УДК 004.056

РАЗРАБОТКА ПРОГРАММНОЙ СРЕДЫ УЧЕБНО-ТРЕНИРОВОЧНОГО КИБЕРПОЛИГОНА

Куц Дмитрий Владимирович, старший преподаватель Учебно-научного центра «Информационная безопасность» Уральского федерального университета имени первого Президента России Б.Н. Ельцина

Поршнев Сергей Владимирович, доктор технических наук, профессор, директор Учебно-научного центра «Информационная безопасность» Уральского федерального университета имени первого Президента России Б.Н. Ельцина

Куц Мария Петровна, преподаватель кафедры Иностранных языков и образовательных технологий Уральского федерального университета имени первого Президента России Б.Н. Ельцина

Аннотация

В статье проводится анализ проблемы оптимизации образовательного процесса в сфере подготовки специалистов по информационной безопасности путём применения созданной программной среды учебно-тренировочного киберполигона. Использование киберполигонов позволяет обеспечить комплексное развитие профессиональных компетенций в сфере информационной безопасности в РФ, направленное на формирование у обучающихся, специалистов и руководителей направлений информационной безопасности и информационных технологий практических навыков защиты от киберугроз и компьютерных атак, повышение безопасности программных и аппаратных компонентов информационной и промышленной автоматизированной инфраструктуры российских организаций, включая программные продукты из Единого реестра российских программ для ЭВМ. Кроме этого, применение киберполигонов способствует совершенствованию организационно-методической базы организаций. В работе авторы реализовали свои идеи структуры киберполигона, его программной реализации и наполнения учебно-методическими материалами. Разработанный киберполигон предназначен для отработки практических навыков в работе со средствами защиты, изучения инструментов и методик атакующих воздействий на информационную инфраструктуру, администрирования подсистемы безопасности операционных систем, работы с файловыми системами.

КЛЮЧЕВЫЕ СЛОВА: киберполигон, информационная безопасность, виртуальная инфраструктура, Proxmox, кибербезопасность, KVM, LXC, Astra Linux.

DEVELOPMENT OF A SOFTWARE ENVIRONMENT FOR AN EDUCATIONAL AND TRAINING CYBERPOLYGON

Kuts Dmitry Vladimirovich, senior teacher of the Training and Scientific Center “Information Security”, Ural Federal University named after the first President of Russia B.N. Yeltsin

Porshnev Sergey Vladimirovich, Doctor of Technical Sciences, Full Professor, Head of Unit, Training and Scientific Center “Information Security”, Ural Federal University named after the first President of Russia B.N. Yeltsin

Kuts Maria Petrovna, teacher of the Department of Foreign Languages and Educational Technologies, Ural Federal University named after the first President of Russia B.N. Yeltsin

Abstract

The article analyzes the problem of optimizing the educational process in the field of training information security specialists through the use of the created software environment of the cyberpolygon training center. The use of cyber polygons allows for the comprehensive development of professional competencies in the field of information security in the Russian Federation, aimed at developing students, specialists and managers of information security and information technology areas with practical skills in protecting against cyber threats and computer attacks, improving the security of software and hardware components of information and industrial automated infrastructure of Russian organizations, including software products from the Unified Register of Russian computer programs. In addition, the use of cyber polygons contributes to the improvement of the organizational and methodological base of organizations. In the work, the authors implemented their

ideas of the cyberpolygon structure, its programmatic implementation and filling with educational and methodological materials. The developed cyberpolygon is designed to develop practical skills in working with security tools, study tools and techniques for attacking information infrastructure, administer the security subsystem of operating systems, and work with file systems.

KEYWORDS: cyberpolygon, information security, virtual infrastructure, Proxmox, cybersecurity, KVM, LXC, Astra Linux.

Введение

В современных реалиях Российская Федерация (РФ) сталкивается с беспрецедентным ростом числа кибератак и киберугроз. Согласно оценке центра исследования киберугроз *Solar* 4*RAYS* РФ находится на втором месте в мире после США по количеству проведенных против нее кибератак [1]. При этом возможности и количество инструментов, используемых злоумышленником для проведения кибератак постоянно возрастает. Отметим, что в последние несколько лет эффективность и результативность кибератак, благодаря применению на различных этапах атаки технологий искусственного интеллекта, существенно возросла [2]. В этой связи, очевидна необходимость своевременной переподготовки и повышения квалификации сотрудников служб информационной безопасности, одним из подходов для реализации которых, как показывает практика, для реализации которых одним из эффективных подходов основан на использовании киберполигонов – программно аппаратных комплексов, позволяющих создавать цифровые двойники компьютерных сетей и моделировать компьютерные атаки на них.

Отметим, что создание и совершенствование компьютерных полигонов для задач информационной безопасности представляет собой сложную и многогранную проблему, привлекающую внимание исследователей по всему миру. В условиях стремительной цифровизации всех сфер общественной жизни и параллельного роста изощренности киберугроз, разработка эффективных инструментов моделирования и анализа атак становится критически важной задачей. Современные научные работы в этой области охватывают широкий спектр вопросов – от фундаментальных принципов построения киберполигонов до узкоспециализированных методик генерации тестовых нагрузок, а также разработки методик использования киберполигонов в процессе подготовки специалистов в области компьютерной безопасности.

В настоящее время Уральский федеральный университет ведёт подготовку специалистов по специальностям бакалавриата 10.03.01 «Безопасность компьютерных систем», специалитета 10.05.04 Информационно-аналитические системы безопасности, 10.05.01 Компьютерная безопасность и 10.05.02 Информационная безопасность

телекоммуникационных систем, магистратуры 10.04.01 Защита информации в ИСПДн, ГИС и значимых объектах КИИ. Образовательные стандарты по этим специальностям представлены в [3–7]. Федеральный государственный образовательный стандарт на специальность 10.05.01 Компьютерная безопасность для ряда специализаций предусматривает оснащение образовательной организации аудиторией учебно-тренировочных средств моделирования информационно-коммуникационной среды (киберполигон) [5]. Создание киберполигонов является приоритетной задачей в рамках федерального проекта «Информационная безопасность» в рамках национальной программы «Цифровая экономика» [8]. Их цель — обучение и тренировка студентов, ИТ-специалистов, экспертов и руководителей современным методам защиты информации. Выполнение мер защиты информации из приказов ФСТЭК [9-12] подразумевает их комплексное применение на объектах инфраструктуры, что можно эффективно моделировать на виртуальной или смешанной инфраструктуре киберполигона.

Основные подходы к архитектуре киберполигонов

На текущем этапе развития технологий информационной безопасности сформировалось несколько ключевых подходов к архитектуре киберполигонов. Виртуализированные среды, основанные на технологиях контейнеризации и программно-определяемых сетях, позволяют создавать гибкие и масштабируемые платформы для моделирования сложных инфраструктур. Гибридные решения, сочетающие физическое оборудование с виртуальными компонентами, обеспечивают необходимый баланс между реалистичностью и управляемостью экспериментальной среды. Особый интерес представляют распределенные киберполигоны, которые дают возможность изучать межсетевые взаимодействия и отрабатывать сценарии защиты территориально-распределенных систем.

Основные подходы для построения киберполигона изложены в [13]. Предложена структурная схема элементов киберполигона и их взаимодействия. Предложена реализация виртуальной инфраструктуры полигона. В работе [14] обосновано применение операционной системы *Linux* для создания сетевой инфраструктуры цифровых двойников. Проблема решается с помощью технологий эмуляции и виртуализации на базе *KVM* и *Open vSwitch* (*OVS*). Работа [15] заключается в представлении сетевой инфраструктуры сложного объекта в виде ориентированного графа, в описании целевой функции как множества маршрутов на графе и систематизации кибератак в виде унарных операций над графом.

Важнейшим аспектом функционирования киберполигонов является генерация тестового трафика, которая должна максимально точно воспроизводить характеристики реальных сетевых взаимодействий. Современные методики включают сложные алгоритмы статистического моделирования, учитывающие временные закономерности, сезонные колебания и специфику различных протоколов. Особое внимание уделяется поведенческим моделям, которые позволяют имитировать действия реальных пользователей и тем самым повышают достоверность тестирования систем защиты.

В рамках исследования [16] разработан научно-методический подход к созданию имитационных моделей сетевой инфраструктуры для специализированных киберполигонов в области информационной безопасности. Разработанный инструментарий позволяет формировать интерактивные сетевые среды, максимально приближенные к реальным условиям эксплуатации информационных систем и телекоммуникационных сетей. Основное назначение предлагаемого решения заключается в повышении уровня защищенности критически важных объектов информационной инфраструктуры за счет комплексного тестирования систем защиты информации. Методика обеспечивает выявление потенциальных уязвимостей защитных механизмов на ранних стадиях посредством их всесторонней проверки в контролируемых условиях киберполигона. Такой подход позволяет моделировать различные сценарии компьютерных атак и оценивать эффективность применяемых средств защиты в условиях, приближенных к реальной эксплуатации, но без риска для работоспособности действующих информационных систем. Реализация данной методики на практике способствует своевременному обнаружению и устранению слабых мест в системах информационной безопасности до момента их эксплуатации в реальных условиях, что существенно снижает вероятность успешных кибератак на защищаемые объекты.

Не менее сложной задачей является моделирование атакующих воздействий. Современные киберполигоны используют детализированные сценарии, основанные на тактиках и техниках из общепризнанных матриц типа *MITRE ATT&CK*. Особую ценность представляют алгоритмы генерации полиморфных вредоносных нагрузок, которые позволяют тестировать системы на устойчивость к сложным, эволюционирующим угрозам. Все более востребованными становятся методики моделирования продолжительных целевых атак (*APT*), требующие комплексного подхода к воспроизведению всех этапов кибератаки – от разведки до достижения конечных целей. Исследование [17] посвящено комплексному анализу технологических и методологических аспектов организации киберполигонов как

инновационного инструмента обеспечения кибербезопасности. Основной фокус исследования направлен на системное изучение архитектурных решений и функциональных возможностей киберполигонов, позволяющих моделировать сложные киберугрозы и отрабатывать методы противодействия им в контролируемой среде.

Несмотря на значительный прогресс в области построения киберполигонов, остается ряд нерешенных проблем. Одной из наиболее сложных является поиск оптимального баланса между реалистичностью моделируемой среды и возможностями контроля и воспроизводимости экспериментов. Серьезной задачей остается масштабирование киберполигонов для моделирования крупных инфраструктур, характерных для современных предприятий и государственных учреждений. Особую актуальность приобретает разработка унифицированных метрик оценки эффективности систем защиты, которые позволяли бы сравнивать результаты, полученные на разных платформах.

Перспективные направления исследований в этой области связаны с интеграцией передовых технологий искусственного интеллекта, которые могут значительно повысить адаптивность и интеллектуальность систем моделирования. Большие надежды возлагаются на развитие стандартизированных платформ, которые позволили бы объединить усилия различных исследовательских групп и создать общее пространство для обмена методиками и результатами. Особое значение приобретает разработка специализированных решений для критически важных инфраструктур, где требования к достоверности моделирования особенно высоки.

Развитие технологий киберполигонов требует тесного взаимодействия специалистов из разных областей – компьютерных наук, криптографии, теории информации, психологии и многих других. Только комплексный, междисциплинарный подход позволит создать инструменты, адекватные современным вызовам в сфере информационной безопасности. Особую важность приобретает разработка унифицированных стандартов и методологий, которые обеспечат сопоставимость результатов исследований и позволят эффективно использовать накопленные знания для противодействия постоянно эволюционирующим киберугрозам.

Выбор платформы виртуализации киберполигона

При проектировании киберполигона ключевым вопросом становится выбор программной платформы, способной обеспечить требуемый уровень гибкости, производительности и масштабируемости. Среди множества доступных решений *Proxmox Virtual Environment* (*VE*) представляет собой наиболее сбалансированный вариант,

сочетающий в себе мощные возможности виртуализации с удобством управления и экономической эффективностью.

Proxmox VE базируется на двух фундаментальных технологиях виртуализации – *KVM* (*Kernel-based Virtual Machine*) для полной виртуализации и *LXC* для контейнеризации. Такая двойственная архитектура позволяет создавать сложные гетерогенные среды, где тяжеловесные виртуальные машины с различными операционными системами (*Windows, Linux* и др.) соседствуют с легковесными контейнерами, что особенно важно при моделировании современных корпоративных инфраструктур.

Ядро системы построено на доверенной платформе *Debian Linux* с долгосрочной поддержкой, что обеспечивает стабильность работы и безопасность. В отличие от многих коммерческих решений, *Proxmox* не требует дорогостоящих лицензий для базового функционала, при этом предлагая корпоративный уровень надежности.

Основным достоинством *Proxmox VE* является его универсальность. Платформа поддерживает все основные функции, необходимые для киберполигона:

- создание сложных сетевых топологий через встроенный менеджер сетей;
- поддержка распределенного хранилища (*Ceph, ZFS, NFS* и др.);
- возможность кластеризации для горизонтального масштабирования;
- встроенная система резервного копирования.

Особого внимания заслуживает веб-интерфейс управления, который предоставляет единую точку контроля над всей инфраструктурой. В отличие от решений типа *VMware vSphere*, требующих дополнительных компонентов для полноценной работы, Proxmox из коробки предлагает комплексный инструмент управления виртуальными машинами, контейнерами, хранилищами и сетями.

С финансовой точки зрения *Proxmox VE* представляет собой исключительно выгодное решение. Бесплатная версия содержит весь необходимый функционал для построения полноценного киберполигона. Коммерческая подписка, доступная по разумной цене, добавляет техническую поддержку и доступ к стабильным репозиториям обновлений, что может быть важно для корпоративных пользователей.

Proxmox прекрасно интегрируется с другими компонентами киберполигона:

- поддерживает работу с инструментами оркестрации (*Ansible, Terraform*);
- позволяет развертывать системы мониторинга (*Zabbix, Prometheus*);
- совместим с большинством *SIEM*-решений;

- обеспечивает взаимодействие с системами генерации трафика.

Выбор *Proxmox VE* в качестве базовой платформы для киберполигона обеспечивает оптимальное сочетание производительности, гибкости и экономической эффективности. Его открытая архитектура, поддержка различных технологий виртуализации и мощные возможности управления делают его идеальным решением для создания реалистичных учебных и тестовых сред в области информационной безопасности. При этом система остается достаточно простой в освоении, что сокращает время развертывания и снижает требования к квалификации обслуживающего персонала.

Разработка учебно-методических материалов и виртуальной инфраструктуры для учебно-тренировочного киберполигона

Учебно-методические материалы составляют концептуальную основу эффективного использования киберполигонов, выступая связующим звеном между технической инфраструктурой и образовательным процессом. Их разработка требует глубокого понимания как технологических аспектов информационной безопасности, так и педагогических принципов формирования профессиональных компетенций. Качественные методические материалы позволяют трансформировать технический потенциал киберполигона в практические навыки специалистов, обеспечивая системный подход к обучению.

Наиболее эффективные учебные программы для киберполигонов строятся по модульному принципу, сочетая теоретические основы с практическими кейсами. Каждый модуль должен включать четко сформулированные учебные цели, детализированные сценарии работы с полигоном, критерии оценки результатов и методические рекомендации по анализу выполненных заданий.

При создании учебно-методического обеспечения необходимо учитывать несколько ключевых принципов. Во-первых, принцип постепенного усложнения – от базовых упражнений по обнаружению простых угроз до комплексных заданий по расследованию сложных инцидентов. Во-вторых, принцип практической направленности, когда каждое теоретическое положение подкрепляется конкретными практическими заданиями на полигоне. В-третьих, принцип адаптивности, позволяющий корректировать сложность заданий в зависимости от уровня подготовки обучающихся. Эти принципы в совокупности обеспечивают формирование устойчивых профессиональных навыков.

Использование *Proxmox VE* в качестве основы киберполигона позволяет создать универсальную платформу, адаптируемую под различные задачи — от базового обучения до

сложных задач по тестированию на проникновения и расследования инцидентов и тестирования средств защиты. На рисунке 1 представлена часть разработанной инфраструктуры киберполигона на базе *Proxmox VE*. Виртуальные машины, подключенные к эмулируемым сетям объединены в группы (пулы, по терминологии Proxmox). Всего разработано более 40 пулов для обеспечения 50 практических и лабораторных работ.

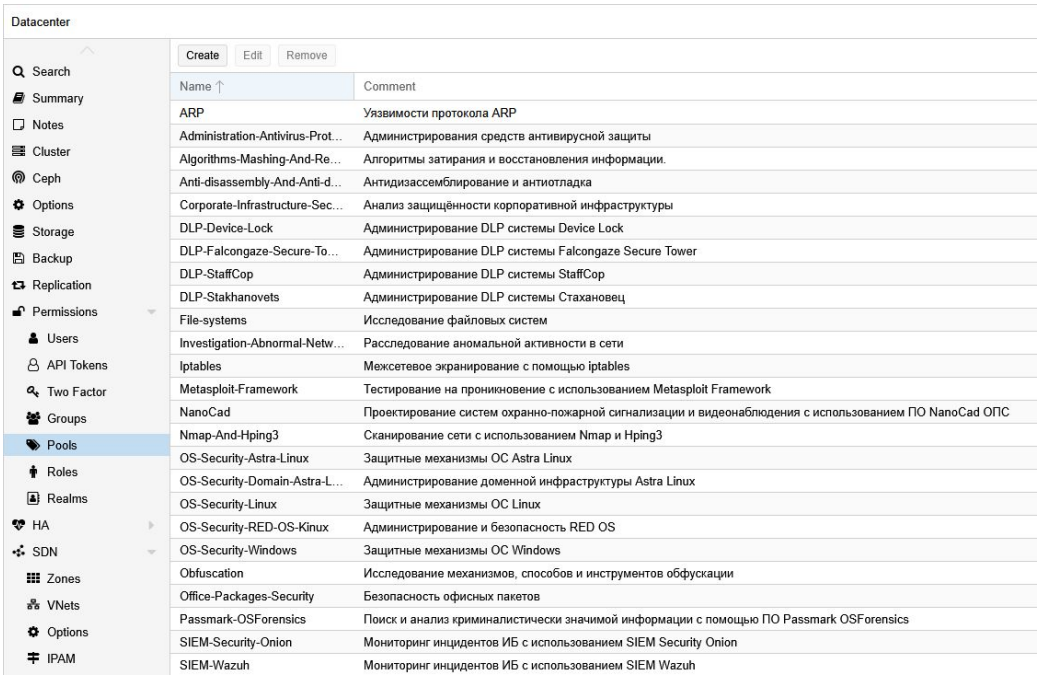

Рис. 1. Инфраструктура учебно-тренировочного киберполигона на базе *Proxmox VE*

Пример содержания отдельного пула в разработанном киберполигоне приведён в рисунке 2. Пул представляет собой набор виртуальных машин, подключённых к одной или нескольким виртуальным сетям и предварительно настроенными в соответствии с заданием по лабораторным или практическим работа.

Разработанный авторами киберполигон, в отличии от большинства подходов в их создании, не виртуализирует подробную инфраструктуру предприятий различного вида деятельности, а эмулирует отдельные элементы типовых инфраструктур предприятий для комплексной отработки навыков администрирования различных решений и продуктов в области информационной безопасности. Также киберполигон предоставляет возможность для практических и лабораторных, а также исследовательских работ в области восстановления данных, компьютерной криминалистики и противодействию вредоносному ПО.

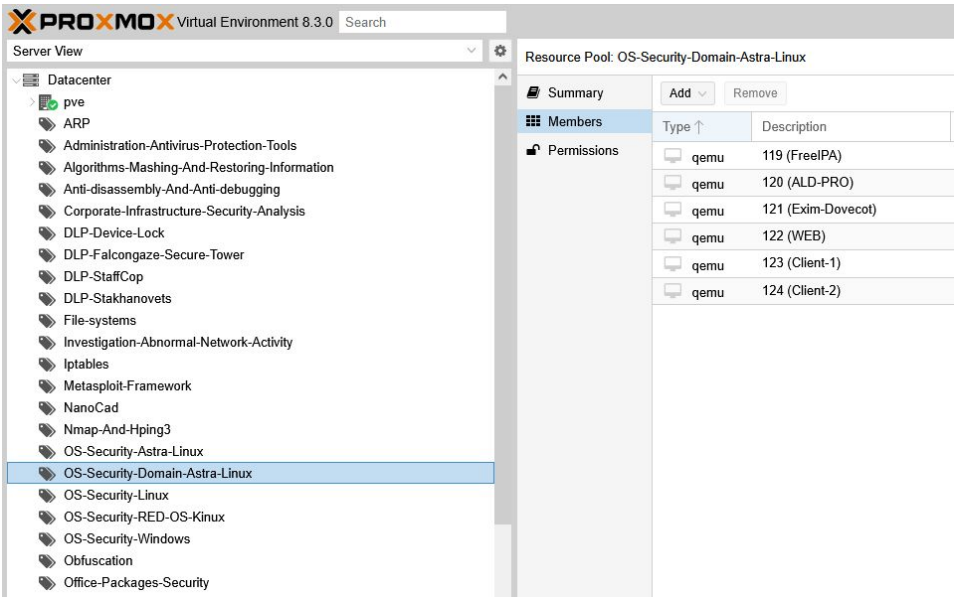

Рис. 2. Пример содержания отдельного пула

Для использования в киберполигоне авторами были разработаны или адаптированы более 50 практических и лабораторных работ, объединённых в 10 групп по различным тематикам.

Перечень практических и лабораторных работ, сгруппированных по темам:

1. Файловые системы:
   a. исследование файловой системы *FAT*32;
   b. исследование файловой системы *NTFS*;
   c. исследование файловой системы *EXT*4;
   d. исследование файловой системы *ExFAT*;
   e. исследование файловой системы *ReFS*;
   f. исследование файловой системы *HFS+*.
2. Администрирование средств защиты от несанкционированного доступа:
   a. администрирование СЗИ от НСД *Secret Net Studio*;
   b. администрирование СЗИ от НСД Страж *NT*;
   c. Администрирование СЗИ от НСД *Dallas lock*;
   d. Администрирование СЗИ от НСД *Аккорд X*;
3. Безопасность офисных пакетов:
   a. безопасность офисного пакета *MSOffice*;
   b. безопасность офисного пакета *LibreOffice*;
   c. безопасность офисного пакета *OnlyOffice*.
4. Безопасность операционных систем:
   a. защитные механизмы ОС *Windows*;

b. защитные механизмы ОС *Linux*;

c. администрирование доменной инфраструктуры *Astra Linux* на базе *FreeIPA*;

d. администрирование доменной инфраструктуры *Astra Linux* на базе *ALD PRO*;

e. защитные механизмы ОС *Astra Linux*.

5. Администрирование средств криптографической защиты:
   a. работа с шифрующей файловой системой *EFS*;
   b. работа с системой криптографической защиты *VeraCrypt*;
   c. администрирование системы криптографической защиты *ViPNet*;
   d. администрирование системы криптографической защиты Континент;
   e. администрирование системы криптографической защиты КриптоПро УЦ.
6. Безопасность компьютерных сетей:
   a. основы работы в анализаторе трафика *Wireshark*;
   b. сканирование сети с использованием *Nmap* и *Hping*3;
   c. обнаружение сетевых атак с использованием СОА *Snort*;
   d. обнаружение сетевых атак с использованием СОА *Suricata*;
   e. использование *Zeek Network Security Monitor* в качестве системы обнаружения вторжений;
   f. межсетевое экранирование с помощью iptables;
   g. анализ защищённости с помощью Сканер-ВС;
   h. тестирование на проникновение с использованием *Metasploit Framework*;
   i. анализ уязвимостей протокола *ARP*;
   j. анализ безопасности *Web*-приложений. *SQL* инъекции.
7. Администрирование DLP систем:
   a. администрирование *DLP* системы *Falcongsze Secure Tower*;
   b. администрирование *DLP* системы *Device Lock*;
   c. администрирование *DLP* системы Стахановец;
   d. администрирование *DLP* системы *StaffCop*.
8. Исследование вредоносного ПО:
   a. базовый статический анализ;
   b. базовый динамический анализ;
   c. продвинутый статический анализ;
   d. продвинутый динамический анализ;
   e. антидизассемблирование, антиотладка и обнаружение виртуализации;

f. администрирования средств антивирусной защиты.

9. Средства централизованного мониторинга:
   a. мониторинг инцидентов ИБ с использованием *SIEM Wazuh*;
   b. Мониторинг инцидентов ИБ с использованием *SIEM Security Onion*.
10. Расследование инцидентов ИБ:
   a. расследование аномальной активности в сети;
   b. поиск и анализ криминалистически значимой информации с помощью ПО *Passmark OSForensics*.

Данный перечень практических и лабораторных работ, реализованный в киберполигоне, обеспечивает эффективное усвоение студентами профессиональных компетенций. Для этого предусмотрено индивидуальное выполнение заданий с контролем затраченного времени, что позволяет более объективно оценивать результаты их выполнения. Система централизованного управления и контроля над учётными записями, позволяет разграничить студенту доступ только в определённым пулам и стендам с контролем его действий в системе. Несомненным достоинством системы является пониженные требования к аппаратной части оборудования студента. Все задания выполняются через браузер при удалённом подключении с ЭВМ практически любого уровня производительности. Основная же вычислительная нагрузка ложится на сервер.

Отметим, что некоторые лабораторные работы, выполняемые обучающимися до начала применения инфраструктуры киберполигона требовали использования высокопроизводительных рабочих станций. В случае использования высокопроизводительного сервера, киберполигон может обеспечить одновременную работу студентов нескольких групп над различными практическими и лабораторными работами. Средствами *Proxmox VE* легко обеспечивается развёртывание множества копий стендов и резервное копирование всей инфраструктуры полигона.

Выводы

В ходе проектирования и реализации инфраструктуры киберполигона, авторами была создана программная среда киберполигона на базе системы виртуализации *Proxmox VE*, были разработаны или использованы существующие методические материалы, включающие серию из 50 лабораторных работ, объединённых в 10 групп общим объёмом более 2090 страниц текстов формата А4, создана, подготовлена и проверена 121 виртуальная машина. Развёрнута инфраструктура киберполигона имеет общий объём более 3,8 Тб, до дублирования необходимых стендов для каждого студента.

Литература

1. «Солар»: более четверти всех кибератак в мире нацелены на российскую инфраструктуру. [Электронный ресурс]. – URL: https://rt-solar.ru/events/news/4941/.
2. Роман Резников. Искусственный интеллект в кибератаках. [Электронный ресурс]. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/iskusstvennyj-intellekt-v-kiberatakah/#id1.
3. Приказ Министерства науки и высшего образования РФ от 17 ноября 2020 г. № 1427 Об утверждении федерального государственного образовательного стандарта высшего образования - бакалавриат по направлению подготовки 10.03.01 информационная безопасность.
4. Приказ Министерства науки и высшего образования РФ от 26.11.2020 № 1460 «Об утверждении федерального государственного образовательного стандарта высшего образования - специалитет по специальности 10.05.04 Информационно-аналитические системы безопасности».
5. Приказ Министерства науки и высшего образования РФ от 26 ноября 2020 г. № 1459 «Об утверждении федерального государственного образовательного стандарта высшего образования - специалитет по специальности 10.05.01 Компьютерная безопасность».
6. Приказ Министерства науки и высшего образования РФ от 26 ноября 2020 г. № 1458 «Об утверждении федерального государственного образовательного стандарта высшего образования - специалитет по специальности 10.05.02 Информационная безопасность телекоммуникационных систем».
7. Приказ Министерства науки и высшего образования РФ от 26 ноября 2020 г. № 1455 «Об утверждении федерального государственного образовательного стандарта высшего образования - специалитет по специальности 10.04.01 Защита информации в ИСПДн, ГИС и значимых объектах КИИ».
8. Паспорт федерального проекта «Информационная безопасность» национальной программы «Цифровая экономика Российской Федерации» (утв. президиумом Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности (протокол от 28.05.2019 № 9)) [Электронный ресурс]. — Режим доступа: garantf1://72202278.0/.
9. Приказ ФСТЭК России № 17 от 11 февраля 2013 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

10. Приказ ФСТЭК России от 18.02.2013 N 21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных".
11. Приказ ФСТЭК России N 31 от 14 марта 2014 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды».
12. Приказ ФСТЭК России от 25.12.2017 N 239 "Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации".
13. Баранов В. В., Корчагина А. П., Лобов Б. Н. Киберполигон как площадка для подготовки специалистов в области информационной безопасности //Проблемы проектирования, применения и безопасности информационных систем в условиях цифровой экономики. - 2022. - С. 31-39.
14. Уймин А.Г., Никитин О.Р. Моделирование телекоммуникационной сети средствами сетевых инструментов Linux: инструменты создания цифровых двойников // i-methods - 2023 - Т. 15, № 2.
15. Лаврова Д. С., Зегжда Д. П., Зайцева Е. А. Моделирование сетевой инфраструктуры сложных объектов для решения задачи противодействия кибератакам //Вопросы кибербезопасности. - 2019. - №. 2 (30). - С. 13-20.
16. Синадский Н. И. Методология синтеза интерактивной сетевой среды для компьютерных полигонов в сфере информационной безопасности : диссертация доктора технических наук : 2.3.6. / Синадский Николай Игоревич; [Место защиты: ФГАОУ ВО «Уральский федеральный университет имени первого Президента России Б.Н. Ельцина» ; Диссовет УрФУ 2.3.12.13]. - Екатеринбург, 2022. - 304 с.
17. Паспорт федерального проекта «Информационная безопасность» национальной программы «Цифровая экономика Российской Федерации» (утв. президиумом Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности (протокол от 28.05.2019 № 9)) [Электронный ресурс]. — Режим доступа: garantf1://72202278.0/.