

## Развёртывание системы Kaspersky Security Center в реальной инфраструктуре

*Саяпин Никита Анатольевич*

*Приамурский государственный университет им.Шолом-Алейхема*

*Студент*

### Аннотация

В статье рассматривается опыт развёртывания и базовой настройки системы централизованного управления защитой Kaspersky Security Center 16 в инфраструктуре высшего учебного заведения. На базе гипервизора Proxmox Virtual Environment и отечественной операционной системы РЕД ОС 8.1. Описаны основные этапы подготовки инфраструктуры, установки сервера администрирования, настройки Kaspersky Web Console и интеграции клиентских рабочих станций через Kaspersky Network Agent.

**Ключевые слова:** Kaspersky Security Center, информационная безопасность, РЕД ОС, Proxmox, централизованное управление защитой, MariaDB, импортозамещение, университетская инфраструктура.

### Deploying Kaspersky Security Center system in real infrastructure

*Sayapin Nikita Anatolyevich*

*Sholom-Aleichem Priamursky State University*

*Student*

### Abstract

The article discusses the experience of deploying and basic configuration of the Kaspersky Security Center 16 centralized security management system in the infrastructure of a higher educational institution. Based on the Proxmox Virtual Environment hypervisor and the Russian RED OS 8.1 operating system, the main stages of infrastructure preparation, administration server installation, Kaspersky Web Console configuration and integration of client workstations via Kaspersky Network Agent are described.

**Keywords:** Kaspersky Security Center, information security, RED OS, Proxmox, centralized security management, MariaDB, import substitution, university infrastructure.

## 1 Введение

### 1.1 Актуальность

В современных условиях цифровизации образования и перехода на отечественное программное обеспечение особую значимость приобретает обеспечение информационной безопасности автоматизированных рабочих мест (АРМ) сотрудников и обучающихся высших учебных заведений. Рост

количества киберугроз, усложнение IT-инфраструктуры вузов и требования федерального законодательства в сфере импортозамещения обуславливают необходимость внедрения централизованных систем управления защитой.

Традиционные подходы к антивирусной защите, основанные на разрозненном управлении отдельными рабочими станциями, не позволяют оперативно реагировать на инциденты, обеспечивать единые политики безопасности и эффективно контролировать состояние парка техники. В этой связи актуальным становится внедрение профессиональных систем централизованного управления защитой, таких как Kaspersky Security Center, адаптированных под отечественные операционные системы. Опыт такого развёртывания в реальной университетской инфраструктуре представляет как научный, так и практический интерес.

## 1.2 Обзор исследований

И.А. Челядин представил программу для автоматизированной установки и настройки средств защиты информации на объектах информатизации в организации предназначена для упрощения и ускорения процессов установки и настройки средств защиты информации на объектах информатизации в организации. Это позволяет сэкономить время и ресурсы, а также минимизировать ошибки и риски при установке и настройке средств защиты информации. Программа может включать в себя модули для управления сертификатами безопасности, автоматического обновления антивирусной базы данных, контроля доступа к ресурсам сети и др [1]. М.В. Вотинов поставил перед собой цель разработки телекоммуникационных функций, позволяющих производить удалённый контроль технологического процесса, его визуализацию, а также удалённо управлять исполнительными механизмами различных технологических объектов (в данном случае - исполнительными механизмами малогабаритной сушильной установки, созданной в Мурманском государственном техническом университете для исследования процессов копчения, вяления и сушки рыбы) [2]. Н.А. Малышев подробно рассмотрел современные методы обеспечения безопасности бизнеса, уделяя практическим аспектам внедрения этих методов, таким как использование антивирусного программного обеспечения, установка систем видеонаблюдения, проведение регулярных финансовых аудитов и обучение основам безопасности [3]. И. Дегтярев в своей статье рассмотрел актуальную тему повышения безопасности корпоративных информационных систем, за счет правильной оценки специфики и принципов работы разных технологий, а также привел анализ проблем защиты конфиденциальных данных в Российской Федерации, способов сохранения корпоративной тайны и поиска причин нарушения безопасности IT-сетей [4]. М.А. Джинджинхадзе произвел выбор средств защиты информации в рамках модернизации системы управления информационной безопасностью предприятия ПАО «Иркутскэнерго». Приводится обоснование сделанного выбора. Предложены следующие меры модернизации системы информационной безопасности:

внедрение автоматизированной СКУД «Elsys»; модернизация системы видеонаблюдения; установка межсетевого экрана [5].

### **1.3 Цель исследования**

Цель исследования заключается в анализе и описании процесса развёртывания системы Kaspersky Security Center 16 в реальной инфраструктуре образовательной организации на базе гипервизора Proxmox и операционной системы РЕД ОС 8 с целью обеспечения централизованного управления информационной безопасностью АРМ сотрудников и студентов.

## **2 Материалы и методы**

Для развёртывания системы централизованного управления защитой в реальной инфраструктуре высшего учебного заведения применяется виртуализированная серверная среда на базе гипервизора Proxmox Virtual Environment. В качестве гостевой операционной системы используется отечественная ОС РЕД ОС 8 (профиль «Сервер с графическим интерфейсом»). Выбор данной платформы обусловлен требованиями программы импортозамещения и совместимостью с Kaspersky Security Center 16.

## **3 Результаты**

### **3.1 Подготовка серверной инфраструктуры на базе Proxmox и РЕД ОС 8**

Для обеспечения отказоустойчивости и удобства управления ресурсами сервер развернут в виртуальной среде. В качестве гипервизора использовался Proxmox Virtual Environment.

В интерфейсе управления Proxmox была создана новая виртуальная машина с выделением необходимых ресурсов (процессорные ядра, оперативная память, дисковое пространство), соответствующих системным требованиям KSC 16 (Рис.3).

В виртуальный CD/DVD-привод смонтирован установочный ISO-образ операционной системы РЕД ОС 8.

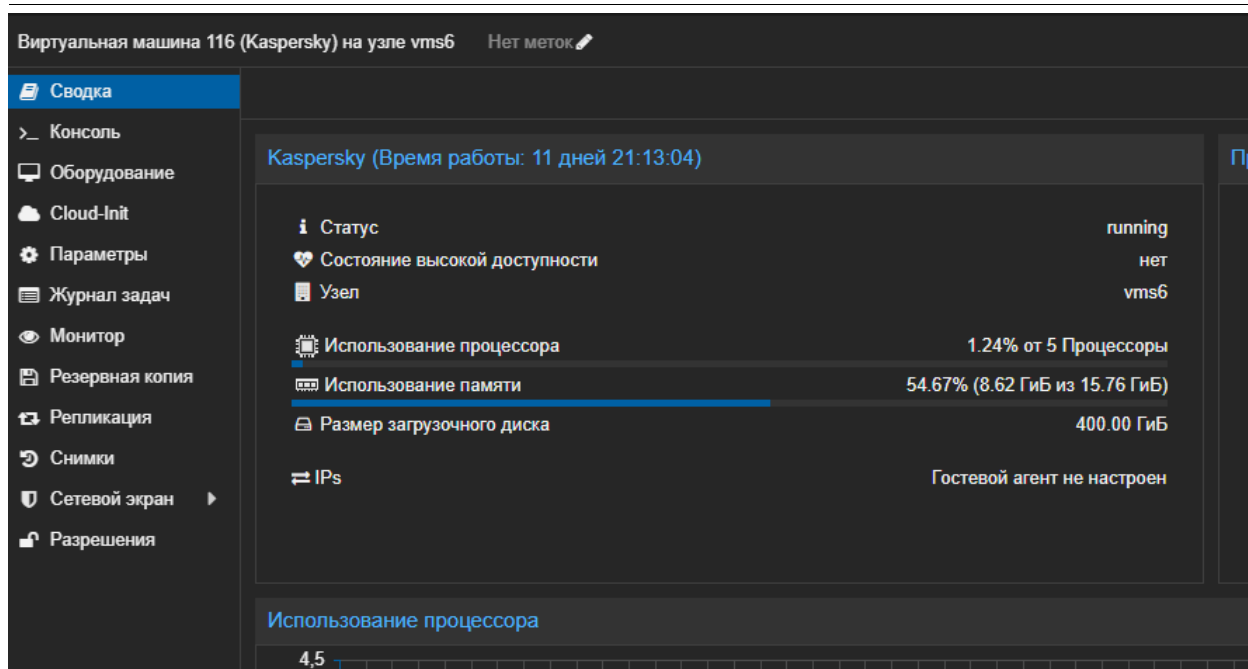


Рисунок 3 – Созданная виртуальная машина на гипервизоре

Произведена базовая установка операционной системы с выбором профиля «Сервер с графическим интерфейсом».

Выполнена настройка сетевого интерфейса: серверу назначен статический IP-адрес для обеспечения постоянного доступа к консоли управления (Рис.4).

Произведено обновление системных пакетов и установка базовых утилит администратора через пакетный менеджер.

```
[user@Ksp Рабочий стол]$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: ens18: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether bc:24:11:5e:ce:11 brd ff:ff:ff:ff:ff:ff
    altname enp0s18
    inet 172.17.16.169/28 brd 172.17.16.175 scope global noprefixroute ens18
        valid_lft forever preferred_lft forever
[user@Ksp Рабочий стол]$
```

Рисунок 4 – Настроенный статический IP-адрес сервера

### 3.2 Развертывание и базовая настройка Kaspersky Security Center 16

Перед непосредственной установкой ядра централизованного управления антивирусной защитой проведен обязательный подготовительный этап по развертыванию и настройке локальной системы управления базами данных (СУБД). В соответствии с официальной технической документацией «Лаборатории Касперского» для работы Сервера администрирования на Linux-платформе в качестве СУБД выбрана MariaDB.

Процесс подготовки начался с установки пакетов MariaDB-сервера из репозитория РЕД ОС 8, запуска соответствующей системной службы и

применения базовых политик безопасности СУБД. Затем, через консольный интерфейс MySQL, произведена настройка инфраструктуры хранения данных. Строго следуя официальной инструкции, созданы специализированные учетные записи пользователей для защищенного управления базами данных, которым назначены все необходимые привилегии. Для обеспечения отказоустойчивости и корректного разделения служебной информации Сервера администрирования созданы две отдельные базы данных (Рис.5).

```
MariaDB [(none)]> SELECT Host, User FROM mysql.user;
```

| Host      | User        |
|-----------|-------------|
| %         | iamdbadmin  |
| %         | kscdbadmin  |
| 127.0.0.1 | iamdbadmin  |
| localhost | iamdbadmin  |
| localhost | kscdbadmin  |
| localhost | mariadb.sys |
| localhost | mysql       |
| localhost | root        |

```
8 rows in set (0,001 sec)
```

Рисунок 5 – Процесс создания пользователей в консоли MariaDB

После успешной подготовки инфраструктуры баз данных инициирован процесс установки самого комплекса Kaspersky Security Center 16. На сервер загружены актуальные дистрибутивы Сервера администрирования для Linux. Запущен процесс установки из rpm-пакета, по завершении которого потребовалось выполнить скрипт первоначальной конфигурации системы. В ходе работы данного скрипта переданы параметры подключения к ранее созданным базам данных MariaDB, введены учетные данные подготовленных пользователей СУБД, а также определены сетевые порты для обмена трафиком с клиентскими агентами (Рис.6).

```
Enter the security group name for services:
kadmins

Enter the account name to start the Administration Server service. The
account must be a member of the entered security group:
ksc

Enter the account name to start other services. The account must be a
member of the entered security group:
ksc

Choose the database type to connect to:
1) MySQL
2) Postgres
Enter the range number (1 or 2):
1

Enter the database address:
127.0.0.1

Enter the database port:
3306

Enter the database name:
mariadb

Enter the database login:
root

Enter the database password:
```

Рисунок 6 – Окно терминала в процессе работы скрипта первоначальной настройки KSC с успешным подключением к БД

Завершающим шагом стала настройка веб-подключения, необходимого для удобного удаленного администрирования инфраструктуры через браузер. Для реализации этой задачи установлен отдельный компонент — Kaspersky Web Console. В конфигурации веб-консоли заданы IP-адрес сервера и порты прослушивания. После запуска службы проверена ее работоспособность и внесены корректировки в правила встроенного межсетевого экрана (firewall) РЕД ОС, разрешающие прохождение входящих соединений к веб-интерфейсу управления (Рис.7).

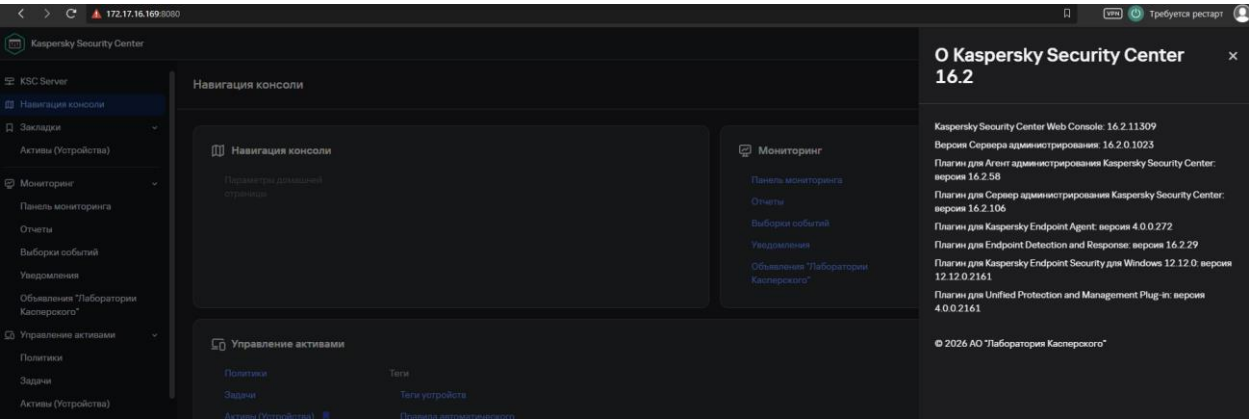


Рисунок 7 – Окно браузера с открытой страницей Kaspersky Web Console по IP-адресу сервера

3.3 Развертывание антивирусной защиты на клиентских ПК и тестирование системы

Для проверки работоспособности системы необходимо подключить клиентские АРМ к Серверу администрирования. Связующим звеном между конечным устройством и сервером выступает Агент администрирования (Kaspersky Network Agent).

В интерфейсе Kaspersky Web Console создан инсталляционный пакет Агента администрирования с указанием IP-адреса нового сервера на базе РЕД ОС.

Сформированный пакет перенесен на тестовые персональные компьютеры (выполняющие роль АРМ сотрудников/студентов) и установлен в штатном режиме (Рис.8).

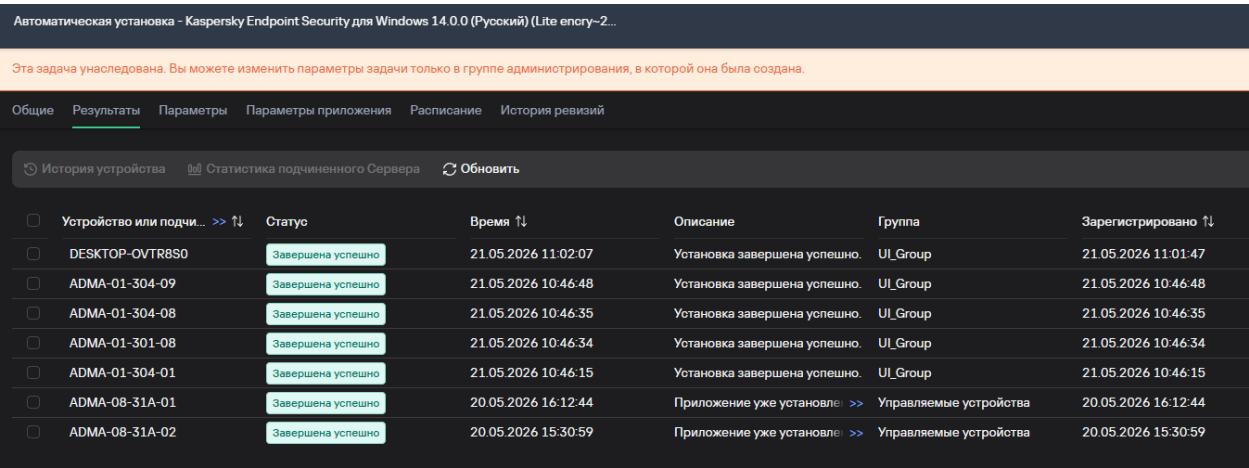


Рисунок 8 – Процесс установки Kaspersky Network Agent на клиентском ПК

После установки Агента проведена проверка сетевой связности и синхронизации:

С помощью утилиты проверки соединения (klnagchk) на стороне клиента подтвержден успешный обмен пакетами с сервером.

В веб-консоли KSC, в разделе «Нераспределенные устройства» (или в заранее созданной группе управления), появились тестовые ПК.

Зафиксирована успешная передача информации о системе (имя ПК, пользователь, статус защиты) на Сервер администрирования (Рис.9).

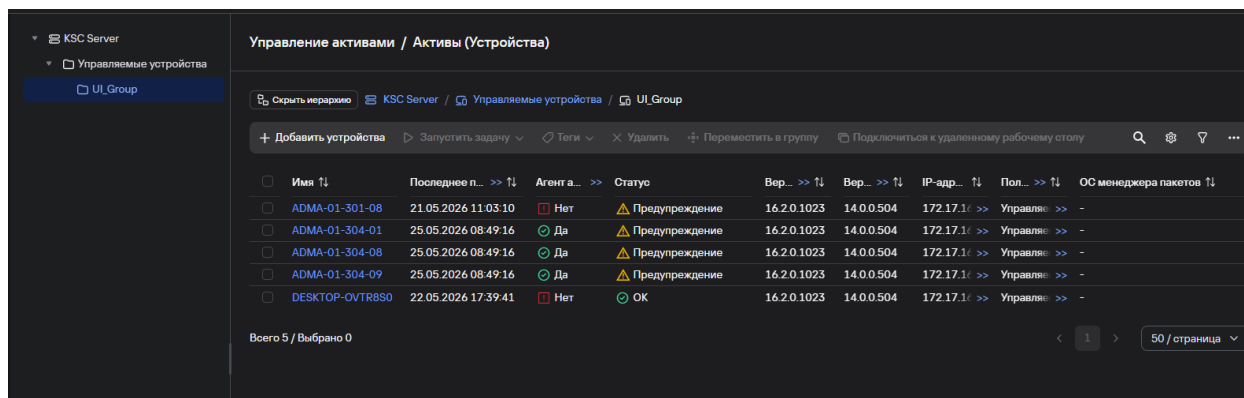


Рисунок 9 – Интерфейс Kaspersky Web Console, раздел «Устройства»

В результате проделанной работы сервер управления успешно введен в эксплуатацию, а тестирование подтвердило корректность работы канала связи между центральным узлом на базе РЕД ОС и конечными рабочими станциями.

#### 4 Выводы

В ходе исследования произведено практическое развёртывание системы централизованного управления защитой Kaspersky Security Center 16 в реальной инфраструктуре высшего учебного заведения с использованием отечественного программного обеспечения — операционной системы РЕД ОС 8 и гипервизора Proxmox Virtual Environment, что подтверждает техническую совместимость и практическую применимость данного решения в условиях импортозамещения.

Подготовительный этап настройки СУБД MariaDB и последующая установка Сервера администрирования прошли без критических затруднений при строгом следовании официальной технической документации производителя, что подчёркивает важность точного соблюдения регламентов развёртывания для систем информационной безопасности подобного класса.

Развёртывание веб-консоли Kaspersky Web Console обеспечило удобный удалённый доступ к управлению системой защиты через браузер, а корректная настройка правил межсетевого экрана РЕД ОС позволила обеспечить безопасный доступ к интерфейсу администрирования без избыточного открытия сетевых портов.

Тестирование подключения клиентских рабочих станций через Kaspersky Network Agent подтвердило корректность работы канала связи между центральным узлом на базе РЕД ОС и конечными АРМ: устройства успешно синхронизировались с Сервером администрирования, что свидетельствует о готовности развёрнутой инфраструктуры к промышленной эксплуатации в условиях университета.

Полученный практический опыт развёртывания KSC 16 на отечественной платформе может быть использован другими

образовательными организациями при переходе на импортонезависимые решения в сфере информационной безопасности, а также служит основой для дальнейшего расширения функциональности системы — настройки политик безопасности, групп управления и автоматизированных отчётов.

### Библиографический список

1. Челядин И. А. Свидетельство о государственной регистрации программы для ЭВМ № 2023662080 Российская Федерация. Программное обеспечение автоматизированной установки и настройки средств защиты информации на объектах информатизации в организации: № 2023661024: заявл. 29.05.2023: опубли. 06.06.2023.
2. Вотин М. В. Особенности построения Web-приложений информационного обеспечения систем автоматического управления // Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика. 2017. № 3. С. 40-47.
3. Малышев Н. А. Методы обеспечения безопасности бизнеса // Управление экономикой, системами, процессами. Сборник статей VIII Международной научно-практической конференции, Пенза, 14–15 октября 2024 года. Пензенский государственный аграрный университет, 2024. С. 312-314.
4. Дегтярев И. Современные методы обеспечения безопасности корпоративных it-систем: практика и технологии // Международный журнал гуманитарных и естественных наук. 2025. № 1-3(100). С. 115-118.
5. Джинджихадзе М. А. Выбор средств защиты в рамках модернизации системы управления информационной безопасностью предприятия // Молодой исследователь: вызовы и перспективы. Сборник статей по материалам CCCXLIII международной научно-практической конференции, Москва, 06 февраля 2024 года. Москва: ООО "Интернаука". 2024. С. 151-165.