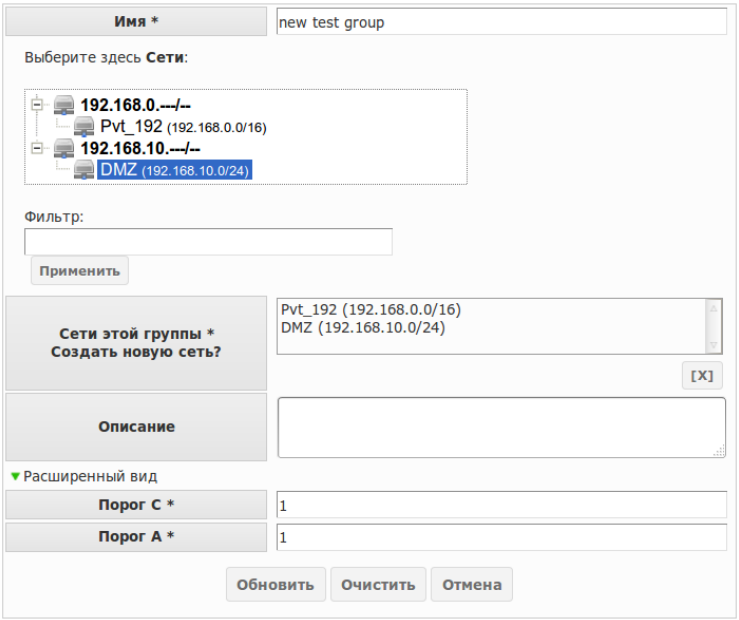



Рисунок 120 – Создание/изменение группы сетей

### 5.2.8.4. Порты

На Рисунке121представлен список записей о TCP/UDP портах. Возможно добавление новых записей о портах, а также их изменение и удаление.

**Примечание:** не рекомендуется удалять или модифицировать записи о портах, это может привести к некорректному отображению информации о событиях и инцидентах ИБ.

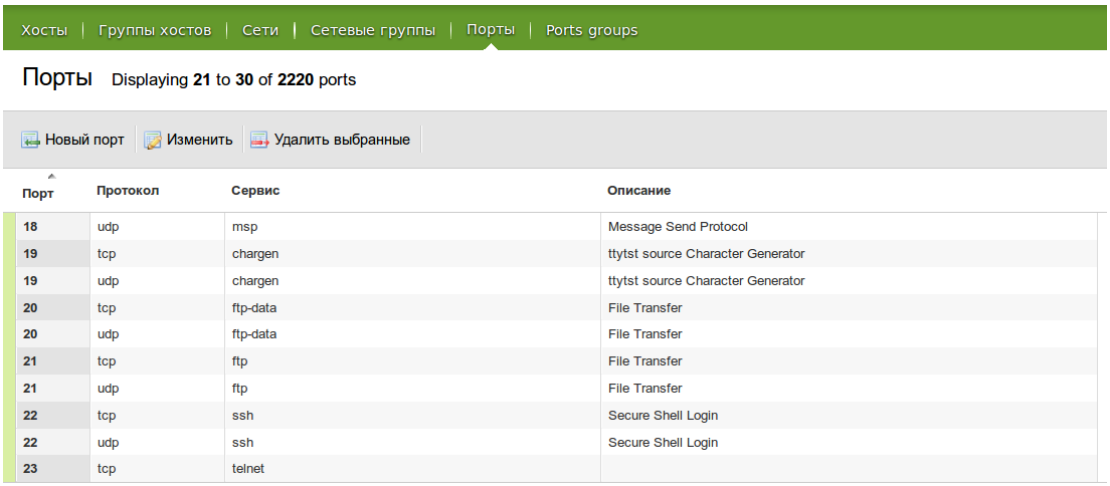



Рисунок 121 – Список TCP/UDP портов

Нажатие на кнопку «**Новый порт**» или «**Изменить**» приведет к открытию диалогового окна представленного на Рисунке 122. Возможно задание следующих параметров: номер порта, протокол (TCP/UDP), название сервиса, описание. После заполнения необходимых полей требуется нажать кнопку «**Обновить**». Кнопка «**Очистить**» возвращает содержимое полей к первоначальному виду. Кнопка «**Отменить**» возвращает к списку портов.

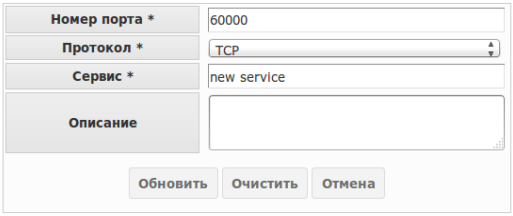



Рисунок 122 – Создание/изменение порта

### 5.2.8.5. Группы портов

На Рисунке123представлен список записей о группах TCP/UDP портов. Возможно добавление новых записей о группах портов, а также их изменение и удаление.

**Примечание**: не рекомендуется удалять или модифицировать запись ANY, это может привести к некорректному отображению информации о событиях и инцидентах ИБ.

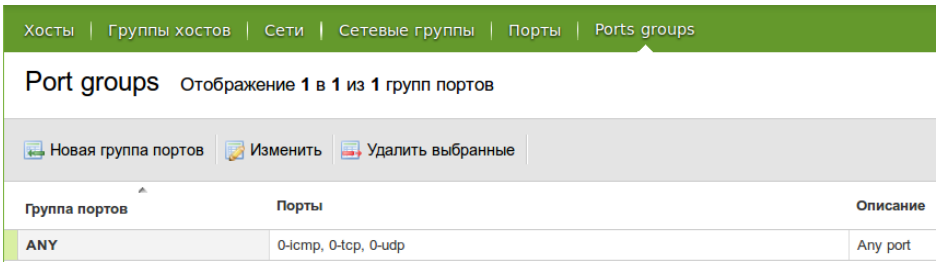



Рисунок 123 – Группы TCP/UDP портов

Нажатие на кнопку «**Новая группа портов**» (Рисунок 124) или «**Изменить**» приведет к открытию диалогового окна, представленного на Рисунке. Возможно задание следующих параметров: номер порта, протокол (TCP/UDP), название сервиса, описание. Порт может быть указан в виде числа (например, 22) или названия порта например (ssh). После заполнения необходимых полей требуется нажать кнопку «**Обновить**». Кнопка «**Очистить**» возвращает содержимое полей к первоначальному виду. Кнопка «**Отменить**» возвращает к списку групп портов.

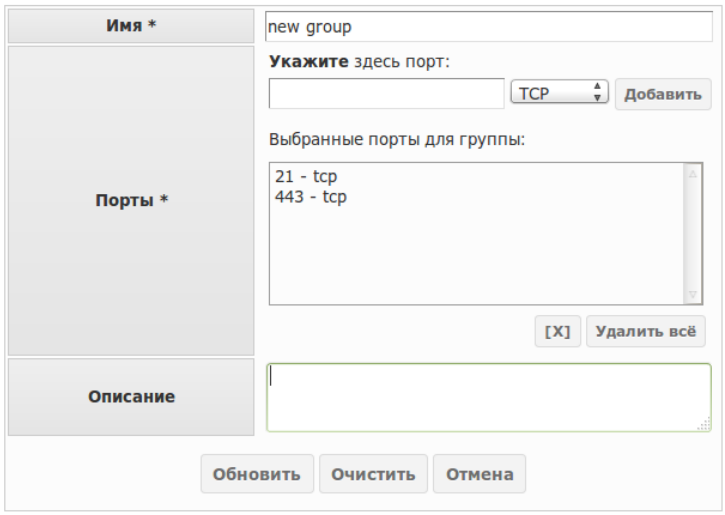



Рисунок 124 – Создание/изменение групп портов

### 5.2.8.6. Редактирование правил Rsyslog

На панели вкладки «**Средства**» доступен раздел «Редактирование правил Rsyslog» (Рисунок 125).

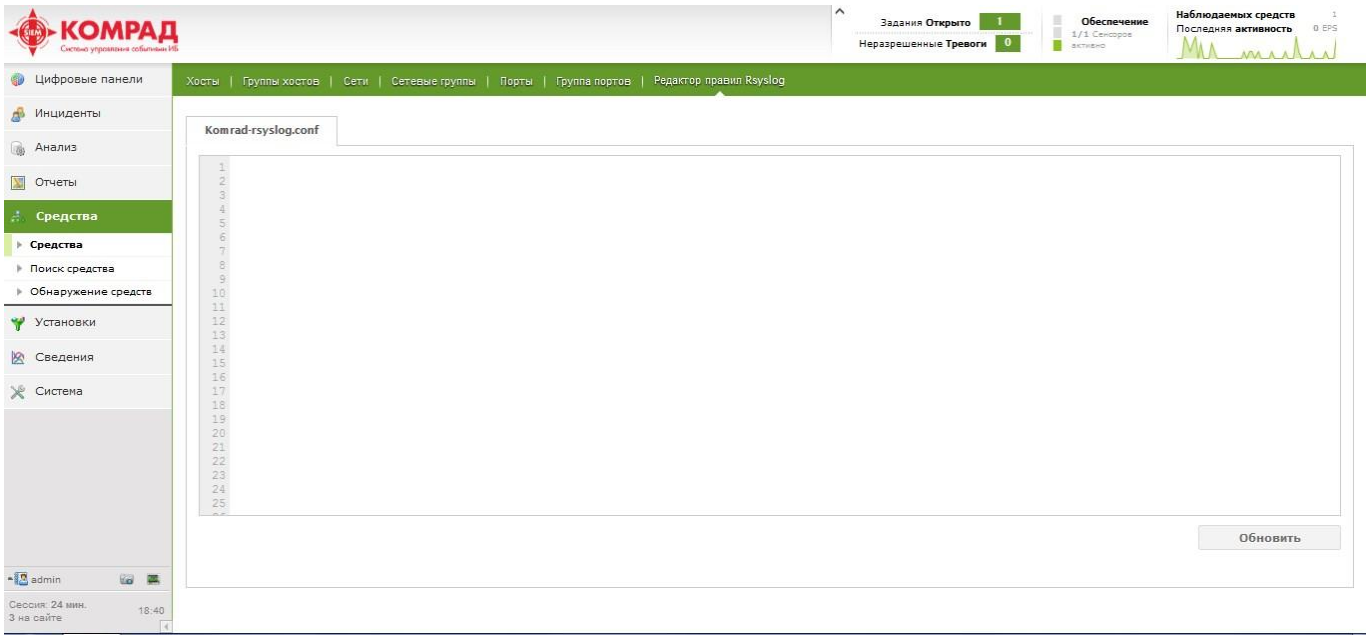
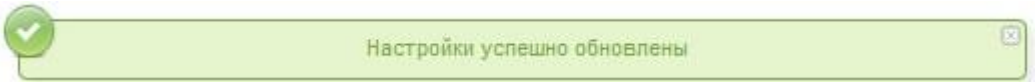



Рисунок 125 – Окно редактирование правил Rsyslog

На данной странице возможно редактирование конфигурационного файла Komrad-rsyslog.conf. После внесения изменений следует нажать кнопку «**Обновить**». В случае успешного обновления будет выдано сообщение о подтверждении:




### 5.2.8.7. Инвентаризация OCS

В ПК «КОМРАД» реализована возможность инвентаризации как аппаратного, так и программного обеспечения, зарегистрированного в системе (соответствует списку «ProgramsandFeatures»).

Инвентаризация средств осуществляется ПК «КОМРАД» после установки агента OCS (Приложение Б).

Для управления инвентаризацией необходимо в веб-интерфейсе перейти во вкладку «**Средства → Средства**» и выбрать в горизонтальном меню пункт «Инвентаризация OCS». Отобразится сводная таблица всего ПО, зарегистрированного в системе (Рисунок 126).

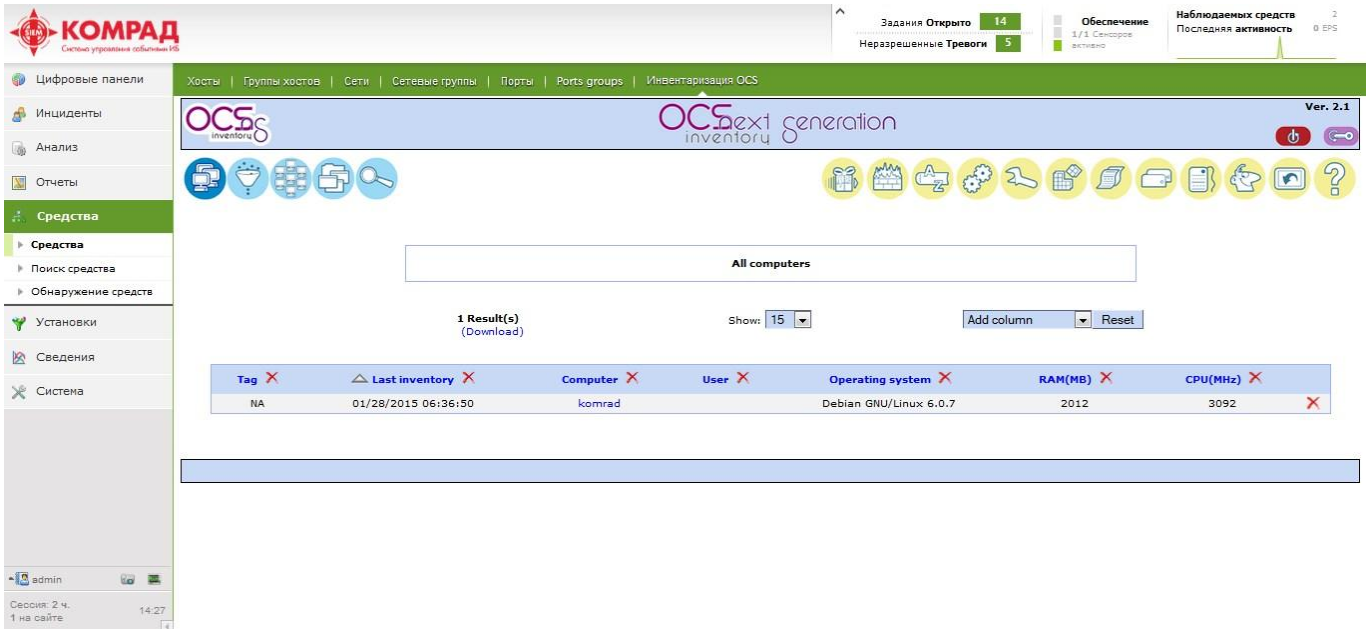



Рисунок 126 – Главное окно системы инвентаризации

В таблице можно изменять отображаемые колонки, выбрав из выпадающего списка (Рисунок 127).

Рисунок 127 – Добавление новой колонки в таблицу

Нажатие на значок ✕ в шапке таблицы удалит колонку из таблицы, а также нажатие на этот значок в теле таблицы удалит выбранноеПОиз списка инвентаризации.

Меню OCScодержит следующие компоненты:

«**Все компьютеры**» – сводная таблица по всем инвентаризованным средствам (можно экспортировать);

«**Тэг / Количество групп компьютеров**» – таблица, содержащая количество ПК с каждым из тегов (можно экспортировать);

«**Группы**» – компьютеры, объединённые в группы (Dynamics, Statics, Servers);

«**Всё программное обеспечение**» – список всего обнаруженного ПО, а также количество экземпляров, установленных в инвентаризованной сети (предусмотрена возможность загрузки всего списка, есть алфавитный указатель и фильтр);

«**Поиск по критериям**»– поисковая подсистема по различным критериям поиска;

«**Развертывание**» содержит подменю:

- «**Сборка**» – сборка пакетов для размещения файлов или выполнение команд на удалённой машине;

- «**Активация**» – менеджер запуска пакетов;

- «**Правила применения**» – условия запуска пакетов;

«**Безопасность**» содержит подменю:

- «**Сетевая информация**» – сводная таблица по IP и подсетям в инвентаризованной сети;

- «**Конфигурация**» – настройка главной подсети - диапазона IP и маски подсети;

«**Словарь**» – реестр установленного ПО (Categories.New, Ignored, Unchanged);

«**Агент**» – меню учёта и управления агентами OCS;

«**Конфигурация**» содержит подменю:

- «**Конфигурация**» – основное меню настроек;

- «**Черный список**» – внесение ограничений для MAC-адресов и серийных номеров serial;;

- «**Файл локализации**» – изменение файла локализации;

«**Реестр**» – интерфейс для изменения реестра Windows;

«**Административная информация**» – интерфейс для правки служебных данных;

«**Дубликаты**» – отслеживание повторяющихся данных по нескольким параметрам, предусмотрена возможность удаления/слиянияповторяющихся записей;

«**Конфигурация файла ярлыков**» –конфигурация файла ярлыков;

«**Пользователи**» – страница управления пользователями (создание и удаление);

«**Локальный импорт**» – форма загрузки файлов на сервер с OCS;

«**Помощь**» – вызов справки.

Подробный отчёт по конкретному хосту можно получить, кликнув по его имени. Детализация хоста отобразится в новом окне (Рисунок 128).

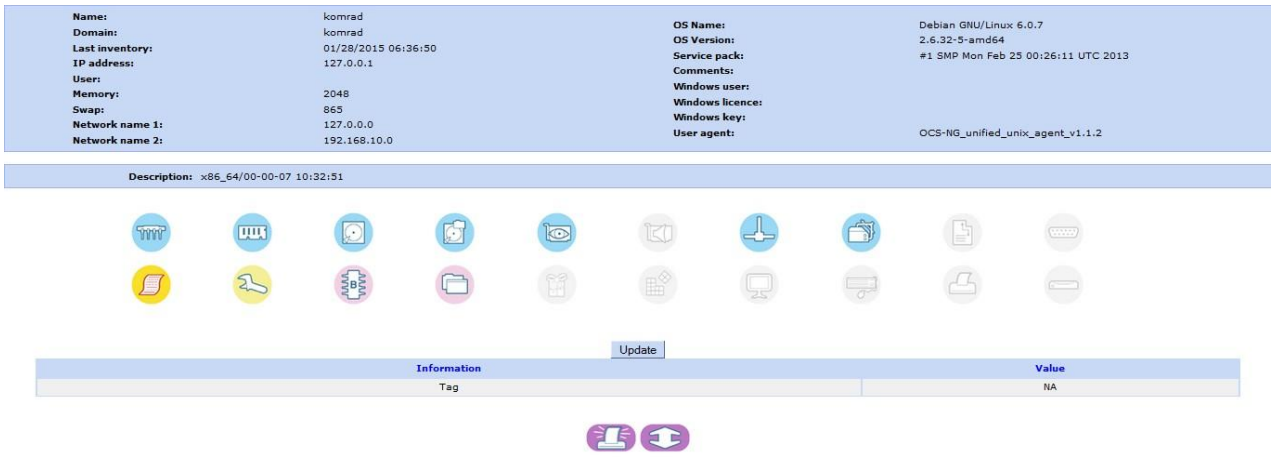



Рисунок 128 – Детальный отчет по выбранному хосту

Нажатие на иконку развернет полную таблицу, отображающую информацию о выбранном хосте.

Возможен импорт результатов в файл CSV (в частности, возможна загрузка сводной таблицы всех хостов, а также списка установленного ПОс указанием количества хостов). Подробную информацию по конкретной машине можно распечатать (либо сохранить в PDF с помощью штатных возможностей браузера и ОС).

### 5.2.9. Создание отчётов

ПК «КОМРАД» обеспечивает возможность построения отчётов на основе собранной информации о событиях и инцидентах ИБ, в том числе с использованием встроенных и созданных пользователем шаблонов.

ПК «КОМРАД» обеспечивает возможность выборки данных за определённый период времени для конкретного устройства или системы или группы объектов ИТ-инфраструктуры.

Веб-интерфейс ПК «КОМРАД» позволяет работать со статистической информацией и создавать отчёты о событиях и инцидентах ИБ во вкладке «**Отчёты**» (Рисунок 129).

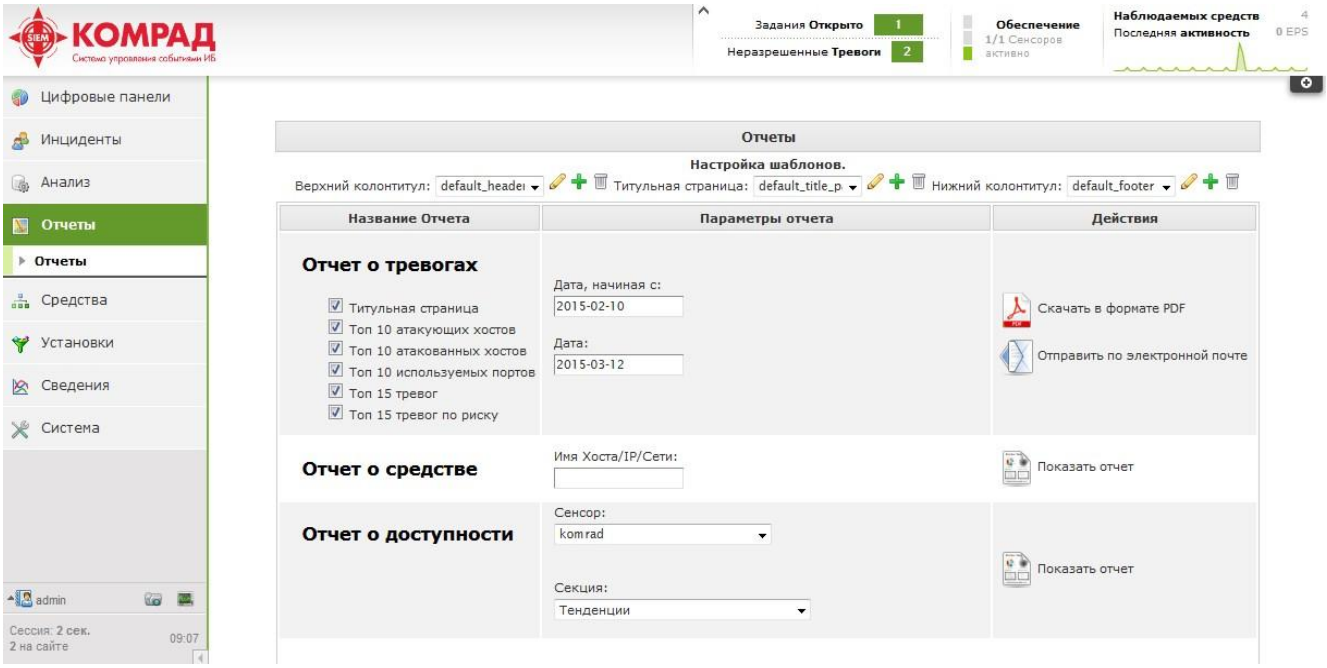



Рисунок 129 – Страница формирования отчётов

Пользователь может сформировать отчёт, пользуясь гибкой системой настроек, после чего просмотреть его, скачать в формате pdf или отправить на адрес электронной почты.

Доступны следующие виды отчётов:

- отчёт об инцидентах ИБ (Отчет о тревогах, Рисунок 130);
- отчёт о конкретном источнике событий (Отчет о средстве);
- отчёт о доступности источника событий (Отчет о доступности);

- обзорные отчёты (Бизнес отчёт);
- территориальные карты угроз (Географический отчет);
- отчёт за период (Метрический отчет);
- отчёты по событиям ИБ (События SIEM);
- отчёт об активности пользователей;
- отчёты по заданиям и их статусам;
- прочие отчёты.

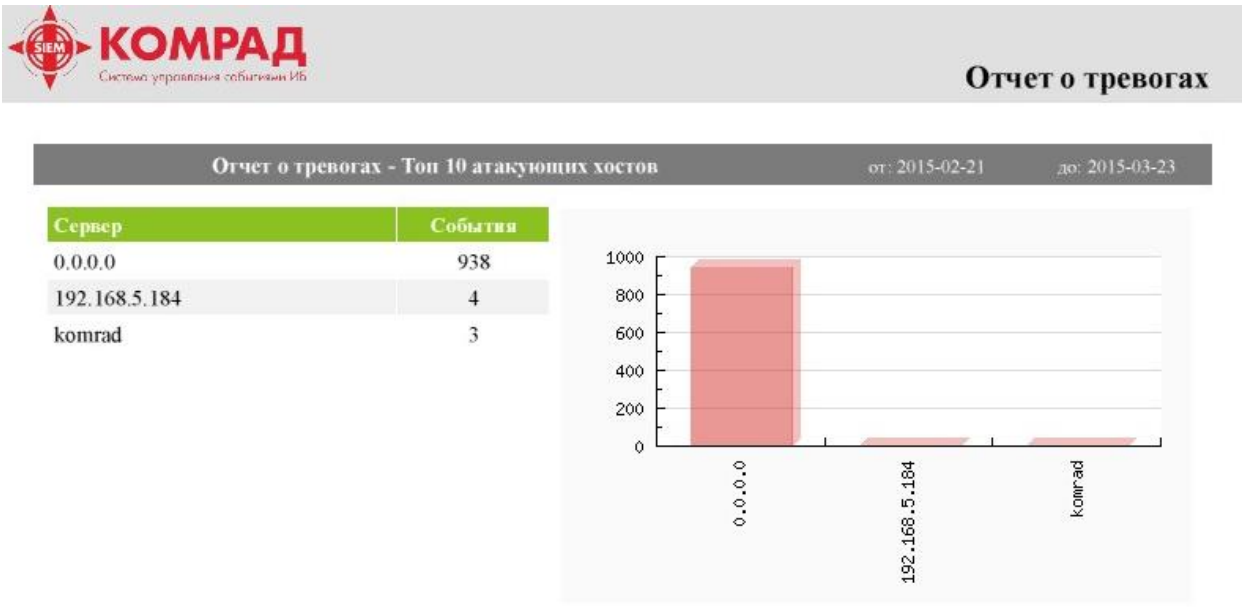



Рисунок 130 – Пример отчёта в формате pdf

При формировании отчёта в веб-интерфейсе ПК «КОМРАД» допускаются дополнительные настройки с помощью фильтров, например Диапазона дат, Пользователя, Действий пользователя.

Также возможно изменение установленных по умолчанию колонтитулов и титульной страницы отчетов. Для этого в поле «Настройка шаблонов» следует выбрать область для изменения (Верхний колонтитул, Титульная страница, Нижний колонтитул) и нажать на пиктограмму:

– для редактирования текущего шаблона;

– для создания нового шаблона;

– для удаления выбранного шаблона.

При создании / редактировании шаблона откроется окно, показанное на Рисунке 131, где доступны следующие инструменты для форматирования:

Вставить→ Вставить изображение;
Вставить ссылку;
Специальные символы;
Горизонтальная линия;
Разрыв страницы;
Вставить дату/время;
Дополнительныеполя;
Неразрывной пробел;
Формат → Полужирный;
Курсив;
Подчеркнутый;
Зачеркнутый;
Верхний индекс;
Нижний индекс;
Формат;
Очистить формат;
Таблица→ Вставить таблицу;
Свойства таблицы;
Удалить таблицу;
Ячейка;
Строка;
Столбец;
Инструменты→ Проверить правописание;
Исходный код

**Примечание:** во вкладке «Вставить→ Дополнительные поля» возможно добавление следующих выражений:

- FOOTER_CONTENT_LEFT – информация о пользователе, дате и времени составления отчета;
- FOOTER_CONTENT_RIGHT – нумерациястраниц;
- MAINTITLE – названиеотчета;
- IT_SECURITY_TITLE – «IT Безопасность»;
- IT_SECURITY_VALUE – название организации;
- ADDRESS_TITLE – «Адрес»;
- TEL_TITLE – «Тел.»;
- TEL_VALUE – телефонорганизации;
- REPORT_DATE_TITLE – «Датаотчета»;
- REPORT_DATE_VALUE – дата и время составления отчета (ставится автоматически);
- REPORT_FILTER_TITLE – фильтротчета;
- DATE_FROM_TITLE – «Дата, начинаяс»;
- DATE_FROM_VALUE – дата, начиная с которой создается отчет (ставится автоматически)
- DATE_TO_TITLE – «Дата:»;
- DATE_TO_VALUE – дата, до которой создается отчет(ставится автоматически);
- ASSETS– выбранные средства (ставится автоматически).

Помимо перечисленных опций форматирования на панели редактора также находятся кнопки для управления выравниванием по ширине, создания маркированных и нумерованных списков, отступов, изменения цвета текста и цвета фона.

После нажатия кнопки «Сохранить», созданный шаблон появится в выпадающем списке рядом с названием области.

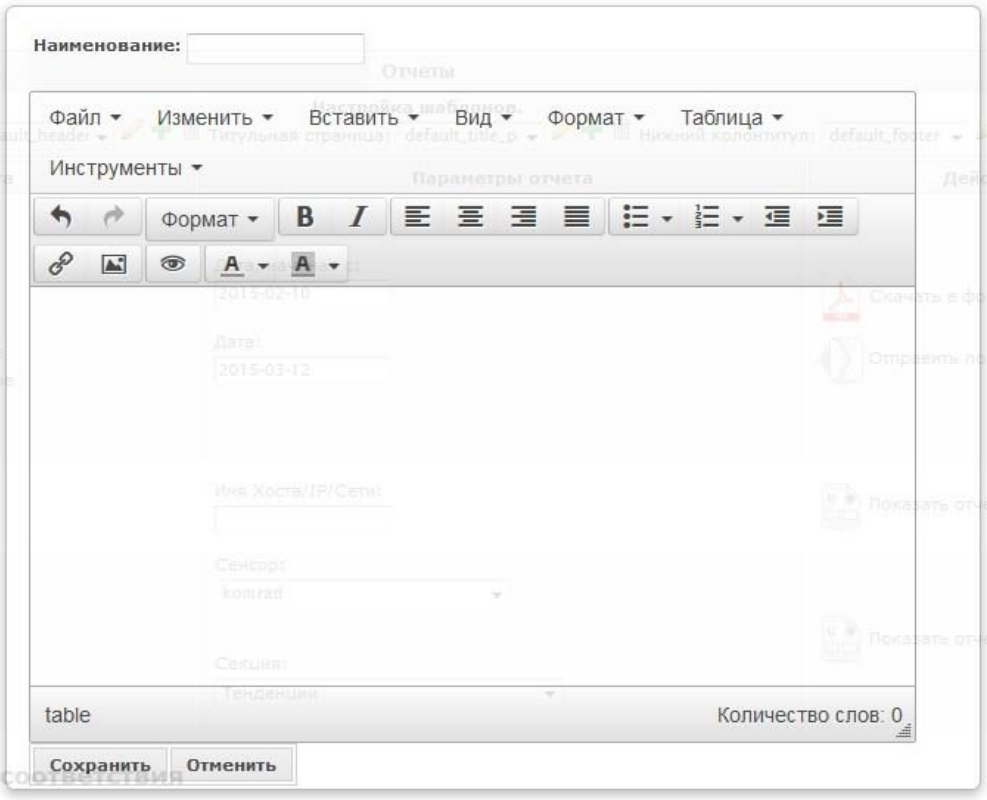



Рисунок 131 – Окно создания нового шаблона отчета

## 5.3. Дополнительные возможности при работе с ПК

### 5.3.1. Настройка отображения статистической информации

Во вкладке «**Цифровые панели**» представлены графики и диаграммы, отображающие статистическую информацию по хранящимся событиям и инцидентам безопасности. Администратор имеет возможность добавлять дополнительные вкладки и виджеты, а также изменять видимость элементов. Для перехода в режим редактирования необходимо нажать иконку . Затем в открывшемся меню (Рисунок 132) выбрать пункт «Изменить».

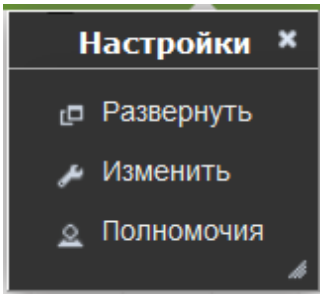



Рисунок 132 – Меню редактирования вкладки «Цифровые панели»

После перехода в режим редактирования на экране появится сообщение (Рисунок 133):

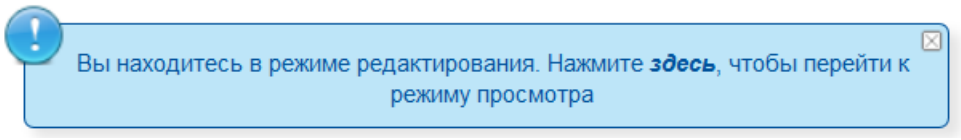



Рисунок 133 – Сообщение о переходе в режим редактирования

В режиме редактирования рядом с именем вкладки отображается знак «+», нажатие на который приводит к вызову меню редактирования вкладки (Рисунок **134**).

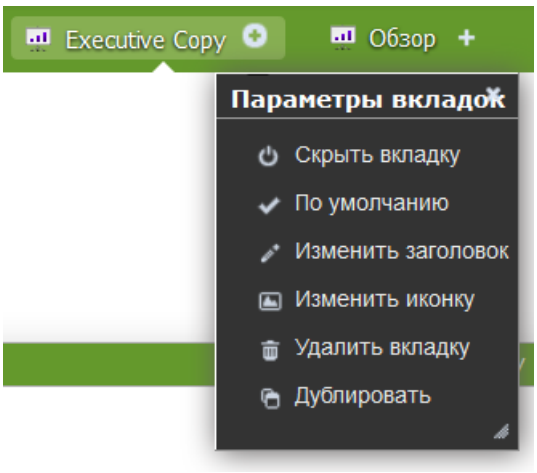



Рисунок 134 – Меню редактирования вкладки

В данном меню доступны следующие действия:

- «Скрыть вкладку» — сделать вкладку невидимой в обычном режиме отображения;

- «По умолчанию» — сделать вкладку основной;

- «Изменить заголовок» — изменить заголовок вкладки;

- «Изменить иконку» — изменить изображение, представленное рядом с именем вкладки;

- «Удалить вкладку» — удалить вкладку без возможности восстановления;

- «Дублировать» — сделать копию вкладки (при этом копируются все виджеты данной вкладки).

В режиме редактирования на виджетах доступны дополнительные функции:

— свернуть виджет;

— настроить виджет (режим, аналогичный добавлению нового виджета);

— удалить виджет.

В режиме редактирования на вкладках доступна кнопка «**Добавить виджет**», нажатие на которую приводит к открытию окна выбора макета виджета (Рисунок 135). Доступны следующие типы виджетов:

- «Диаграмма» — отображение данных системы в виде столбчатой или круговой диаграммы;

- «Изображение» — добавление изображения (загружается пользователем);

- «Облако тэгов» — виджет в виде интерактивного облака;

- «Режим реального времени» — отображение событий безопасности поступающих в систему в реальном времени;

- «Измерения» — виджет для отображения рисков инцидентов или заданий;

- «Потоки сети» —виджет-диаграммы загрузки сети.

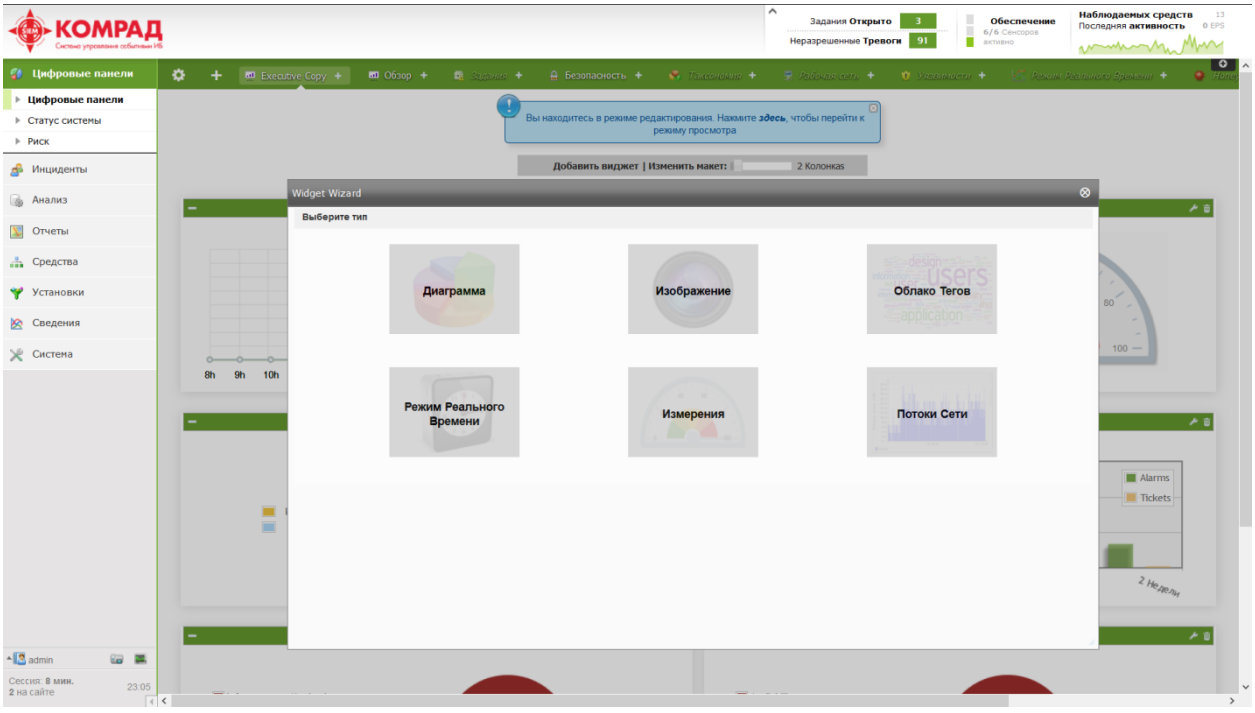



Рисунок 135 – Окно выбора макета нового виджета

После нажатия на любой из типов виджетов откроется окно выбора параметра (Рисунок 136), для которого настраивается отображение (например, количество событий за каждый час или распределение событий по типам).

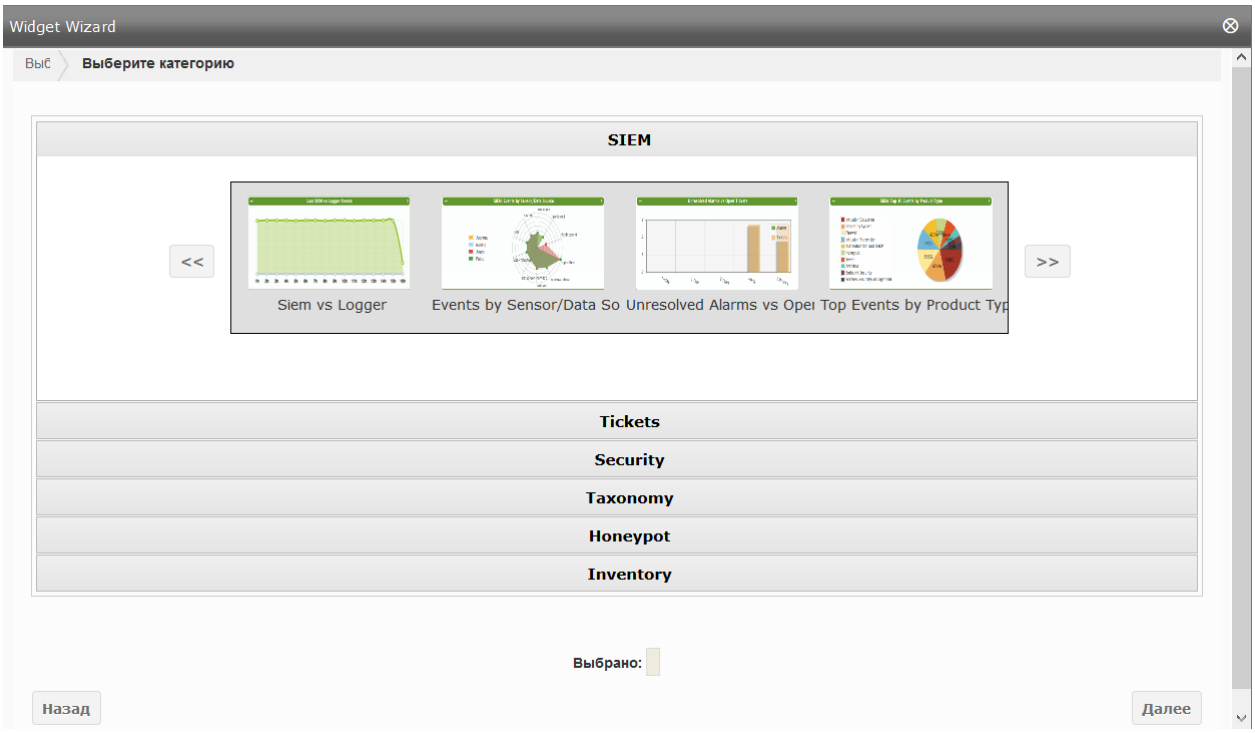



Рисунок 136 – Выбор параметров виджетов

После выбора конкретного параметра откроется окно настройки внешнего вида виджета (Рисунок 137), в котором можно выбрать название виджета, цвет рамки, положение и ряд других параметров. После окончания настройки необходимо нажать кнопку «**Далее**».

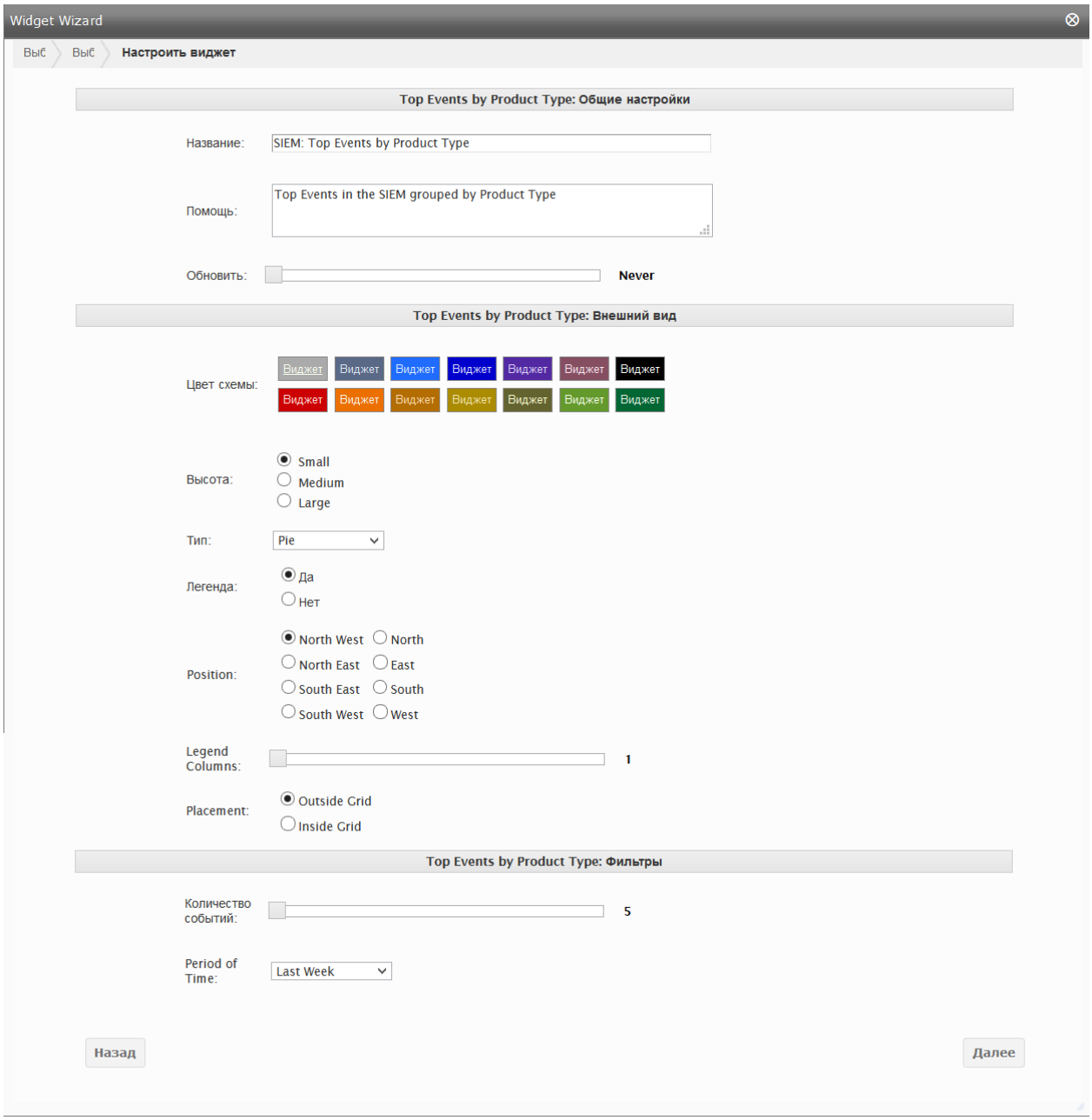



Рисунок 137 – Настройка внешнего вида виджета

Далее открывается окно предварительного просмотра виджета (Рисунок 138). Нажатие на кнопку «**Сохранить виджет**» приведёт к созданию нового виджета в выбранной вкладке.

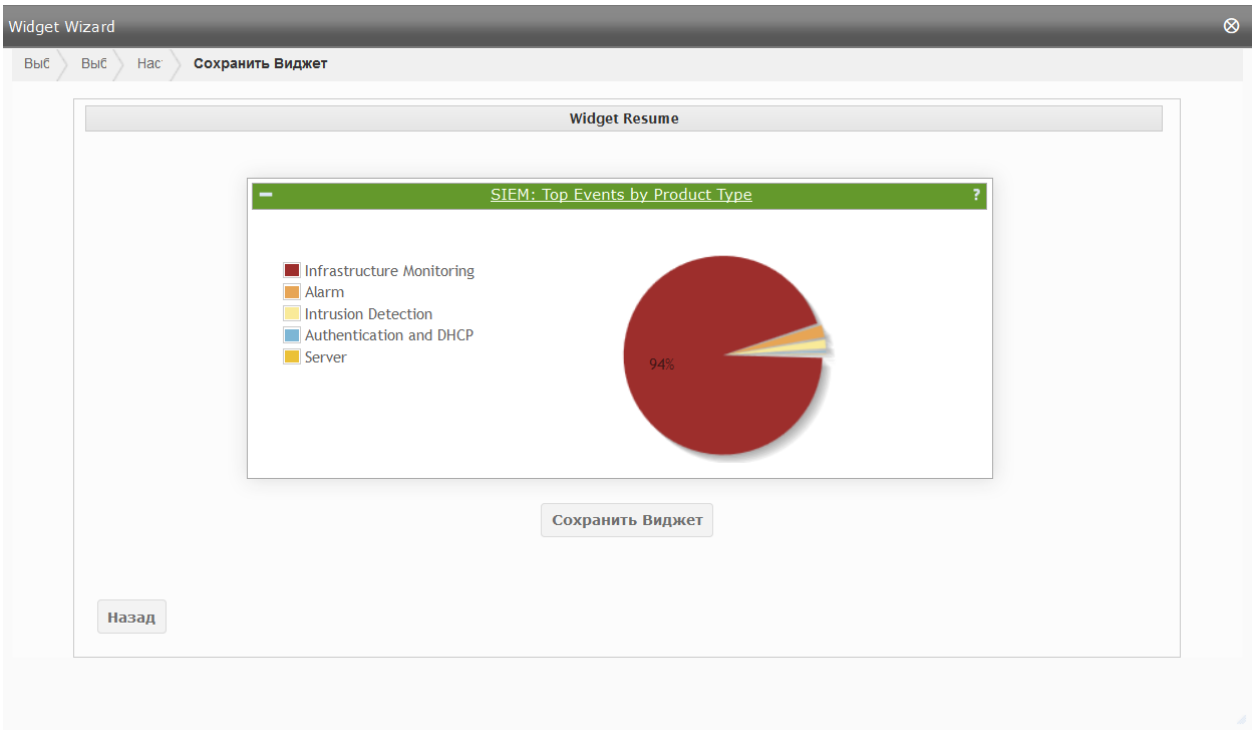



Рисунок 138 – Окно предварительного просмотра виджета

**Примечание**: при необходимости в режиме редактирования можно перетаскивать виджеты, удерживая левую кнопку мыши.

После завершения редактирования необходимо нажать на слово «**здесь**» в окне режима редактирования.

### 5.3.2. Настройка механизма уведомлений

Уведомление пользователей о новых инцидентах безопасности и новых заданиях на их обработку осуществляется двумя способами – путем оповещения в веб-интерфейсе ПК и путем отправки писем на электронные почтовые адреса, указанные администратором.

#### 5.3.2.1. Отправка электронных писем о новых тревогах

Настройка отправки писем о новых тревогах осуществляется через механизм политик и действий ПК «КОМРАД». Необходимо создать новое действие на странице «**Установки→Политика и Действия**»,вкладка «Действия»(Рисунок 139). Поля «Имя» и «Описание» задают имя и описание действия; тип события –«Отправить e-mail»; состояние —«Только если это тревога»; также необходимо указать почто-

вые адреса отправителя и получателя (может быть указан один получатель).

При составлении темы и текста письма могут быть использованы переменные, описание которых находится на странице, при формировании уведомления переменные заменяются данными программного комплекса (кроме того, в тексте письма будут содержаться значения всех полей, которые присутствуют в описании события). После того как все параметры будут указаны, необходимо нажать кнопку«**Обновить**».

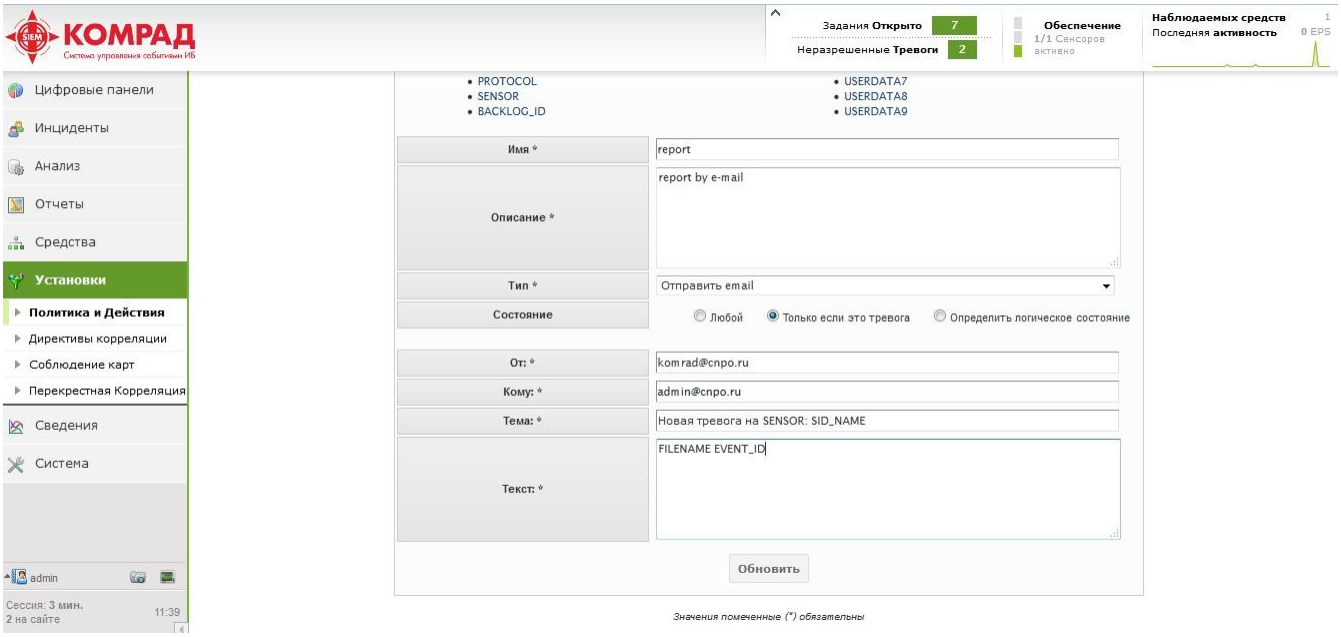



Рисунок 139 – Настройка уведомления

После создания действия необходимо настроить соответствующую политику.На странице «**Установки**» →«**Политика и Действия**»,вкладка «Политики»в разделе«Политики для событий на сервере» необходимо нажать кнопку «**Создать**».На открывшейся странице (Рисунок 140) в таблице «Условия политики» заполнить следующие поля:«Источник» и «Назначение» в дереве средств выбрать источник событий для которого создается оповещение;в поле «Типы событий»выбрать «Directive events» (Рисунок 141).

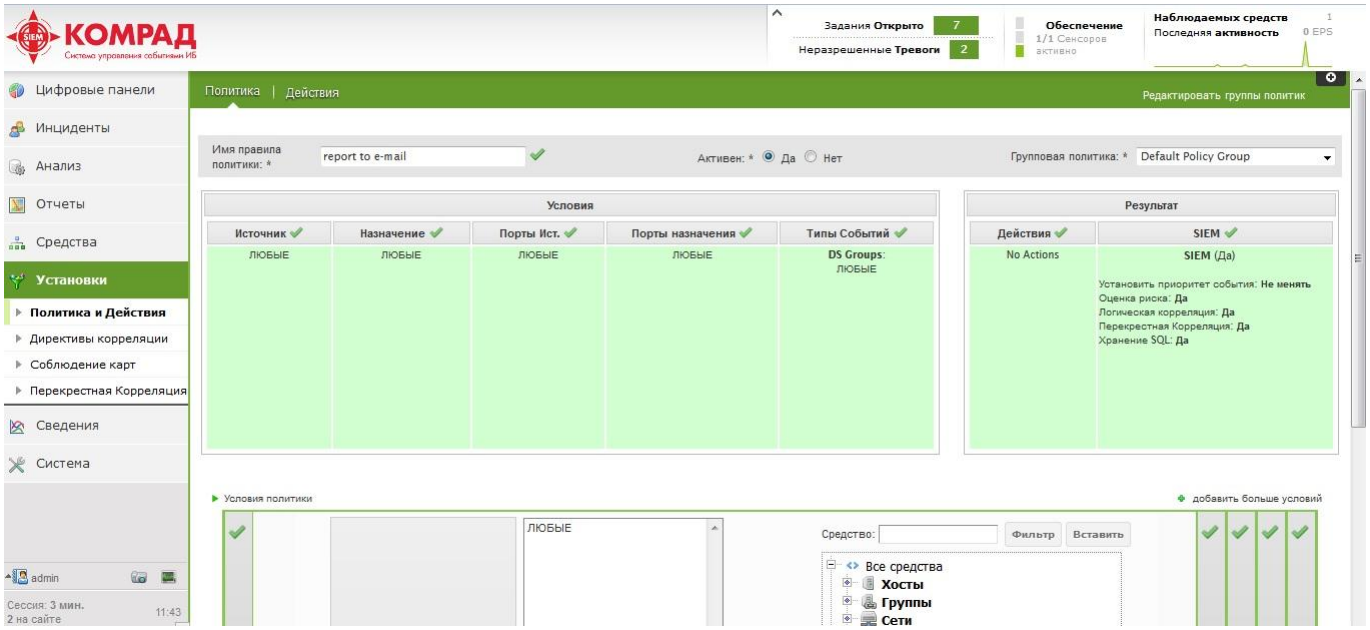



Рисунок 140 – Настройка политики отправки уведомлений

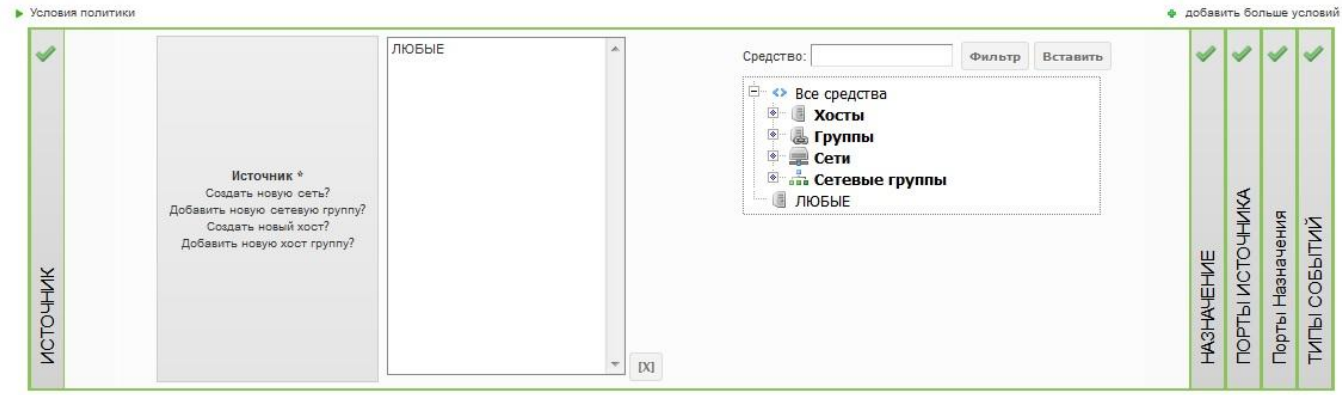



Рисунок 141 – Настройка политики отправки уведомлений пункт «Источник»

**Примечание**:возможно добавление дополнительных условий срабатывания политики нажатием на ссылку «Добавить больше условий».

Затем необходимо развернуть список параметров «Последствия политики» (Рисунок 142), в котором следует перетащить в левый столбец, созданное на предыдущем шаге,действие. После этого нужно нажать кнопку «**Обновить политику**».

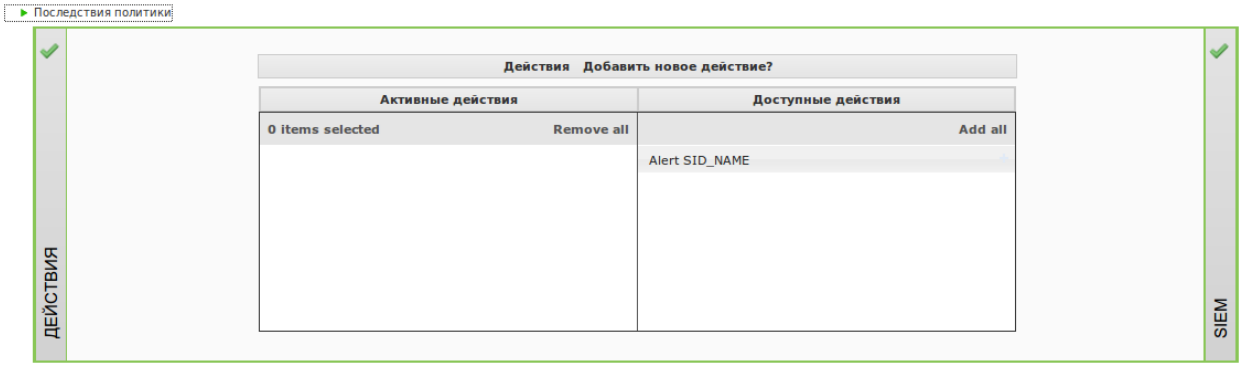



Рисунок 142 – Настройка последствий политики

В результате описанных действий на адрес электронной почты, указанный в качестве адреса получателя, будут поступать письма о новых тревогах без создания задач.

### 5.3.2.2. Настройка оповещений о новых заданиях на обработку инцидентов безопасности

Для включения функции уведомлений при работе с заданиямина обработку инцидентов ИБ необходимо настроить пункт «**Задания**» на странице «**Установки→Основное**»в соответствии с Рисунком 143.

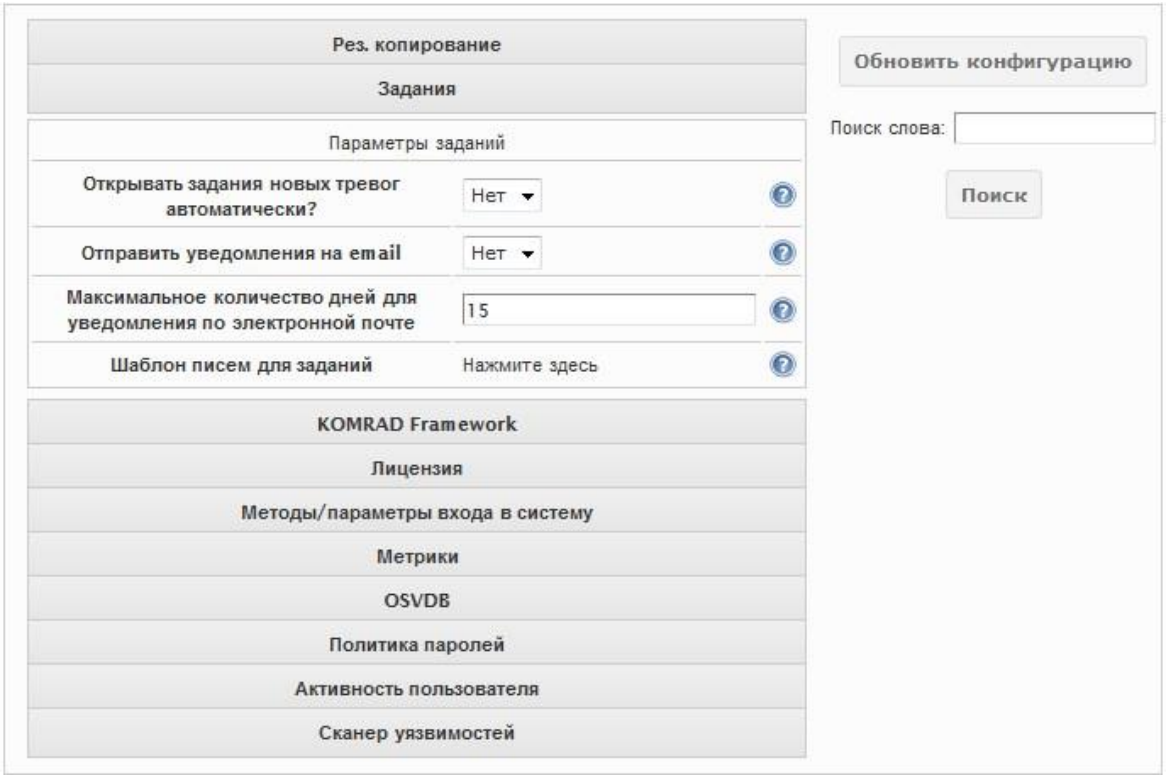



Рисунок 143 – Настройка оповещений при обработке инцидентов

После автоматического создания задания на каждый инцидент будет отправлено письмо на адрес пользователя «admin».

При добавлении пользователя к заданию отправка письма данному пользователю осуществляется автоматически.

В поле «Шаблон писем для заданий» возможно изменение шаблона письма с уведомлением (Рисунок 144).

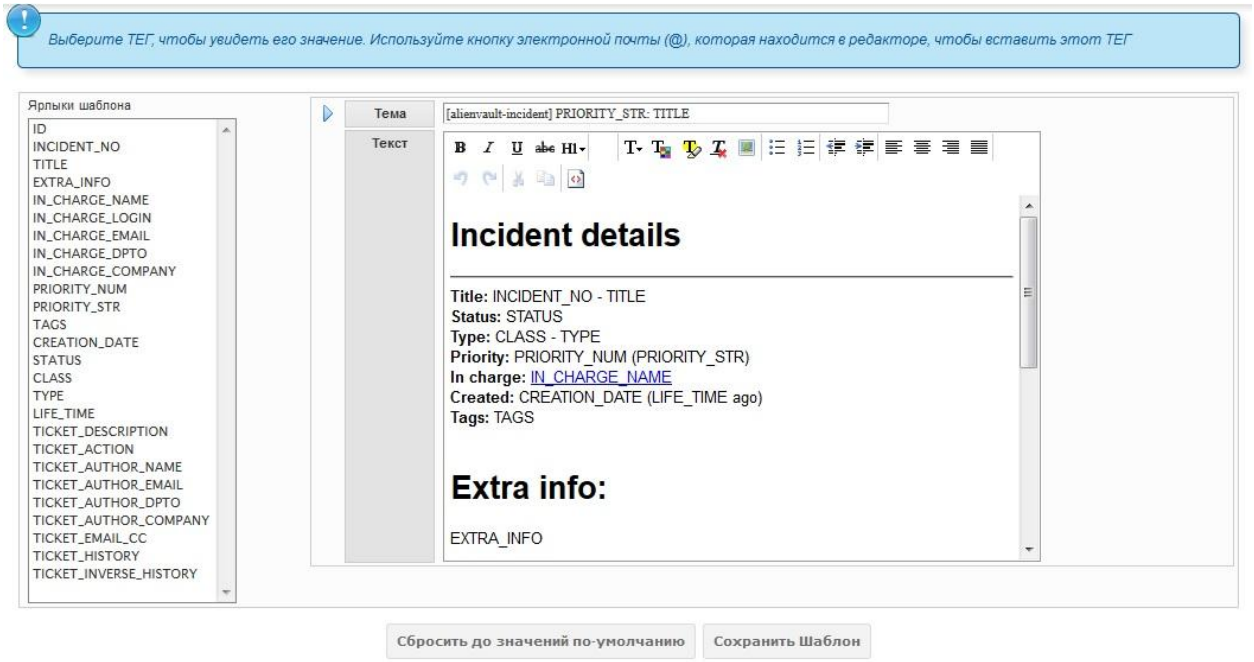



Рисунок 144 – Окно шаблона уведомления

### 5.3.3. Контроль соответствия

В разделе «**Установки→ Контроль соответствия»** доступен рабочий интерфейс для контроля соответствия политик ИБ. В ПК «КОМРАД» имеется два стандарта безопасности данных – ISO 27001 (Рисунок 145) и PCI DSS 2.0 (Рисунок 146).

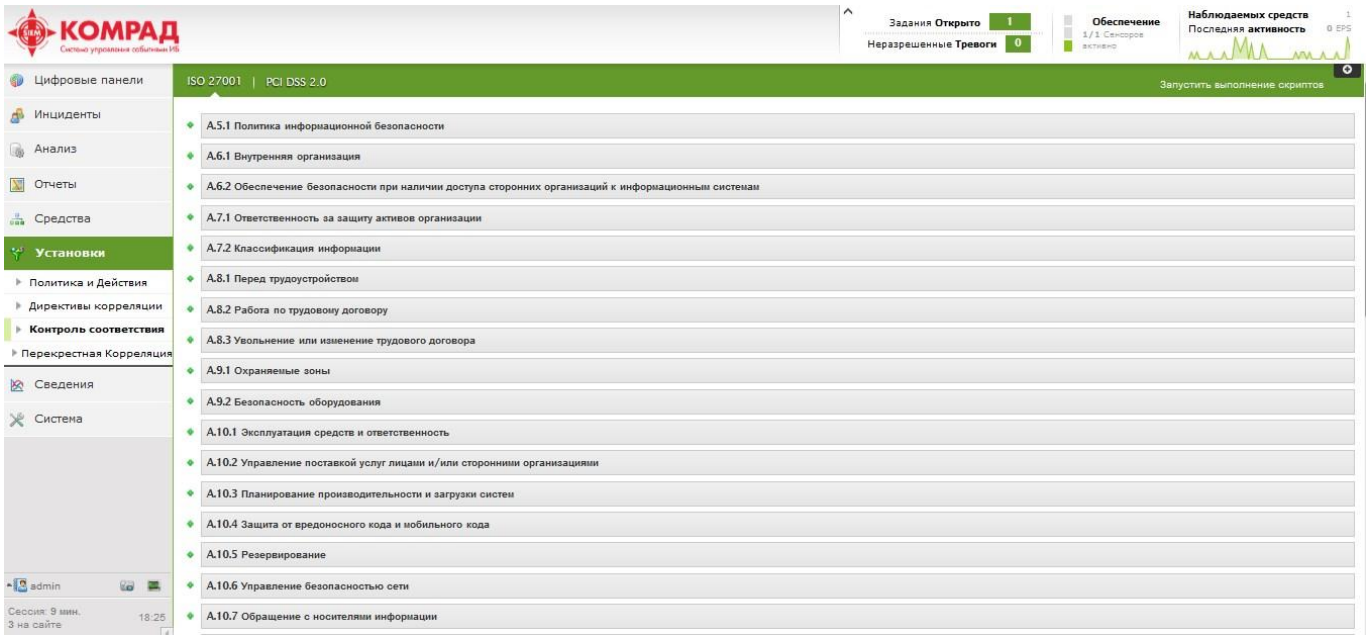



Рисунок 145 – Страница политик стандарта ISO 27001

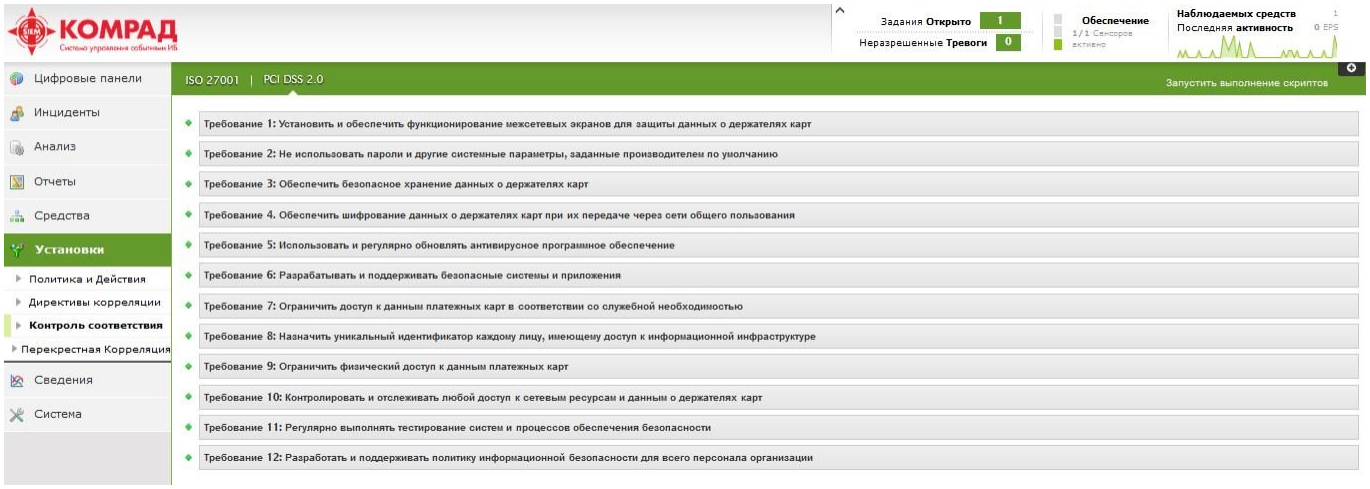



Рисунок 146 – Страница политик стандарта PCI DSS 2.0

При нажатии на значок откроется перечень политик, входящих в выбранную категорию (Рисунок 147).

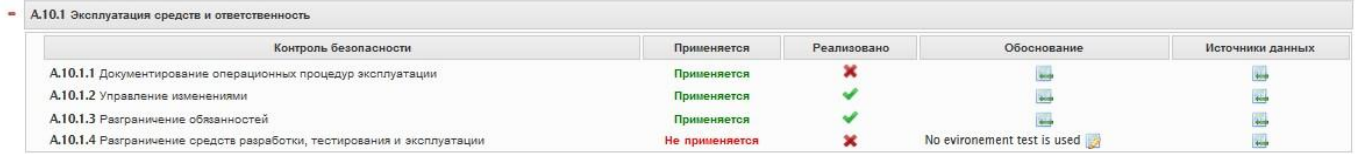



Рисунок 147 – Список политик, входящих в одну группу

В таблице имеются следующие поля:

- «Контроль безопасности» – название политики безопасности;

- «Применяется» –необходимость применения данной политики на предприятии (при нажатии на текущий статус политики он изменится на противоположный; возможны два состояния – Применяется / Не применяется );
- «Реализовано» – статус того, реализовано ли применение данной политики на предприятии (при нажатии на пиктограмму ✔ / ✖ она изменится на противоположную);
- «Обоснование» – обоснование применения данной политики. При нажатии на пиктограмму откроется окно (Рисунок 148), где возможно добавление комментария. После внесения изменений нажать кнопку «**Обновить**». Для последующего редактирования текста обоснования следует нажать на пиктограмму ;

Рисунок 148 – Добавление обоснования политики ИБ

- «Источники данных» – добавление директив, реализующих данную политику безопасности(Рисунок 149, Рисунок 150). Для последующего редактирования используется пиктограмма .

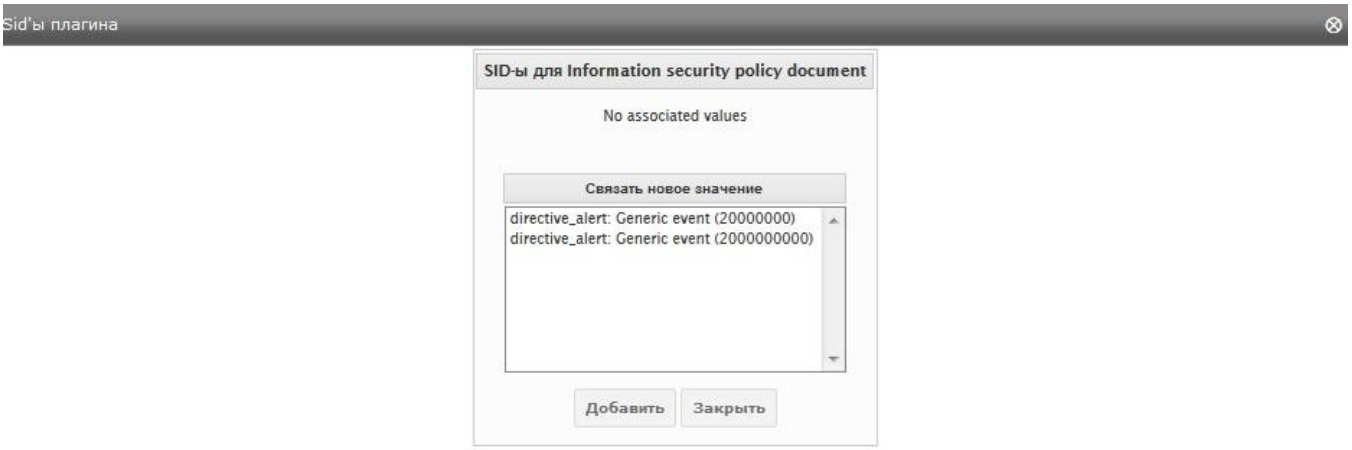



Рисунок 149 – Добавление директив, реализующих данную политику безопасности

Рисунок 150 – Связывание нового значения

### 5.3.4. Отслеживание трафика сети

Во вкладке «**Сведения → Рабочая сеть → Трафик**» доступна детализированная информация о текущем трафике в режиме реального времени (Рисунок 151).

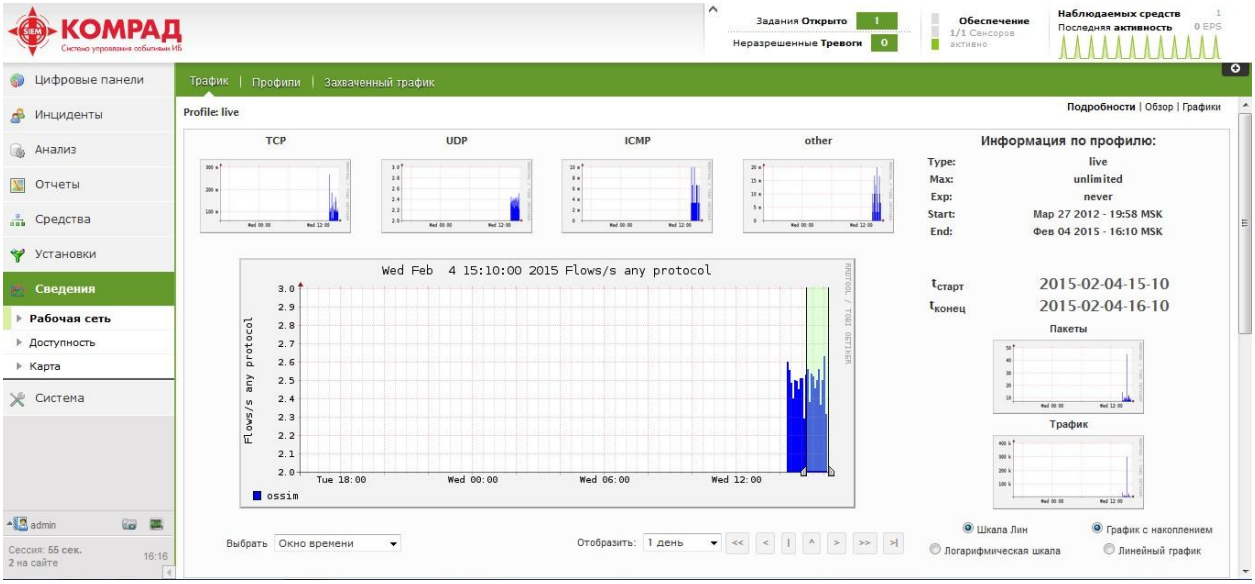



Рисунок 151 – Страница отображения информации по трафику

Данная страница разделена на две основных части: в верхней части доступны инструменты навигации, а также выбора слота времени или временного окна; в нижней части страницы содержатся инструменты обработки трафика за выбранный промежуток времени.

При нажатии на любой график протоколов из потоков,пакетов, или трафика он будет отображен в главном окне. Таким образом осуществляется переключение между графиками.

Изменение временного интервала для отображаемого графика возможно при выборе иного значения из выпадающего списка под основным графиком.

Изменить слот времени графика можно, поместив курсор в другое положение или перетащив ползунок на шкале в пределах выбранного интервала.

При изменении слота времени на графике, его границы автоматически отобразятся в полях$t_{старт}$и$t_{конец}$справа от графика, обновится статистическая информация в таблице в нижней части страницы.

Также смена слота времени возможна с помощью панели управления под графиком, где:

<< – перемещение назад на величину полного временного интервала графика;

< – предыдущий слот времени, перемещение на 5 минут назад;

| – перемещение в центр временной шкалы графика;

^ – перемещениенато время, где было зафиксировано максимальное значение по оси *y*( за +/- 1 час, отсчитывая с текущей позиции курсора);

> – следующий слот времени, перемещение на 5 минут вперед;

>> – перемещение вперед на величину полного временного интервала графика;

>| – перемещение в конец текущего слота времени.

Иногда предпочтительнее выбрать для отображения не слот времени, а окно времени. Для этого из выпадающего списка под графиком следует выбрать «**Окно времени**».

В данном режиме ползунок на шкале будет разделен на 2 части, которые следует перемещать, таким образом обозначая границы временного окна.

Время и дата границ временного окна автоматически отобразятся справа от графика в полях $t_{старт}$и$t_{конец}$.

Графики имеют следующие опции отображения:

**шкала:** линейная ось *y*, логарифмическая ось *y*;

**тип графика:** график с накоплением, линейный график.

Опции отображении можно изменить, нажав на соответствующую радиокнопку справа от панели управления временной шкалой.

Статистическая информация по выбранному слоту времени (окну времени) доступна в таблице (Рисунок 152).

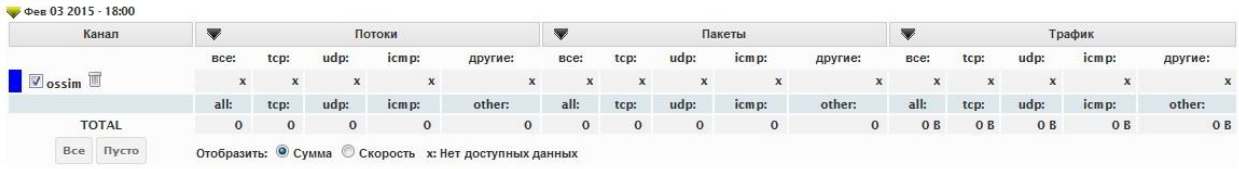



Рисунок 152 – Статистическая информация по трафику

В данной таблице представлена информация о потоках, пакетах и общем трафике.

Каждой строке таблицы соответствует один источник NetFlow. В цветовом поле рядом с названием канала показано, каким цветом информация по данному каналу отображается на графике. Выключить (включить) отображение какого-либо канала на графике можно, убрав (поставив) галочку рядом с названием канала.

В таблице доступно отображение данных о суммарных значениях или о скорости – кнопки

соответственно.

Страница автоматически обновляется каждые 5 минут или при изменении временной шкалы.

После выбора окна времени возможна обработка и настройка фильтров по данным NetFlow (Рисунок 153).

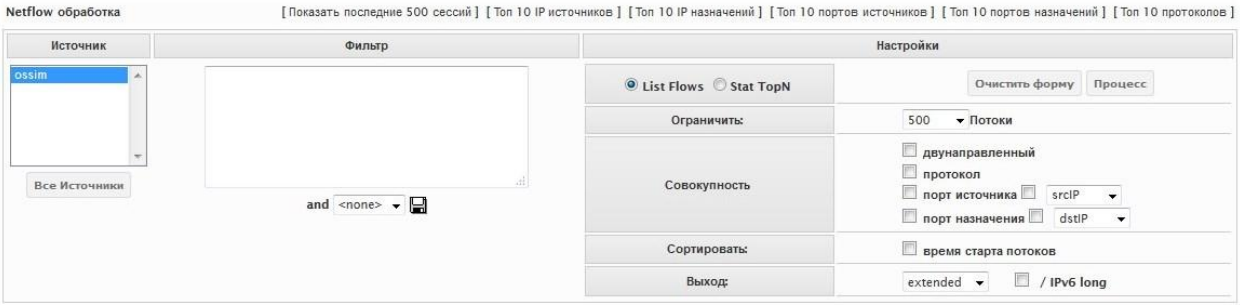



Рисунок 153 – Настройка фильтров по обработке данных NetFlow

После выбора параметров фильтрации необходимо нажать на кнопку «**Процесс**», отобразится таблица анализа сетевого трафика (Рисунок 154).

| Дата видимого потока gmt+3:00 | Продолжительность | Протокол | IP адрес | Потоки(%) | Пакеты(%) | Байты(%) | pps | bps | Bpp |
|---|---|---|---|---|---|---|---|---|---|
| 2015-02-05 14:20:25..497 | 4108.102 | any | 255.255.255.255 | 7651(74.3) | 8933(17.9) | 1.6M(16.4) | 2 | 3098 | 178 |
| 2015-02-05 14:22:17..423 | 3996.176 | any | 192.168.5.40 | 7558(73.4) | 8098(16.3) | 1.2M(12.6) | 2 | 2460 | 151 |
| 2015-02-05 14:23:55..519 | 3897.159 | any | komrad | 2229(21.6) | 16174(32.5) | 6.1M(62.7) | 4 | 12522 | 377 |
| 2015-02-05 14:24:02..920 | 3861.406 | any | 192.168.0.2 | 1112(10.8) | 1118(2.2) | 109712(1.1) | 0 | 227 | 98 |
| 2015-02-05 14:23:55..519 | 3893.941 | any | 192.168.1.27 | 834(8.1) | 10240(20.6) | 3.6M(36.8) | 2 | 7361 | 349 |
| 2015-02-05 14:22:17..423 | 4047.377 | any | 192.168.5.255 | 352(3.4) | 24417(49.1) | 2.0M(20.8) | 6 | 4003 | 82 |
| 2015-02-05 14:24:39..048 | 3851.253 | any | 192.168.5.48 | 160(1.6) | 1967(4.0) | 955997(9.8) | 0 | 1985 | 486 |
| 2015-02-05 14:24:00..220 | 1043.704 | any | 192.168.5.42 | 107(1.0) | 1007(2.0) | 207314(2.1) | 0 | 1589 | 205 |
| 2015-02-05 14:42:26..566 | 2786.112 | any | 192.168.5.58 | 81(0.8) | 1857(3.7) | 1.1M(11.5) | 0 | 3211 | 602 |
| 2015-02-05 14:30:13..615 | 3544.871 | any | 192.168.5.60 | 61(0.6) | 1804(3.6) | 433789(4.5) | 0 | 978 | 240 |

Рисунок 154 – Окно анализа сетевого трафика

### 5.3.5. Карта мониторинга доступности

В разделе «**Сведения → Карта**» осуществляется создание и управление картами, отображающими доступность узлов и сервисов.

Меню раздела имеет следующий вид:

В меню доступны следующие пункты:

Открыть → Обзор

Действия → Поиск

Действия → Изменить вид

Действия → Экспорт в статическую карту

Редактировать карту → Прикрепить/Переместить все объекты

Редактировать карту → Показать/скрыть сетку

Редактировать карту → Добавить значок → Узел

Редактировать карту → Добавить значок → Сервис

Редактировать карту → Добавить значок → Группа узлов

Редактировать карту → Добавить значок → Группа сервисов

Редактировать карту → Добавить значок → Карта

Редактировать карту → Добавить линию → Узел

Редактировать карту → Добавить линию → Сервис

Редактировать карту → Добавить линию → Группа узлов

Редактировать карту → Добавить линию → Группа сервисов

Редактировать карту → Добавить линию → Карта

Редактировать карту → Особые фигуры → Форма

Редактировать карту → Особые фигуры → Текстовое поле

Редактировать карту → Особые фигуры → Без состояний Линия

Редактировать карту → Особые фигуры → Container

Редактировать карту → Управление шаблонами

Редактировать карту → Настройки карты

Настройки → Общие настройки

Настройки → Управление бэкендами

Настройки → Управление фонами

Настройки → Управление картами

Настройки → Управление формами

**Примечание:** все пункты меню становятся доступными только при добавлении хотя бы одной карты.

В ПК «КОМРАД» возможно создание трех типов объектов – карты, вложенной карты и автокарты.

## Карта

Для создания картынеобходимо перейти в«**Настройки → Управление картами**» (Рисунок 155).

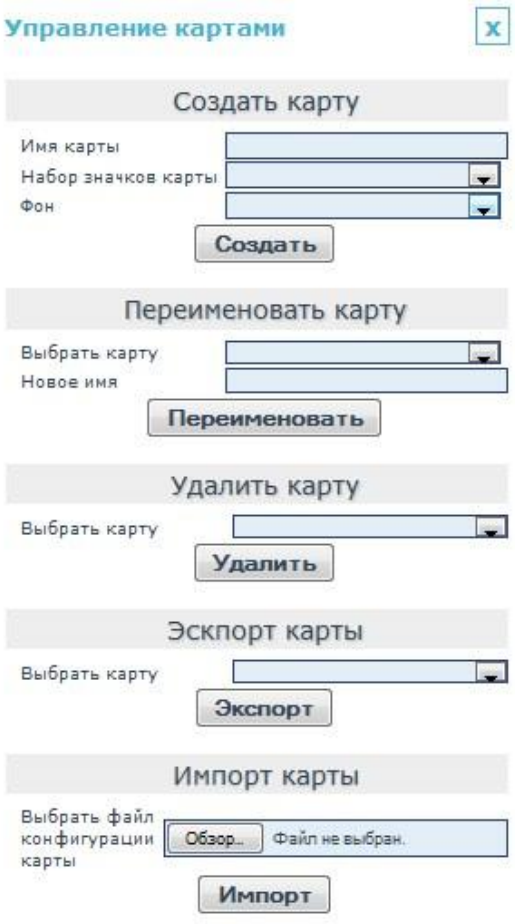



Рисунок 155 – Окно управления картами

В поле «Создать карту» ввести название карты, выбрать вид отображаемых значков (big, dot, medium, small), выбрать фон и нажать «**Создать**». Созданная карта отобразится в текущем окне.

**Примечание:** в модуле «Карты» все названия вводятся только латиницей и без пробелов, в противном случае система выдаст сообщение об ошибке.

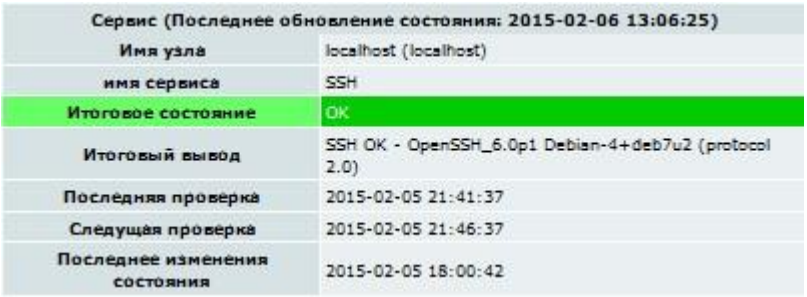
**Примечание:**в ПК «КОМРАД» изначально уже доступны два фоновых изображения –MapKOMRAD-civil.pngи MapKOMRAD-MO.png.

Чтобы добавить элемент (узел, сервис, группа узлов, группа сервисов, карта) на карту, нужно обратиться к меню «**Редактировать карту → Добавить значок →** …». Следует поместить курсор в место на карте, куда нужно установить значок, затем в появившемся меню настроить параметры объекта и нажать «**Сохранить**». Пример карты с отображенным узлом и сервисом показан на Рисунке 156.

Рисунок 156 – Пример карты

При наведении курсора мыши на объект на картепоявляется всплывающее меню (hovermenu), котороевключено по умолчанию (Рисунок 157). 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 |
| Следущая проверка | 2015-02-05 21:46:37 |
| Последнее изменения состояния | 2015-02-05 18:00:42 |

Рисунок 157 – Всплывающее меню для узла

Для включения режима редактирования карты следует перейти в «**Редактировать карту → Прикрепить/Переместить все объекты**», при этом на панели меню отобразится сообщение:

Выход из режима редактирования осуществляется аналогичным образом.

В меню «**Открыть → Обзор**» отображаются все имеющиеся в системе карты и статус доступности их объектов (Рисунок 158). При наведении курсора мыши на пиктограмму состояния отобразится детализированная информация о доступности.

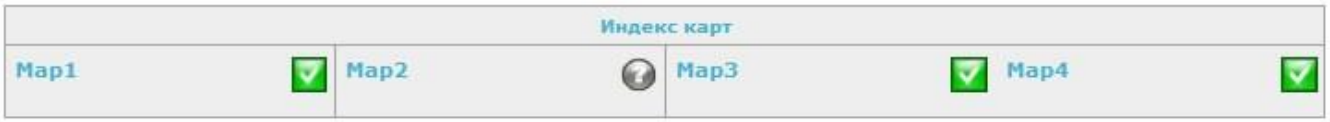



Рисунок 158 – Обзор состояния карт

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).

Для того чтобы переименовать существующую карту,нужно перейти в«**Настройки → Управление картами**» (Рисунок 155), в поле «Переименовать карту» выбрать карту из выпадающего списка, присвоить ей новое имя и нажать «**Переименовать**».

Для удаления картынужно перейти в«**Настройки → Управление картами**» (Рисунок 155), в поле «Удалить карту» выбрать карту из выпадающего списка и нажать «**Удалить**».

Для экспорта карты перейти в«**Настройки → Управление картами**» (Рисунок 155), в поле «Экспорт карты» выбрать карту из выпадающего списка и нажать «**Экспорт**». При этом карта сохранится локально с расширением *.cfg*. Открыв документ в текстовом редакторе, можно поменять вручную конфигурацию. Чтобы импортировать карту, необходимо в «**Настройки → Управление картами**» (Рисунок 155), в поле «Импорт карты» выбрать сохраненную локально карту и нажать «**Импорт**». Пример импортируемой карты приведен на Рисунке 159.

```
define global {
object_id=0
map_image=MapKOMRAD-civil.png
iconset=std_big
}

define host {
object_id=17fdfe
host_name=komrad
x=227
y=367
}

define service {
object_id=e56f20
host_name=localhost
service_description=Total Processes
x=218
y=210
view_type=icon
}
```

Рисунок 159 – Пример экспортированной карты

**Примечание:** имя импортируемой карты не должно содержать пробелов.

Управление фонами осуществляется из меню «**Настройки → Управление фонами**» (Рисунок 160). В поле «Создание нового изображения» можно задать имя нового фонового изображения, настроить цвет, используя палитру, или, указав код цвета в шестнадцатеричномвиде, затем нажать «**Сохранить**».

В данном меню также возможны загрузка нового изображения и удаление уже загруженных.

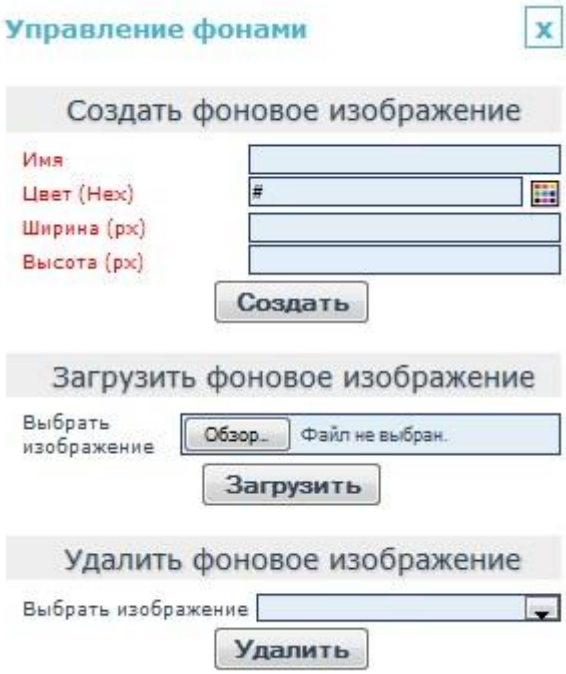



Рисунок 160 – Управление фонами

В меню «**Настройки → Общие настройки**» возможна подробная конфигурация различных настроек модуля «**Карты**»(Рисунок 161). Параметры настроек соответствуют пунктам текстового конфигурационного файла, доступного в интерфейсе командной строки.

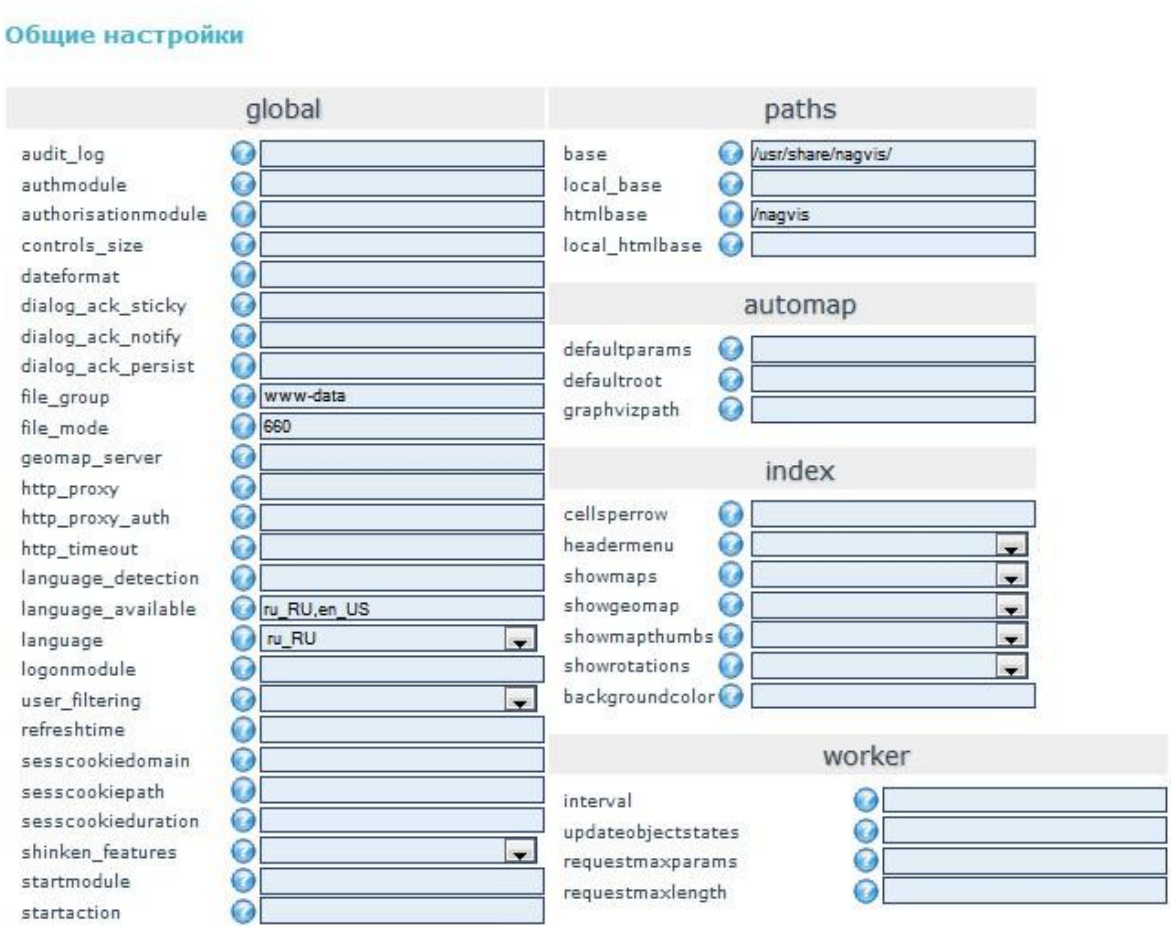



Рисунок 161 – Окно общих настроек

**Вложенная карта**

Создание вложенной карты осуществляется с помощью «**Редактировать карту → Добавить значок →Карта**». Вложенная карта помещается в виде значка на уже существующую карту.

**Примечание:**если хотя бы один объект на вложенной карте станет недоступным, то цвет иконки вложенной карты изменится на красный, и иконка начнет мигать.

**Автокарта**

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

Чтобы создать автокарту необходимо перейти в «**Настройки → Управление картами**» и создать новую карту, выбрав фоновое изображение и вид отображаемых значков. Созданная карта отобразится в текущем окне.

Затем в меню перейти в «**Редактировать карту → Настройки карты**», поставить галочку рядом с полем «sources», в появившемся текстовом поле ввести *automap*и нажать «**Сохранить**» (Рисунок 162). Созданная автокарта отобразится в текущем окне (Рисунок 163).

Рисунок 162 – Создание автокарты

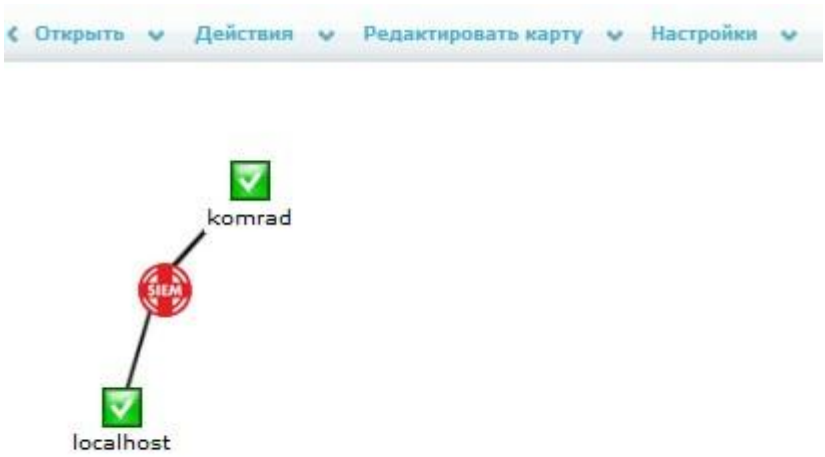



Рисунок 163 – Автокарта

Возможен экспорт автокарты в статическую карту: «**Действия → Экспорт в статическую карту**». При этом следует задать имя новой статической карты и нажать «**Сохранить**» (Рисунок 164).

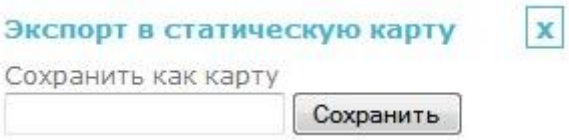



Рисунок 164 – Экспорт автокарты в статическую карту

### 5.3.6. Конфигурирование настроек сервера и сенсора

В разделе «**Система →Конфигурация**» доступна информация по текущему состоянию ПК «КОМРАД» (Рисунок 165). Представлена информация по используемому дисковому пространству, загрузке процессора и оперативной памяти, а также текущие настройки сетевых интерфейсов.

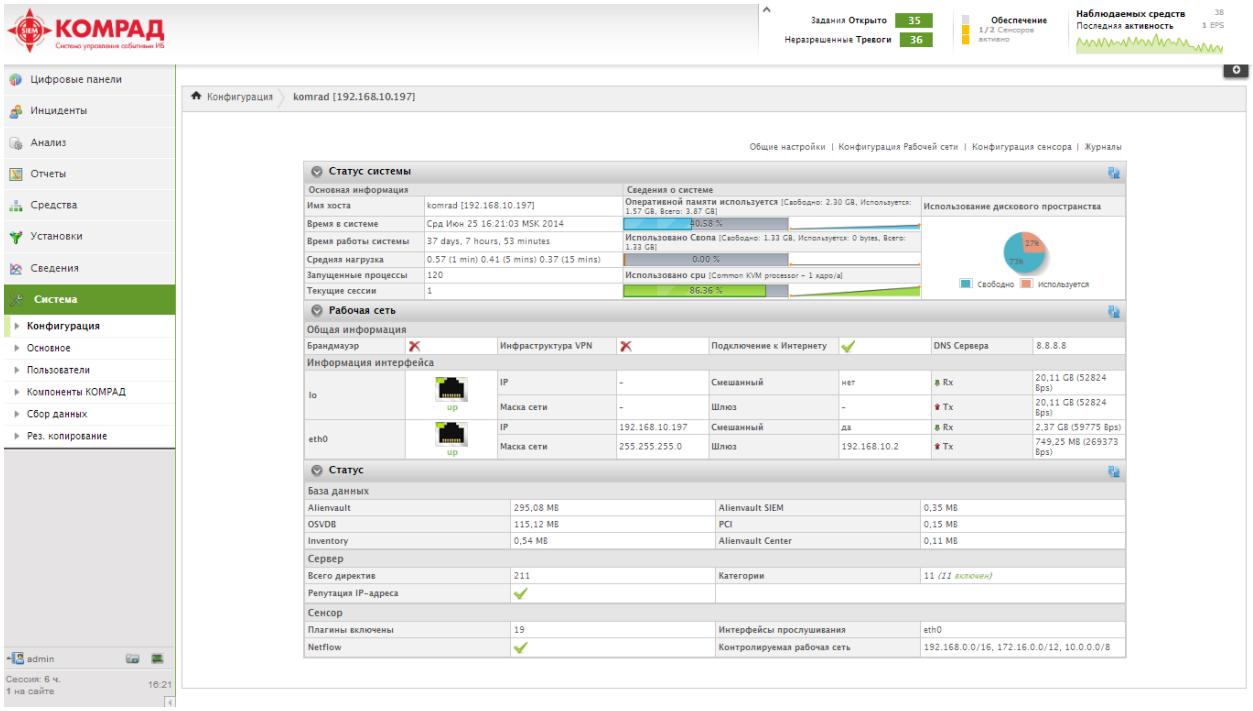



Рисунок 165 – Состояние системы ПК «КОМРАД»

Нажатие на ссылку «**Общие настройки**» позволяет перейти к настройкам сервера ПК «КОМРАД» (Рисунок 166). Доступны настройки IP-адреса веб-интерфейса ПК «КОМРАД», NTP-сервера, почтового сервера.

Нажатие на ссылку «**Конфигурация рабочей сети**» позволяет перейти к настройкам сетевых интерфейсов сервера ПК «КОМРАД» (Рисунок 167).

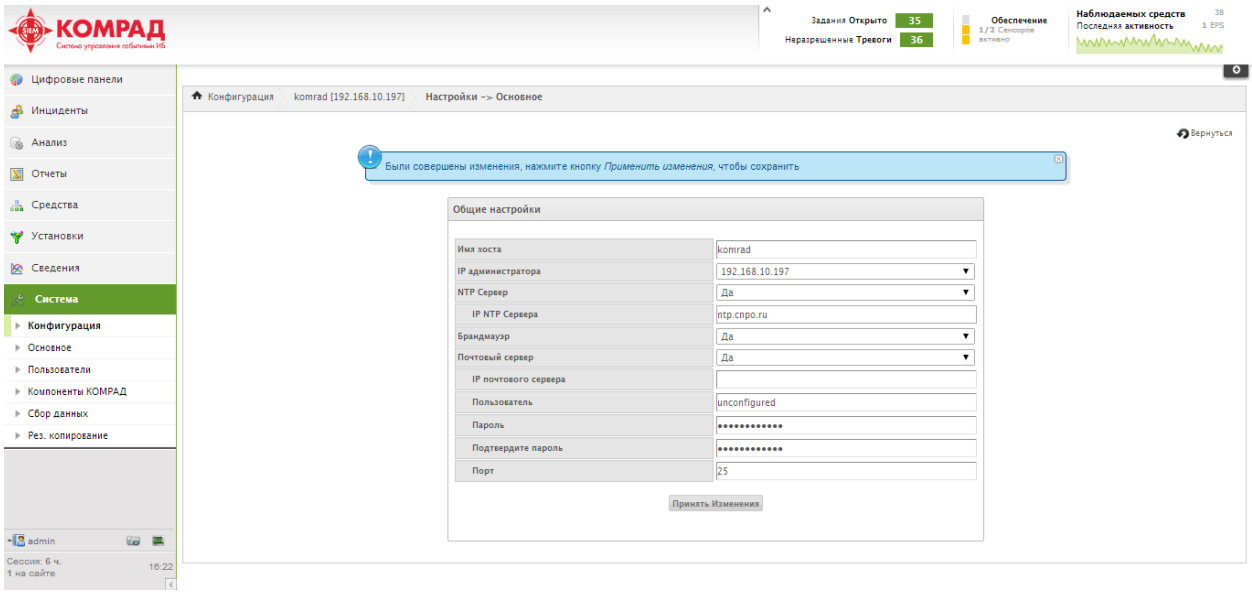



Рисунок 166 – Настройка сервера ПК «КОМРАД»

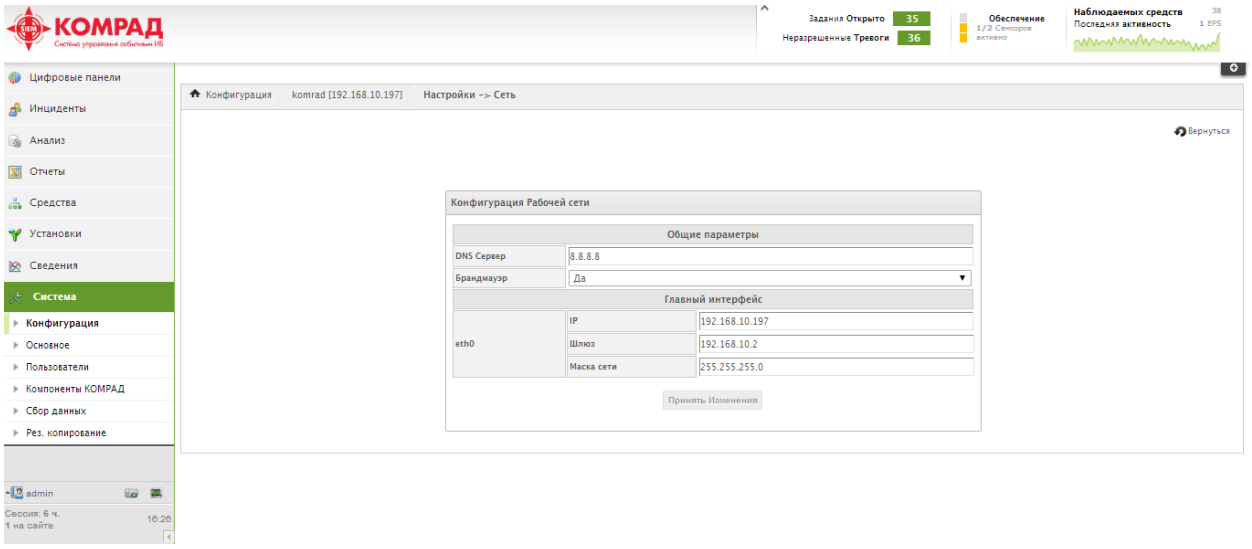



Рисунок 167 – Настройка сетевых интерфейсов сервера ПК «КОМРАД»

Нажатие на ссылку «**Конфигурация сенсора**» открывает страницу с настройками сенсоров. Возможны следующие настройки: сетевые настройки (Рисунок 168), дополнительные настройки (Рисунок 169), настройки плагинов (Рисунок 170).

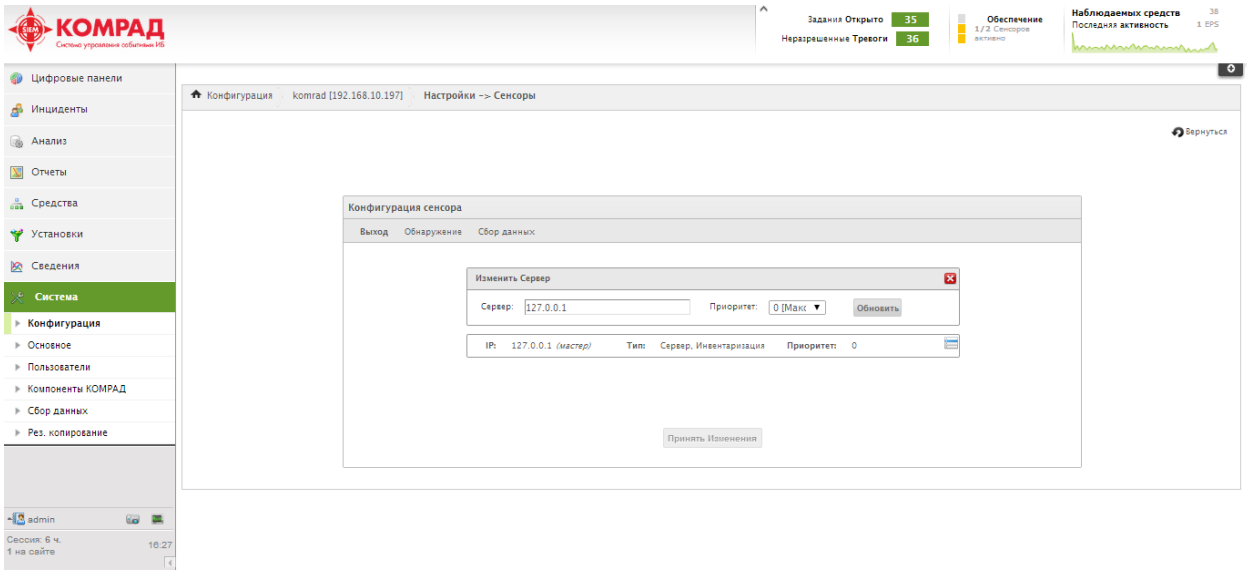



Рисунок 168 – Сетевые настройки сенсора ПК «КОМРАД»

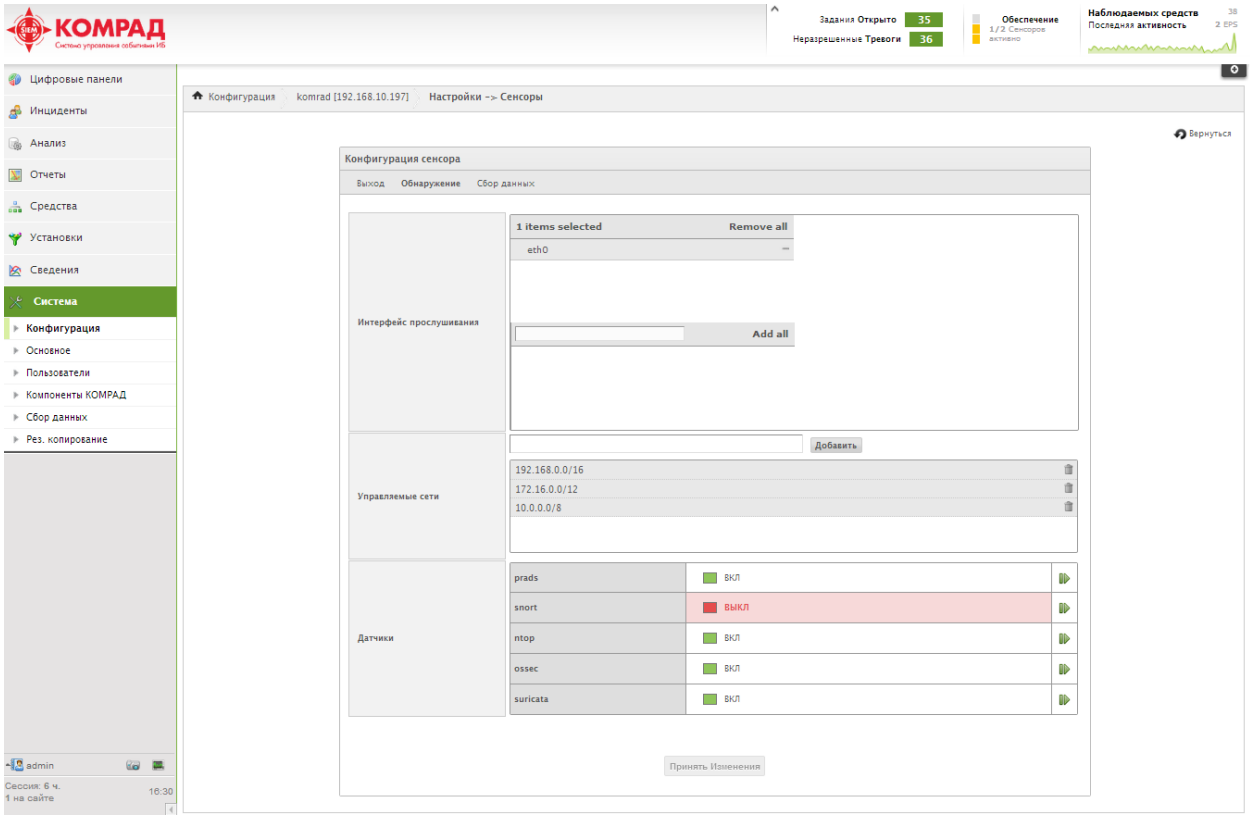



Рисунок 169 – Дополнительные настройки сенсоров ПК «КОМРАД»

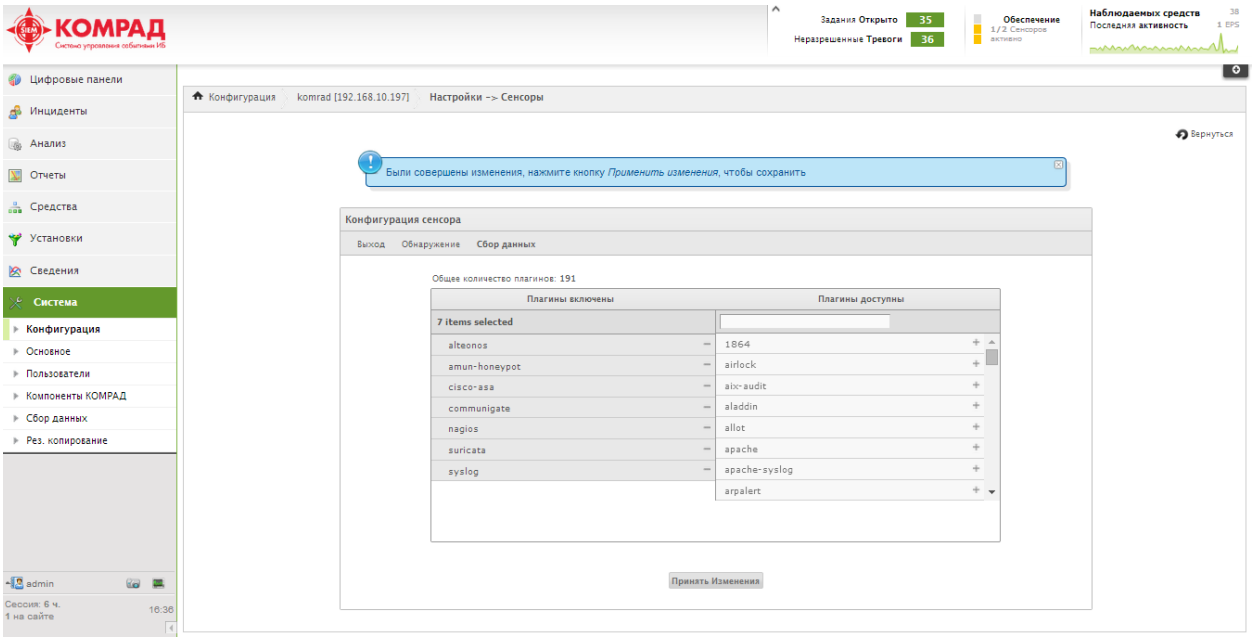



Рисунок 170 – Настройки плагинов сенсора ПК «КОМРАД»

С левой стороны находится блок подключенных плагинов, с правой стороны плагины доступные для подключения. Нажатие на знак «+» позволяет добавить плагин, нажатие на знак «-» позволяет отключить плагин. Для удобства поиска над полем со спискомдоступных плагинов расположена строка поиска. После добавления нужных плагинов необходимо нажать на кнопку «**Принять изменения**».

**Примечание:** добавление плагинов возможно из интерфейса командной строки (подробное описание приведено в разделе «Настройка плагинов ПК «КОМРАД» настоящего руководства).

Для просмотра журналов системы необходимо нажать на ссылку «**Журналы**» (Рисунок 171).

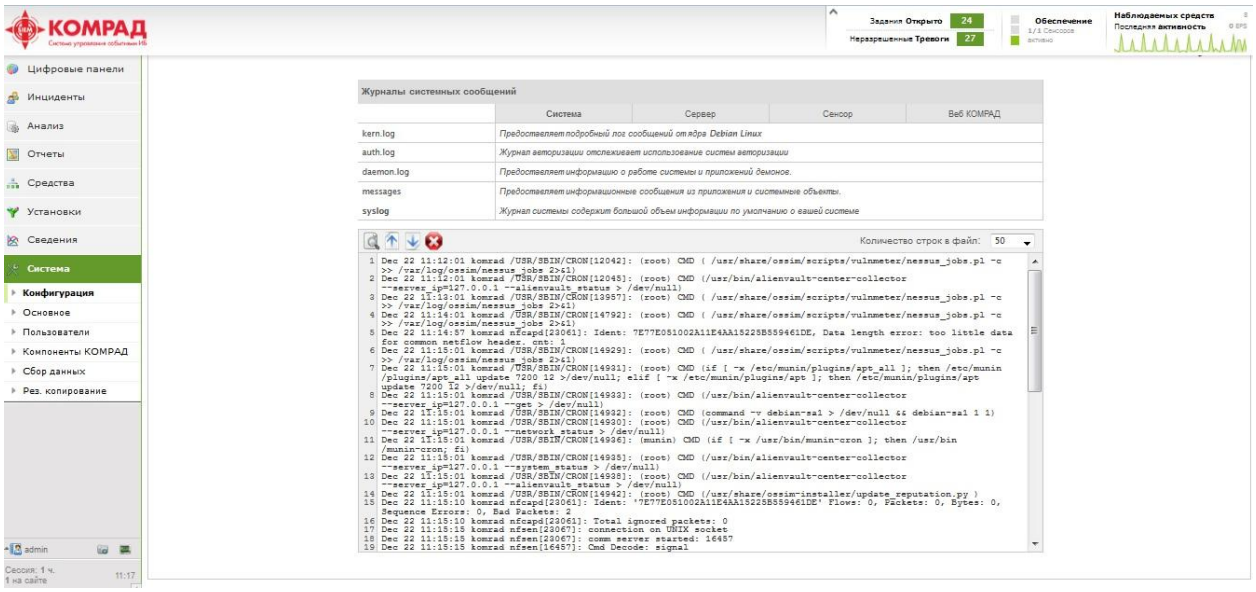



Рисунок 171 – Просмотр журналов системы

Для просмотра в веб-интерфейсе доступны типы журналов (Таблица 8):

Таблица 8. Типы журналов, доступных с помощью веб-интерфейса

| **Тип журнала** | **Расположение журнала** | **Содержимое журнала** |
|---|---|---|
| Система | /var/log/kern.log | Сообщения от ядра linux |
| | /var/log/auth.log | Сообщения об использовании систем аутентификации |
| | /var/log/daemon.log | Сообщения о работе системы и служб |
| | /var/log/messages | Общесистемные некритичные сообщения |
| | /var/log/syslog | Все системные сообщения, кроме событий аутентификации |
| Сервер | /var/log/ossim/server.log | Журнал сервера ПК «КОМРАД» |
| Сенсор | /var/log/ossim/agent_stats.log | Подробная информация о процессе сбора данных |
| | /var/log/ossim/agent.log | Журнал получения сенсо- |

| | | |
|---|---|---|
| | | ром сведений о событиях ИБ |
| Веб-интерфейс | /var/log/apache2/access.log | Журнал доступа к веб-интерфейсу |
| | /var/log/apache2/error.log | Ошибки http-сервера |

Помимо этогодля OSSECво вкладке «**Анализ→ Обнаружение →OSSECуправление**» доступен **«Журнал OSSEC»** (путь: /var/ossec/logs/ossec.log) и отдельный **«Журнал Оповещений»** (путь: /var/ossec/logs/alerts/alerts.log).

### 5.3.7. Выявление и анализ уязвимостей системы

В ПК «КОМРАД» реализована возможность выявления и анализа уязвимостей информационной системы. Для этого необходимо перейти на вкладку **«Анализ → Уязвимости»** (Рисунок 172**)** и нажать пункт «**Задания на сканирование**» (Рисунок 173) а затем кнопку «**Новое задание сканирования**».

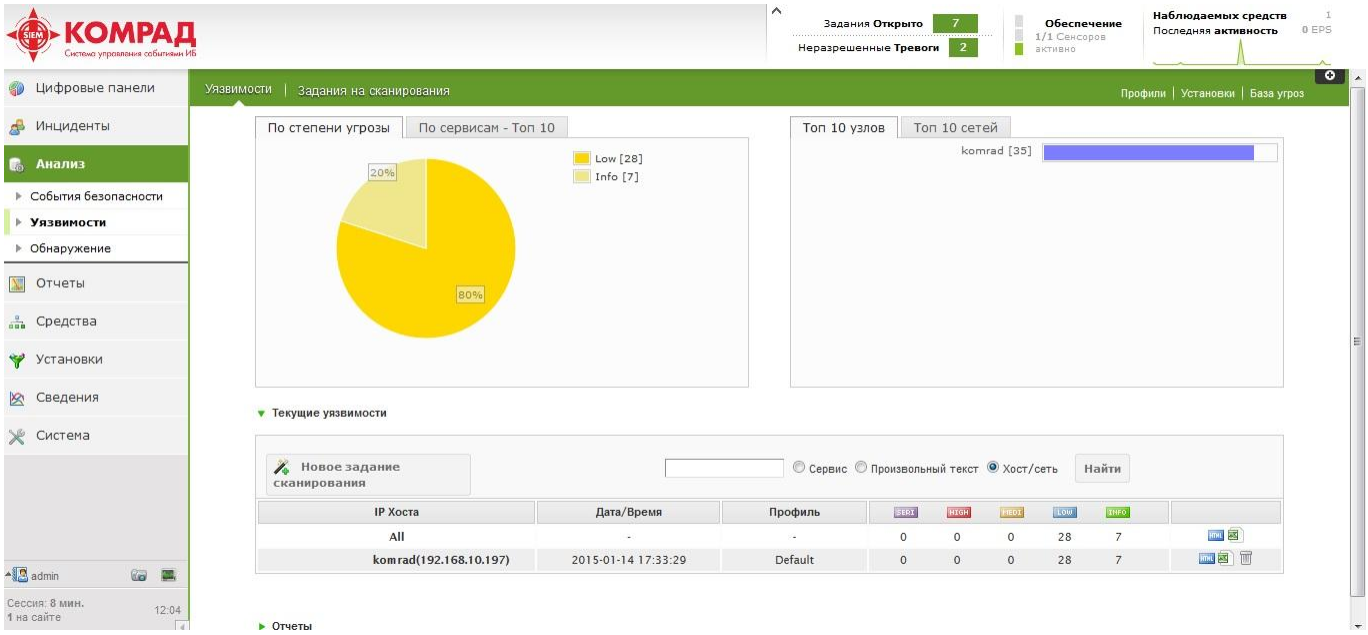



Рисунок 172– Вкладка «Уязвимости»

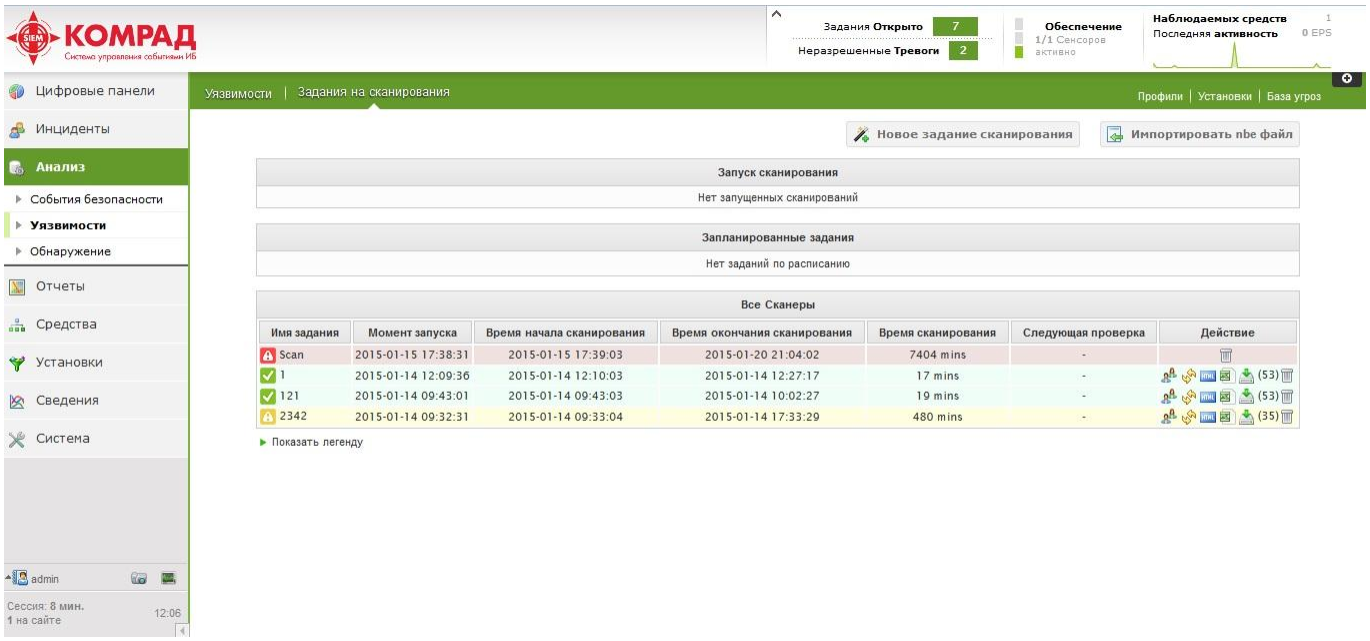



Рисунок 173 – Пункт «Задания на сканирование»

В открывшемся окне (Рисунок 174) ввести имя задания, в дереве средств выбрать хост, затем нажать кнопку «**Новое задание**».

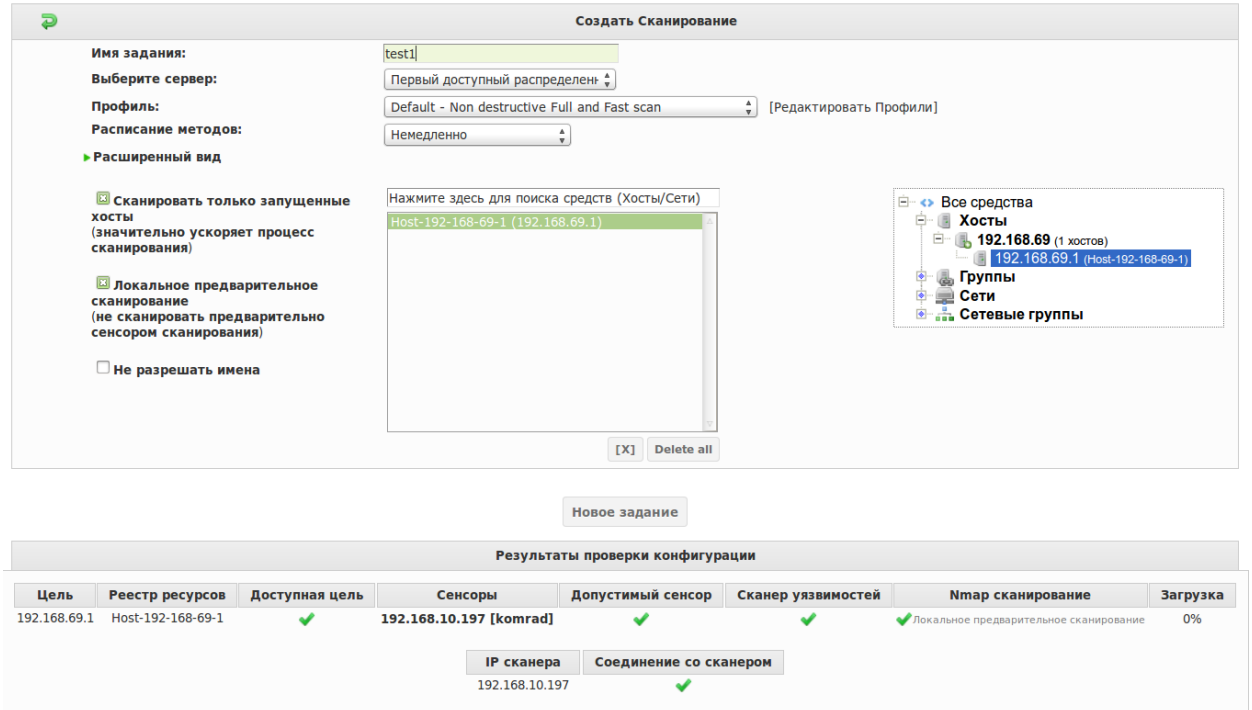



Рисунок 174 – Выбор цели для сканирования

Дождаться окончания сканирования (Рисунок 175) и нажать на кнопку импорта в Excel .

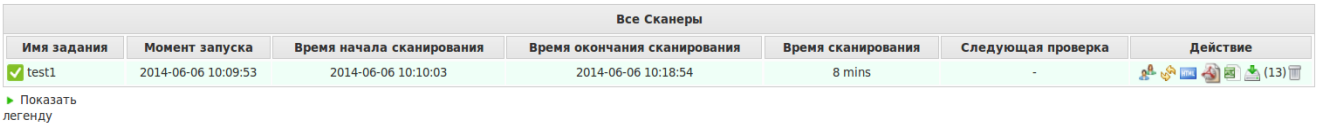



Рисунок 175 – Завершение сканирования

В горизонтальном меню раздела «**Уязвимости**» также доступны кнопки: «**Профили**» – выбор профиля для сканирования (Рисунок 176).

Рисунок 176 – Профили сканирования уязвимостей

Доступны следующие типы профилей:

1) **Deep** – полное сканирование с использованием всех возможных тестов (полный перебор) без использования деструктивных тестов;
2) **Default** – полное сканирование с интеллектуальным построением карты тестирования;
3) **Ultimate** – полное сканирование с интеллектуальным построением карты тестирования, включает в себя деструктивные тесты.

Нажатие на кнопку «**Создать новый профиль**» позволяет создать новый профиль сканирования (Рисунок 177).

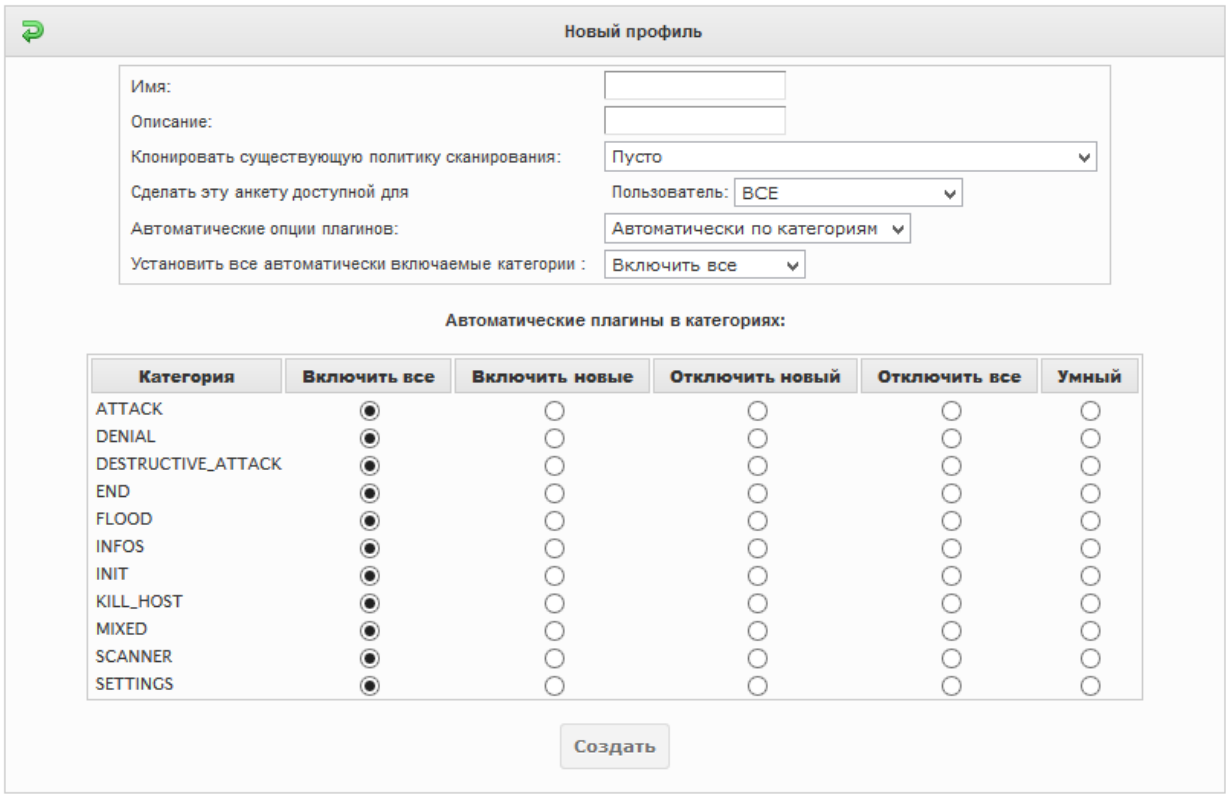



Рисунок 177 – Создание нового профиля сканирования

В разделе **«Анализ → Уязвимости→Установки»** возможно задание сканирования с дополнительными полномочиями (Рисунок 178).

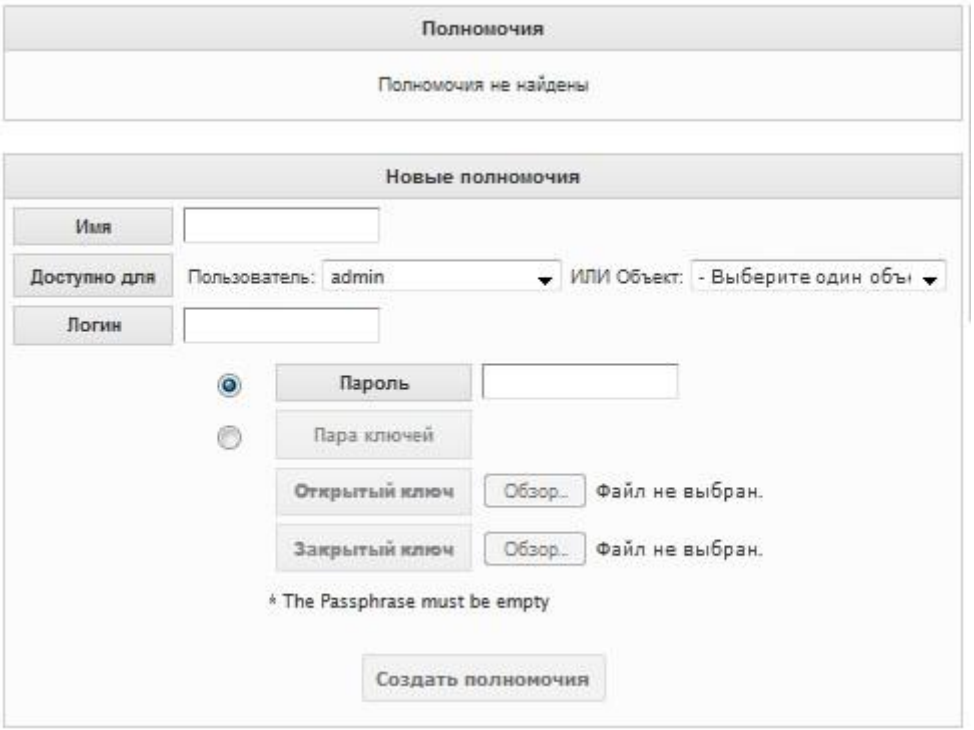
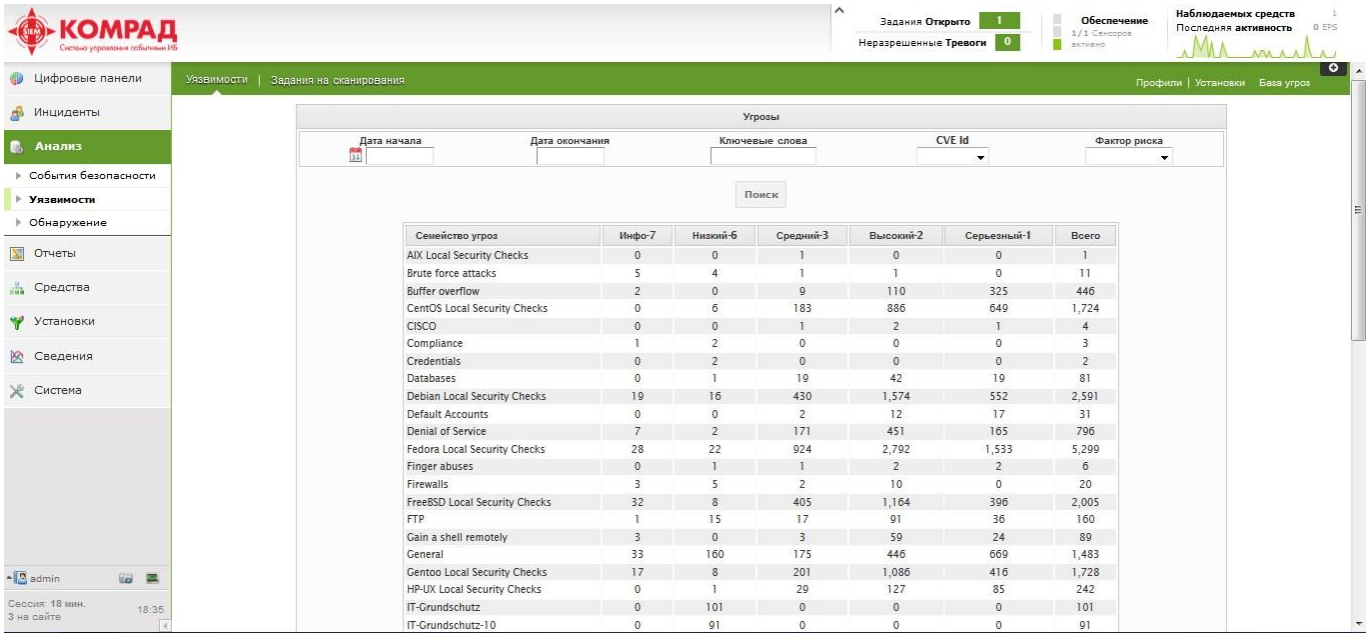


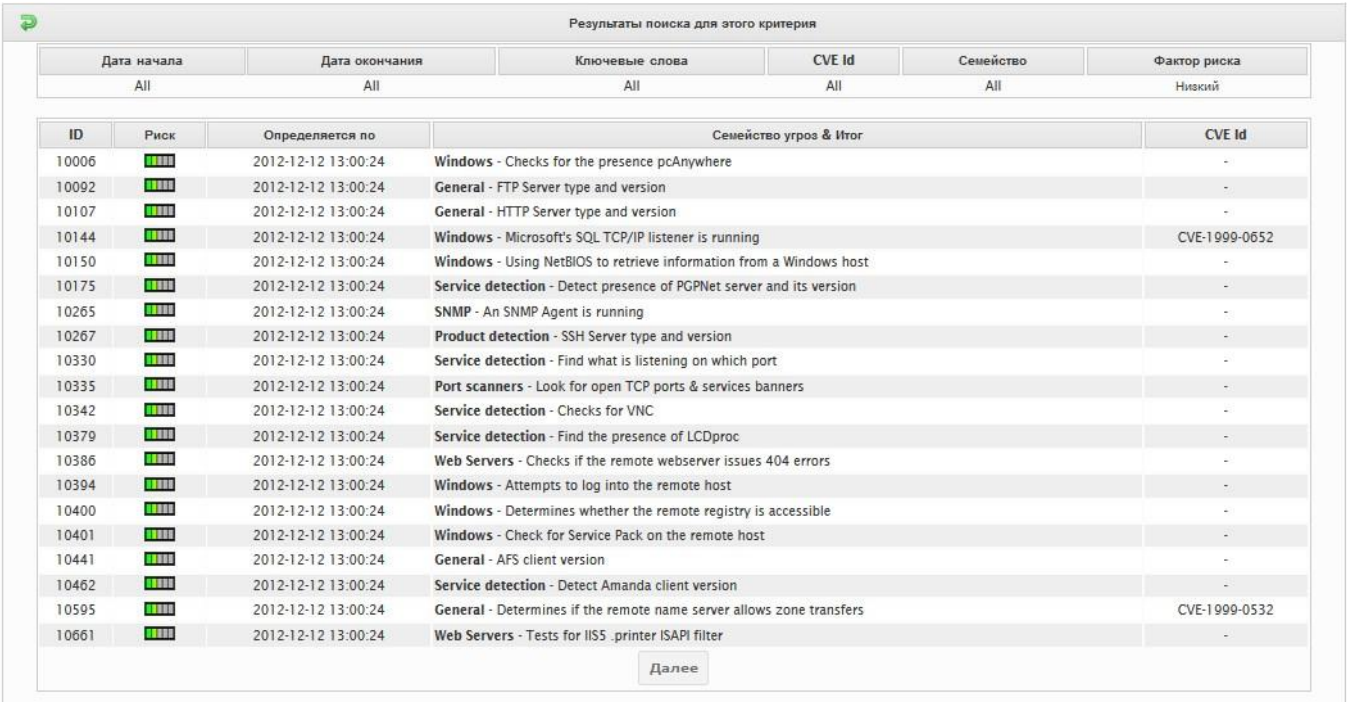

Рисунок 178 – Задания полномочий для сканирования

В горизонтальном меню раздела «**Уязвимости**» также доступна «**База угроз**» – база сигнатур с возможностью поиска по критериям (Рисунок 179, Рисунок 180).




| Семейство угроз | Инфо-7 | Низкий-6 | Средний-3 | Высокий-2 | Серьезный-1 | Всего |
|---|---|---|---|---|---|---|
| AIX Local Security Checks | 0 | 0 | 1 | 0 | 0 | 1 |
| Brute force attacks | 5 | 4 | 1 | 1 | 0 | 11 |
| Buffer overflow | 2 | 0 | 9 | 110 | 325 | 446 |
| CentOS Local Security Checks | 0 | 6 | 183 | 886 | 649 | 1,724 |
| CISCO | 0 | 0 | 1 | 2 | 1 | 4 |
| Compliance | 1 | 2 | 0 | 0 | 0 | 3 |
| Credentials | 0 | 2 | 0 | 0 | 0 | 2 |
| Databases | 0 | 1 | 19 | 42 | 19 | 81 |
| Debian Local Security Checks | 19 | 16 | 430 | 1,574 | 552 | 2,591 |
| Default Accounts | 0 | 0 | 2 | 12 | 17 | 31 |
| Denial of Service | 7 | 2 | 171 | 451 | 165 | 796 |
| Fedora Local Security Checks | 28 | 22 | 924 | 2,792 | 1,533 | 5,299 |
| Finger abuses | 0 | 1 | 1 | 2 | 2 | 6 |
| Firewalls | 3 | 5 | 2 | 10 | 0 | 20 |
| FreeBSD Local Security Checks | 32 | 8 | 405 | 1,164 | 396 | 2,005 |
| FTP | 1 | 15 | 17 | 91 | 36 | 160 |
| Gain a shell remotely | 3 | 0 | 3 | 59 | 24 | 89 |
| General | 33 | 160 | 175 | 446 | 669 | 1,483 |
| Gentoo Local Security Checks | 17 | 8 | 201 | 1,086 | 416 | 1,728 |
| HP-UX Local Security Checks | 0 | 1 | 29 | 127 | 85 | 242 |
| IT-Grundschutz | 0 | 101 | 0 | 0 | 0 | 101 |
| IT-Grundschutz-10 | 0 | 91 | 0 | 0 | 0 | 91 |

Рисунок 179 – Страница базы угроз




| Дата начала | Дата окончания | Ключевые слова | CVE Id | Семейство | Фактор риска |
|---|---|---|---|---|---|
| All | All | All | All | All | Низкий |

| ID | Риск | Определяется по | Семейство угроз & Итог | CVE Id |
|---|---|---|---|---|
| 10006 | | 2012-12-12 13:00:24 | **Windows** - Checks for the presence pcAnywhere | - |
| 10092 | | 2012-12-12 13:00:24 | **General** - FTP Server type and version | - |
| 10107 | | 2012-12-12 13:00:24 | **General** - HTTP Server type and version | - |
| 10144 | | 2012-12-12 13:00:24 | **Windows** - Microsoft's SQL TCP/IP listener is running | CVE-1999-0652 |
| 10150 | | 2012-12-12 13:00:24 | **Windows** - Using NetBIOS to retrieve information from a Windows host | - |
| 10175 | | 2012-12-12 13:00:24 | **Service detection** - Detect presence of PGPNet server and its version | - |
| 10265 | | 2012-12-12 13:00:24 | **SNMP** - An SNMP Agent is running | - |
| 10267 | | 2012-12-12 13:00:24 | **Product detection** - SSH Server type and version | - |
| 10330 | | 2012-12-12 13:00:24 | **Service detection** - Find what is listening on which port | - |
| 10335 | | 2012-12-12 13:00:24 | **Port scanners** - Look for open TCP ports & services banners | - |
| 10342 | | 2012-12-12 13:00:24 | **Service detection** - Checks for VNC | - |
| 10379 | | 2012-12-12 13:00:24 | **Service detection** - Find the presence of LCDproc | - |
| 10386 | | 2012-12-12 13:00:24 | **Web Servers** - Checks if the remote webserver issues 404 errors | - |
| 10394 | | 2012-12-12 13:00:24 | **Windows** - Attempts to log into the remote host | - |
| 10400 | | 2012-12-12 13:00:24 | **Windows** - Determines whether the remote registry is accessible | - |
| 10401 | | 2012-12-12 13:00:24 | **Windows** - Check for Service Pack on the remote host | - |
| 10441 | | 2012-12-12 13:00:24 | **General** - AFS client version | - |
| 10462 | | 2012-12-12 13:00:24 | **Service detection** - Detect Amanda client version | - |
| 10595 | | 2012-12-12 13:00:24 | **General** - Determines if the remote name server allows zone transfers | CVE-1999-0532 |
| 10661 | | 2012-12-12 13:00:24 | **Web Servers** - Tests for IIS5 .printer ISAPI filter | - |

Далее

Рисунок 180 – Результаты поиска в базе угроз по фактору риска

### 5.3.8. Настройка параметров хранения событий безопасности

Настройка параметров хранения событий и инцидентов производится на вкладке«**Система → Основное → Рез.копирование**» (Рисунок 181).

Пункт «События, которые необходимо сохранить в базе данных (Количество дней)» позволяет задать интервал (в сутках) для хранения событий безопасности. Пункт «События, которые необходимо сохранить в базе данных (Количество событий)» позволяет задать количество событий безопасности хранящихся в БД.

**Примечание:** события удаляются 1 раз за сутки (по умолчанию удаление производится в 00:00 по GMT).

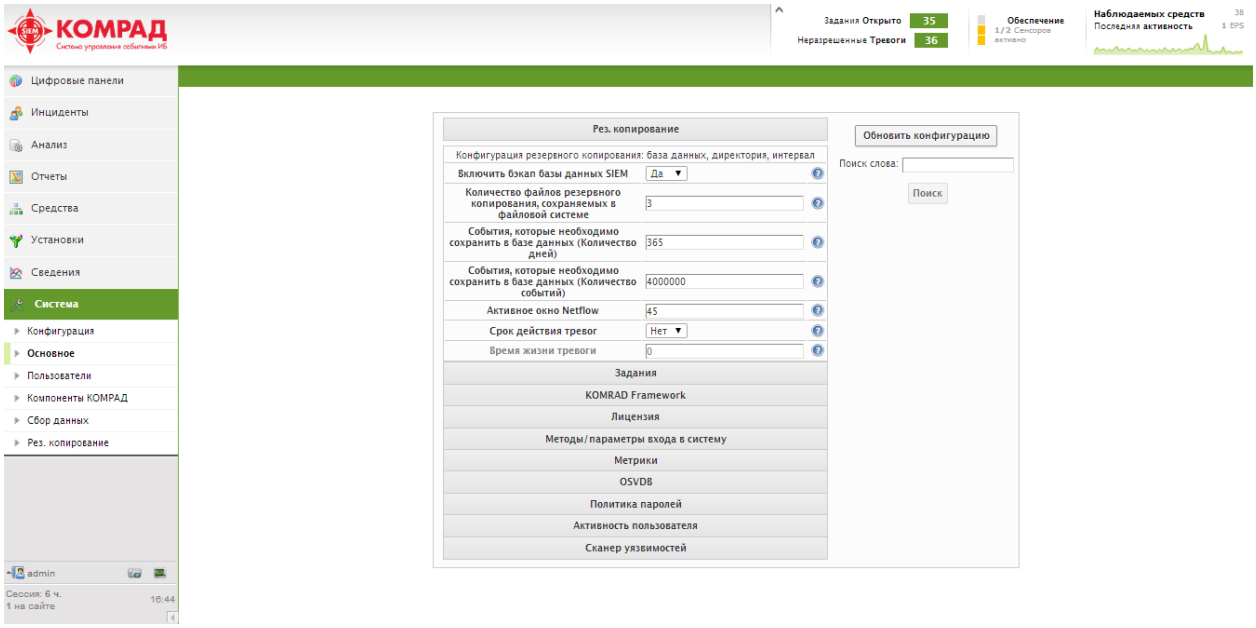



Рисунок 181 – Настройка параметров хранилища данных

### 5.3.9. Резервное копирование системы

Для настройки резервного копирования необходимо в веб-интерфейсе ПК «КОМРАД» перейти на вкладку «**Система»→ Основное→Рез. копирование**» (Рисунок 182).

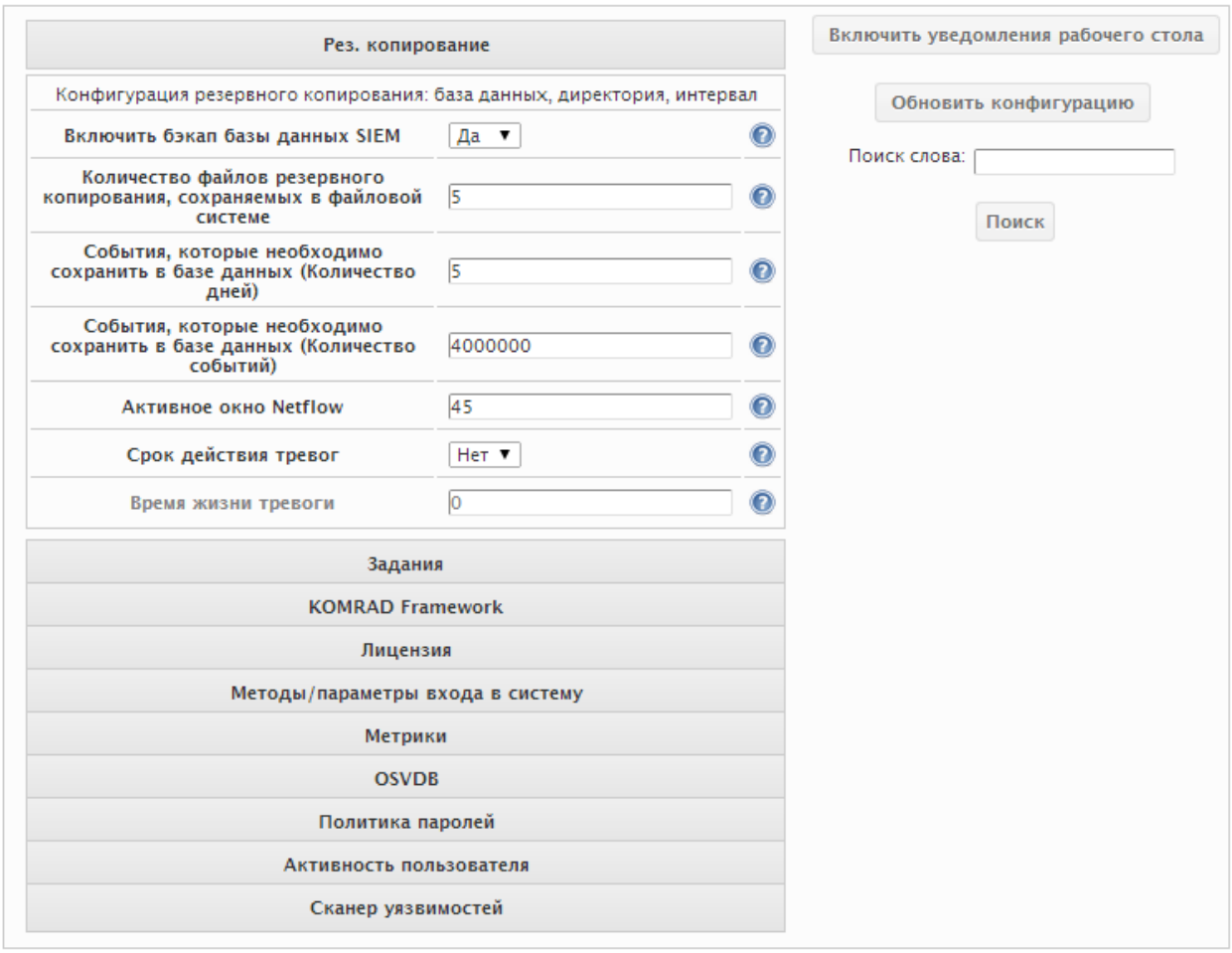



Рисунок 182 – Окно настройки резервного копирования

В появившемся окне администратору безопасности предоставляются следующие возможности: включение/отключение резервного копирования базы данных ПК «КОМРАД» (**Включить бэкап базы данных SIEM**); определение количества файлов резервного копирования, сохраняемых в файловой системе; определение срока хранения событий и количества сохраняемых событий и другие. После выбора требуемых значений необходимо нажать на кнопку «**Обновить конфигурацию**».

Сведения о резервном копировании и доступ к сохраненной базе можно получить во вкладке «**Система → Рез.копирование**» (Рисунок 183).

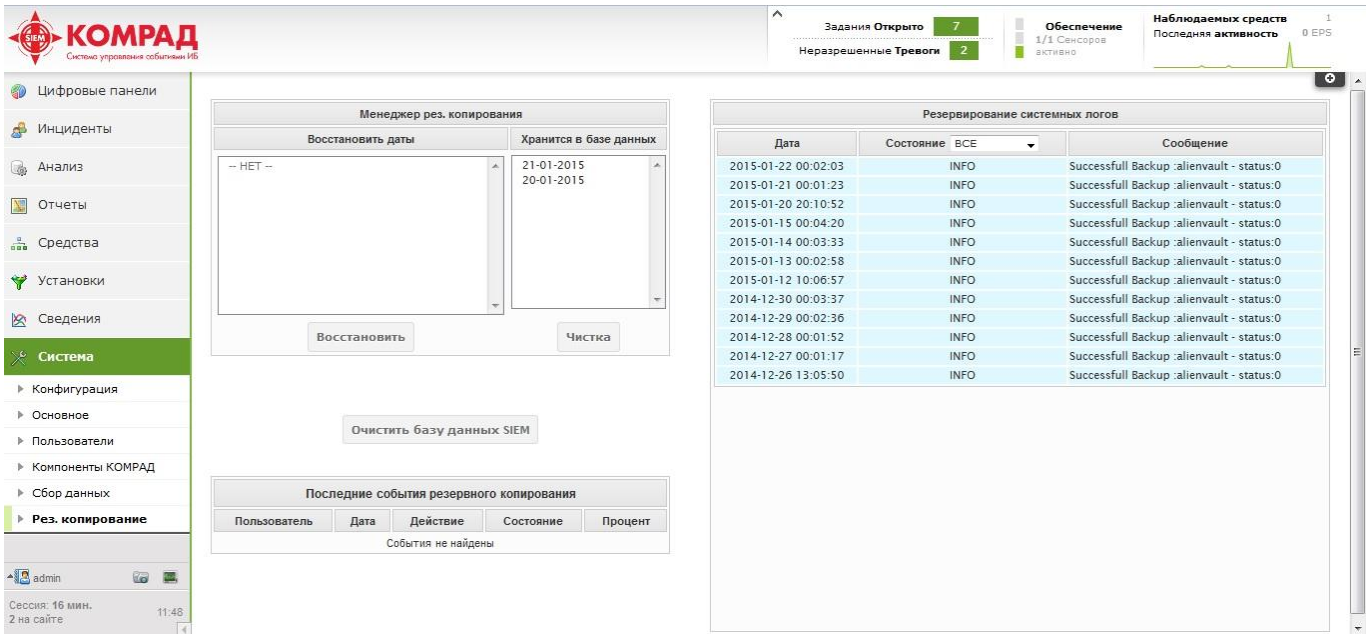



Рисунок 183 – Сведения о резервном копировании

В данном окне можно получить информацию по хранимым в базе данных резервным копиям и действиям по резервированию системных логов.

Помимо этого ПК «КОМРАД» обеспечивает резервирование базы данных средствами консольных утилит из состава СУБД MySQL, при этом резервная копия может быть экспортирована в виде файла, расположенного на сервере ПК «КОМРАД» по адресу */var/lib/ossim/backup*. ПК «КОМРАД» предоставляет возможность создания администратором резервных копий конфигурационных файлов посредством интерфейса командной строки, при этом может быть выполнен возврат (откат) к ранее сохранённой конфигурации с помощью заранее выполненных резервных копий базы данных ПК «КОМРАД».

# ПРИЛОЖЕНИЕ А

# МАТРИЦА ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ ПК «КОМРАД»

| **Источник/ Назначение** | | **Назначение** | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Сервер ПК «КОМРАД» | Unix-системы | Windows-системы | Активное сетевое оборудование | IDS | БД MSSQL | БД MySQL | Сервер электронной почты | ОператорПК «КОМРАД» | АдминистраторПК «КОМРАД» |
| **Источник** | Сервер ПК «КОМРАД» | X | UDP 1514 | UDP 514 | UDP 514 | UDP 514 | MSSQL (TCP 1433) | MySQL (TCP 3306) | SMTP (TCP 25) | HTTPS (TCP 443) | HTTPS (TCP 443) SSH (TCP 22) |
| | Unix-системы | UDP 1514 | X | X | X | X | X | X | X | X | X |
| | Windows-системы | UDP 514 | X | X | X | X | X | X | X | X | X |
| | Активное сетевое оборудование | UDP 514 | X | X | X | X | X | X | X | X | X |
| | IDS | UDP 514 | X | X | X | X | X | X | X | X | X |
| | БД MSSQL | MSSQL (TCP 1433) | X | X | X | X | X | X | X | X | X |
| | БД MySQL | MySQL (TCP 3306) | X | X | X | X | X | X | X | X | X |
| | Сервер электронной почты | SMTP (TCP 25) | X | X | X | X | X | X | X | POP3 (TCP 110) | POP3 (TCP 110) |
| | Оператор ПК «КОМРАД» | HTTPS (TCP 443) | X | X | X | X | X | X | POP3 (TCP 110) | X | X |
| | Администратор ПК «КОМРАД» | HTTPS (TCP 443) SSH (TCP 22) | X | X | X | X | X | X | POP3 (TCP 110) | X | X |

# ПРИЛОЖЕНИЕ Б
# ПРИМЕРЫ ПО НАСТРОЙКЕ НЕКОТОРЫХ ТИПОВ ИСТОЧНИКОВ СОБЫТИЙ

## 1. ТРЕБОВАНИЯ ПО УСТАНОВКЕ АГЕНТАOSSEC

### *Установка агента OSSEC для Linux*

1. Для получения архива с OSSEC HIDS необходимо на странице «**Система → Сбор данных → Загрузки**» скачать OSSEC Агент для Linux

2. Для распаковки полученного архива следует выполнить в интерфейсе командной строки следующую команду:

*$ xzfossec-hids-2.8.tar.gz*

3. Для перехода в распакованный каталог необходимо выполнить в интерфейсе командной строки команду:

*$ cd ossec-hids-2.7*

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

*$ /bin/bash ./install.sh*

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

«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?:»**XXX.XXX.XXX.XXX (IPсервера«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.**

Продолжить установку нажатием клавиши **Enter**.

Основные команды для работы с OSSEC:

- для запускаOSSECHIDS необходимо выполнить в интерфейсе командной строки команду:

*$ /var/ossec/bin/ossec-control start*

- для остановкиOSSECHIDS необходимо выполнить в интерфейсе командной строки команду:

*$ /var/ossec/bin/ossec-control stop*

- для управления необходимо выполнить в интерфейсе командной строки следующую команду:

*$ /var/ossec/bin/manage_agents*

## *УстановкаOSSEC-агентадляWindows*

Для установки агента OSSEC в веб-интерфейсе ПК «КОМРАД» следует перейти во вкладку «**Система → Сбор данных → Загрузка**» и выбрать пункт «OSSEC Agent для Windows» (Рисунок Б1), а затем сохранить файл с дистрибутивом агента на жестком диске целевого компьютера.

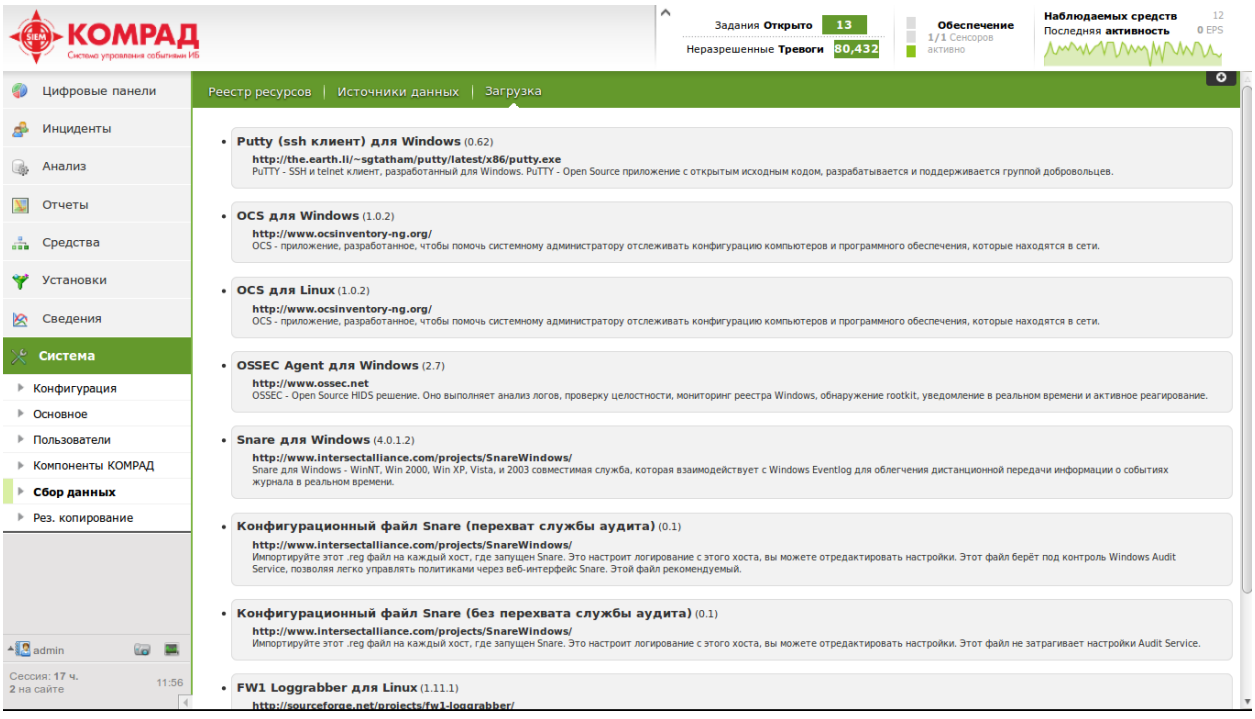



Рисунок Б1 – Загрузка агента OSSEC для Windows

Для запуска процесса установки агента необходимо запустить сохраненный файл (Рисунок Б2).

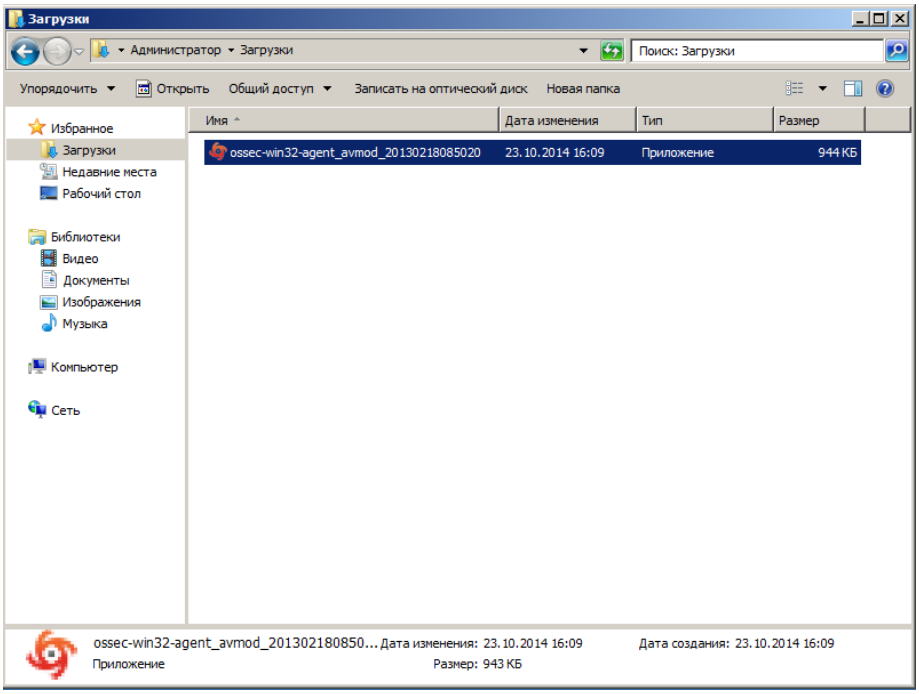



Рисунок Б2 – Файл установки агента OSSEC

В первом окне необходимо нажать “Next >” (Рисунок Б3).

Рисунок Б3 – Окно установки агента OSSEC

В следующем окне необходимо принять условия установки, нажав «I agree» (Рисунок Б4).

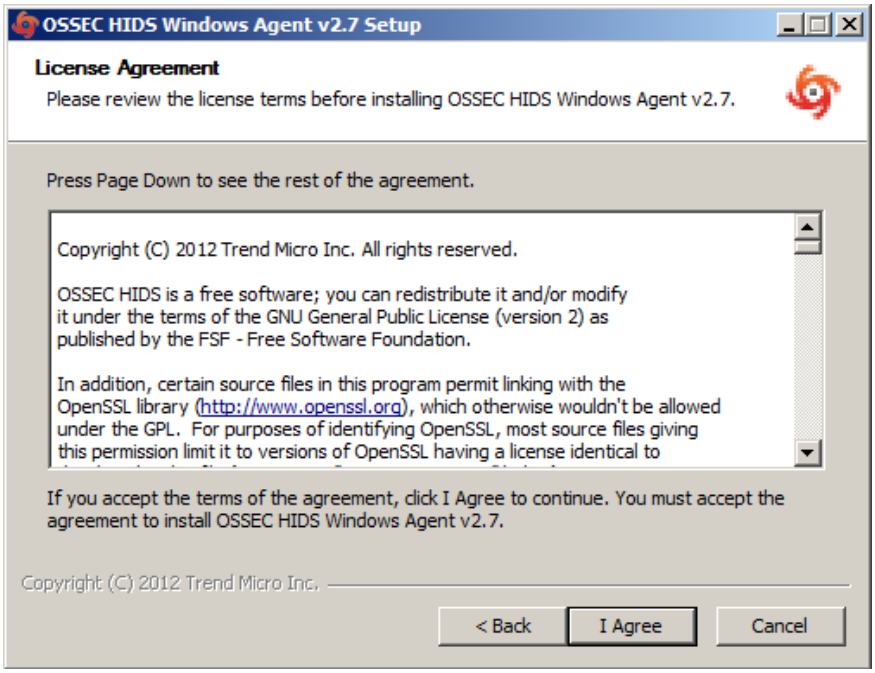



Рисунок Б4 – Окно установки агента OSSEC

В следующем окне (Рисунок Б5) можно выбрать мониторинг журналов службы ISS (“Scan and monitor IIS logs”), а также мониторинг целостности файлов (“Enable integrity checking”). После выбора необходимых параметров следует нажать кнопку “Next >”.

**Примечание:** мониторинг целостности настраивается в конфигурационном файле после установки агента OSSEC.

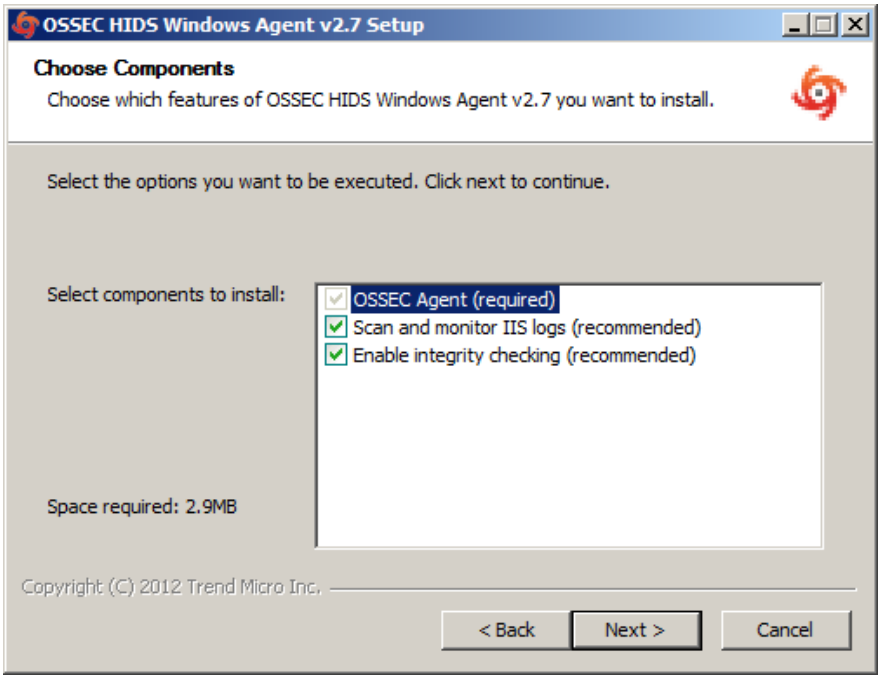


Рисунок Б5 – Выбор дополнительных параметров мониторинга

В следующем окне осуществляется выбор пути установки агента OSSEC (по умолчанию C:\Program Files (x86)\ossec-agent). После выбора пути установки необходимо нажать «Install» (Рисунок Б6).

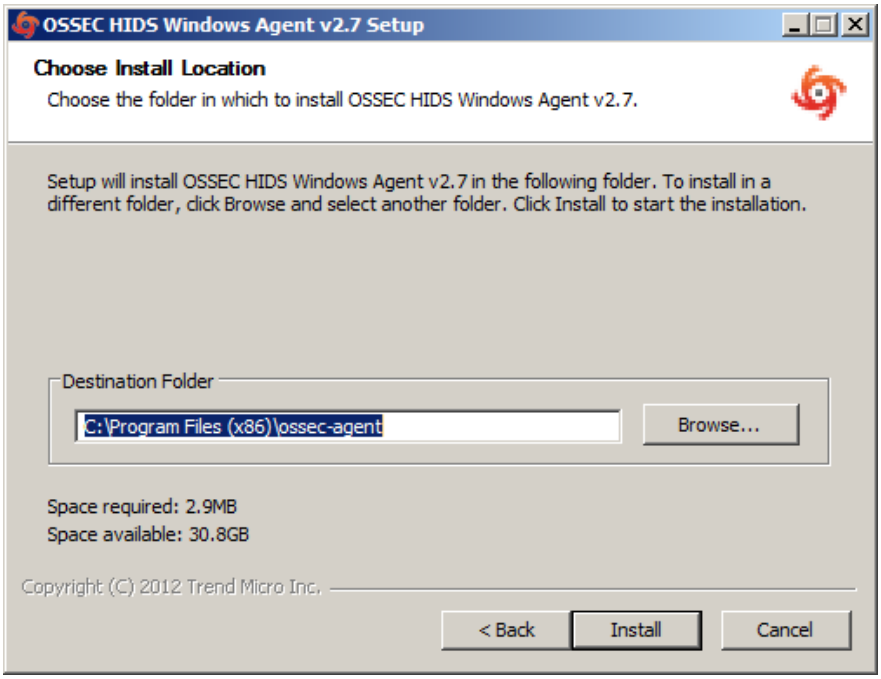



Рисунок Б6 – Окно выбора пути установки агента OSSEC

После успешной установки откроется окно, представленное на РисункеБ7. Нажатие на кнопку «Finish» завершает процесс установки.

Рисунок Б7 – Завершение установки агента OSSEC

1. Для создания аутентификационной информации, необходимой для установки соединения источника событий с ядром ПК «КОМРАД», следует в веб-интерфейсе ПК «КОМРАД»перейти по вкладке «**Анализ → Обнаружение»** и выбрать **Агенты**.

2. Выбрать**Добавить средство**, ввести имя для агента и его IP-адрес (Рисунок Б8).

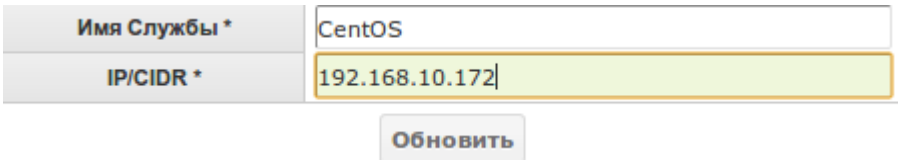



Рисунок Б8 – Окно для ввода имени для агента и его IP-адреса

Новый агент после добавления появляется в список агентов.

3. Для получения сгенерированной для нового агентааутентификационной информации необходимо нажать на значок ключанапротив имени данного средства (Рисунок Б9).

Рисунок Б9 – Появление агента в списке

4. Скопировать аутентификационную информацию и вернуться к настройке ossec-agent на конечном устройстве.

Для добавления аутентификационной информации к агенту:

1. Перейти в режим управления, выполнив с правами администратора конечного устройства в интерфейсе командной строки команду:

*$ /var/ossec/bin/manage_agents*

2. На предложение выбрать действие, выбрать

**(I)mport key from the server**

и вставить полученныйаутентификационную информацию в строку.

3. Подтвердить и выйти изрежима управления manage_agents, выбрав **(Q)uit.**

4. Дописать скрипт удалённого управления агентом, выполнив в интерфейсе командной строки следующую команду:

*$ echo -e 'restart-ossec0 - restart-ossec.sh - 0\nrestart-ossec0 - restart-ossec.cmd - 0' > /var/ossec/etc/shared/ar.conf*

Для перезапуска агентаOSSEC необходимовыполнить в интерфейсе командной строки следующую команду:

*$ /var/ossec/bin/ossec-control restart*

**Примечание**: аутентификационная информацияуспешно добавлена, если работа скрипта завершилась сообщением: «**completed».**

Чтобы проверить корректность всех настроек, необходимо войти в веб-интерфейс ПК «КОМРАД» на вкладку «**Анализ → Обнаружение → Агенты**» и убедиться, что напротив имени источника событий в столбце **Состояние** стоит значение «Active».

**Примечание:** после настроек агента OSSEC необходимо убедиться, что плагины для обработки поступающих событий включены на ПК «КОМРАД».

# 2. НАСТРОЙКА ФИЛЬТРАЦИИ СОБЫТИЙ АГЕНТОМ OSSEC

Правила OSSEC, имеющиеся в ПК «КОМРАД» по умолчанию, большую часть событий от машин под управлением Windows не считают «алертом» (и, соответственно, не транслируют в журнал логовalerts.log). Это поведение продиктовано значением параметра “level”, которое для большинства событий остаётся равным 0.

Правила OSSEC, выполняющие фильтрацию событий от win-машин, записаны в файле msauth_rules.xml.

.....

*<group name="windows,">*

*<rule id="18100" level="0">*

*<category>windows</category>*

*<description>Group of windows rules.</description>*

*</rule>*

.....

*<rule id="18105" level="4">*

*<if_sid>18100</if_sid>*

*<status>^AUDIT_FAILURE|^failure</status>*

*<description>Windows audit failure event.</description>*

*</rule>*

.....

Чтобы исправить данную ситуацию, можно последовать одному из двух возможных вариантов:

1. Установить ненулевое значение параметра “level” для всех уже существующих правил OSSEC. Данный способ является быстрым и надёжным, но влечёт избыток сообщений от данного источника, так как фильтрация незначительных сообщений оказывается отключённой.

2. Создать правило в указанном файле, которое бы охватило все события, содержащие фразу “SecurePackRus”, и для них увеличить значение “level”, например:

.....

*<rule id="18146" level="14">*

*<if_sid>18100</if_sid>*

*<match>Secure Pack Rus:</match>*

*<description>Secure Pack Rus event</description>*

*</rule>*

.....

## *Дополнительные настройки агента OSSEC*

Дополнительные настройки агента OSSEC возможны в конфигурационном файле ossec.conf в директории с установленным агентом OSSEC (по умолчанию:C:\ProgramFiles (x86)\ossec-agent\ossec.conf). Открыть конфигурационный файл можно из меню Пуск, “Пуск→ Все программы →OSSEC→EditConfig”.

По умолчанию агент OSSEC настроен на сбор событий безопасности из журналов Application, Security, System. Имеется возможность добавить дополнительный источник сбора информации. Для этого в секцию Localfile добавляется запись следующего вида:

*<localfile>*

*<location>Security</location>*

*<log_format>eventlog</log_format>*

*</localfile>*

Где <location> - имя системного журнала или полный путь к файлу журнала.

<log_format> - тип журнала

## *Настройка агента OSSEC для проверки целостности файлов в ОС Windows*

**1.** Дописать соответствующую опцию C:\ProgramFiles\ossec-agent\ossec.conf:

*<syscheck>*

*<frequency>120</frequency>*

***<directories check_all='yes'>C:\Test</directories>***

**2.** Создать названную папку, в ней - некоторый файл:

C:\Users\Administrator> mkdir C:\Test

C:\Users\Administrator> echo > C:\Test\1.txt

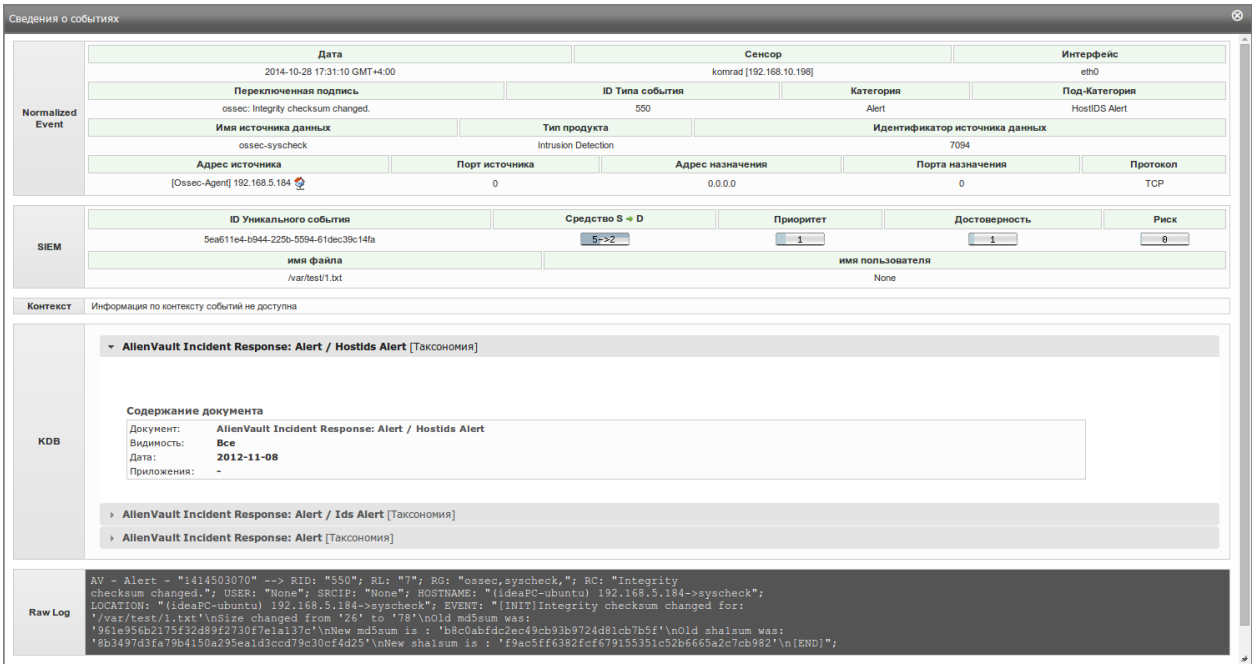
**3.** Перезапустить ossec-agent:

**4.** Изменить созданный ранее в контролируемом каталоге файл:

C:\Users\Administrator> echo ‘some_text’ >> C:\Test\1.txt

**5.** Дождатьсясобытия “ossec: Integrity checksum changed.” ввеб-интерфейсеПК «КОМРАД»:

*AV - Alert - "1414503070" --> RID: "550"; RL: "7"; RG: "ossec,syscheck,"; RC: "Integrity checksum changed."; USER: "None"; SRCIP: "None"; HOST-NAME: "(WIN2008) 192.168.10.105->**syscheck**"; LOCATION: "(WIN2008) 192.168.10.105->syscheck"; EVENT: "[INIT]**Integrity checksum changed for: 'C:\Test\1.txt'**\nSize changed from '26' to '78'\nOld md5sum was: '961e956b2175f32d89f2730f7e1a137c'\nNew md5sum is : 'b8c0abfdc2ec49cb93b9724d81cb7b5f'\nOld sha1sum was: '8b3497d3fa79b4150a295ea1d3ccd79c30cf4d25'\nNew sha1sum is : 'f9ac5ff6382fcf679155351c52b6665a2c7cb982'\n[END]";*


Сведения о событиях
Normalized Event
Дата
2014-10-28 17:31:10 GMT+4:00
Сенсор
komrad [192.168.10.198]
Интерфейс
eth0
Переключенная подпись
ossec: Integrity checksum changed.
ID Типа события
550
Категория
Alert
Под-Категория
HostIDS Alert
Имя источника данных
ossec-syscheck
Тип продукта
Intrusion Detection
Идентификатор источника данных
7094
Адрес источника
[Ossec-Agent] 192.168.5.184
Порт источника
0
Адрес назначения
0.0.0.0
Порта назначения
0
Протокол
TCP
SIEM
ID Уникального события
5ea611e4-b944-225b-5594-61dec39c14fa
Средство S → D
5->2
Приоритет
1
Достоверность
1
Риск
0
имя файла
/var/test/1.txt
имя пользователя
None
Контекст
Информация по контексту событий не доступна
KDB
AlienVault Incident Response: Alert / Hostids Alert [Таксономия]
Содержание документа
Документ: AlienVault Incident Response: Alert / Hostids Alert
Видимость: Все
Дата: 2012-11-08
Приложения: -
AlienVault Incident Response: Alert / Ids Alert [Таксономия]
AlienVault Incident Response: Alert [Таксономия]
Raw Log
AV - Alert - "1414503070" --> RID: "550"; RL: "7"; RG: "ossec,syscheck,"; RC: "Integrity
checksum changed."; USER: "None"; SRCIP: "None"; HOSTNAME: "(ideaPC-ubuntu) 192.168.5.184->syscheck";
LOCATION: "(ideaPC-ubuntu) 192.168.5.184->syscheck"; EVENT: "[INIT]Integrity checksum changed for:
'/var/test/1.txt'\nSize changed from '26' to '78'\nOld md5sum was:
'961e956b2175f32d89f2730f7e1a137c'\nNew md5sum is : 'b8c0abfdc2ec49cb93b9724d81cb7b5f'\nOld shalsum was:
'8b3497d3fa79b4150a295ea1d3ccd79c30cf4d25'\nNew shalsum is : 'f9ac5ff6382fcf679155351c52b6665a2c7cb982'\n[END]";

# 3. УСТАНОВКА АГЕНТА OCS ДЛЯ WINDOWS И LINUX

Для инвентаризации программного обеспечения и оборудования в системе требуется установить агент OCS.

## *OCS агент для Windows*

1. Для установки OCSагента для Windowsнеобходимо в веб-интерфейсе ПК «КОМРАД» перейти во вкладку «**Система → Сбор данных → Загрузка**» и выбрать пункт «OCSдля Windows».
2. Распаковать загруженный архив
3. Используя текстовый редактор, ввести корректный IP-адресПК «КОМРАД» в файлах ***install.bat*** и ***invertorize_now.bat*** (Рисунок Б10).

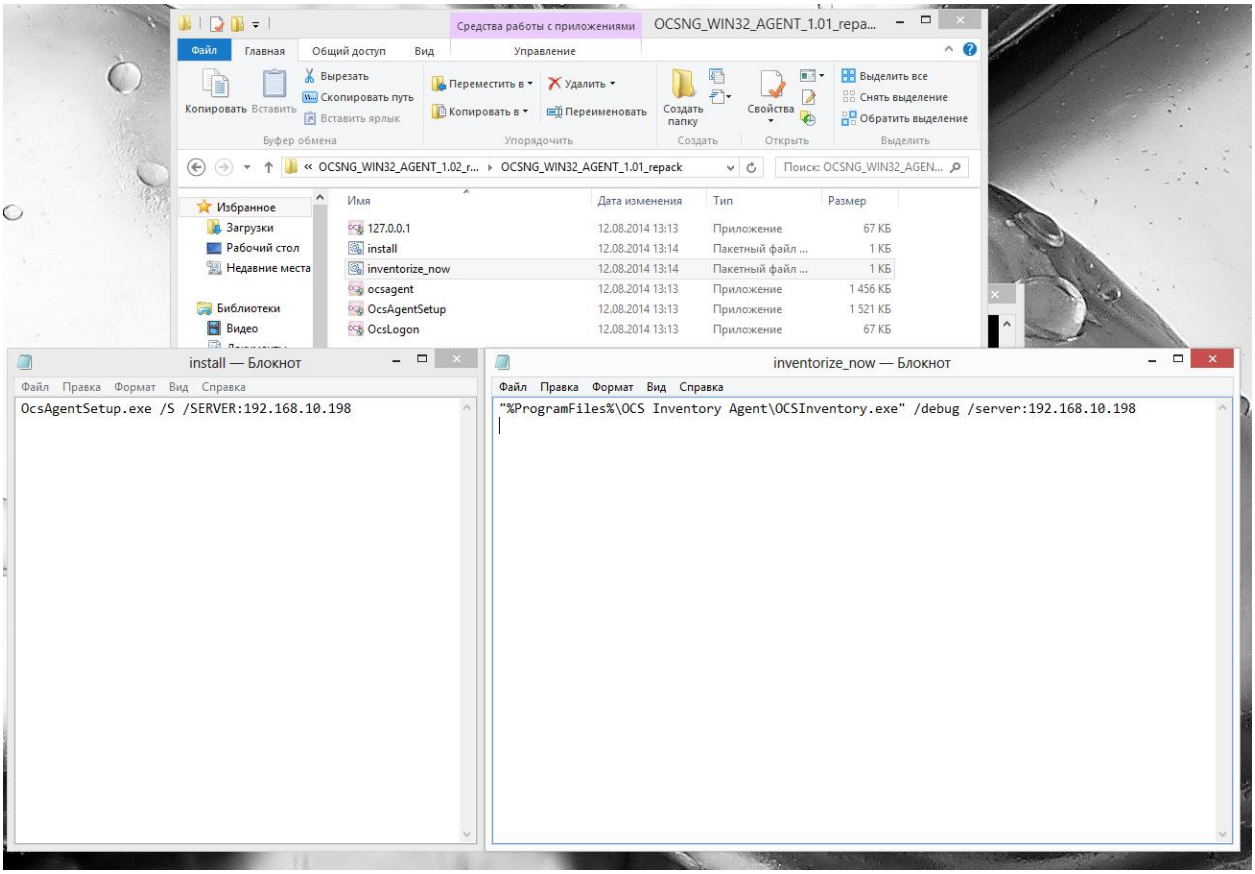



Рисунок Б10 – Модификация сценариев установки агента

4. Запустить с правами администратора последовательно сначала сценарий установки ***install.bat***, затем сценарий инвентаризации ***invertorize_now.bat***.

5. Дождаться появления на вкладке **«Средства→Средства→ Инвентаризация OCS»**строки, соответствующей добавленному в систему инвентаризации хосту (Рисунок Б11).

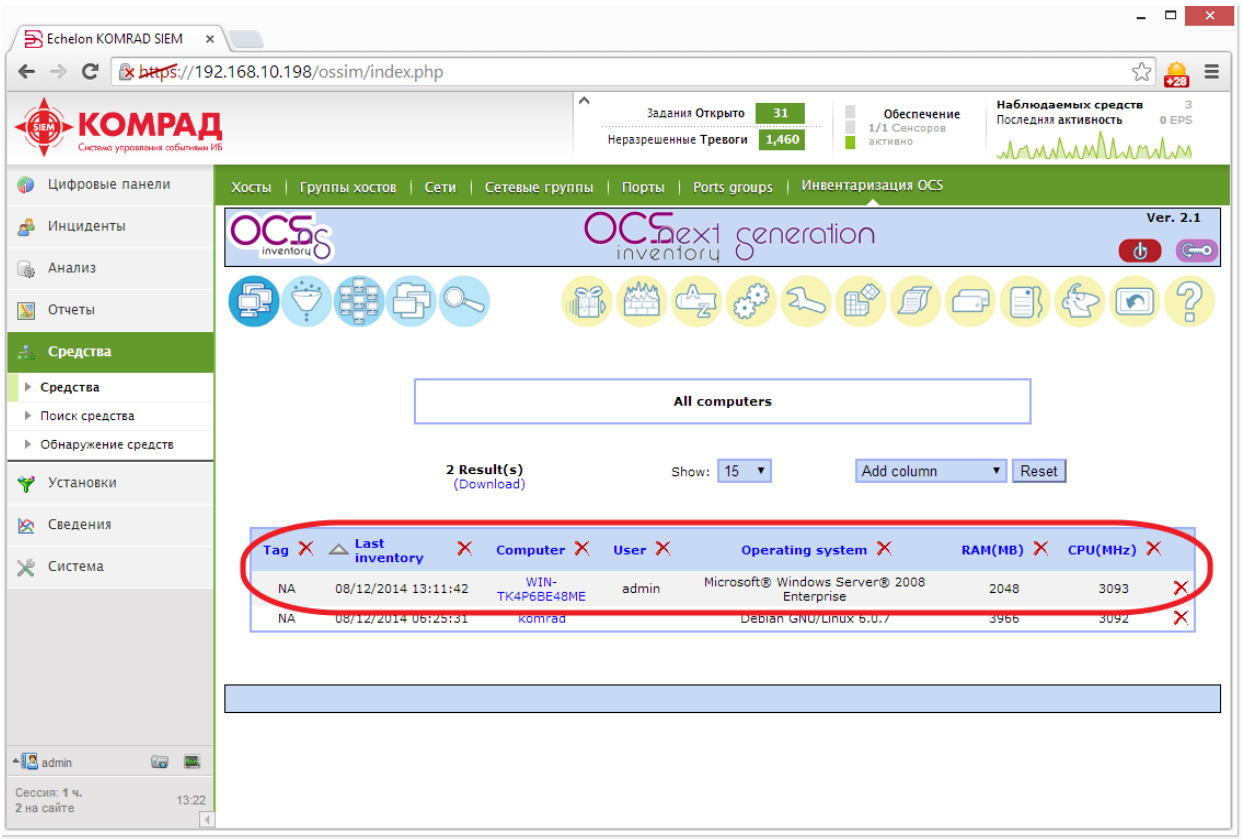



Рисунок Б11 – Добавление нового средства в список инвентаризации

## *OCSагентдляLinux*

*#: apt-getinstallocsinventory-agent*

Во время установки будет запрошен IP-адрес сервера OCS Inventory

## 4. НАСТРОЙКА АГЕНТА OSSEC ДЛЯ ПРОВЕРКИ ЦЕЛОСТНОСТИ ФАЙЛОВ В ОС UNIX

**1.** Дописать соответствующую опцию /var/ossec/etc/ossec.conf:

...

*<syscheck>*

*<frequency>120</frequency>*

***<directories check_all='yes'>/var/test</directories>***

**2.** Создать названную папку, в ней - некоторый файл:

*# mkdir /var/test*

*# touch /var/test/1.txt*

**3.** Перезапустить ossec-agent:

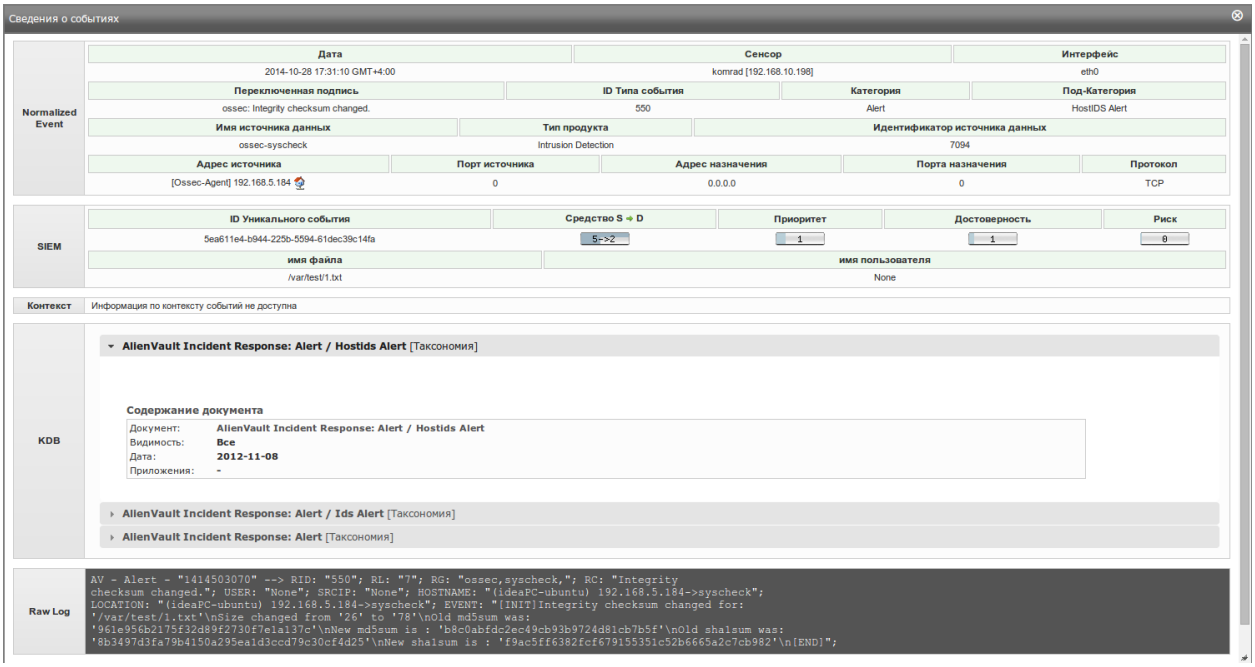
*# /var/ossec/bin/ossec-control restart*

**4.** Изменить созданный ранее в контролируемом каталоге файл:

*# echo ‘some_text’ >> /var/test/1.txt*

**5.** Дождатьсясобытия “ossec: Integrity checksum changed.” ввеб-интерфейсеПК «КОМРАД»:

*AV - Alert - "1414503070" --> RID: "550"; RL: "7"; RG: "ossec,syscheck,"; RC: "Integrity checksum changed."; USER: "None"; SRCIP: "None"; HOST-NAME: "(ideaPC-ubuntu) 192.168.5.184->**syscheck**"; LOCATION: "(ideaPC-ubuntu) 192.168.5.184->syscheck"; EVENT: "[INIT]**Integrity checksum changed for: '/var/test/1.txt**'\nSize changed from '26' to '78'\nOld md5sum was: '961e956b2175f32d89f2730f7e1a137c'\nNew md5sum is : 'b8c0abfdc2ec49cb93b9724d81cb7b5f'\nOld sha1sum was: '8b3497d3fa79b4150a295ea1d3ccd79c30cf4d25'\nNew sha1sum is : 'f9ac5ff6382fcf679155351c52b6665a2c7cb982'\n[END]";*



# 5. ТРЕБОВАНИЯ ПО НАСТРОЙКЕ СЕРВЕРОВ И РАБОЧИХ СТАНЦИЙ ПОД УПРАВЛЕНИЕМ ОС CENTOS И DEBIAN

1. Необходимо добавить в файл***/var/ossec/etc/ossec.conf*** следующие строки:

*<localfile>*

*<log_format>syslog</log_format>*

*<location>/var/log/syslog</location>*

*</localfile>*

*<localfile>*

*<log_format>syslog</log_format>*

*<location>/var/log/auth.log</location>*

*</localfile>*

Это позволит отслеживать следующие события:

- вход, подключение (попытка входа, подключения) пользователя (удалённого, интерактивного);
- ошибка ввода пароля;
- создание, удаление, блокировка учётной записи;
- сброс (смена) пароля администратором;
- изменение состава групп с учётными записями пользователей;
- установление SSH-соединения с контролируемого компонента ИТ-инфраструктуры;
- изменение полномочий sudo.

2. Необходимо добавить в файл ***/var/ossec/etc/ossec.conf*** следующие строки:

ДляОССentOS

*<localfile>*

*<log_format>syslog</log_format>*

*<location>/var/log/yum.log</location>*

ДляОСDebian

*</localfile>*

*<localfile>*

*<log_format>syslog</log_format>*

*<location>/var/log/apt/history.log</location>*

*</localfile>*

Это позволит отслеживать установку (пакета) программного обеспечения (ПО).

3. В случае если ОС развернута как виртуальная машина в среде OpenVZ, необходимодобавить в папку **/usr/bin** следующие файлы inotify (см. приложение А):

- inotify_groups.sh;
- inotify_shadow.sh;
- inotify_sshd_config.sh;
- inotify_rsyslog_conf.sh;
- inotify_rsyslog_d.sh;
- inotify_my_cnf.sh;
- inotify_nginx_conf.sh;
- inotify_ipt.sh;
- inotify_syslog.sh;
- inotify_rclocal.sh
- inotify_auth_log.sh;
- inotify_yum_log.sh.

Следует добавить в файл***/var/ossec/etc/ossec.conf*** следующие строки:

*<localfile>*

*<log_format>syslog</log_format>*

*<location>/var/log/inotify.log</location>*

*</localfile>*

Это позволит отслеживать следующие события:

- изменение контролируемого файла;
- изменение прав доступа к каталогу (файлу);

- удаление / модификация журнала событий;
- изменение правил ведения журнала событий.

После этого необходимо настроить сервис logrotate для автоматической ротации и архивации журнала inotify.log(см. раздел 11«Требования по настройке logrotate»), если он не был настроен ранее.

# 6. ТРЕБОВАНИЯ ПО УСТАНОВКЕ АГЕНТА SNARE

Для получения установочного файла открыть веб-интерфейс ПК «КОМРАД» в браузере на конечном устройстве, выбрать **Система → Сбор данных → Источники событий → Snare для Windows**и скачать установочный файл SnareForWindows-4.0.1.2-MultiArch.exe.

ЗапуститьустановочныйфайлSnareForWindows-4.0.1.2-MultiArch.exe.

1. В появившемся диалоговом окне *SnareAuditing*выбрать**No**и нажать кнопку **Next>** (Рисунок Б12).

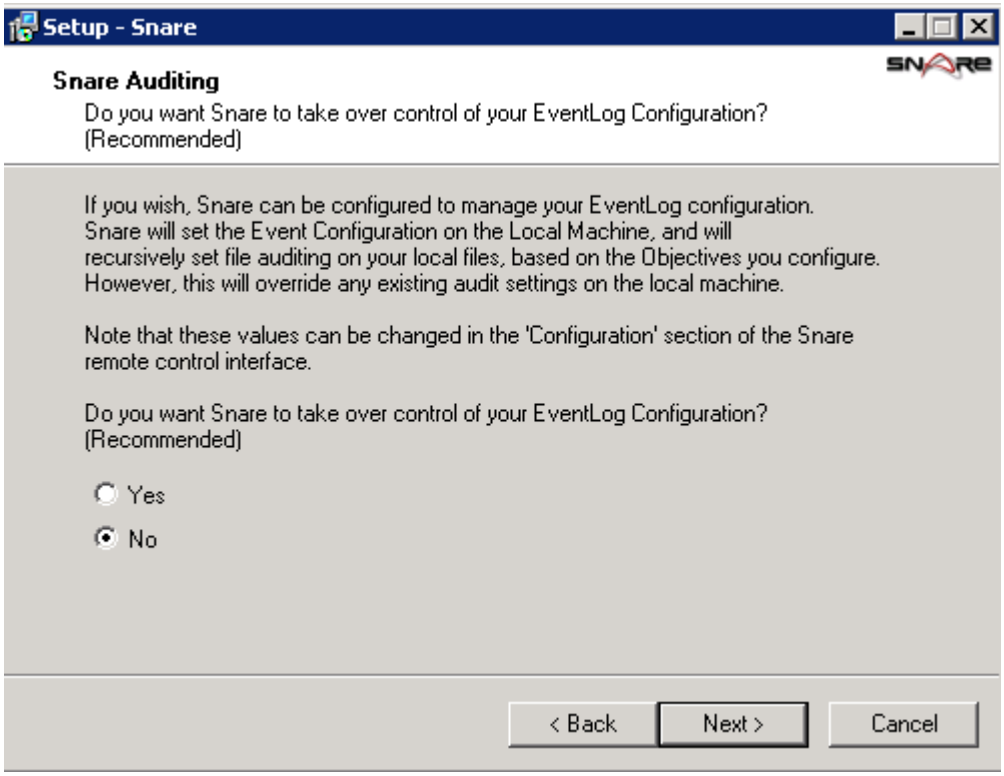



Рисунок Б12 –ДиалоговоеокноSnareAuditing

2. Вследующемдиалоговомокне*ServiceAccount*выбратьпункт «**UseSystemAccount**» инажатькнопку**Next>** (РисунокБ13).

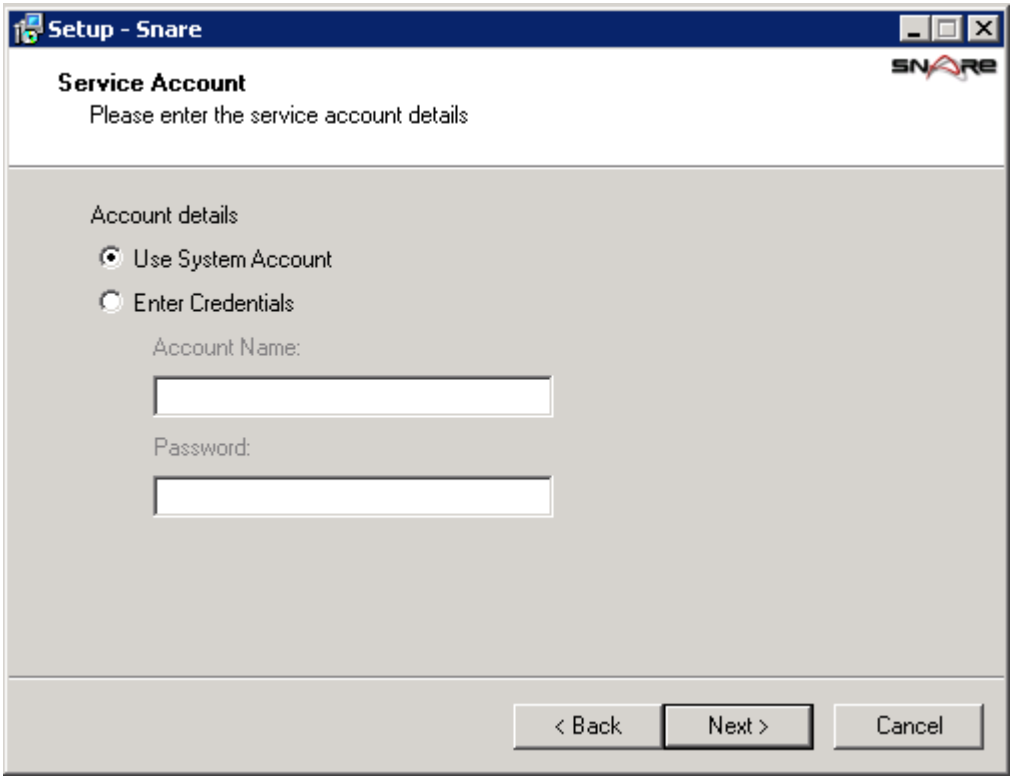
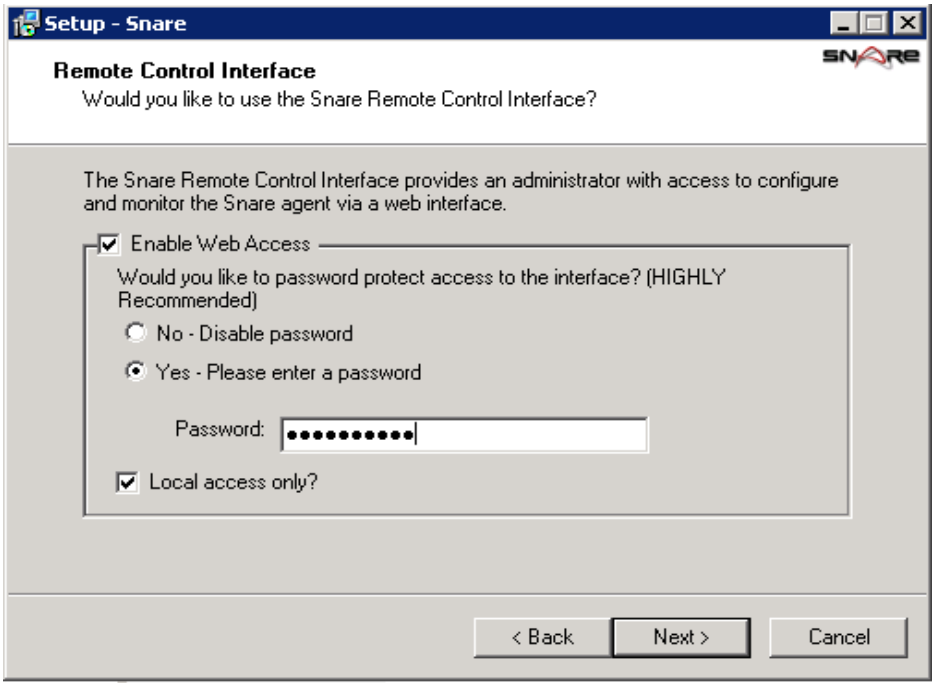


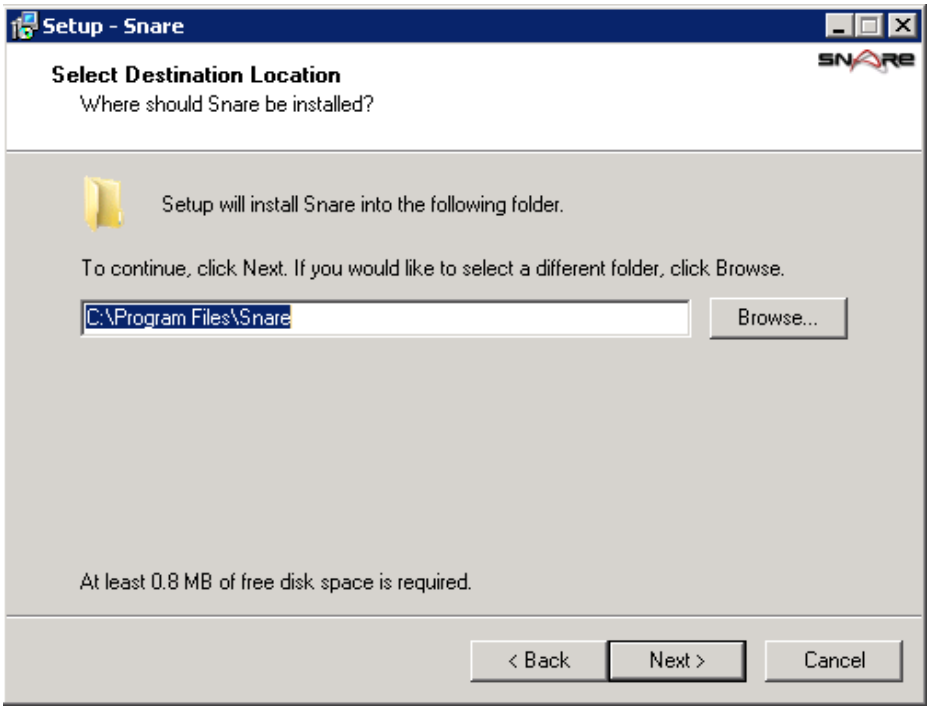

Рисунок Б13 –ДиалоговоеокноServiceAccount

3. Вдиалоговомокне*RemoteControlInterface*поставитьгалочкинапротивпунктов «**EnableWebAccess**» и «**Localaccessonly?**». Также выбрать пункт **Yes-Pleaseenterapassword** и ввести в поле «**Password:**» пароль, который будет использоваться для защищённого доступа к интерфейсу удалённого контроля Snare. После этого нажать кнопку **Next>** (Рисунок Б14).



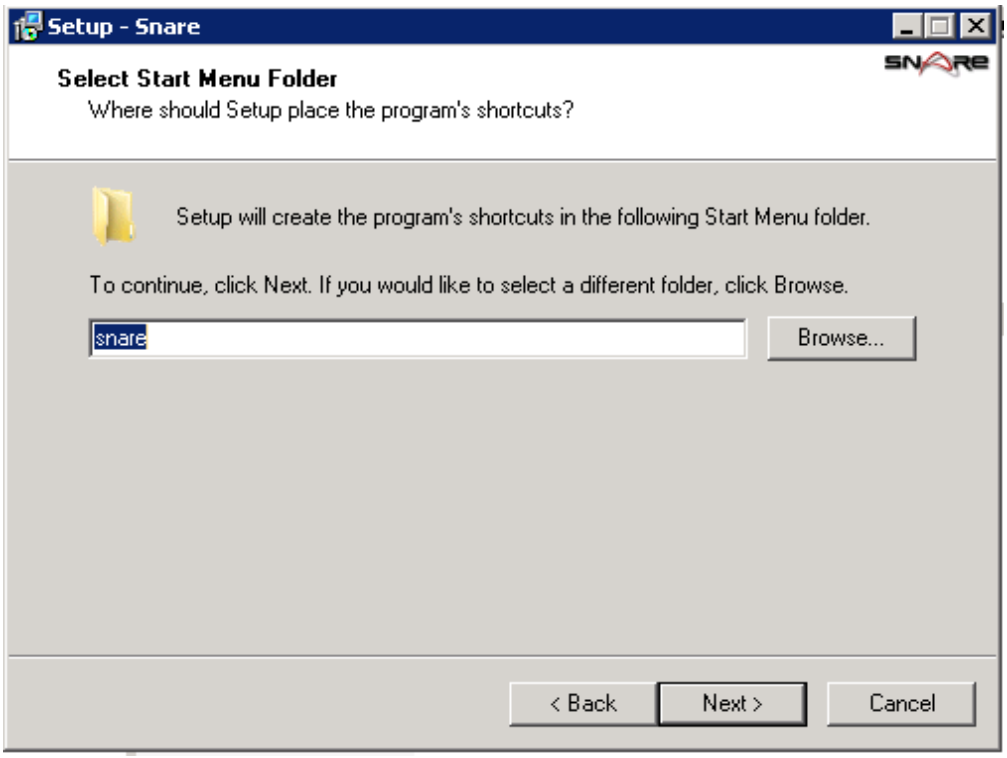

РисунокБ14 –ДиалоговоеокноRemoteControlInterface

4. Вдиалоговомокне*SelectDestinationLocation*выбратьпапкудляустановкиSnare (по умолчанию **C:\ProgramFiles\Snare**) инажатькнопку**Next>** (РисунокБ15).




РисунокБ15 –ДиалоговоеокноSelectDestinationLocation

5. Вдиалоговомокне*SelectStartMenuFolder*оставить всё без изменений и нажать кнопку **Next>** (Рисунок Б16).




РисунокБ16 –ДиалоговоеокноSelectStartMenuFolder

6. Вокне*ReadytoInstall*нажатькнопку**Install** (РисунокБ17).

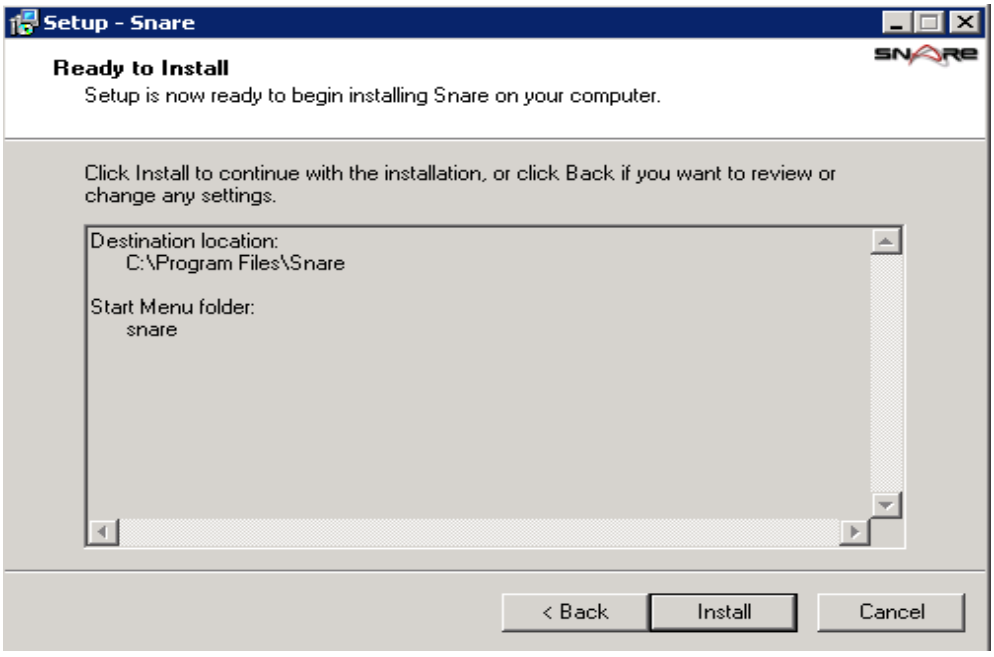



Рисунок Б17 –ДиалоговоеокноReadytoInstall

# 7. ТРЕБОВАНИЯ ПО НАСТРОЙКЕ СЕРВЕРОВ С ОС MICROSOFT WINDOWS SERVER 2008/2012 И РАБОЧИХ СТАНЦИЙ С ОС MICROSOFT WINDOWS VISTA/7/8 В ДОМЕНЕ ПОД УПРАВЛЕНИЕМ СЛУЖБЫ ACTIVE DIRECTORY

Необходимо произвести настройки агента Snare, политики WindowsAuditpolicyи аудита событий доступа к каталогам и файлам в Windows для отслеживания следующих событий:

- вход, подключение (попытка входа, подключения) пользователя (удалённого, интерактивного);
- ошибка ввода пароля;
- создание, удаление, блокировка учётной записи;
- сброс (смена) пароля администратором;
- изменение состава групп с учётными записями пользователей;
- изменение контролируемого файла;
- изменение прав доступа к каталогу (файлу);
- установка ПО (пакета);
- запуск / остановка сервиса;
- удаление / модификация журнала событий;
- изменение правил ведения журнала событий.

## *Настройка агента Snare*

1. После установки на конечном устройстве агента Snare необходимоввести в веб-браузере адрес http://localhost:6161,имя пользователя Snare и пароль, который был задан при установке.

2. На загрузившейся странице выбрать в находящемся в левой части окна меню пункт **NetworkConfiguration**и ввести следующие данные (Рисунок Б18):

Поле«**Override detected DNS Name with:**»оставитьпустым.

Вполе«**Destination Snare Server address**» ввестиIP-адрессервера.

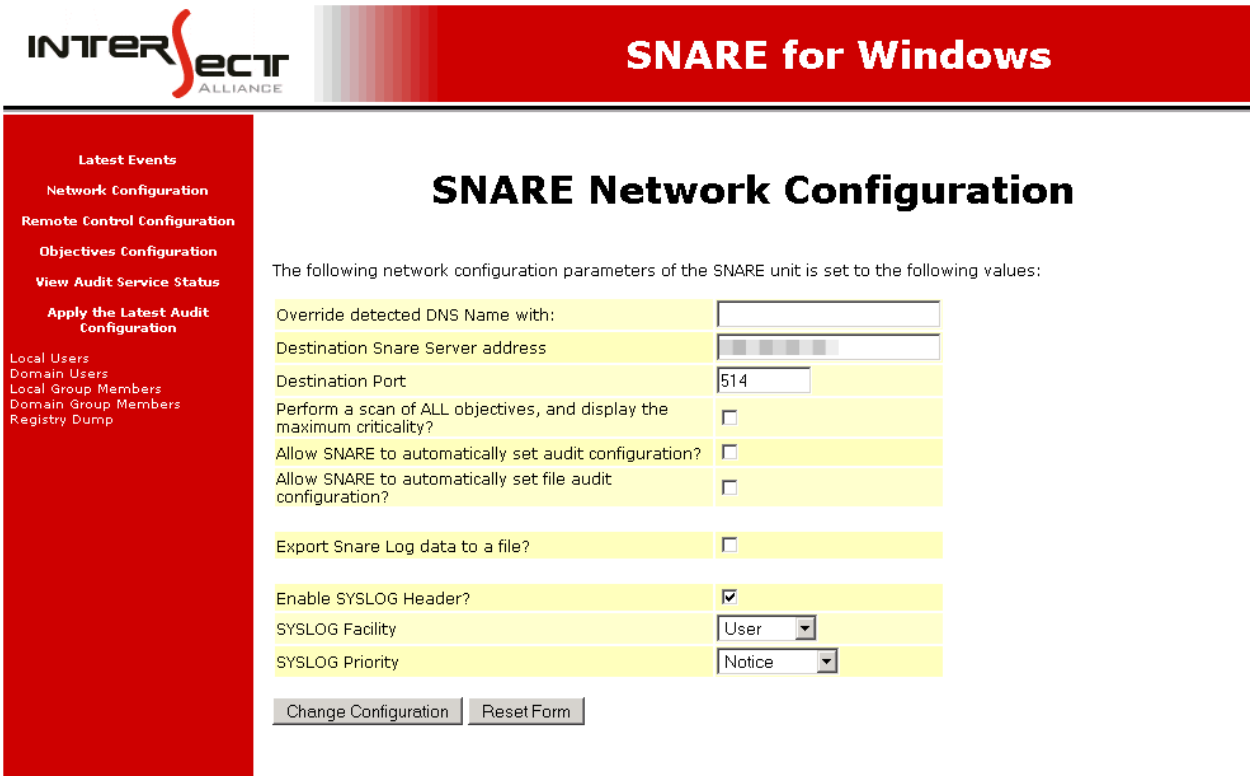
В поле «**DestinationPort**»ввести **514** (номер порта).

Убедиться, что со всех пунктов, кроме «**EnableSYSLOGHeader?**»снято выделение, в противном случае снять выделение вручную.

В поле «**SYSLOGFacility**»выбрать **User**;

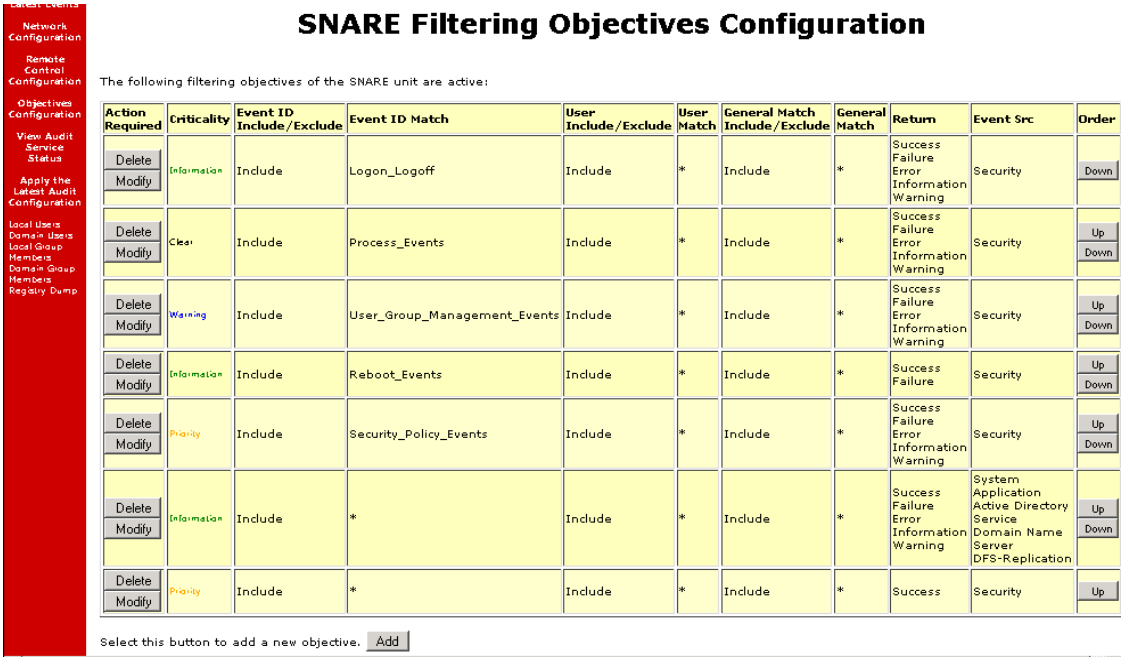
Вполе«**SYSLOGPriority**»выбрать**Notice**.

Нажать **Change Configuration**.




РисунокБ18 –СтраницаSNARENetworkConfiguration

3. Выбрать пункт **ObjectivesConfiguration**в расположенном в левой части окна меню. Добавить строку конфигурации для получения данных из журнала SecurityEventLog. Для этого на открывшейся странице нажать кнопку **Add** (Рисунок Б19).




РисунокБ19 –СтраницаSNAREFilteringObjectivesConfiguration

На открывшейся странице ввести следующие данные (Рисунок Б20):

Вполе«**Identifythehighlevelevent**»выбратьпункт«Anyevent(s)».

Вполе«**Select the Event ID Match Type**»выбратьпункт«Include».

Вполе«**EventIDSearchTerm**»вставить символ «*».

Вполе«**Select the General Search Type**»выбратьпункт«Include».

Вполе«**GeneralSearchTerm**»вставить символ «*».

Вполе«**Select the User Match Type**»выбратьпункт«Include».

Вполе«**UserSearchTerm**»вставить символ «*».

Вполе«**Identify the event types to be captured**» выделитьпункты«Success Audit» и«Failure Audit».

Вполе«**Identify the event logs**»выделитьпункт«Security».

Вполе«**Select the Alert Level**»выбратьпункт«Priority».

Нажать **Change Configuration**.

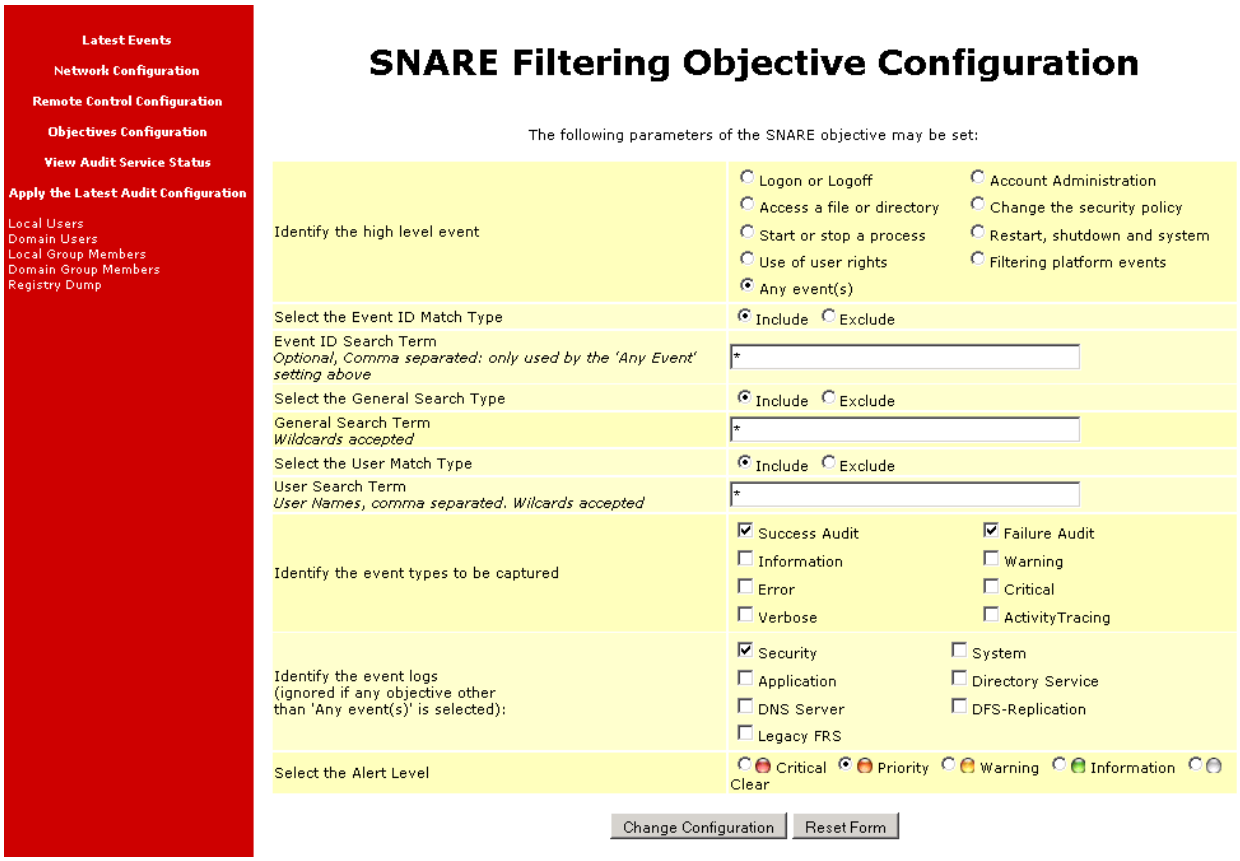



Рисунок Б20 –Страница добавления строки конфигурации для получения данных из журнала SecurityEventLog

4. Перейтинавкладку**ApplytheLatestAuditConfiguration**инажатьнакнопку **ReloadSettings**дляприменениявсехнастроек (Рисунок Б21).

РисунокБ21 –СтраницаApplyLatestConfiguration

# *Настройка Windows Audit policy*

1. Для настройки Windows Audit Policy в Microsoft Windows 2008 R2 необходимо запустить командную строку ***cmd.exe***.

2. В командной строке выполнить команду:

*>auditpol /get /category:**

После этого следует убедиться, что включен аудит следующих подкатегорий событий:

**«Logon»— success and failure;**

**«Logoff»— success;**

**«Registry»— success and failure;**

**«File system»— success and failure;**

**«Special Logon»— success and failure;**

**«Audit Policy Change»— success;**

**«Authentication Policy Change» — success;**

**«User Account Management»— success and failure;**

**«Computer Account Management»— success and failure;**

**«Security Group Management»— success and failure;**

**«Other Account Management Events»— success and failure;**

**«Directory Service Changes»— success and failure;**

**«Directory Service Replication»— success and failure;**

**«Credential Validation»— success and failure.**

3. Если аудит этих событий не включен, то ввести следующие команды для включения аудита соответствующих подкатегорий событий:

*>auditpol /set /subcategory:» Logon» /success:enable /failure:enable*

*>auditpol /set /subcategory:»Logoff « /success:enable*

*>auditpol /set /subcategory:»Registry /success:enable /failure:enable*

*>auditpol /set /subcategory:»File system» /success:enable /failure:enable*

*>auditpol /set /subcategory:»Special Logon» /success:enable /failure:enable*

*>auditpol /set /subcategory:»Audit Policy Change» /success:enable*

*>auditpol /set /subcategory:»Authentication Policy Change» /success:enable*

*>auditpol /set /subcategory:»User Account Management» /success:enable /failure:enable*

*>auditpol /set /subcategory:»Computer Account Management» /success:enable /failure:enable*

*>auditpol /set /subcategory:»Security Group Management» /success:enable /failure:enable*

*>auditpol /set /subcategory:»Other Account Management Events» /success:enable /failure:enable*

*>auditpol /set /subcategory:»Directory Service Changes» /success:enable /failure:enable*

*>auditpol /set /subcategory:»Directory Service Replication» /success:enable /failure:enable*

*>auditpol /set /subcategory:»Credential Validation» /success:enable /failure:enable.*

4. Для корректного мониторинга событий аутентификации пользователей непосредственно на контроллере домена (в первую очередь удачной и неудачной авторизаций) необходимо убедиться, что в разделе Default Domain Controller Policy на контроллере включен аудит соответствующих категорий (Рисунок Б22).

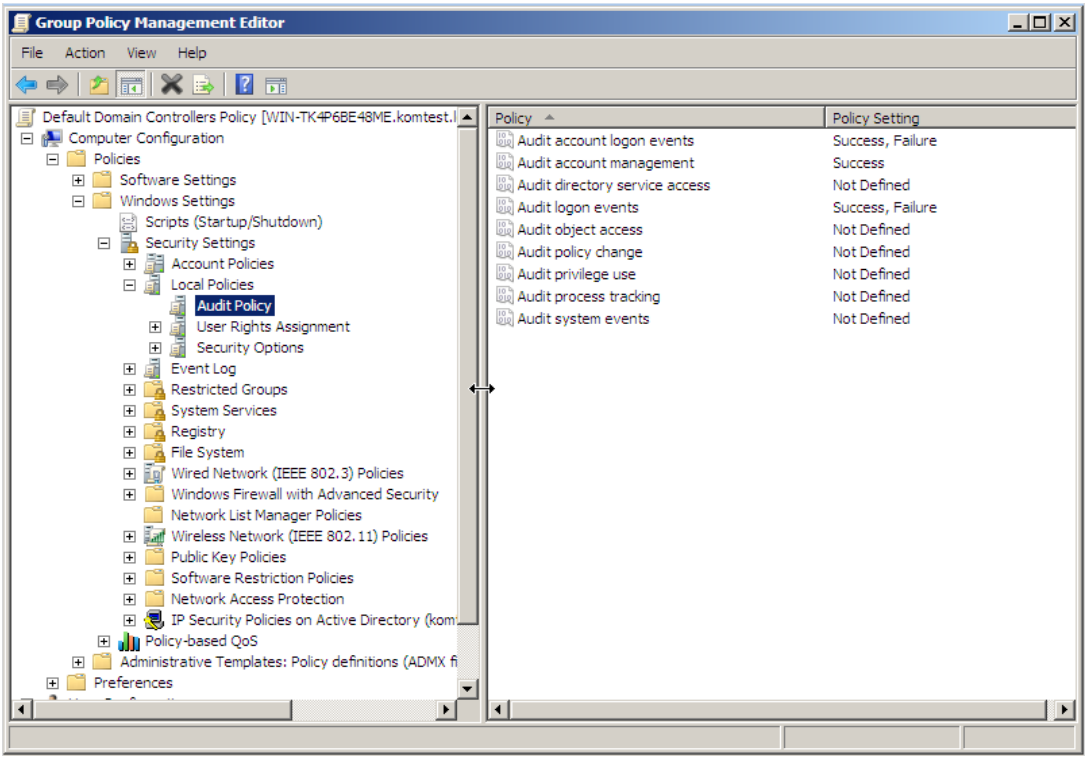



Рисунок Б22 –Настройки политик аудита

## *Настройка аудита событий доступа к каталогам и файлам в Windows*

Для того чтобы в журнал «Безопасность»конечного устройства под управлением Windows поступали события доступа к каталогам и файлам, необходимо проверить, что включен аудит событий файловой системы «Filesystem» в режиме«successandfailure» (пункт «Настройка Windows Audit policy»), а такжевключить аудит данных событий для конкретной интересующей директории или файла. Для этого необходимо выполнить следующие действия:

1. Открыть меню«**Свойства**»заданной папки (Рисунок Б23).

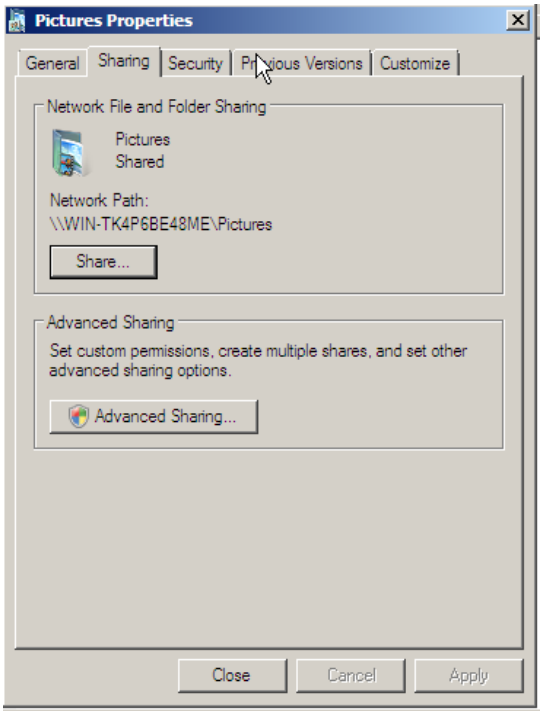



Рисунок Б23 – Меню «Свойства» папки

2. Перейти на вкладку **Безопасность** (**Security**), а затем нажать на кнопку**Дополнительно** (**Advanced**) (РисунокБ24).

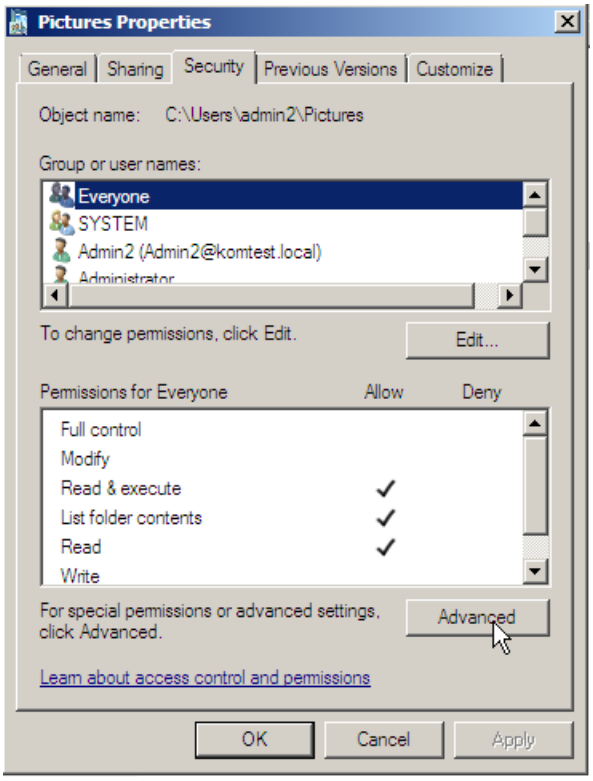
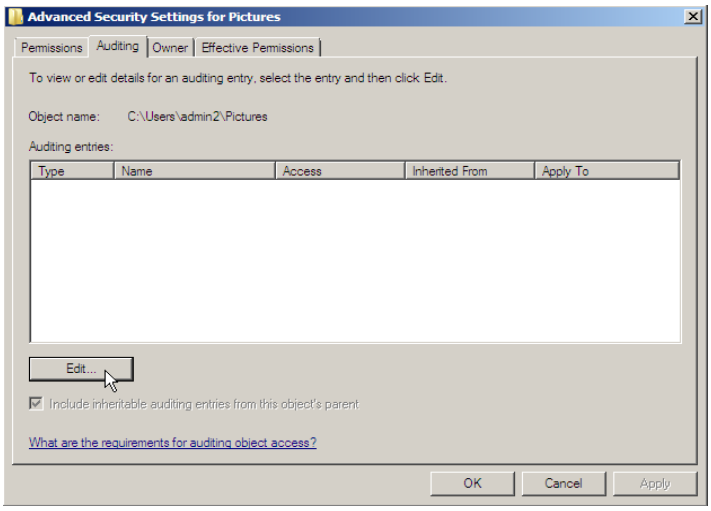



Рисунок Б24 – Вкладка «Security» в окне свойств папки

3. В открывшемся окне перейти на вкладку **Аудит** (**Auditing**). Для настройки аудита нажать на кнопку**Редактировать** (**Edit**)(РисунокБ25).




РисунокБ25 –Вкладка«Auditing»окна«AdvancedSecuritySettings»

4. Добавить группы пользователей, для которых будет осуществляться аудит, и настроить под каждую из групп параметры аудита. Например, на Рисунке Б26показано включение аудита всех успешных событий доступа для пользователей, входящих в группу Domain Users. При необходимостиотключитьаудитдлявложенныхкаталогов следует установитьгалочкунапротивпункта«**Applytheseauditingentriestoobjectsand/orcontainerswithinthiscontaineronly**»вокне*Auditingentry*.

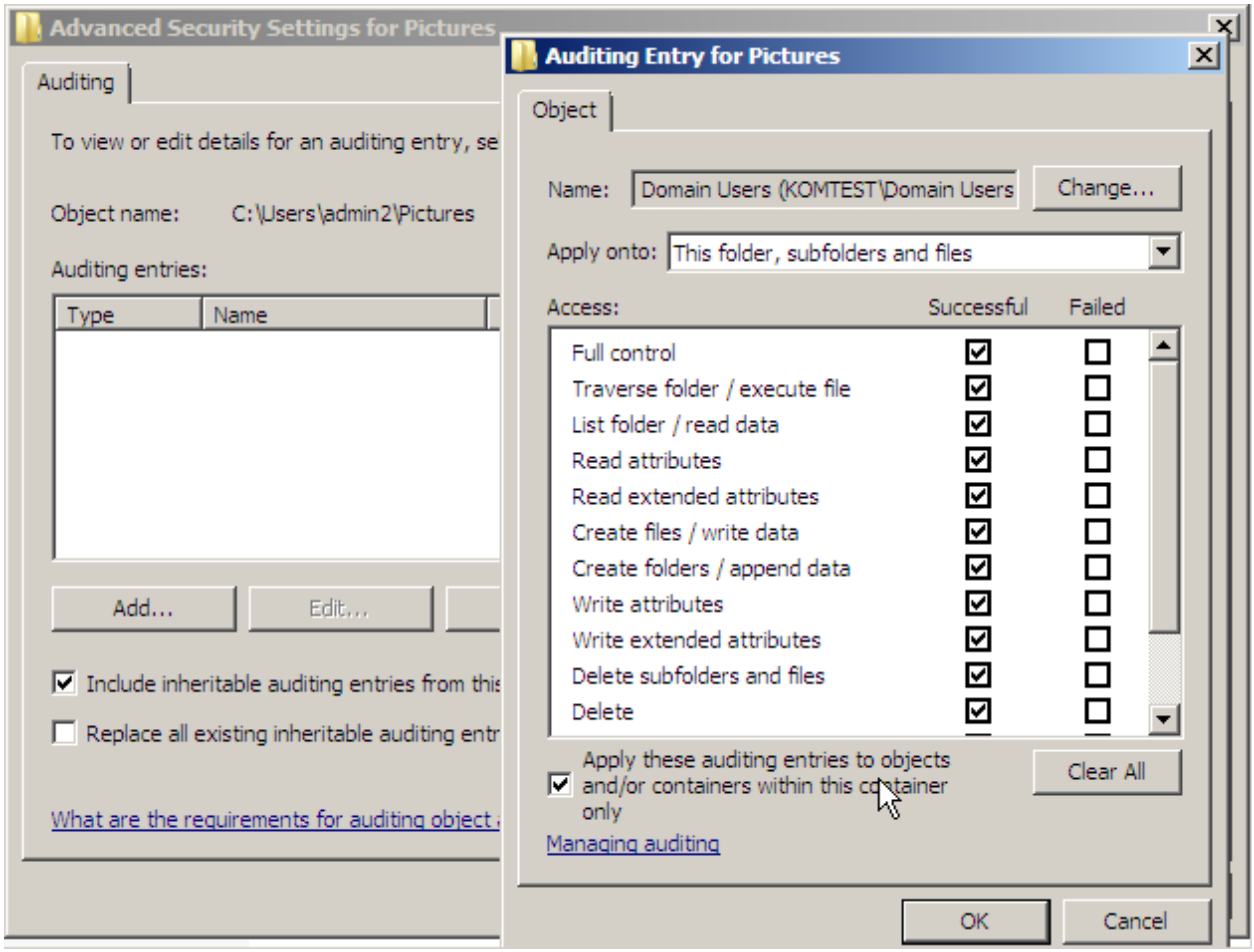



Рисунок Б26 – Окно настройки аудита для группы пользователей

# 8. ТРЕБОВАНИЯ ПО НАСТРОЙКЕ ПОЧТОВОГО СЕРВЕРА (COMMUNIGATE)

Необходимодобавитьвфайл***/var/ossec/etc/ossec.conf***следующиестроки:

*<localfile>*

*<log_format>syslog</log_format>*

*<location>/var/log/communigate.log</location>*

*</localfile>*

Это позволит отслеживать следующие события:

- вход, подключение (попытка входа, подключения) пользователя (удалённого, интерактивного);
- ошибка ввода пароля;
- создание, удаление, блокировка учётной записи;
- сброс (смена) пароля администратором;
- изменение состава групп с учётными записями пользователей.

Кроме того, необходимо настроить контроль за изменением и удалением файла конфигурации и журнала сервиса Communigate. Для этого необходимо изменить конфигурационный файл службыauditd /etc/audit/audit.rules, добавив в него строки:

*-w/var/CommuniGate/SystemLogs/%date%.log -p wa*

*-w/var/CommuniGate/Settings -p wa*

Если использование службы auditd невозможно, то необходимо использовать inotify-tools. Для этого проверить, что агент ossec следит за журналом /var/log/inotify.log (пункт 2 данного приложения) и настроен сервис logrotate для автоматической ротации и архивации журнала inotify.log(пункт 14 данного приложения).

# 9. ТРЕБОВАНИЯ ПО НАСТРОЙКЕ WALLIXADMINBASTION

Средство мониторинга, контроля доступа и защиты от несанкционированного доступа к ИТ-инфраструктуре WallixAdminBastion имеет собственную базу данных журнала аутентификации.

Необходимо в веб-интерфейсе WallixAdminBastion настроить отправку событий безопасности на сервер ПК «КОМРАД» по протоколу UDP на порт 514 (РисунокБ27) для отслеживания следующих событий:

- вход, подключение (попытка входа, подключения) пользователя (удалённого, интерактивного).

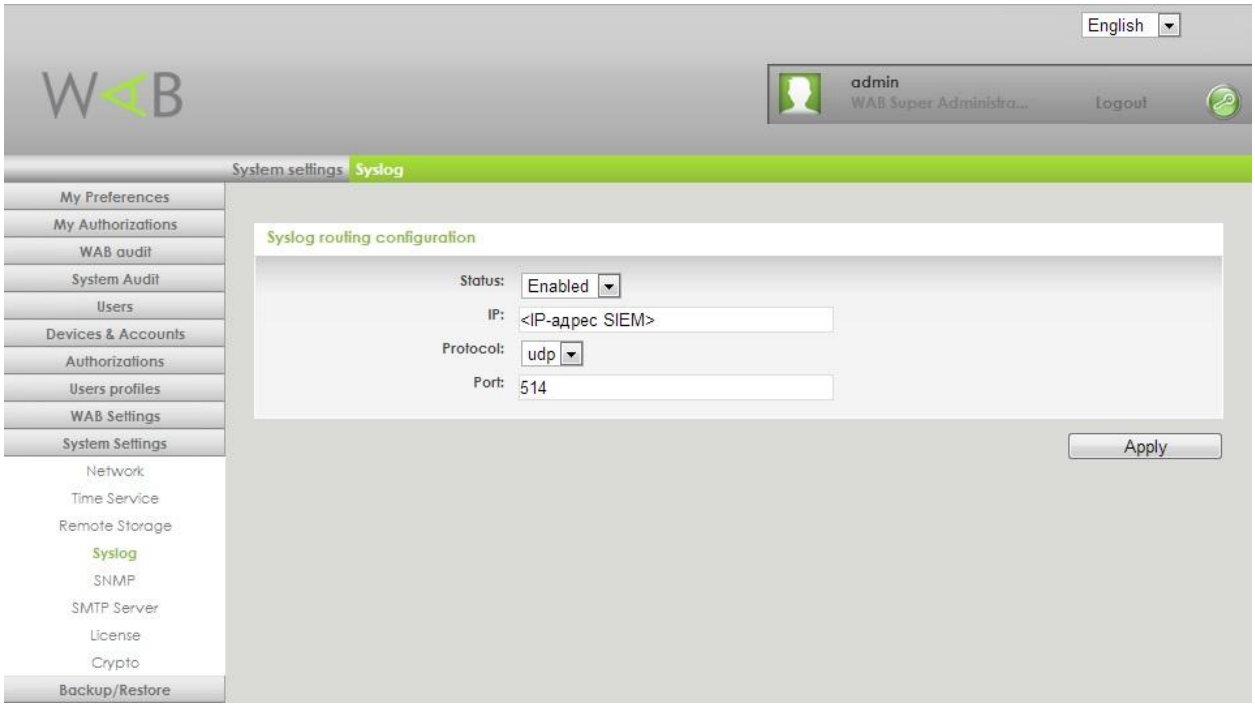



Рисунок Б27 – Веб-интерфейс настройки отправки событий безопасности Wallix AdminBastion

# 10. ТРЕБОВАНИЯ ПО НАСТРОЙКЕ СУБД MYSQL

Необходимо добавить в файл ***/var/ossec/etc/ossec.conf*** следующие строки:

*<localfile>*

*<log_format>syslog</log_format>*

*<location>/var/log/mysql/mysql.log</location>*

*</localfile>*

Это позволит отслеживать следующие события:

- вход, подключение (попытка входа, подключения) пользователя (удалённого, интерактивного);
- ошибка ввода пароля;
- создание, удаление, блокировка учётной записи;
- сброс (смена) пароля администратором.

Кроме того, необходимо настроить контроль за изменением и удалением файла конфигурации и журнала MySQL. Для этого необходимо изменить конфигурационный файл службы auditd /etc/audit/audit.rules, добавив в него строки:

*-w /var/log/mysql/mysql.log -p wa*

*-w /etc/my.conf -p wa*

Если использование службы auditd невозможно, то необходимо использовать inotify-tools. Для этого проверить, что агент ossec следит за журналом /var/log/inotify.log (пункт 2 данного приложения) и настроен сервис logrotate для автоматической ротации и архивации журнала inotify.log(пункт 14 данного приложения).

# 11. ТРЕБОВАНИЯ ПО НАСТРОЙКЕ NGINX

Необходимо добавить в файл ***/var/ossec/etc/ossec.conf*** следующие строки:

*<localfile>*

*<log_format>syslog</log_format>*

*<location>/var/log/nginx/access.log</location>*

*</localfile>*

Это позволит отслеживать следующие события:

- вход, подключение (попытка входа, подключения) пользователя (удалённого, интерактивного);
- ошибка ввода пароля;
- создание, удаление, блокировка учётной записи;
- сброс (смена) пароля администратором.

Кроме того, необходимо настроить контроль изменения и удаления файла конфигурации и журнала nginx. Для этого необходимо изменить конфигурационный файл службыauditd /etc/audit/audit.rules, добавив в него строки:

*-w >/var/log/nginx/access.log -p wa*

*-w/usr/local/nginx/conf/nginx.conf -p wa*

Если использование службы auditd невозможно, то необходимо использовать inotify-tools. Для этого проверить, что агент ossec следит за журналом /var/log/inotify.log (пункт 2 данного приложения) и настроен сервис logrotate для автоматической ротации и архивации журнала inotify.log(пункт 14 данного приложения).

# 12. ТРЕБОВАНИЯ ПО НАСТРОЙКЕ СЕТЕВОГО ОБОРУДОВАНИЯ CISCO

Необходимо произвести настройку устройства для отправки данных журналов событий по протоколу syslogв ядро ПК «КОМРАД» отдельно для межсетевого экрана и маршрутизатора. При этом контролируются следующие события:

- вход, подключение (попытка входа, подключения) пользователя (удалённого, интерактивного);
- ошибка ввода пароля;
- создание, удаление, блокировка учётной записи;
- сброс (смена) пароля администратором;
- изменение состава групп с учётными записями пользователей;
- установление SSH-соединения
- изменение правил межсетевого взаимодействия.

## *Настройка межсетевого экрана Cisco ASA 5500-x*

В терминале устройства выполнить следующие команды:

*#config terminal*

*#logging facility local5*

*#logging trap notification*

*# logging list notif-cfg-changes message 111008*

*# logging list notif-cfg-changes message 605004-605005*

*# logging list notif-cfg-changes level errors*

*# logging trap notif-cfg-changes*

*# logging host Management <KOMRAD-IP>*

*# ^Z*

*# writemem*

# *Настройка маршрутизатора Cisco 3900*

В терминале устройства выполнить следующие команды:

*#conf t*

*#archive*

*#log config*

*#logging <KOMRAD-IP>*

*#notify syslog*

*#login on-success log*

*#login on-failure log.*

# 13. ТРЕБОВАНИЯ ПО НАСТРОЙКЕ СИСТЕМЫ IDSSURICATA

Для обеспечения передачи данных журналов событий по протоколу syslog в ядро ПК «КОМРАД» необходимо добавить следующие строки в конфигурационный файл системы IDS**/etc/suricata/suricata.yaml**:

*...*

*# a line based alerts log similar to fast.log into syslog*

*- syslog:*

*enabled: yes*

*# reported identity to syslog. If ommited the program name (usually*

*# suricata) will be used.*

*identity: «snort»*

*...*

*# Define your logging outputs. If none are defined, or they are all*

*# disabled you will get the default - console output.*

*...*

*- syslog:*

*enabled: yes*

*facility: local5*

# 14. ТРЕБОВАНИЯ ПО НАСТРОЙКЕ AUDITD

Для обеспечения мониторинга конкретных директорий и файлов конечных устройств с помощью службы auditdнеобходимо изменитьконфигурационный-файлслужбы **/etc/audit/audit.rules**, добавив в него строки:

*-w /etc/group -p w*

*-w /etc/shadow -p w*

*-w /etc/ssh/sshd_config -p w*

*-w /etc/rsyslog.conf -p w*

*-a exit,always –F dir=/etc/rsyslog.d/ -F perm=w*

*-w /var/log/syslog -p w*

*-w /var/log/auth.log -p w*

*-w /var/log/yum.log -p w*

*-w /var/log/secure -p w*

*-w /sbin/iptables-multi-1.4.7 -p x -k iptables*

*-w /usr/bin/ssh -p x*

*-a exit,always –F dir=/var/CommuniGate/Settings/ -F perm=w*

# 15. ТРЕБОВАНИЯ ПО НАСТРОЙКЕ MYSQLPROXY

Необходимо добавить в файл ***/var/ossec/etc/ossec.conf*** следующие строки:

*<localfile>*

*<log_format>syslog</log_format>*

*<location>/var/log/users-queries.log</location>*

*</localfile>*

Данная команда позволяет отслеживать обращение пользователей к базам данных через MySQLProxy.

# ПРИЛОЖЕНИЕ В
# СПИСОК ЖУРНАЛОВ ПК «КОМРАД»

| **Системные журналы** | |
|---|---|
| **Расположение файла** | **Содержимое журнала** |
| /var/log/kern.log | Сообщения от ядра linux |
| /var/log/auth.log | Сообщения об использовании систем аутентификации |
| /var/log/daemon.log | Сообщения о работе системы и демонов |
| /var/log/messages | Общесистемные некритичные сообщения: info, notice, warn |
| /var/log/syslog | Все системные сообщения, кроме событий аутентификации |
| **Логи служб и приложений ПК «КОМРАД»** | |
| **Расположение файла** | **Содержимое лога** |
| /var/log/ossim/server.log | Журнал сервера ПК «КОМРАД» |
| /var/log/ossim/agent.log | Журнал сведений о событиях ИБ, полученных ядром ПК «КОМРАД» |
| /var/log/ossim/frameworkd.log | Журнал службы ossim-framework |
| /var/log/ossim/mysql.log | Журнал СУБД MySQL (базы данных СМИБ) |

# ПРИЛОЖЕНИЕ Г
# РАСПРЕДЕЛЕНИЕ ПРАВ ДОСТУПА ПОЛЬЗОВАТЕЛЕЙ К ФУНКЦИОНАЛУ В ВЕБ-ИНТЕРФЕЙСЕ ПК «КОМРАД»

| Вкладка веб-интерфейса ПК «КОМРАД» | Оператор | Администратор |
|---|---|---|
| **Цифровые панели** | | |
| Цифровые панели → Цифровые панели | X | X |
| Цифровые панели → Статус системы | | X |
| Цифровые панели → Риск | | X |
| **Инциденты** | | |
| Инциденты → Тревоги | X | X |
| Инциденты → Тревоги → Удалить тревоги | | X |
| Инциденты → Тревоги → Отчёты | X | X |
| Инциденты → Задания | X | X |
| Инциденты → Задания → Открыть задания | X | X |
| Инциденты → Задания →Закрыть/Удалить | | X |
| Инциденты → Задания → Отчёт | | X |
| Инциденты → Задания → Типы | | X |
| Инциденты → Задания → Теги | | X |
| Инциденты → Задания → Шаблон письма инцидента | | X |
| Инциденты → База знаний | | X |
| **Анализ** | | |
| Анализ→ События безопасности | X | X |
| Анализ→ События безопасности→Удалить события | X | X |
| Анализ→ События безопасности →Режим Реального Времени | X | X |
| Анализ→ Журналы | | X |
| Анализ→ Уязвимости→ Показать | | X |

| Вкладка веб-интерфейса ПК «КОМРАД» | Оператор | Администратор |
|---|---|---|
| Анализ⟶ Уязвимости⟶ Сканировать/Импортировать | | X |
| Анализ⟶ Уязвимости⟶ Удалить отчёт | | X |
| Анализ⟶ Обнаружение ⟶ HIDS⟶ Показать | | X |
| Анализ⟶ Обнаружение ⟶ HIDS ⟶ Настройки | | X |
| **Отчёты** | | |
| Отчёты⟶ Отчёт о средстве | X | X |
| Отчёты⟶Пользовательские отчёты | X | X |
| Отчёты⟶Пользовательские отчёты → Отчёты | | X |
| Отчёты⟶Пользовательские отчёты⟶Планировщик | | X |
| **Средства** | | |
| Средства ⟶Поиск средства | | X |
| Средства ⟶Средства ⟶Хосты | | X |
| Средства ⟶Средства ⟶Сети | | X |
| Средства ⟶Средства ⟶Порты | | X |
| Средства ⟶Средства ⟶Реестр ресурсов | | X |
| Средства ⟶Обзор средств | | X |
| **Установки** | | |
| Установки ⟶Политика | | X |
| Установки ⟶Действия | | X |
| Установки ⟶Директивы корреляции | | X |
| Установки ⟶Контроль соответствия | | X |
| Установки ⟶Перекрестная Корреляция | | X |
| **Сведения** | | |
| Сведения ⟶Рабочая сеть → Трафик | | X |
| Сведения → Рабочая сеть → Захват траффика | | X |

| Вкладка веб-интерфейса ПК «КОМРАД» | Оператор | Администратор |
|---|---|---|
| Сведения → Рабочая сеть → Профили | | X |
| Сведения →Доступность | X | X |
| Сведения → Репутация IP-адреса | | X |
| Сведения → Карта | | X |
| **Система** | | |
| Система → Пользователи | | X |
| Система → Пользователи → Активность пользователя | | X |
| Система → Компоненты КОМРАД → Сенсоры | | X |
| Система → Компоненты КОМРАД → Серверы | | X |
| Система → Сбор данных → Источники данных | | X |
| Система → Сбор данных → Реестр ресурсов | | X |
| Система → Сбор данных →DS группы | | X |
| Система → Сбор данных → Загрузка | | X |
| Система → Сбор данных → Сбор событий | | X |
| Система → Сбор данных → Активность пользователя | | X |
| Система → Рез. копирование | | X |

# ПРИЛОЖЕНИЕ Д

# ИНТЕГРАЦИЯ ПК «КОМРАД» С САЗ «СКАНЕР-ВС»

ПК «КОМРАД» имеет возможность интеграции с сертифицированным САЗ «Сканер-ВС» в рамках функционала Сканера безопасности. Подключение сертифицировнного САЗ «Сканер-ВС» позволяет ПК «КОМРАД» расширить функционал сканирования уязвимостей.

Интеграция со «Сканером-ВС» позволяет создавать задания на сканирование уязвимостей, просматривать отчеты о проведенных сканированиях. Управление осуществляется из веб-интерфейса ПК «КОМРАД», при этом имеется возможность переключения между экземплярами «Сканер-ВС», запущенными на разных узлах сети, а также консолидация информации об уязвимостях, поступившей от разных экземпляров САЗ «Сканер-ВС на одном узле» ПК «КОМРАД».

Таким образом, ПК «КОМРАД» может выступать центральным узлом САЗ «Сканер-ВС» и использоваться для управления сканированием и формирования общего отчета.

## *Настройка интеграции со «Сканером-ВС»*

1. Загрузить «Сканер-ВС»
2. В «Сканере-ВС» в файле /etc/default/openvas-manager заменить *MANAGER_ADDRESS=127.0.0.1* на *MANAGER_ADDRESS=0.0.0.0,* чтобы разрешить подключение к менеджеру по сети. Например, выполнитьвтерминалекоманду
   *#sudo sed -i 's/\(MANAGER_ADDRESS\)=127.0.0.1/\1=0.0.0.0/g' /etc/default/openvas-manager*
3. Запустить на панели задач «Сканер безопасности» и дождаться открытия веб-интерфейса (Рисунок Д1).

Рисунок Д1 – Веб-интерфейс «Сканера безопасности» в «Сканер-ВС»

4. В веб-интерфейсе ПК «КОМРАД» в меню «**Система→ Компоненты Комрад**» создать новый сенсор (Рисунок Д2).

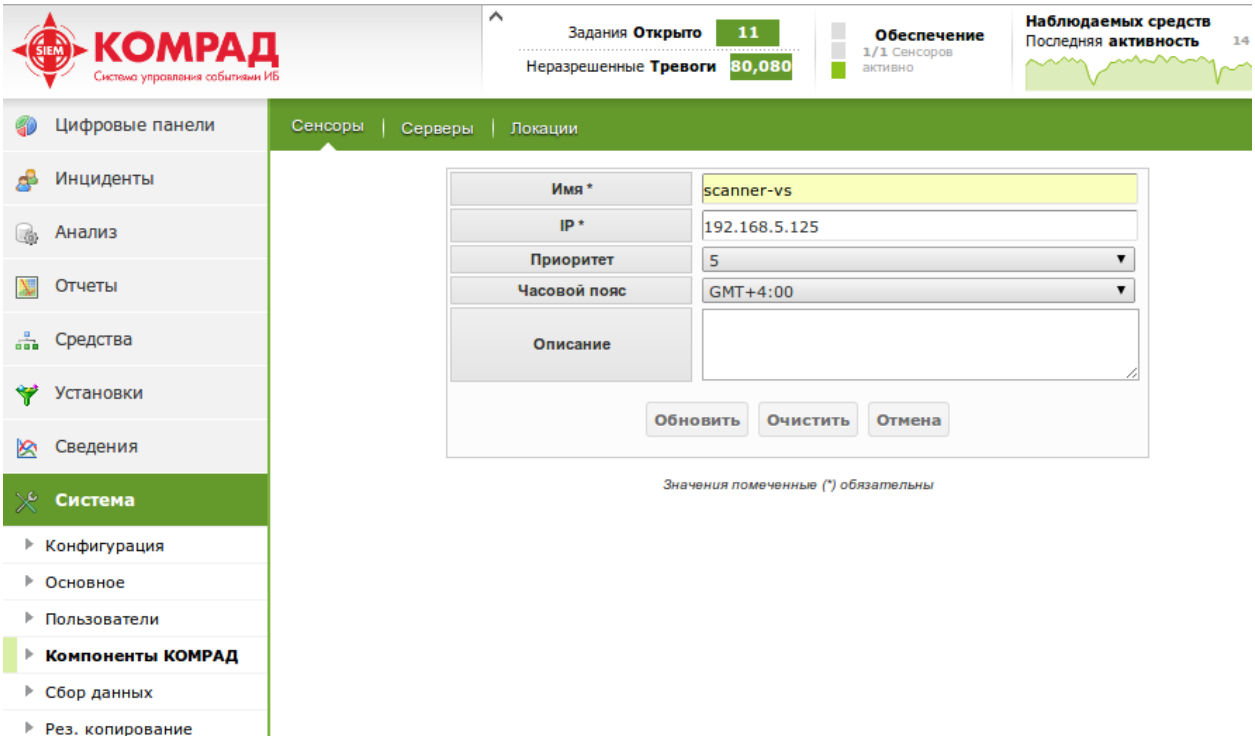



Рисунок Д2– Настройка дополнительного сенсора ПК «КОМРАД»

5. Выбрать в списке созданный сенсор и нажать «**Изменить**». В разделе «Опции сканера уязвимостей» указать в качестве логина/пароля admin/admin и нажать «**Обновить**» (Рисунок Д3).

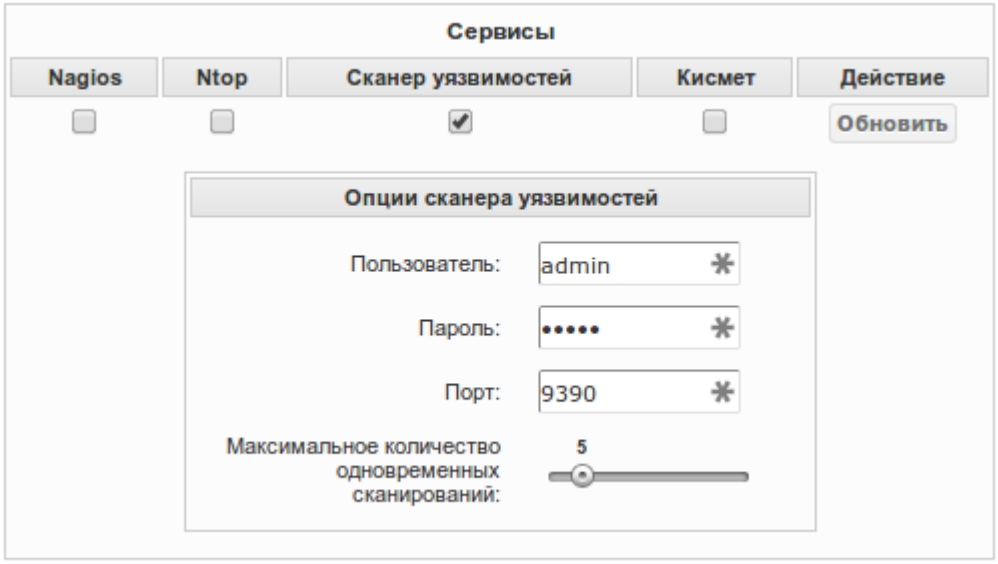



Рисунок Д3– Настройка сканера уязвимостей для нового сенсора

6. Перейти в «**Анализ→Уязвимости→Задания на сканирования**» и нажать на«**Новое задание сканирования**», где в качестве сервера указать сенсор со «Сканером-ВС» (Рисунок Д4).

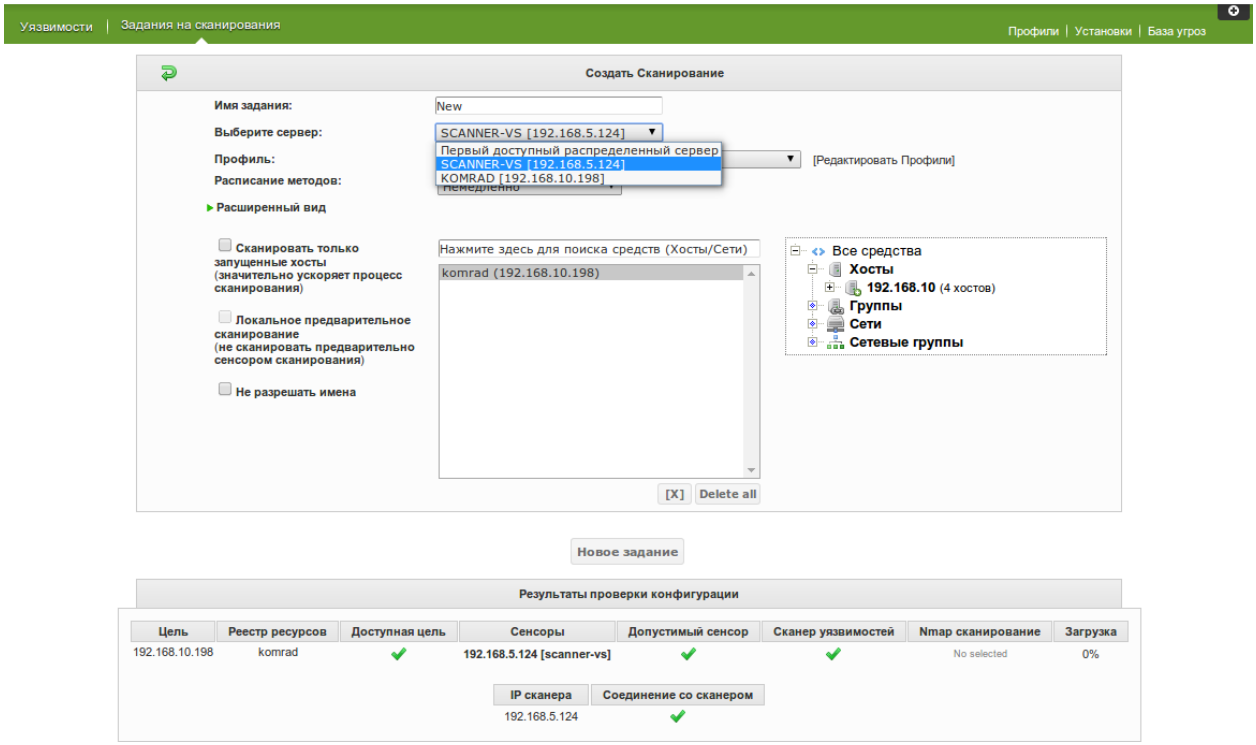



Рисунок Д4– Выбор Сканера-ВС при создании задания сканирования

7. После настройки всех параметров сканирования, нажать кнопку «**Новое задание**» и дождаться запуска и завершения сканирования.
8. Проверить соединение со сканером из интерфейса командной строки ПК «КОМРАД» можно, выполнив следующую команду:

   *# omp -h 192.168.5.124 -u admin -w admin -g*

   В результате должна появиться информация о доступных профилях сканирования следующего вида:

   *daba56c8-73ec-11df-a475-002264764cea  Full and fast*

   *698f691e-7489-11df-9d8c-002264764cea  Full and fast ultimate*

   *708f25c4-7489-11df-8094-002264764cea  Full and very deep*

   *74db13d6-7489-11df-91b9-002264764cea  Full and very deep ultimate*

   *085569ce-73ed-11df-83c3-002264764cea  empty*

## Лист регистрации изменений

| Изм. | Номера листов (страниц) | | | | Всего листов (страниц) в докум. | № докум. | Входящий № сопроводи-тельного докум. | Подпись | Дата |
|---|---|---|---|---|---|---|---|---|---|
| | измененных | замененных | новых | аннулированных | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |