УДК 004.453.4

CYBERLAB MANAGEMENT TOOL ДЛЯ АВТОМАТИЗАЦИИ ОБРАЗОВАТЕЛЬНОГО КИБЕРПОЛИГОНА

БЕЛОУСОВА ЕЛЕНА СЕРГЕЕВНА
к.т.н., доцент кафедры защиты информации
Белорусского государственного университета информатики и радиоэлектроники (БГУИР),
Минск, Беларусь

ВЕРБИЛО НИКОЛАЙ АЛЕКСАНДРОВИЧ
учащийся учреждения образования «Национальный детский технопарк» (УО НДТП),
Минск, Беларусь

ФИЛИППОВ АНДРЕЙ СЕРГЕЕВИЧ
учащийся учреждения образования «Национальный детский технопарк» (УО НДТП),
Минск, Беларусь

Аннотация: *В статье рассматривается вопрос важности развития знаний и навыков у учащихся средних и высших учебных заведений в области информационной безопасности посредством использования тренировочных стендов, киберполигонов. При этом актуальным является их автоматизация, доступность и масштабируемость, что требует дополнительного программного обеспечения. Авторами разработана и рекомендуется к использованию программа для автоматизации образовательного киберполигона CyberLab Management Tool, которая предоставляет удобный графический интерфейс для быстрой установки и обновления виртуальных машин образовательного киберполигона. CyberLab Management Tool может быть использован преподавателями и учащимися для обучения методам реализации, обнаружения и предотвращения кибератак.*

Ключевые слова: *автоматизированная система управления, виртуализация, кибератаки, киберполигон, VirtualBox, CyberLab, Cloudflare*

В условиях стремительного роста киберугроз и цифровизации всех сфер жизни, формирование навыков информационной безопасности становится важным уже на уровне среднего и высшего образования. Киберполигоны – виртуальные тренировочные среды, имитирующие реальные сценарии кибератак и защиты, представляют собой мощный инструмент для подготовки будущих специалистов.

Однако широкое распространение киберполигонов сталкивается с рядом инфраструктурных и методических особенностей. Одной из них является хранение и распространение преднастроенных образов виртуальных машин, необходимых для симуляции сценариев. Эти образы, как правило, имеют значительный объём, требуют согласованной версии гипервизора, и часто не масштабируются без потери целостности конфигурации. В условиях ограниченных ресурсов учебных заведений, ручное управление такими средами становится неэффективным и подверженным ошибкам.

Для решения этих задач был разработан CyberLab Management Tool (CLMT) – автоматизированная система управления виртуальной средой образовательного киберполигона. CLMT обеспечивает централизованное хранение и развертывание виртуальных машин, удобство использования преподавателями и учащимися, что позволяет внимательнее сосредоточиться на содержательной части обучения. Депонируемый объект «Программа для автоматизации образовательного киберполигона CyberLab Management Tool» внесен в Реестр компьютерных программ Национального центра интеллектуальной собственности Республики Беларусь [1]. CyberLab Management Tool доступен для скачивания на ресурсах [2–3].

Хранение образов виртуальных машин на платформе Cloudflare R2 представляет собой рациональное решение для задач, связанных с распространением образов виртуальных машин. В отличие от аналогичных облачных хранилищ, таких как Amazon S3 или Google Cloud Storage, выбранная платформе Cloudflare R2 предлагает модель без платы за исходящий трафик, что существенно снижает расходы при массовой раздаче данных, особенно в случаях, когда образы распространяются среди большого числа пользователей или учебных учреждений. Это преимущество становится особенно значимым при организации киберполигонов, где требуется регулярное обновление и загрузка преднастроенных виртуальных машин на локальные устройства или в виртуальные среды. Интеграция с CDN-слоем Cloudflare обеспечивает низкую латентность и географически распределенный доступ, позволяя пользователям из различных регионов получать доступ к образам без задержек и перегрузки канала.

При установке киберполигона критически важно корректно сконфигурировать сеть между виртуальными машинами. Ошибки в маршрутизации, неправильное распределение IP-адресов или неверная конфигурация межсетевых экранов могут привести к нарушению логики DMZ или полной недоступности отдельных компонентов инфраструктуры. Особенно важно обеспечить изоляцию внутренних сегментов от внешнего трафика, соблюдая принципы минимизации доверия и четкого разграничения зон. Неправильная настройка может не только исказить учебный или тестовый сценарий, но и создать риски при подключении к реальным сетям. Поэтому сеть внутри образовательного киберполигона полностью изолирована от сети устройства на котором он запущен.

CLMT реализован на Python 3.12 и распространяется как в виде исходных файлов, так и в виде автономных бинарных сборок для Windows, Linux и macOS. Точка входа в приложение объединяет графический интерфейс (GUI), построенный на PyQt6, и интерфейс командной строки (CLI), что позволяет использовать CLMT как интерактивный инструмент (рисунок 1), так и интегрировать его в автоматизированные сценарии. Такое объединение стало возможным благодаря объектно-ориентированному подходу и чистой архитектуре, обеспечивающей чёткое разделение логики, интерфейсов и конфигурационных слоёв. Программа поставляется вместе с YAML-файлом конфигурации, в котором описан каждый узел киберполигона: имя виртуальной машины, название соответствующего образа на Cloudflare R2, контрольная сумма для верификации и параметры сетевой конфигурации. Это позволяет точно воспроизводить инфраструктуру и гарантировать согласованность между компонентами при развертывании.

CLMT использует VBoxManage, консольную утилиту командной строки, входящую в состав Oracle VirtualBox, для программного управления виртуальными машинами. В отличие от графического интерфейса VirtualBox CLMT характеризуется следующими функциями:

1 Автоматизация вызовов VBoxManage на основе правил, заданных в конфигурационном файле.

2 Стандартизация выполнения операций с виртуальными машинами.

3 Абстракция сложных команд VBoxManage в простые инструкции.

CLMT предоставляет основные механизмы автоматизации: автономную установку, запуск и остановку в соответствии с правилами, а также контроль киберполигона через систему снимков состояния.

Процесс установки виртуальных машин в CLMT представляет собой последовательность автоматизированных этапов, обеспечивающих загрузку, импорт и настройку виртуальных сред для образовательного киберполигона. Данный механизм учитывает требования к надежности и эффективности, что позволяет минимизировать участие пользователя и снизить вероятность возникновения ошибок.

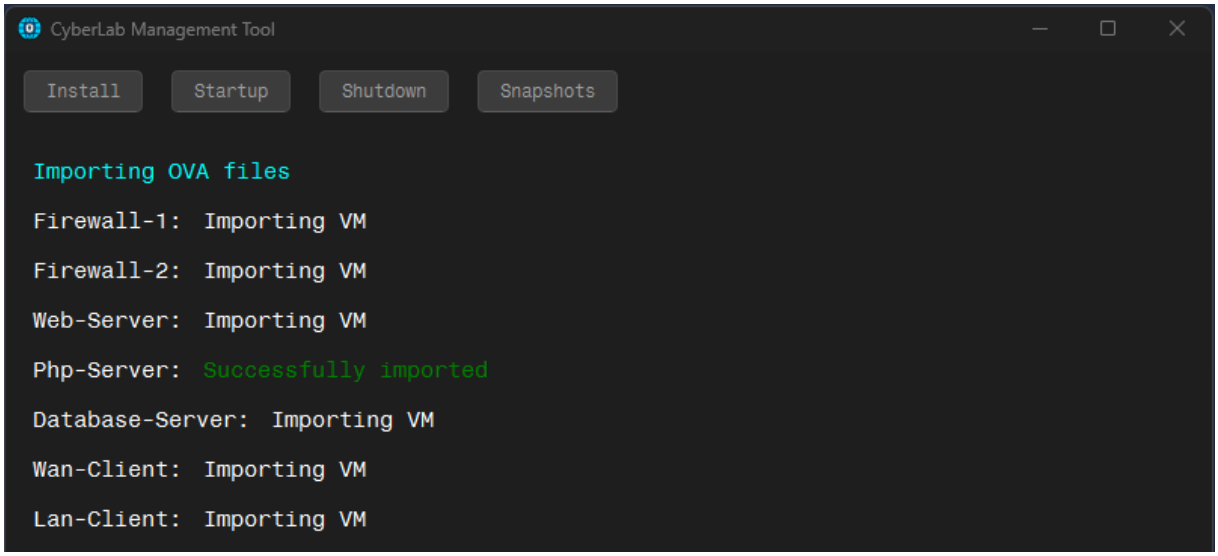

Рисунок 1 – Графический интерфейс CyberLab Management Tool

Процесс установки образовательного киберполигона включает следующие этапы:

1 При первичном запуске CLMT анализирует наличие импортированных виртуальных машин. Если виртуальная машина отсутствует в VirtualBox, интерфейс отображает статус “vm is not installed” для каждого компонента (например, “Web-Server: vm is not installed”).

2 Пользователь активирует процесс установки через интерфейсную кнопку “Install”, после чего CLMT начинает поочередную загрузку OVA-образов из Cloudflare S3. В процессе загрузки интерфейс динамически обновляется: текстовые статусы заменяются визуальными индикаторами прогресса, где завершенная загрузка отображается как “vm is downloaded”.

3 После завершения загрузки образов система приступает к их параллельному импорту в VirtualBox. Каждая виртуальная машина обрабатывается индивидуально, и интерфейс отображает статус каждой операции: например, сообщение “Web-Server: Importing VM” указывает на начало процесса, тогда как “Firewall-2: Successfully imported” подтверждает его успешное завершение. Для обеспечения прозрачности работы и удобства диагностики проблем в CLMT реализована система логирования импорта. Файлы логов сохраняются в директорию, указанную в конфигурационном файле.

4 Когда импорт завершен, CLMT останавливает все виртуальные машины, переводя их в состояние «vm is stopped», означающее готовность к запуску.

Помимо графического интерфейса, CLMT предоставляет возможность установки виртуальных машин через командную строку с использованием команды cli install. Этот режим поддерживает специализированные флаги для гибкого управления процессом: флаг --no-verify отключает проверку контрольных сумм (хешей) OVA-файлов. Флаг --skip-download исключает этап загрузки образов из сети и применяется, когда OVA-файлы уже находятся в локальном хранилище, в таком случае CLMT сразу приступает к импорту виртуальных машин в VirtualBox, экономя время и сетевой трафик.

Установка образовательного киберполигона посредством CLMT завершается полной интеграцией виртуальных машин в среду VirtualBox (рисунок 2). После завершения процесса они становятся доступны из графического интерфейса, а их файлы сохраняются в директорию vms, расположенной рядом с исполняемым файлом CLMT. Этот путь задан в конфигурации по умолчанию, но может быть изменен при необходимости. В результате весь комплекс виртуальных машин готов к дальнейшему использованию без дополнительных ручных операций.

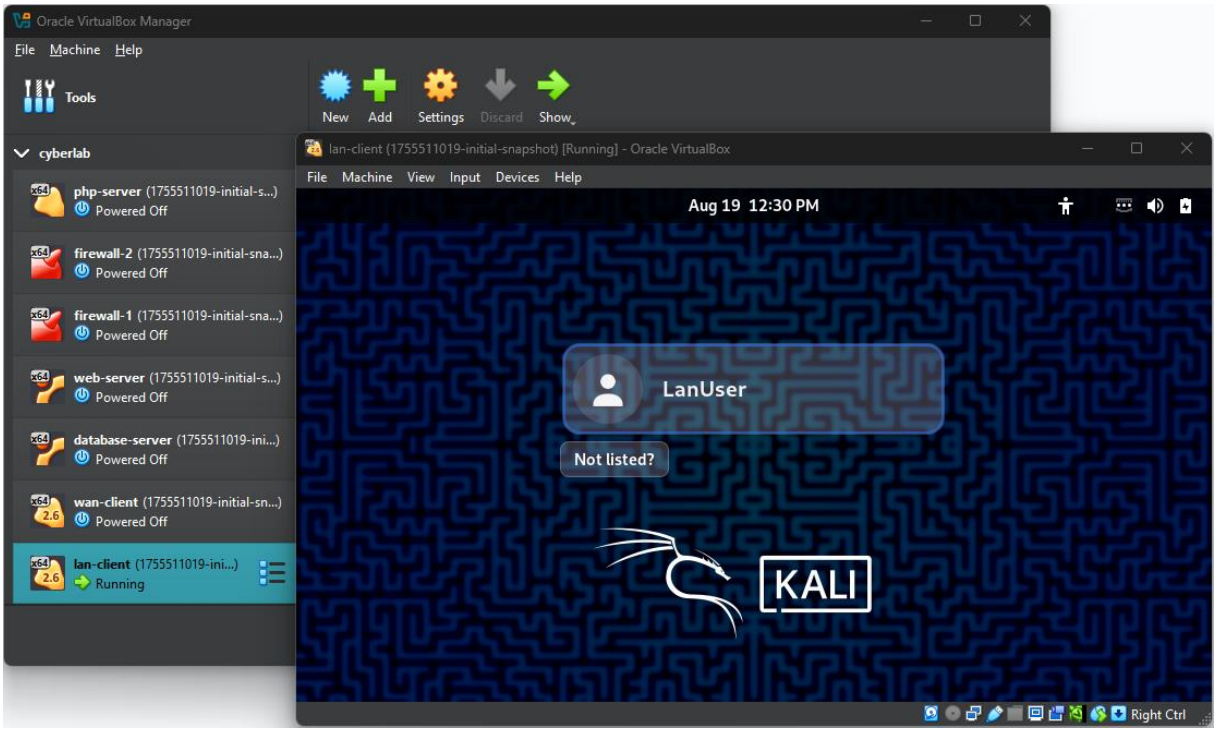

Рисунок 2 – Установленные виртуальные машины в интерфейсе VirtualBox

Анализ практического применения CLMT позволил выделить следующие уровни системных требований: минимальный, обеспечивающий базовую работоспособность приложения, и рекомендуемый, способствующий достижению оптимального пользовательского опыта при взаимодействии с образовательным киберполигоном [3].

Минимальные системные требования:

1 Оперативная память: не менее 8 GB RAM.

2 Центральный процессор: 4 физических ядра и 8 логических потоков.

3 Дисковое пространство: от 70 GB.

4 Операционная система: 64-разрядные версии Windows, Linux или macOS.

5 Поддержка виртуализации: наличие VirtualBox версии 6.0 и выше, активированная VT-x или AMD-V в BIOS.

Рекомендуемые системные требования:

1 Оперативная память: от 16 GB RAM.

2 Центральный процессор: 6 физических ядер и 12 логических потоков.

3 Дисковое пространство: от 80 GB.

Данные системные требования обеспечивают стабильную работу как CLMT, так и образовательного киберполигона. Виртуальные машины запускаются и функционируют надежно, не вызывая сбоев при одновременной нагрузке. Дисковое пространство позволяет сохранять снимки состояния, что позволяет быстро восстановить виртуальную среду после изменений или ошибки. Так достигается удобство и устойчивость образовательного киберполигона в условиях активной эксплуатации.

Авторами статьи продолжается работа над развитием и совершенствованием образовательного киберполигона. Ведутся работы по созданию различных сценарий по реализации кибератак, их обнаружению и предотвращению. На ресурсе [5] осуществляется добавление сценариев, подсказок для их прохождения.

Таким образом, разработанный киберполигон и программа для его автоматизации CyberLab Management Tool рекомендуются к использованию в средних и высших учебных заведениях с целью профориентации и подготовки будущих специалистов в области информационной безопасности и защиты информации. Также киберполигон CyberLab может

быть рекомендован для личного использования для развития и совершенствования навыков обнаружения и предотвращения кибератак в сетевой инфраструктуре.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Реестр компьютерных программ Национального центра интеллектуальной собственности Республики Беларусь [Электронный ресурс]. – Режим доступа: https://search.ncip.by/depon/index.php?pref=1&lng=ru&page=3&target=2315. Дата доступа: 06.09.2025.
2. Release v2.0.1 – CyberLab Management Tool [Электронный ресурс]. – Режим доступа: https://github.com/nickolay3132/cyberlab/releases/tag/v2.0.1. Дата доступа: 06.09.2025.
3. CyberLab Releases [Электронный ресурс]. – Режим доступа: https://techno-cyber-lab.store/download. Дата доступа: 06.09.2025.
4. System Requirements [Электронный ресурс]. – Режим доступа: https://github.com/nickolay3132/cyberlab?tab=readme-ov-file#2-%EF%B8%8F-system-requirements. Дата доступа: 06.09.2025.
5. Training Scenarios [Электронный ресурс]. – Режим доступа: https://techno-cyber-lab.store/scenarios. Дата доступа: 06.09.2025.