



МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ  
ФЕДЕРАЦИИ ФГБОУ ВО «Южно-Российский государственный  
политехнический университет (НПИ) имени М.И. Платова»



Департамент по специальному образованию и делам казачества  
Кафедра: «Информационная безопасность»  
Направление подготовки: 10.04.01 Информационная безопасность

**Семенов Дмитрий Юрьевич**

Доклад выпускной квалификационной работы  
на тему:

**«Разработка предложений по внедрению системы  
управления событиями информационной безопасности  
в систему безопасности организации»**

НАУЧНЫЙ РУКОВОДИТЕЛЬ: заведующий кафедрой «Информационная безопасность»  
кандидат военных наук, доцент **Баранов Владимир Витальевич**



## **Цель:**

Разработка программного обеспечения для интеграции различных средств и систем защиты информации в систему управления событиями информационной безопасности и внедрения её в учебный процесс кафедры.

## **Объект исследования:**

Функциональная структура системы управления событиями информационной безопасности Комрад 4.0.

## **Предмет:**

Методы интеграции различных систем и средств защиты информации в систему управления событиями информационной безопасности организации.



## Задачи исследования:

1. Предоставить краткую характеристику SIEM-систем как класса систем управления событиями информационной безопасности.
2. Провести сравнительный анализ возможностей SIEM-систем отечественного производства. Выбрать наиболее оптимальный вариант SIEM-системы.
3. Определить порядок внедрения в систему безопасности организации выбранной системы управления событиями информационной безопасности.
4. Разработать модель функциональной структуры SIEM-системы.
5. Сформировать методики для реализации программных компонентов, обеспечивающих подключение средств и систем защиты к SIEM-системе.
6. Произвести разработку программных компонентов.
7. Представить описание процесса развертывания SIEM-системы в организации для использования ее в учебном процессе кафедры.
8. Провести эксперимент по проверке работоспособности SIEM-системы с подключенными к ней разнотипными системами и средствами защиты.
9. Провести оценку эффективности результатов исследования.



## Структура исследования

### **1. АНАЛИЗ ФУНКЦИОНАЛЬНЫХ ВОЗМОЖНОСТЕЙ SIEM-СИСТЕМ И ОБОСНОВАНИЕ НЕОБХОДИМОСТИ ИХ ВНЕДРЕНИЯ В СИСТЕМУ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ**

- 1.1 Анализ структуры и функционирования системы защиты информации в организации и обоснование необходимости применения SIEM-систем.
- 1.2 Сравнительный анализ отечественных SIEM-систем и обоснование выбора системы управления событиями информационной безопасности Комрад 4.0.
- 1.3 Формирование учебного варианта структуры системы защиты информации в организации.
- 1.4 Анализ возможностей системы по проведению интеграции разнотипных средств и систем защиты информации.
- 1.5 Выбор языка программирования для создания программного обеспечения для интеграции различных средств и систем защиты.



## **2. МЕТОДИКА СОЗДАНИЯ ИНТЕГРИРОВАННОЙ СИСТЕМЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В ОРГАНИЗАЦИИ НА ОСНОВЕ СИСТЕМЫ УПРАВЛЕНИЯ СОБЫТИЯМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.**

2.1 Разработка модели функционирования интегрированной системы безопасности информации на основе системы управления событиями информационной безопасности Комрад 4.0.

2.2 Методика разработки программного обеспечения для интеграции разнотипных средств и систем защиты информации в систему управления событиями информационной безопасности.

2.3 Методика оценки эффективности функционирования и применения в учебном процессе интегрированной системы безопасности информации в организации.



### **3. ПРЕДЛОЖЕНИЯ ПО РАЗВЁРТЫВАНИЮ В ОРГАНИЗАЦИИ ИНТЕГРИРОВАННОЙ СИСТЕМЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ НА ОСНОВЕ СИСТЕМЫ УПРАВЛЕНИЯ СОБЫТИЯМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОМРАД 4.0.**

3.1 Разработка программного обеспечения для интеграции разнотипных средств и систем защиты информации.

3.2 Развертывание интегрированной системы безопасности информации на основе системы управления событиями информационной безопасности Комрад 4.0.

3.3 Проведение эксперимента по проверки работоспособности интегрированной системы безопасности информации на основе системы управления событиями информационной безопасности Комрад 4.0.

3.4 Оценка эффективности функционирования и внедрения в учебный процесс интегрированной системы безопасности информации на основе системы управления событиями информационной безопасности Комрад 4.0.

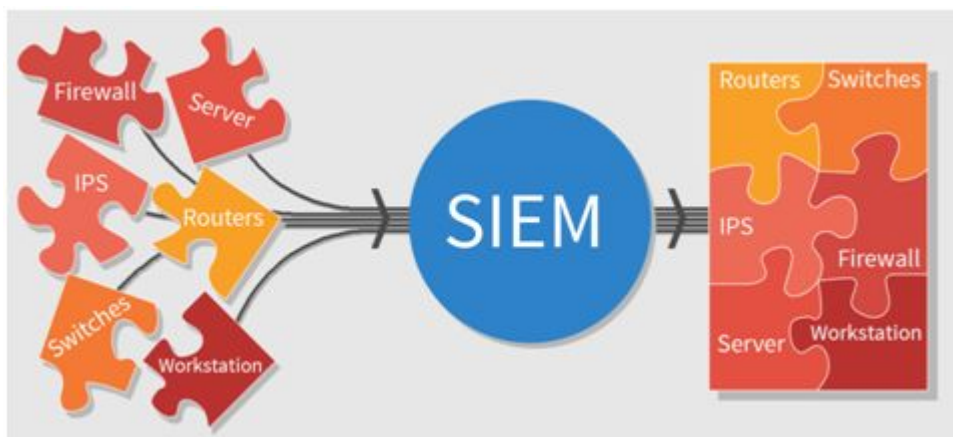


## 1.1 Понятие и функциональные возможности SIEM-систем

Аббревиатура SIEM образована от **security information and event management**, что дословно можно перевести как **система управления событиями и информационной безопасностью**. SIEM обеспечивает анализ в реальном времени событий, происходящих в ИТ-инфраструктуре. Подобный анализ необходим для обнаружения и определения среди всех событий информационной безопасности и реагирования на них.

**SIEM-система собирает, анализирует и представляет информацию из сетевых устройств и устройств безопасности.** Также в эту систему могут входить приложения для управления идентификацией и доступом, инструменты управления уязвимостями, базы данных и приложений. Для наглядности мы выделим несколько функций, которые обычно реализуются SIEM-системами:

- **Возможность отправки предупреждений на основе predefined настроек.**
- **Отчеты и логирование для упрощения аудита.**
- **Возможность просмотра данных на разных уровнях детализации.**



## 1.1 Сценарии использования SIEM-систем

### Сценарии использования SIEM:

- Отслеживание **аутентификации и обнаружение компрометации** аккаунтов пользователей и администраторов. Отслеживание случаев заражения.
- **Обнаружение вредоносных программ** с использованием исходящих журналов брандмауэра и журналов веб-прокси, а также внутренних журналов подключения и сетевых потоков.
- **Мониторинг подозрительного исходящего трафика** и передаваемых по сети данных с использованием журналов брандмауэра, журналов веб-прокси и NetFlow.
- **Обнаружение кражи данных** и других подозрительных внешних соединений. **Отслеживание системных изменений** и других административных действий во внутренних системах и их соответствия разрешенной политике.
- **Отслеживание атак на веб-приложения** и их последствий с использованием журналов веб-сервера, WAF (Web Application Firewall, экран для защиты веб-приложений) и логов приложений.







## 1.2 Сравнительный анализ отечественных SIEM-систем

Критерии оценки/вендор	КОМРАД 4.0	RuSIEM	MaxPatrol SIEM
Название компании	АО «НПО Эшелон»	ООО «РУСИЕМ»	АО «Позитив технолоджиз»
Целевой сегмент	Крупный и средний бизнес. Банковский, государственный секторы.	Государственный сектор, средний бизнес.	Все секторы, любой размер бизнеса.
Крупнейшее из известных внедрений в России	Вооруженные силы РФ	ГБУ СО "Сахалинский областной центр информатизации"	ГК Росатом
Наличие в реестре отечественного ПО	Регистрационный номер в реестре 239	Регистрационный номер в реестре 3808	Регистрационный номер в реестре 1143
Оповещение об инциденте	SMTP, скрипты	SMTP	SMTP, скрипты
Интеграция с системами Service Desk	Да (API, email, syslog)	Да (API, email, syslog)	Да (API, email)
Наличие сформированных образов для платформ виртуализации	VMWare, Hyper- Да (API, email, syslog), KVM, QEMU.	VMWare, Hyper- Да (API, email, syslog), KVM, QEMU.	VMWare.
Средняя степень сжатия при хранение нормализованных событий	x2-10	x0.7	x5
Безопасные протоколы передачи данных между компонентами системы	TLS/SSL	TLS/SSL	TLS
Управление правилами корреляции	Объектный конструктор	Графический конструктор	Язык поисковых запросов
Парсинг, возможность изменять и создавать новые коннекторы к разным типам устройств	Парсеры могут быть изменены или созданы пользователем. Разработка парсеров в рамках поддержки	Парсеры могут быть изменены или созданы пользователем	Все источники заказчика в рамках техподдержки
Автообнаружение источников событий	Да	Да	Да

## 1.2 Сравнительный анализ отечественных SIEM-систем

Критерии оценки	Характеристики Комрад 4.0	Расшифровка характеристик
Средняя степень сжатия при хранении нормализованных событий	x2-10	Малые требования к ресурсам сервера для хранения данных.
Управление правилами корреляции	Объектный конструктор	Упрощение написания правил корреляции
Парсинг, возможность изменять и создавать новые коннекторы к различным типам устройств	Парсеры могут быть изменены или созданы пользователем. Разработка парсеров в рамках поддержки	Возможность разработки парсеров сотрудником организации, возможность разработки парсеров в рамках технической поддержки



## 1.2 Сравнительный анализ отечественных SIEM-систем Обоснование необходимости внедрения в учебный процесс

В настоящее время SIEM-системы получили широкое распространение. В данный момент есть необходимость в подготовленных специалистах, которые способны работать с этими системами. Помимо научной цели, решается задача внедрения класса данных систем в учебный процесс, а именно разработка учебно-методических материалов по:

1. Установке ПО;
2. Настройке модулей системы;
3. Формированию графа подключений;
4. Работы с отчётами.



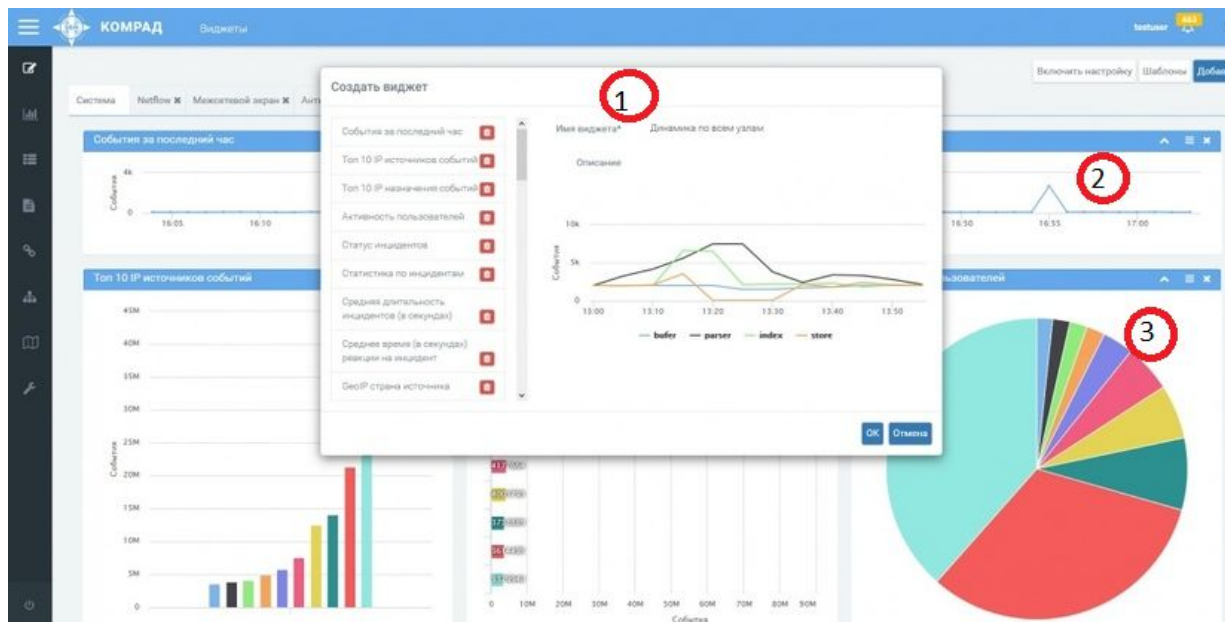
## 1.2 Сравнительный анализ отечественных SIEM- систем

### Комрад 4.0 – Система управления событиями ИБ

**КОМРАД 4.0 – гибкая и масштабируемая система централизованного управления событиями информационной безопасности, поддерживающая широкий спектр отечественных средств защиты информации.**

Применение КОМРАД позволяет:

1. осуществлять централизованный мониторинг событий ИБ,
2. выявлять и оперативно реагировать на инциденты ИБ,
3. выполнять требования, предъявляемые регуляторами к защите персональных данных, а также к обеспечению безопасности государственных информационных систем и контролю критической информационной инфраструктуры предприятия.
4. отправлять данные о событиях и инцидентах ИБ во внешние системы (например, ГосСОПКА).



### 1.3 Исходные данные системы защиты информации организации (учебный вариант)

№ п./п.	Профили защиты	Класс защиты
7	Класс средств защиты систем обнаружения вторжений	4-й класс защиты
8	Класс защищенности средств антивирусной защиты информации	4-й класс защиты
9	Тип средств антивирусной защиты	Тип «В» (на автоматизированных рабочих местах)
10	Класс защиты средств доверенной загрузки	4-й класс защиты
11	Класс защиты средств контроля съемных машинных носителей	4-й класс защиты
12	Класс операционных систем для обеспечения защиты информации	4-й класс операционных систем

## 1.4 Оборудование организации и возможность его совмещения с системой управления событиями ИБ Комрад 4.0

Средство защиты информации	Протокол передачи данных	Возможность совмещения с системой управления событиями ИБ Комрад 4.0
<b>Средства защиты от НСД</b>		
ОС Astra Linux	Rsyslog+ssl	Есть
ОС RedOS	Rsyslog	Есть
ПАК VipNet	IP/241	Есть
ПО SecretNet Studio	AD LDS	Есть
ОС Windows 10	Rsyslog	Есть
<b>Средства защиты от ТКУИ</b>		
Комплекс виброакустической защиты Соната АВ	ИК-канал	Нет
Устройство защиты МП-1А	Электрические импульсы	Нет
Система постановки акустических и виброакустических помех Шорох-5Л	RS-485	Нет
Устройство защиты от ПЭМИН Соната-Р2	ИК-канал	Нет

## 1.4 Оборудование организации и возможность его совмещения с системой управления событиями ИБ Комрад 4.0

Средство защиты информации	Протокол передачи данных	Возможность совмещения с системой управления событиями ИБ Комрад 4.0
Средства инженерно-технической защиты		
Система видеонаблюдения <b>Falcon eye</b>	TSP/IP	Есть
Средства каналообразования		
Мультиплексор <b>Маком-MX</b>	RS232/RS-422	Требует исследования
Сетевое оборудование		
Коммутатор <b>D-Link</b>	Multiple Spanning Tree	Есть
Маршрутизатор <b>MikroTik</b>	Nstreme	Есть
ПО аттестационных испытаний ИС		
Инструмент по тестированию и анализу защищённости информационных систем <b>Сканер ВС</b>	TSP/IP	Есть
Сетевой сканер <b>Ревизор сети</b>	SSL	Есть
Сканер уязвимостей <b>XSpider</b>	SSL	Есть



## 1.5 Сравнительный анализ и выбор средств разработки программного обеспечения

Параметры/язык	Perl	Delphi	Python	PHP
Объектно-ориентированная парадигма	-	+	+	+
Бесплатная лицензия	+	-	+	+
Возможность распараллеливания	-	-	+	+
Динамическая типизация	+	+	+	+
Ленивые вычисления	-	-	+	-
Множественное наследование	+	-	+	-
Возможность создания макросов	+	-	+	-





## 2.1 Функциональная схема интегрированной системы безопасности

### Средства защиты от НСД

- Операционная система **Astra Linux**
- Операционная система **RED OS**
- Операционная система **Windows 10**
- ПАК **VIPNET**
- ПО **SecretNet Studio**
- Сетевой сканер **Ревизор Сети**
- Сканер уязвимостей **X Spider**



### Средства защиты от ТКУИ

- Система постановки акустических и виброакустических помех **Шорох-5Л**



### Средства инженерно-технической защиты

- Камеры видеонаблюдения **Falcon eye**



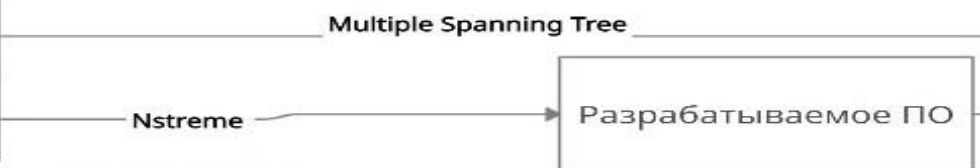
### Средства каналообразования

- Мультиплексор **Маком-MX**



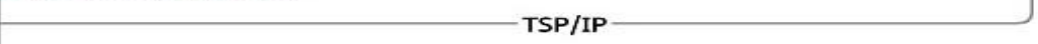
### Сетевое оборудование

- Коммутатор **D-Link**
- Маршрутизатор **MikroTik**



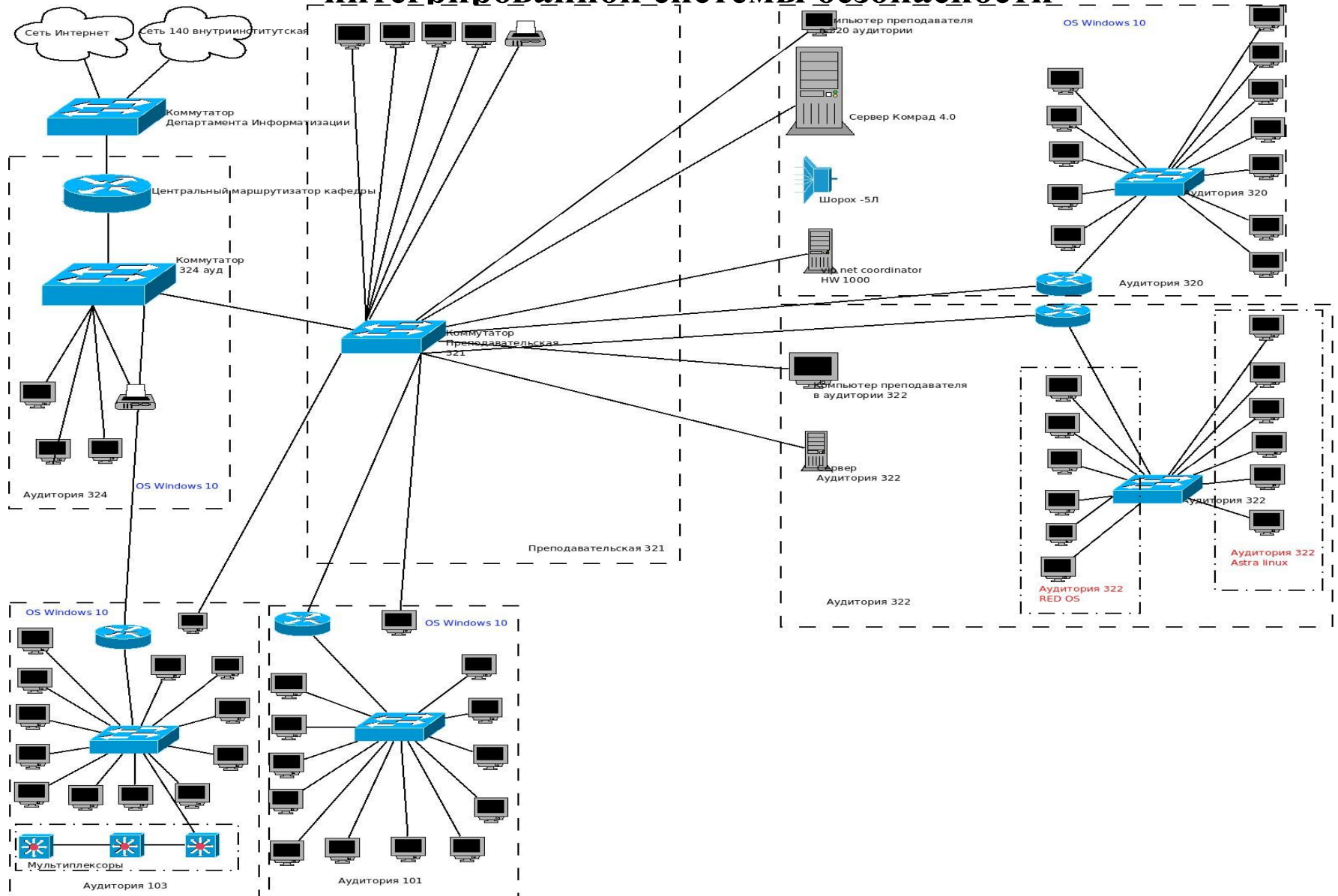
### Сканер безопасности информационных систем

- Сканер уязвимостей **X Spider**

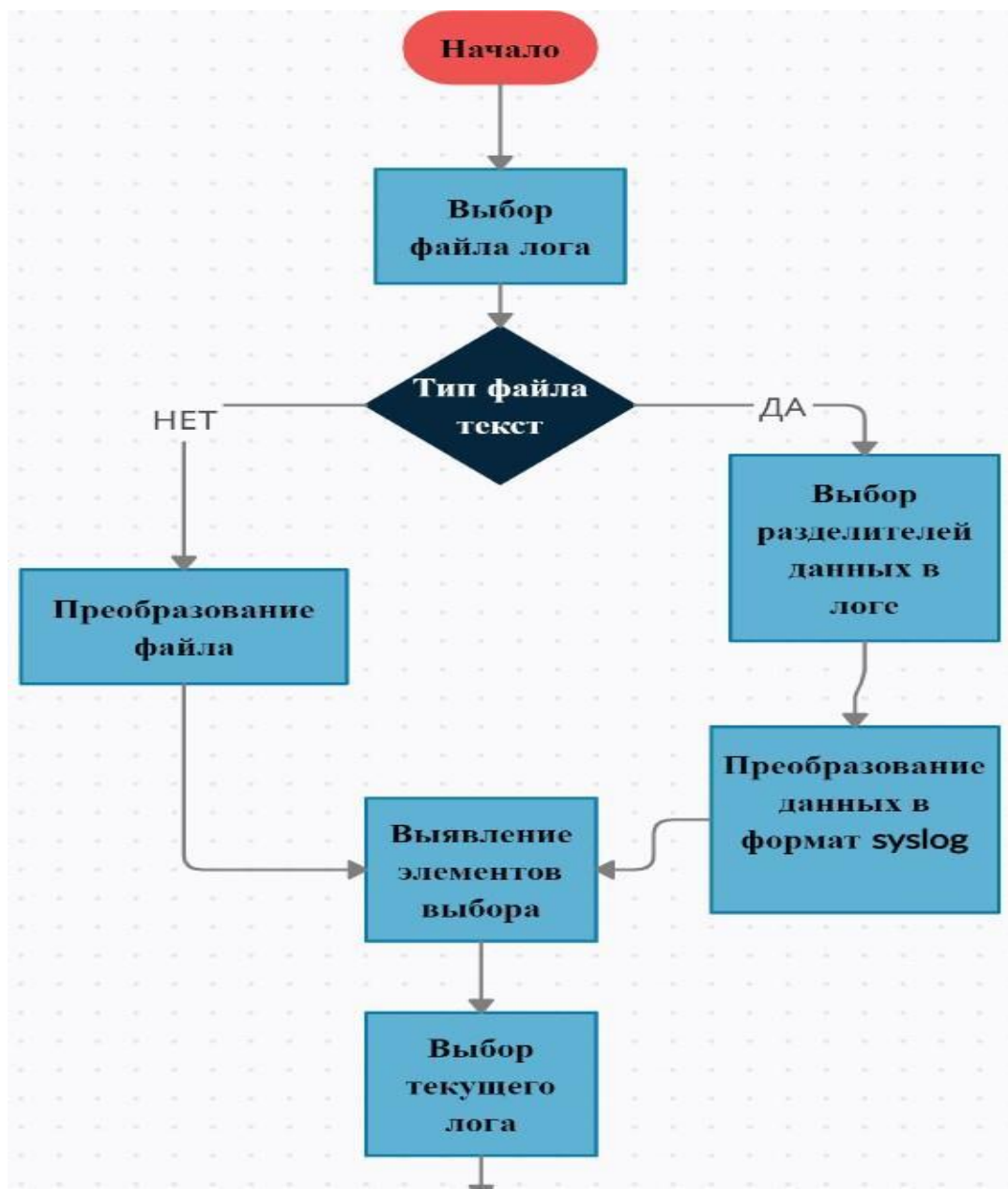


**Система управления событиями информационной безопасности Комрад 4.0.**

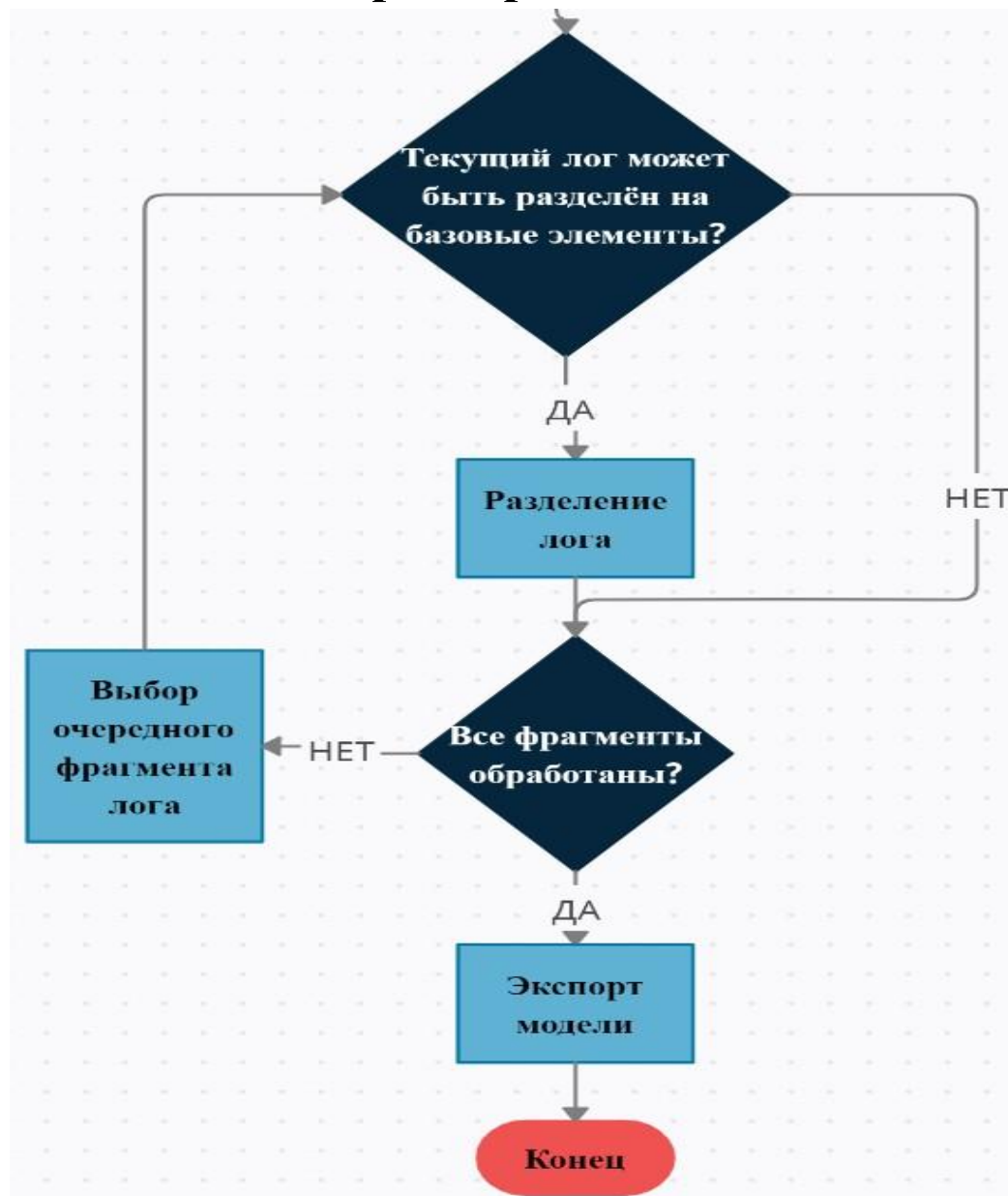
## 2.1 Структурная схема интегрированной системы безопасности



## 2.2 Алгоритм работы ПО



## 2.2 Алгоритм работы ПО





## 2.3 Оценка показателей эффективности внедрения интегрированной системы

Процесс функционирования SIEM-системы	Для организации	Для учебного процесса
Результативность	Повышение вероятности выявления инцидентов.	Достижение требуемого уровня компетенций.
	Снижение ущерба в результате реализации информационных угроз.	Материальное обеспечение.
Ресурсоёмкость	Задействование сервера: 130 000 р. Разработка программного обеспечения.	Разработка лабораторных работ и лекционных материалов.
Оперативность	Сокращение времени на реагирование на инциденты безопасности.	Сокращение времени на разработку учебно-методических материалов.
	Сокращение времени проведения расследования обстоятельств инцидентов по зарегистрированным событиям.	



## 3.1 Подключенные средства и КОМПЛЕКСЫ

№ п/п	Средства и комплексы, подключённые к системе Комрад 4.0	Разработанное ПО для интеграции с системой Комрад 4.0
Средства защиты от НСД		
1	ОС Astra Linux	Не требуется
2	ОС RedOS	Не требуется
3	ОС Windows 10	Не требуется
4	ОС Windows Server 2016	Не требуется
5	Сетевой сканер Ревизор Сети	Не требуется
Сетевое оборудование		
6	Коммутатор D-Link	Не требуется
7	Маршрутизатор MikroTik	Разработано
Средства защиты от ТКУИ		
8	Система постановки акустических и виброакустических помех Шорох-5Л	Разработано



## 3.2 Развёртывание интегрированной системы.

### 3.2.1 Установка базовой системы Комрад 4.0

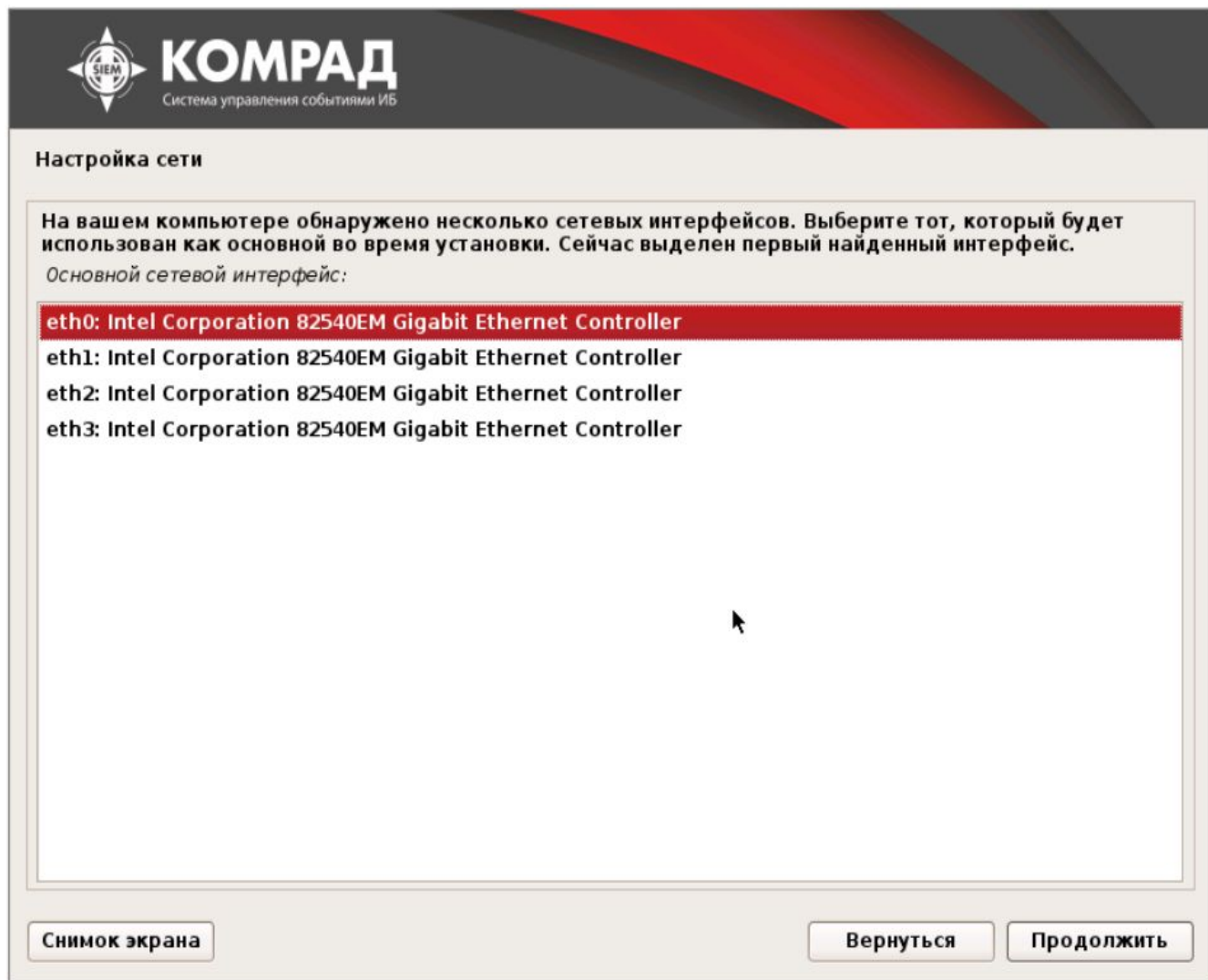


**Загрузка дополнительных компонентов**



## 3.2 Развёртывание интегрированной системы.

### 3.2.1 Установка базовой системы Комрад 4.0



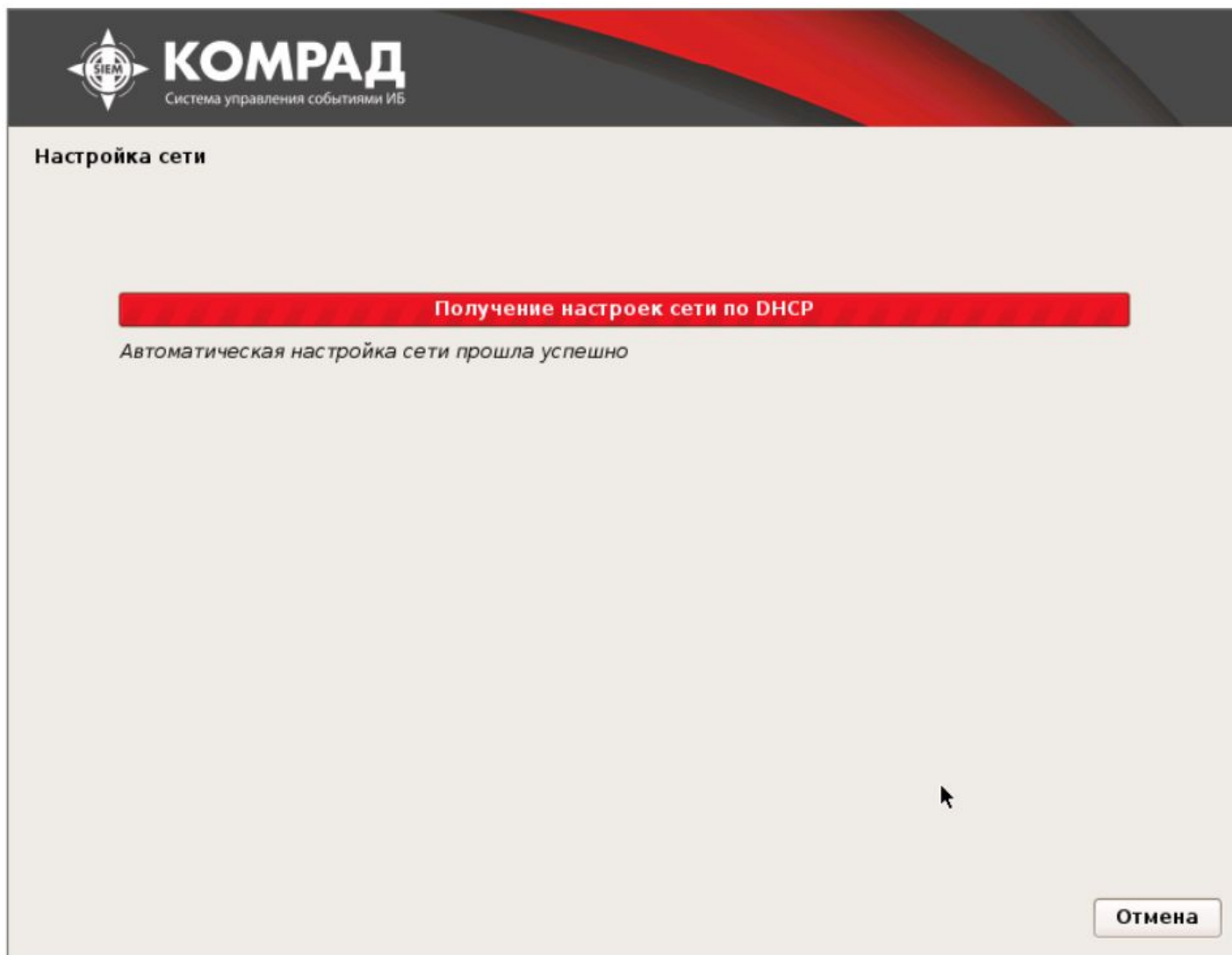
Выбор сетевого интерфейса





## 3.2 Развёртывание интегрированной системы

### 3.2.1 Установка базовой системы Комрад 4.0



**Получение настроек по DHCP**



## 3.2 Развёртывание интегрированной системы.

### 3.2.1 Установка базовой системы Комрад 4.0

**КОМРАД**  
Система управления событиями ИБ

Настройка учётной записи admin

Для управления системой будет создан специальный пользователь - admin.  
Пожалуйста, придумайте надёжный пароль для этого пользователя.

Введите пароль для пользователя admin:

Введите пароль ещё раз:

Снимок экрана

Вернуться

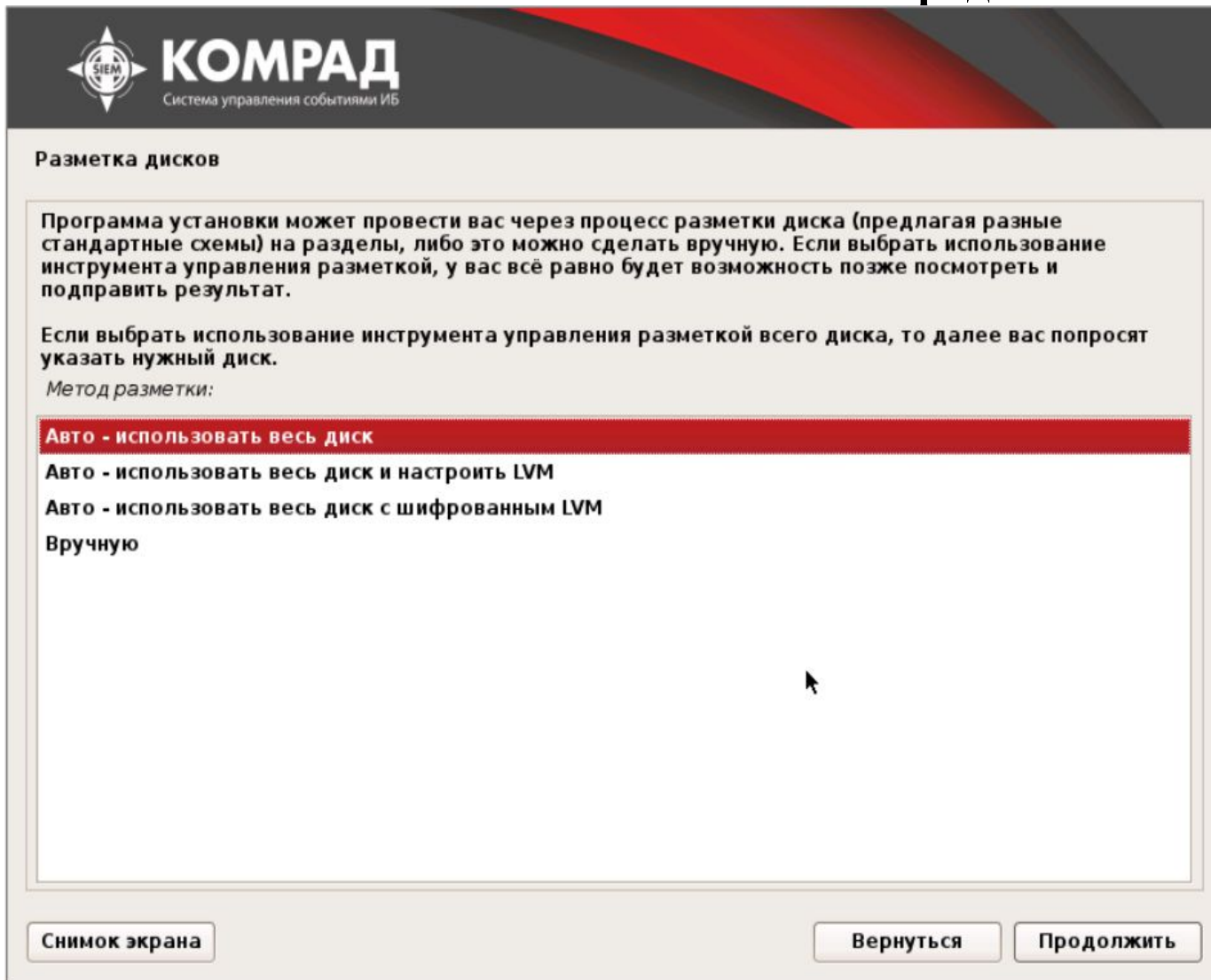
Продолжить

Настройка учётной записи администратора



## 3.2 Развёртывание интегрированной системы.

### 3.2.1 Установка базовой системы Комрад 4.0



**Выбор жёсткого диска, на который будет установлена система**



## 3.2 Развёртывание интегрированной системы

### 3.2.1 Установка базовой системы Комрад 4.0

**Справка по разметке**

Разметка диска заключается в выделении области для установки новой системы. Вам нужно выбрать какой(ие) раздел(ы) будет(ут) использоваться для установки.

Выберите свободное пространство, в котором будут созданы разделы.

Выберите то устройство, на котором будут удалены все разделы и создана новая пустая таблица разделов.

Выберите раздел для удаления или для указания, как он будет использоваться. Как минимум нужен один раздел, содержащий так называемую корневую файловую систему (точка монтирования /). Многие считают, что также нужен отдельный раздел подкачки. "Подкачка" -- место на жёстком диске без определённой структуры, которое используется системой в качестве "виртуальной памяти".

Если раздел уже содержит файловую систему, вы можете оставить и воспользоваться уже существующими в разделе данными. Подобные разделы помечены "К" в главном меню разметки дисков.

В общем случае вы скорее всего захотите отформатировать раздел. ПРИМЕЧАНИЕ: все данные в разделе при форматировании будут безвозвратно уничтожены. Если вы решитесь отформатировать раздел, уже содержащий файловую систему, то он будет помечен "F" в главном меню разметки дисков, в противном случае метка будет "f".

чтобы изменить его, чтобы создать новый

Снимок экрана | Справка | Продолжить | Продолжить



## 3.2 Развёртывание интегрированной системы

### 3.2.1 Установка базовой системы Комрад 4.0



**Установка базовой системы**



## 3.2 Развёртывание интегрированной системы

### 3.2.1 Установка базовой системы Комрад 4.0

**КОМРАД**  
Система управления событиями ИБ

#### Выбор программного обеспечения

В данный момент, установлена только основа системы. Исходя из ваших потребностей, вы можете выбрать один и более из уже готовых наборов программного обеспечения.  
*Выберите устанавливаемое программное обеспечение:*

- Центр управления КОМРАД SIEM
- Модуль корреляции событий безопасности
- Модуль обработки событий безопасности
- Модуль сбора событий безопасности

Снимок экрана      Продолжить

Выбор программного обеспечения



## 3.2 Развёртывание интегрированной системы

### 3.2.1 Установка базовой системы Комрад 4.0





## 3.2 Развёртывание интегрированной системы


### 3.2.1 Установка базовой системы Комрад 4.0





## 3.2 Развёртывание интегрированной системы

### 3.2.2 Подключение модулей системы



Главный\_узел\_Коррелятор

Главный\_узел\_Процессор

Главный\_узел\_Коллектор

Узел

Загрузить лицензию

Владелец лицензии	Для учебных целей (не для коммерческого использования)
Дата истечения	2022-02-15 12:14:00
Схема подключения	aiо
Номер лицензии	DEMO

**IP адрес:** 192.168.1.10

Деактивировать

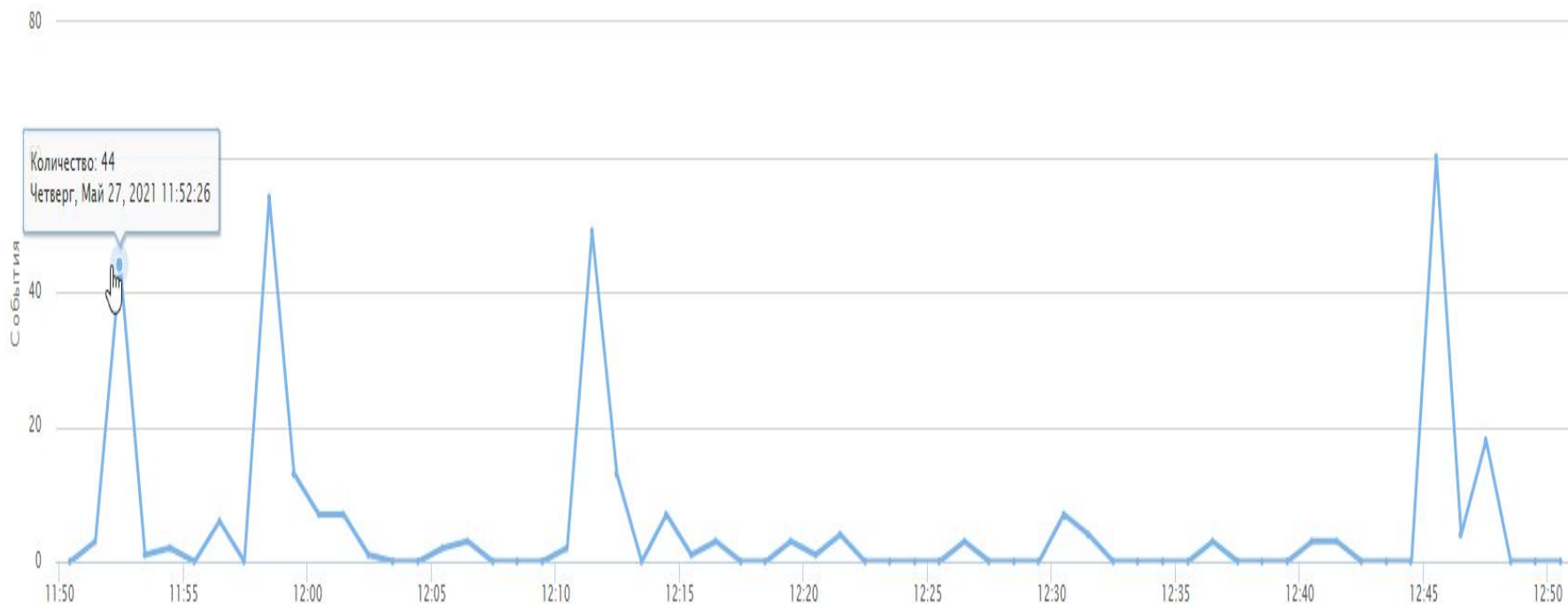
Подробнее

**Модули:**

Веб консоль	Активный
Коррелятор	Активный
Процессор	Активный
Коллектор	Активный

## 3.2 Развёртывание интегрированной системы

### 3.2.3 Виджет «События за последний час»



**События за последний час**



## 3.2 Развёртывание интегрированной системы

### 3.2.4 Подключение внешних устройств

Поиск...

Источники +

Имя	Адрес	Логин	Действия
WinServer2008R2	192.168.5.112	wmi_user	
Notebook_WL91	192.168.0.89	wmi_user	

Меню подключения внешних устройств

Поиск...

Задачи +

Включить Отключить Перезагрузить Удалить

<input type="checkbox"/>	Имя	Интервал	Источник	Действия
<input type="checkbox"/>	Notebook_WL91_Application	10	Notebook_WL91	<span>Выключен</span>
<input type="checkbox"/>	WinServer2008R2_Security	10	WinServer2008R2	<span>Включен</span>
<input type="checkbox"/>	WinServer2008R2_System	10	WinServer2008R2	<span>Включен</span>
<input type="checkbox"/>	Notebook_WL91_Security	10	Notebook_WL91	<span>Выключен</span>
<input type="checkbox"/>	WinServer2008R2_Application	10	WinServer2008R2	<span>Включен</span>
<input type="checkbox"/>	Notebook_WL91_System	10	Notebook_WL91	<span>Выключен</span>

Меню управления  
подключенными устройствами

Настройка маппинга

Ключ	Значение	Действия
ИД безопасности	ИД безопас	
Имя конечной учетной з	Имя польза	
Имя процесса	Команда	
Имя учетной записи	Имя польза	
Порт	Порт источ	
Порт источника	Порт источ	
Сетевое имя учетной за	Имя польза	
Сетевой адрес	IP источник	
Сетевой адрес источник	IP источник	

+

OK Отмена

Настройка маппинга  
подключенных устройств

## 3.2 Развёртывание интегрированной системы

### 3.2.5 Разработка ПО для интеграции средств и систем

```
37 from typing import List
38 import random
39 import unittest
40 import logging
41 import os
42 import subprocess
43
44 # logging.disable(level=logging.CRITICAL)
45 logging.basicConfig(level=logging.DEBUG, format="%(levelname)s %(message)s")
46
47 # ps = subprocess.run(f"pstree -asp {os.getpid()}", capture_output=True, shell=True)
48 # logging.debug(f"{ps.stdout.decode('utf-8')}")
49
50 class SolutionSingle1:
51     def twoSum(self, nums: List[int], target: int) -> List[int]:
52         for i in range(len(nums)-1): #
53             complement = target - nums[i]
54             print(i, complement)
55             for j in range(i+1, len(nums)):#linear search
56                 if complement == nums[j]:
57                     print(j)
58                     return [i, j]
59         return None
60
61
```

Процесс разработки ПО

```
1  [||] 2.1% 5 [||] 0.2%
2  [||] 2.4% 6 [||] 1.2%
3  [||] 3.3% 7 [||] 1.4%
4  [||] 3.1% 8 [||] 1.4%
Mem[||||] 1484/15971MB Tasks: 113, 414 thr; 1 running
Swp[ ] 0/32537MB Load average: 0.48 0.41 0.37
Uptime: 00:24:34
```

PID	USER	PRI	NI	VIRT	RES	SHR	S	CPU%	MEM%	TIME+	Command
2306	root	20	0	650M	38932	5680	S	2.9	0.2	0:14.98	python /usr/share
1494	root	20	0	556M	23300	5684	S	2.4	0.1	0:20.82	python /usr/share
2419	root	20	0	650M	38932	5680	S	2.4	0.2	0:14.88	python /usr/share
1400	root	20	0	1316M	112M	10040	S	1.9	0.7	0:24.42	python /usr/share
1496	root	20	0	556M	23324	5712	S	1.9	0.1	0:20.78	python /usr/share
1504	root	20	0	556M	23328	5716	S	1.9	0.1	0:18.75	python /usr/share
1495	root	20	0	556M	23328	5716	S	1.4	0.1	0:20.78	python /usr/share
2585	root	20	0	1020M	108M	5208	S	1.4	0.7	0:22.44	python /usr/share
1500	root	20	0	556M	23300	5684	S	1.4	0.1	0:18.76	python /usr/share
2612	root	20	0	1020M	108M	5208	S	1.4	0.7	0:18.65	python /usr/share
2593	root	20	0	1316M	112M	10040	S	1.4	0.7	0:18.69	python /usr/share
1518	root	20	0	556M	23324	5712	S	1.4	0.1	0:18.74	python /usr/share
2107	root	20	0	771M	26640	9872	S	0.5	0.2	0:07.31	python /usr/share

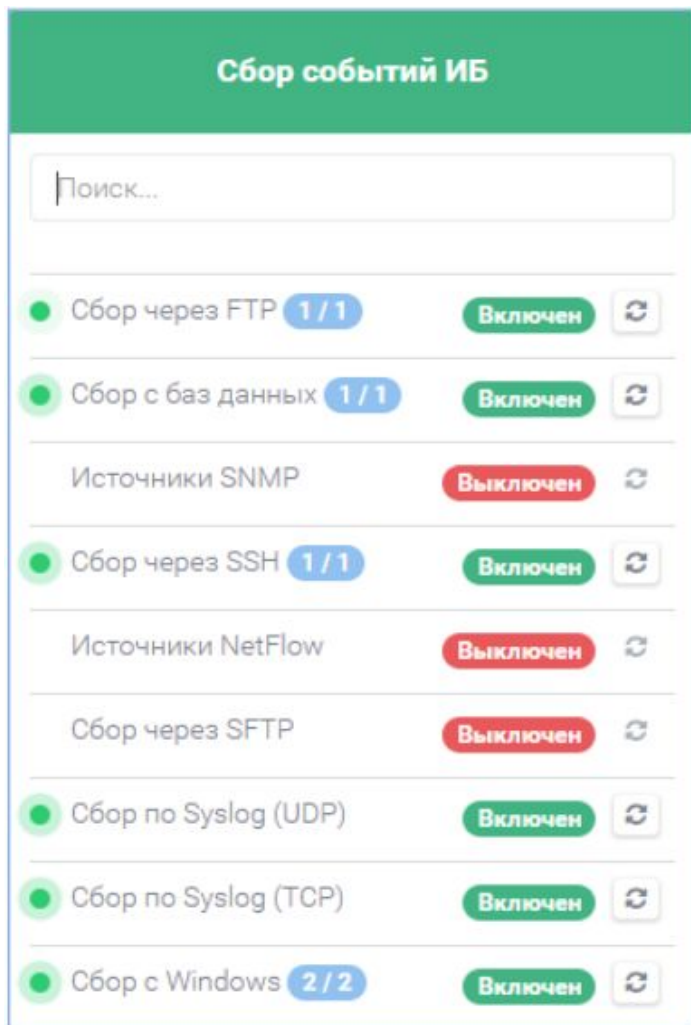
F1Help F2Setup F3Search F4Filter F5Tree F6SortBy F7Nice -F8Nice +F9Kill F10Quit

Текущие процессы от источников событий



## 3.2 Развёртывание интегрированной системы

### 3.2.6 Особенности подключения устройств



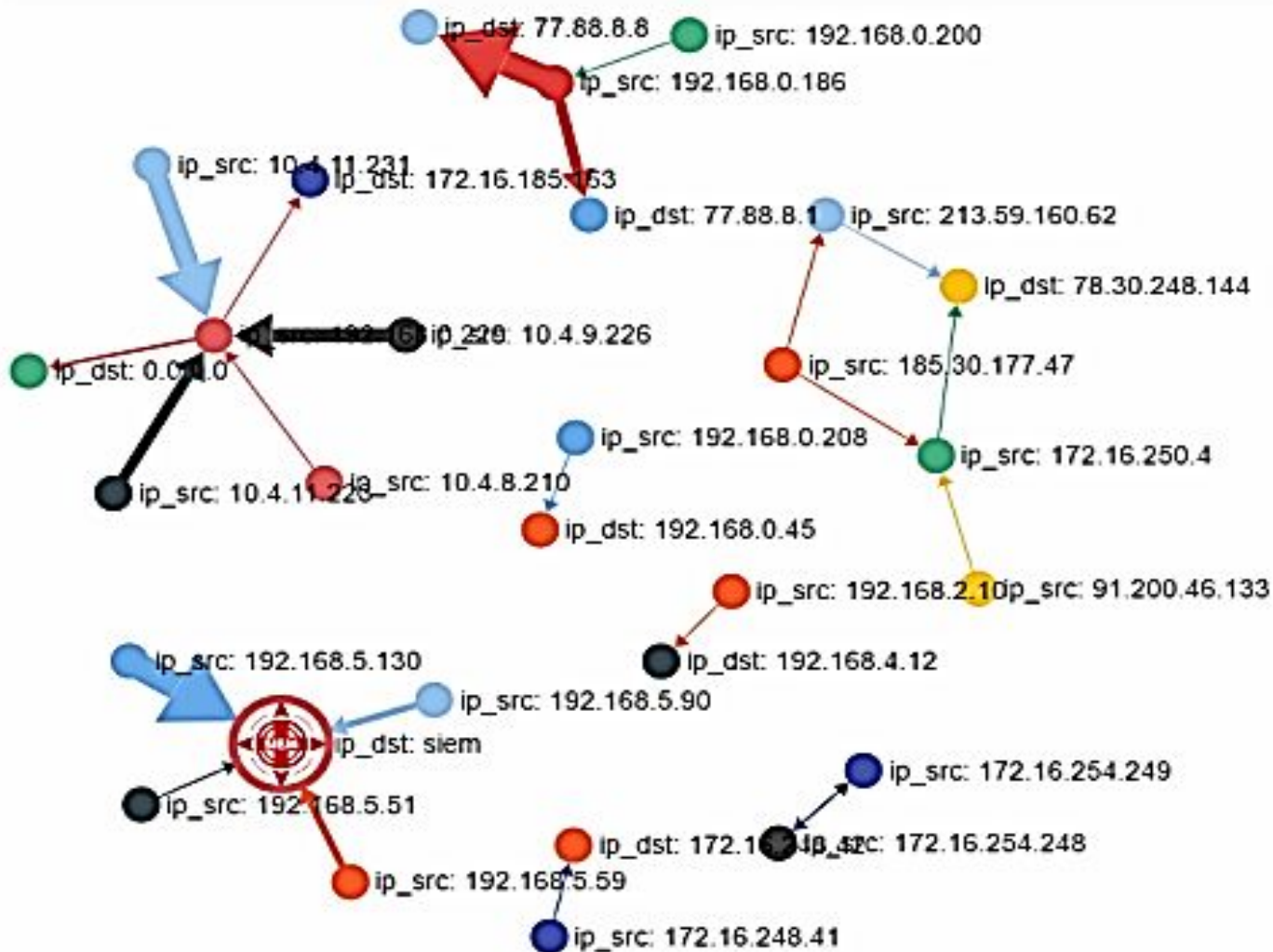
Плагины сбора	Тип сбора событий
Syslog (UDP)	Пассивный
Syslog (TCP)	Пассивный
NetFlow	Пассивный
FTP	Активный
SFTP	Активный
Базы данных	Активный
SNMP	Активный
SSH	Активный
WMI	Активный

Тип плагинов сбора событий

Список плагинов подключения  
внешних устройств

## 3.2 Развёртывание интегрированной системы

### 3.2.7 Граф подключений источников событий



Граф подключений событий



## 3.2 Развёртывание интегрированной системы

### 3.2.8 Работа модулей с внешними подключениями

```
May 7 10:23:01 komrad CRON[7612]: (root) CMD ( python /usr/share/komrad-framework/iptables_manager.py)
May 7 10:23:01 komrad CRON[7614]: (root) CMD ( python /usr/share/komrad-framework/update_authorized_keys.py && sudo -u framework cat /etc/s
May 7 10:23:01 komrad CRON[7613]: (root) CMD ( python /usr/share/komrad-framework/update_instances_api_link.py)
May 7 10:23:02 komrad systemd[1]: Stopping LSB: komrad-gambolputty-agregator.
May 7 10:23:02 komrad komrad-gambolputty-agregator[7649]: Stopping komrad-gambolputty-agregator: Traceback (most recent call last):
May 7 10:23:02 komrad komrad-gambolputty-agregator[7649]: File "/usr/sbin/komrad-gambolputty-agregator", line 34, in <module>
May 7 10:23:02 komrad komrad-gambolputty-agregator[7649]: daemon.stop()
May 7 10:23:02 komrad komrad-gambolputty-agregator[7649]: File "/usr/share/komrad-gambolputty/manager/epmanager.py", line 261, in stop
May 7 10:23:02 komrad komrad-gambolputty-agregator[7649]: self.gambolputtyStop()
May 7 10:23:02 komrad komrad-gambolputty-agregator[7649]: File "/usr/share/komrad-gambolputty/manager/epmanager.py", line 184, in gambolputtyS
May 7 10:23:02 komrad komrad-gambolputty-agregator[7649]: self.gambolputtyShutdown()
May 7 10:23:02 komrad komrad-gambolputty-agregator[7649]: File "/usr/share/komrad-gambolputty/manager/epmanager.py", line 192, in gambolputtyS
May 7 10:23:02 komrad komrad-gambolputty-agregator[7649]: self.logging.error("Could not open %s" % self.childs_file)
May 7 10:23:02 komrad komrad-gambolputty-agregator[7649]: AttributeError: epmanager instance has no attribute 'childs_file'
May 7 10:23:02 komrad systemd[1]: komrad-gambolputty-agregator.service: control process exited, code=exited status=1
May 7 10:23:02 komrad systemd[1]: Unit komrad-gambolputty-agregator.service entered failed state.
May 7 10:23:02 komrad systemd[1]: Starting LSB: komrad-gambolputty-agregator...
May 7 10:23:02 komrad komrad-gambolputty-agregator[7654]: Starting komrad-gambolputty-agregator: komrad-gambolputty-agregator.
May 7 10:23:02 komrad systemd[1]: Started LSB: komrad-gambolputty-agregator.
May 7 10:23:42 komrad systemd[1]: Stopping LSB: komrad-gambolputty-agregator...
May 7 10:23:42 komrad komrad-gambolputty-agregator[7802]: Stopping komrad-gambolputty-agregator: Traceback (most recent call last):
May 7 10:23:42 komrad komrad-gambolputty-agregator[7802]: File "/usr/sbin/komrad-gambolputty-agregator", line 34, in <module>
May 7 10:23:42 komrad komrad-gambolputty-agregator[7802]: daemon.stop()
May 7 10:23:42 komrad komrad-gambolputty-agregator[7802]: File "/usr/share/komrad-gambolputty/manager/epmanager.py", line 261, in stop
May 7 10:23:42 komrad komrad-gambolputty-agregator[7802]: self.gambolputtyStop()
May 7 10:23:42 komrad komrad-gambolputty-agregator[7802]: File "/usr/share/komrad-gambolputty/manager/epmanager.py", line 184, in gambolputtyS
May 7 10:23:42 komrad komrad-gambolputty-agregator[7802]: self.gambolputtyShutdown()
May 7 10:23:42 komrad komrad-gambolputty-agregator[7802]: File "/usr/share/komrad-gambolputty/manager/epmanager.py", line 192, in gambolputtyS
May 7 10:23:42 komrad komrad-gambolputty-agregator[7802]: self.logging.error("Could not open %s" % self.childs_file)
May 7 10:23:42 komrad komrad-gambolputty-agregator[7802]: AttributeError: epmanager instance has no attribute 'childs_file'
May 7 10:23:42 komrad systemd[1]: komrad-gambolputty-agregator.service: control process exited, code=exited status=1
May 7 10:23:42 komrad systemd[1]: Unit komrad-gambolputty-agregator.service entered failed state.
May 7 10:23:42 komrad systemd[1]: Starting LSB: komrad-gambolputty-agregator...
May 7 10:23:42 komrad komrad-gambolputty-agregator[7807]: Starting komrad-gambolputty-agregator: komrad-gambolputty-agregator.
```

Сообщение  
начале  
подключения  
системе

Сообщение  
остановке  
загрузчика

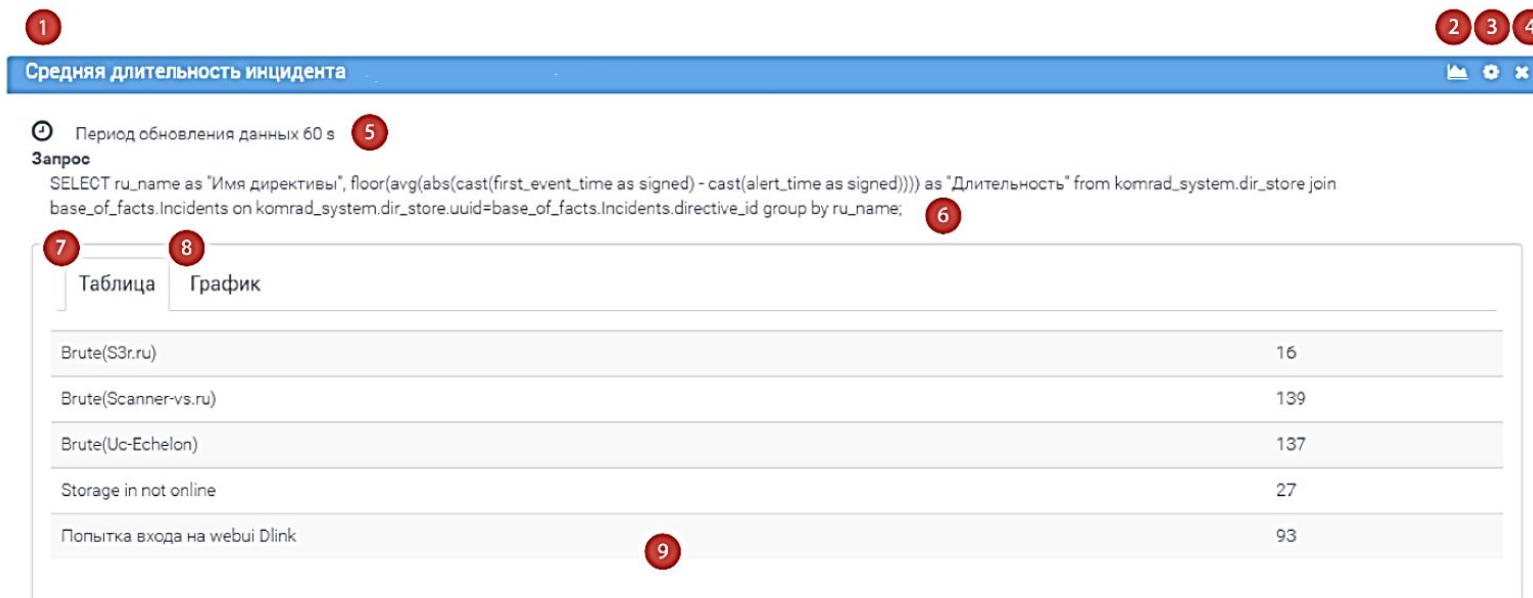
0

к

об

### Подключение устройств к интегрированной системе

### 3.3 Проведение эксперимента по проверки работоспособности интегрированной системы 3.3.1 Настройка оповещений об инцидентах



1

2 3 4

Средняя длительность инцидента

5

Период обновления данных 60 s

Запрос

```
SELECT ru_name as "Имя директивы", floor(avg(abs(cast(first_event_time as signed) - cast(alert_time as signed)))) as "Длительность" from komrad_system.dir_store join base_of_facts.Incidents on komrad_system.dir_store.uuid=base_of_facts.Incidents.directive_id group by ru_name;
```

6

7 8

Таблица График

Brute(S3r.ru)	16
Brute(Scanner-vs.ru)	139
Brute(Uc-Echelon)	137
Storage in not online	27
Попытка входа на wehui Dlink	93

9

#### Настройка оповещения об инциденте

Рабочая область запроса содержит следующие элементы:

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





### 3.3 Проведение эксперимента по проверки работоспособности интегрированной системы

#### 3.3.2 Карточка инцидента

1703

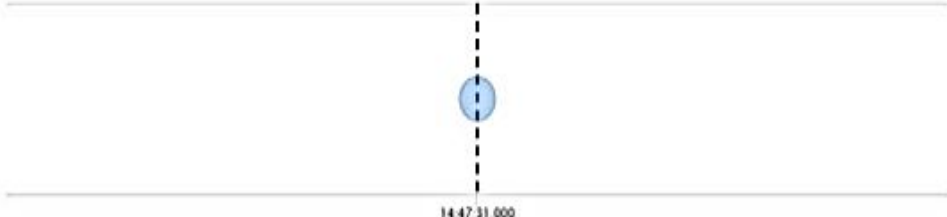
Имя директивы Brute(S3r.ru)

Риск **высокий**

Статус **Просмотрен**

Группа **Безопасность**

Уровень опасности



14:47:31.000

События История изменений

Правило: #0

ID плагина	SID плагина	Данные
40005	1	3.0.04506.648; NET CLR 3.5.21022) s3r.ru 193.201.224.220 -- "POST /wp-login.php HTTP/1.0" 503 2911 "https://s3r.ru/wp-login.php" Mozilla/4.0 (compatible; MSIE 9.0; Windows NT 6.1; 125LA; NET CLR 2.0.50727; NET CLR
40005	1	3.0.04506.648; NET CLR 3.5.21022) s3r.ru 193.201.224.220 -- "POST /wp-login.php HTTP/1.0" 503 2911 "https://s3r.ru/wp-login.php" Mozilla/4.0 (compatible; MSIE 9.0; Windows NT 6.1; 125LA; NET CLR 2.0.50727; NET CLR
40005	1	3.0.04506.648; NET CLR 3.5.21022) s3r.ru 193.201.224.220 -- "POST /wp-login.php HTTP/1.0" 503 2911 "https://s3r.ru/wp-login.php" Mozilla/4.0 (compatible; MSIE 9.0; Windows NT 6.1; 125LA; NET CLR 2.0.50727; NET CLR
40005	1	3.0.04506.648; NET CLR 3.5.21022) s3r.ru 193.201.224.220 -- "POST /wp-login.php HTTP/1.0" 503 2911 "https://s3r.ru/wp-login.php" Mozilla/4.0 (compatible; MSIE 9.0; Windows NT 6.1; 125LA; NET CLR 2.0.50727; NET CLR
40005	1	3.0.04506.648; NET CLR 3.5.21022) s3r.ru 193.201.224.220 -- "POST /wp-login.php HTTP/1.0" 503 2911 "https://s3r.ru/wp-login.php" Mozilla/4.0 (compatible; MSIE 9.0; Windows NT 6.1; 125LA; NET CLR 2.0.50727; NET CLR



### 3.3 Проведение эксперимента по проверки работоспособности интегрированной системы

#### 3.3.3 Хранилище инцидентов

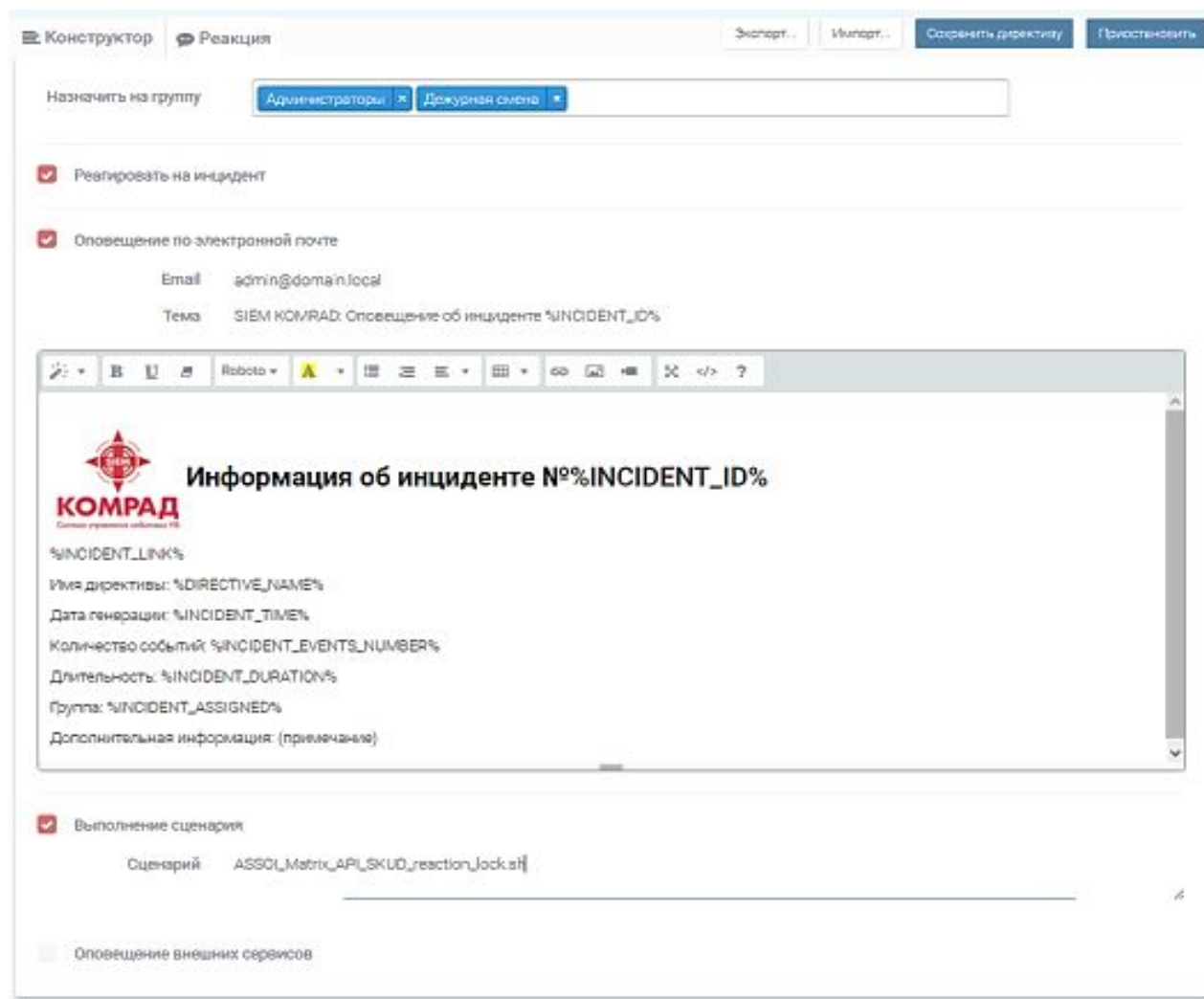
192.168.1.10

▼    
Время хранения: 30  
Время хранения архива: 15

<input type="checkbox"/>	№	Дата	Состояние	Контрольная сумма
<input type="checkbox"/>	15	27/05/2021	Текущий	0
<input type="checkbox"/>	14	26/05/2021	Только для чтения	40e710c7000bbee14cd4f8845a6c5e1ba1fff267194bd8e4cf4e19296c4b65b6
<input type="checkbox"/>	13	25/05/2021	Только для чтения	d8db40fd245838cac9753ff1931921dbc67e92893840fe8248ff6ab511b17b7c
<input type="checkbox"/>	12	22/05/2021	Только для чтения	c5c5efc1e5381a841bd84e43f6a08e58892571ee5479b9b0320512ec919c9194
<input type="checkbox"/>	11	21/05/2021	Только для чтения	56a72b1dcb6994365616b9d1fc112ecafb7083fe3f1f4fa88dbe6ed2283eff16
<input type="checkbox"/>	10	20/05/2021	Только для чтения	9dada1343c7443b25351042616b09b977aa19d9472c0cb5601bf2d2f48abb916
<input type="checkbox"/>	9	19/05/2021	Только для чтения	d819ad41a4a5411d4d765e44340245e724c3f6cf669877b611adedf7bdea1b46
<input type="checkbox"/>	8	18/05/2021	Только для чтения	bb2bf7f651a076dfafd020b7b94c059077665b940c9fee617e52179ac64d34fa
<input type="checkbox"/>	7	16/05/2021	Только для чтения	b49cdf660d01035b6942d7a477bcd8810d17706f14c408c6fa32a48a3db637df
<input type="checkbox"/>	6	15/05/2021	Только для чтения	23f9c0a5eb141acc3d191899724cbefa2127f14a52fcace2d3fe25ba06a892ad

### 3.3 Проведение эксперимента по проверки работоспособности интегрированной системы

#### 3.3.4 Меню информации об инциденте



Конструктор Реакция Экспорт... Импортировать... Сохранить директиву Проверить

Назначить на группу: Администраторы Дежурная смена

Реагировать на инцидент

Оповещение по электронной почте

Email: admin@domain.local

Тема: SIEM KOMRAD: Оповещение об инциденте %INCIDENT\_ID%

**Информация об инциденте №%INCIDENT\_ID%**

**КОМРАД**  
Система управления событиями ИС

%INCIDENT\_LINK%

Имя директивы: %DIRECTIVE\_NAME%

Дата генерации: %INCIDENT\_TIME%

Количество событий: %INCIDENT\_EVENTS\_NUMBER%

Длительность: %INCIDENT\_DURATION%

Группа: %INCIDENT\_ASSIGNED%

Дополнительная информация: (примечание)

Выполнение сценария

Сценарий: ASSOCI\_Matrix\_API\_SKUD\_reaction\_Jock.stf

Оповещение внешних сервисов



### **3.4 Оценка эффективности внедрения в учебный процесс интегрированной системы безопасности информации на основе системы управления событиями информационной безопасности Комрад 4.0**

***Спасибо  
за внимание!***