20.01.00

Образовательный киберполигон для имитации киберинцидентов

Белоусова Е.С.
Белорусский государственный университет информатики и радиоэлектроники (БГУИР), г. Минск, Республика Беларусь
ORCID: https://orcid.org/0000-0001-9834-6074
e-mail: Belousova@bsuir.by

Вербило Н.А.
Учреждение образования «Национальный детский технопарк» (УО НДТП), г. Минск, Республика Беларусь
ORCID: https://orcid.org/0009-0005-9149-6666
e-mail: nickolay3132@gmail.com

Филиппов А.С.
Учреждение образования «Национальный детский технопарк» (УО НДТП), г. Минск, Республика Беларусь
ORCID: https://orcid.org/0009-0007-8654-9692
e-mail: filipov_andrew@mail.ru

В статье представлен процесс планирования и разработки образовательного киберполигона для имитации киберинцидентов, цель которого развитие знаний, навыков и умений у детей и молодежи средних и высших учебных заведений в области информационной безопасности. Разработка образовательного киберполигона реализуется авторами в рамках индивидуальной учебной программы дополнительного образования одаренных детей и молодежи дистанционной формы получения образования по направлению «Информационная безопасность (“Образовательный киберполигон для имитации киберинцидентов”)» Учреждения образования «Национальный детский технопарк». К разрабатываемому образовательному киберполигону сформулированы требования: автономность, гибкость, универсальность и др. Для построения архитектуры образовательного киберполигона выбрана топология сети с двумя межсетевыми экранами, аналогичная топологиям корпоративных сетей. В стуктуре киберполигона добавлены виртуальные машины с разными операционными системами (Kali Linux, Ubuntu, Alpine), которые имитируют серверные и/или клиентские устройства. В качестве межсетевого экрана выбран pfSense ввиду его надежности, производительности и гибкости. Разработанный киберполигон рекомендуется к использованию в учреждениях образования для повышения мотивации учащихся к научным исследованиям и профессиональной ориентации

в области информационной безопасности. Авторами продолжается работа над совершенствованием методической базы для развития образовательного киберполигона.

Ключевые слова: информационная безопасность, киберучения, киберполигон, киберинцидент, кибератака, межсетевой экран

Для цитаты: *Белоусова Е.С., Вербило Н.А., Филиппов А.С.* Образовательный киберполигон для имитации киберинцидентов // Цифровая гуманитаристика и технологии в образовании (DHTE 2025): сб. статей VI международной научно-практической конференции. 13—14 ноября 2025 г. / Под ред. В.В. Рубцова, М.Г. Сороковой, Н.П. Радчиковой. М.: Издательство ФГБОУ ВО МГППУ, 2025. 56—66 с.

Введение

В Республике Беларусь Национальный центр обеспечения кибербезопасности и реагирования на киберинциденты, созданный в структуре Оперативно-аналитического центра при Президенте Республики Беларусь, проводит учения по действиям при возникновении киберинцидентов на объектах информационной инфраструктуры, разрабатывает программы и методики проведения таких учений, сценарии реагирования на кибератаки (О кибербезопасности ..., 2023). Такие киберучения проводятся для специалистов с опытом работы в области информационной безопасности. При этом важно отметить формирования знаний о методах противодействия кибератакам у учащихся средних и высших учебных заведений. Поэтому актуальным представляется проведение занятий с использованием образовательного киберполигона для имитации киберинцидентов в учреждении образования «Национальный детский технопарк» для учащихся направления «Информационная безопасность», а также его внедрение в учебный процесс на кафедре защиты информации Белорусского государственного университета информатики и радиоэлектроники. Разработка образовательного киберполигона для имитации киберинцидентов ведется в рамках индивидуальной учебной программы дополнительного образования одаренных детей и молодежи дистанционной формы получения образования по направлению «Информационная безопасность (“Образовательный киберполигон для имитации киберинцидентов”)» Учреждения образования «Национальный детский технопарк».

Цель создания образовательного киберполигона заключается в формировании и развитии знаний, навыков и умений в области информационной безопасности у детей и молодежи средних и высших учебных заведений, формирование и развитие творческих способностей, удовлетворение их индивидуальных потребностей в интеллектуальном совершенствовании, повышение мотивации к научным исследованиям, профессиональную ориентацию.

Для разработки образовательного киберполигона был сформирован перечень требований:

1. Автономность — пользователь образовательного киберполигона может самостоятельно развернуть его структуру на любом устройстве.
2. Гибкость — пользователь может вносить изменения в конфигурацию каждого элемента образовательного киберполигона, на основе этого разрабатывать свои сценарии киберинцидентов и способов защиты от них.
3. Автоматизация — процесс установки образовательного киберполигона на устройстве пользователя должен проходит в фоновом режиме без дополнительных действий.
4. Масштабируемость — в структуру образовательного киберполигона пользователь может добавлять новые виртуальные машины, приложения и др.
5. Универсальность — образовательный киберполигон может быть запущен на устройствах с Windows и Linux подобных операционных системах.
6. Открытость — любой пользователь образовательного киберполигона может разрабатывать новые сценарии кибератак, способов их блокировки.

Методы

Для выбора виртуализации платформы для реализации образовательного киберполигона произведено сравнение трех распространенных программных продуктов: VirtualBox, VMware Workstation, Proxmox VE. Как следует из данных, представленных в табл., VirtualBox представляет собой оптимальное решение для виртуализации благодаря своей бесплатной лицензии GPL, что делает его доступным для широкого круга пользователей в отличие от коммерческих аналогов, таких как VMware Workstation Pro. Поддержка

множества операционных систем, включая Windows, Linux, macOS и даже менее распространенные варианты вроде BSD, обеспечивает гибкость при развертывании виртуальных машин в различных средах. Простота и удобство графического интерфейса позволяют быстро освоить платформу даже начинающим пользователям, минимизируя время на настройку и управление виртуальными машинами. Эти факторы, в сочетании с активным сообществом и обширной документацией, делают VirtualBox предпочтительным выбором для образовательного киберполигона.

Таблица

Сравнительный анализ платформ виртуализации

Критерий	**VirtualBox**	**VMware Workstation**	**Proxmox VE**
Тип виртуализации	Полная (аппаратная + программная)	Полная (аппаратная)	Гипервизор Type 1 + LXC
Лицензия	Бесплатная (GPL)	Платная	Бесплатная (AGPL); платная поддержка
Поддержка операционными системами (ОС)	Windows, Linux, macOS	Windows, Linux	Только Linux (Debian-based)
Производительность	Средняя	Высокая	Близкая к нативной (KVM)
Сетевые возможности	NAT, мост, Host-only	NAT, мост (сложнее в настройке)	VLAN, SDN, мосты

В ходе разработки архитектуры образовательного киберполигона было решено реализовать топологию локальной сети с демилитаризованной зоной на основе двух межсетевых экранов (рис. 1). В результате анализа рынка межсетевых экранов было сделано заключение, что pfSense демонстрирует ряд преимуществ:

1. Основан на операционной системе FreeBSD, что обеспечивает высокую производительность и устойчивость системы.
2. Гибкость конфигурации сетевых параметров.
3. Поддержка технологий обнаружения вторжений (Snort и Suricata).
4. Понятный графический интерфейс.

Таким образом, выбор межсетевого экрана pfSense 2.8.0-RELEASE обусловлен его высокой надежностью, производительностью и гибкостью, что идеально подходящую для экспериментов

и обучения в условиях образовательного киберполигона. На рис. 2 показано успешное подключение и оптимальная работа межсетевого экрана pfSense 2.8.0-RELEASE в архитектуре образовательного киберполигона.

В архитектуре образовательного киберполигона выделены следующие зоны (рис. 1):

1. WAN — сегмент сети, имитирующий глобальный интернет, из которого есть доступ к публичным сервисам, находящимся внутри сегментов DMZ-1 и DMZ-2. В роли внешнего клиента используется виртуальная машина с ОС Kali Linux 2025.1 с доступом к Web-Server через HTTP и HTTPS по порту 80 и 443 соответственно, а также к PHP-Server по HTTP с портом 8080. В контексте образовательного киберполигона WAN зона используется для реализации имитации кибератак и тестирования уязвимостей.
2. DMZ-1 — сегмент сети, имитирующий классическую модель одноуровневой демилитаризованной зоны. В данном сегменте сети находится веб-сервер на базе Ubuntu Server с Wordpress, NGINX и OpenSSL, имитируя один из самых популярных выборов стека технологий для хостинга сайта.
3. DMZ-2 — сегмент, моделирующий двухуровневую архитектуру демилитаризованной зоны. Здесь размещен сервер с минималистичной ОС Alpine Linux, где развернуто тестовое веб-приложение с базовыми уязвимостями (SQLi, XSS и др.) для анализа, отработки и обучения методам противодействия кибератакам на уровне веб-приложений.
4. LAN — внутренний сегмент, выполняющий роль защитного уровня для пользователей сети. Виртуальная машина с ОС Kali Linux, размещенная в данном сегменте, выполняет роль администратора сети с доступом ко всем серверам по SSH и к панели администратора межсетевых экранов посредствам веб-интерфейса pfSense. ОС Kali Linux, несмотря на свою популярность в качестве «хакерской» операционной системы, стала отличным выбором из-за наличия множества предустановленных программ и утилит для анализа и эксплуатации уязвимостей. Также в LAN сегменте размещен сервер базы данных с ОС Ubuntu Server. Для каждого сервиса в демилитаризованной зоне создан свой пользователь и база данных, а Firewall-2 предоставляет доступ только нужным серверам.

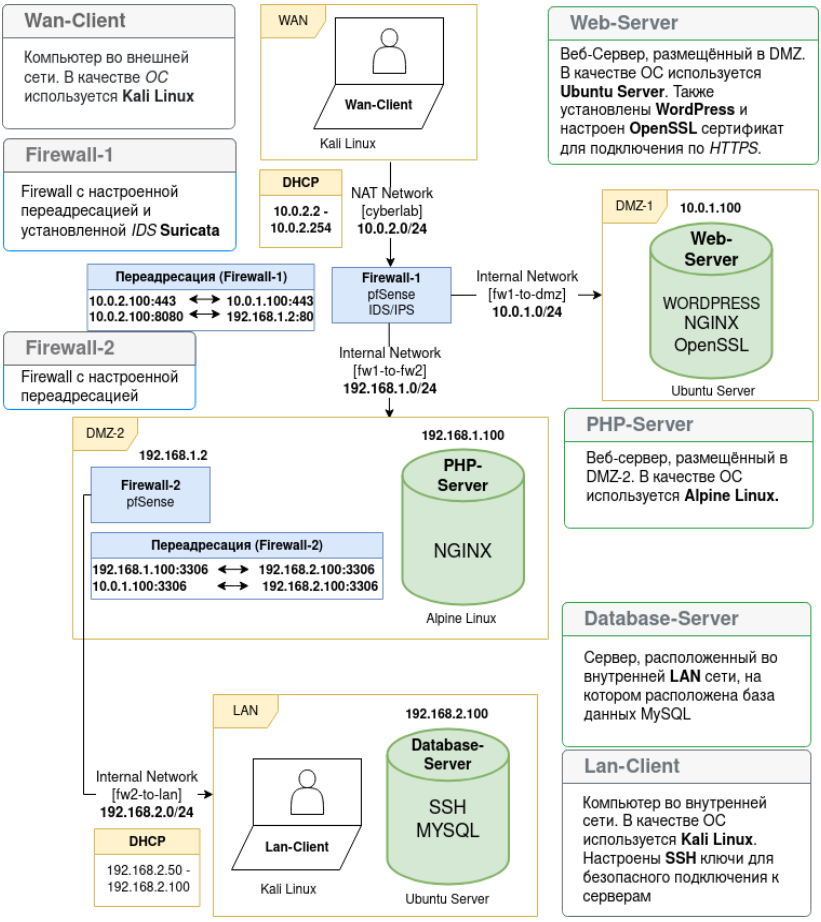

Рис. 1. Архитектура образовательного киберполигона

ОС Ubuntu Server 24.04.2 LTS был использован как основная операционная система для узлов — веб-сервера и сервера базы данных. Это решение обусловлено зрелостью и широким распространением дистрибутива в профессиональной среде, а также наличием обширной документации, актуальной поддержки и высокой степенью совместимости с популярным программным обеспечением.

Для веб-сервера была выбрана платформа Nginx, которая благодаря своей архитектуре, ориентированной на асинхронную

обработку соединений, обеспечивает высокую производительность при минимальных затратах ресурсов. Применение Nginx в связке с WordPress демонстрирует типичный стек CMS (Content Management System), применяемый в корпоративных и коммерческих сценариях, что делает среду образовательного киберполигона максимально приближенной к реальным условиям.

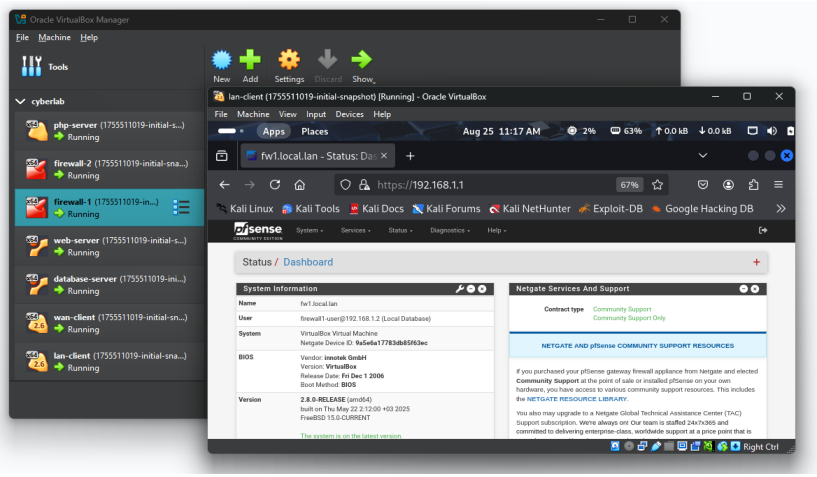

Рис. 2. Результат работы образовательного киберполигона

Сервер базы данных, работающий на MySQL, реализует типичную архитектуру разделения доступа: два пользователя, каждый из которых имеет доступ к собственной базе данных. Это позволяет моделировать реальные ситуации, в которых конфиденциальность, ограничение прав и разграничение доступа играют ключевую роль. MySQL как СУБД остается одним из наиболее популярных решений благодаря своей простоте, стабильности и широкой поддержке со стороны экосистемы Linux, включая Ubuntu.

Отдельное внимание заслуживает сервер с операционной системой Alpine Linux v3.22, дистрибутив, ориентированный на минимализм и безопасность, что делает его идеальным выбором для развертывания сервисов в условиях нехватки ресурсов. На базе данного сервера было решено развернуть PHP-приложение для демонстрации уязвимостей веб-ресурсов.

Выбранная архитектура серверов представляет собой проверенную, гибкую и масштабируемую архитектуру, способную эффективно поддерживать задачи моделирования, обучения и тестирования в рамках образовательного киберполигона. На рис. 3 показано успешное подключение клиента из сегмента WAN образовательного киберполигона к веб-серверу на базе Ubuntu Server с Wordpress в сегменте DMZ-1.

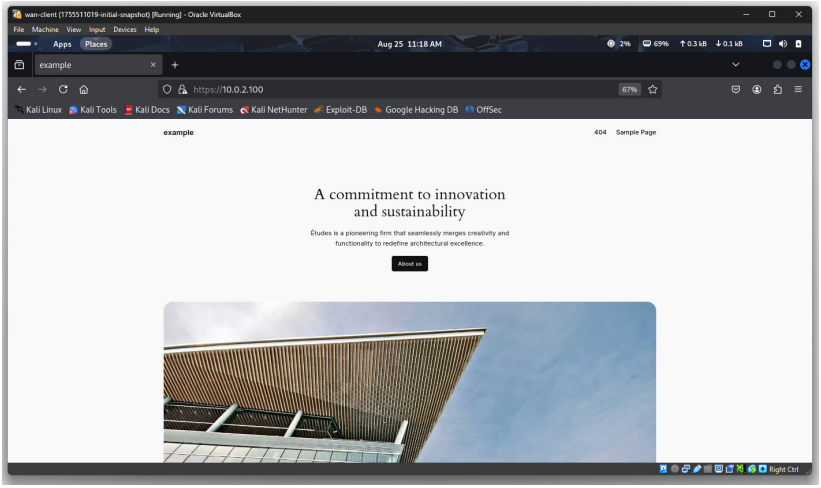

Рис. 3. Результат получения доступа к HTTP серверу в DMZ-1 зоне

Заключение

В заключении можно отметить, что при работе над образовательным киберполигоном были учтены все сформулированные к нему требования. Так для обеспечения его автономности, универсальности и гибкости было решено использовать VirtualBox, ввиду его доступности, эргономичности и простоте использования. Для будущей масштабируемости киберполигона была выбрана топология корпоративной сети на основе двух межсетевых экранов. На основе сравнительного анализа межсетевых экранов был выбран pfSense, так как он обеспечивает высокую производительность и устойчивость системы.

Авторами продолжается работа над совершенствованием образовательного киберполигона. На текущий момент ведется разработка

программы для автоматизации образовательного киберполигона CyberLab Management Tool для обеспечения его автоматизации, а также составляются сценарии реализации кибератак и реагирования на них.

Таким образом, разрабатываемый образовательный киберполигон рекомендуется к внедрению в учебный процесс в учреждениях образования Республики Беларусь, в результате чего могут быть достигнуты следующие результаты:

1. Совершенствование образовательной, методической, технической и научной базы.
2. Повышение уровня знаний учащихся в области информационной безопасности.
3. Стимулирование развития учащихся в области информационной безопасности.
4. Развитие обмена знаниями и умениями между специалистами в области информационной безопасности и учащимися средних и высших учебных заведений.

Список источников

1. *О кибербезопасности: Указ Президента Республики Беларусь от 14 февраля 2023 г. № 40*. (2023). Минск. URL: https://president.gov.by/ru/documents/ukaz-no-40-ot-14-fevralya-2023-g (Дата обращения: 25.08.2025).

Информация об авторах

Белоусова Елена Сергеевна, кандидат технических наук, доцент кафедры защиты информации, Белорусский государственный университет информатики и радиоэлектроники (БГУИР), г. Минск, Республика Беларусь, ORCID: https://orcid.org/0000-0001-9834-6074, e-mail: Belousova@bsuir.by

Вербило Николай Александрович, учащийся направления «Информационная безопасность ("Образовательный киберполигон для имитации киберинцидентов")», Учреждение образования «Национальный детский технопарк» (УО НДТП), г. Минск, Республика Беларусь, ORCID: https://orcid.org/0009-0005-9149-6666, e-mail: nickolay3132@gmail.com

Филлипов Андрей Сергеевич, учащийся направления «Информационная безопасность ("Образовательный киберполигон для имитации киберинцидентов")», Учреждение образования «Национальный детский технопарк» (УО НДТП), г. Минск, Республика Беларусь, ORCID: https://orcid.org/0009-0007-8654-9692, e-mail: filipov_andrew@mail.ru

Cyber Training Polygon for Simulating Cyber Incidents

Elena S. Belousova
Belarusian State University of Informatics and Radioelectronics, Minsk, Belarus
ORCID: https://orcid.org/0000-0001-9834-6074
e-mail: Belousova@bsuir.by

Mikalai A. Viarbila
Educational institution "National Children's Technopark", Minsk, Belarus
ORCID: https://orcid.org/0009-0005-9149-6666
e-mail: nickolay3132@gmail.com

Andrei S. Filipau
Educational institution "National Children's Technopark"Minsk, Belarus
ORCID: https://orcid.org/0009-0007-8654-9692
e-mail: filipov_andrew@mail.ru

The article presents the process of planning and developing a cyber training polygon for simulating cyber incidents. Its goal is to develop knowledge, skills and abilities in children and young people of secondary and higher educational institutions in the field of information security. The development of cyber training polygon is being implemented by the authors within the framework of an individual educational program for additional education of gifted children in the distance learning format in the field of «Information Security ("Cyber Training polygon for Simulating Cyber Incidents")» in Educational institution «National Children's Technopark». The following requirements have been formulated for developed cyber training polygon: autonomy, flexibility, versatility, etc. A network topology with two firewalls was chosen for the architecture of the cyber training polygon, because it is similar to the topologies of corporate networks. The cyber polygon structure has been supplemented with virtual machines with different operating systems (Kali Linux, Ubuntu, Alpine). They simulate server and/or client devices. The developed cyber training polygon is recommended for use in educational institutions to increase students' motivation for scientific research and professional orientation in the field of information security. The authors continue to work on improving the methodological base for the cyber training polygon.

Keywords: information security, cyber training, cyber polygon, cyber incident, cyber-attack, firewall

For citation: Belousova E.S., Viarbila M.A., Filipau A.S. Cyber training polygon for simulating cyber incidents *// Digital Humanities and Technology in Education (DHTE 2025): Collection of Articles of the V International Scientific and Practical Conference. November 13—14, 2025* / V.V. Rubtsov, M.G. Sorokova, N.P. Radchikova (Eds). Moscow: Publishing house MSUPE, 2025. 56—66 p. (In Russ., abstr. in Engl.).

Information about the authors

Elena S. Belousova, PhD of Technical Sciences, Associate Professor, Associate Professor of the Informational Security Department of Belarusian State University of Informatics and Radioelectronics, Minsk, Belarus, ORCID: https://orcid.org/0000-0001-9834-6074, e-mail: Belousova@bsuir.by

Mikalai A. Viarbila, student of the course "Information Security ("Educational cyber polygon for simulating cyber incidents")", Educational institution "National Children's Technopark", Minsk, Belarus, ORCID: https://orcid.org/0009-0005-9149-6666, e-mail: nickolay3132@gmail.com

Andrei S. Filipau, student of the course "Information Security ("Educational cyber polygon for simulating cyber incidents")", Educational institution "National Children's Technopark", Minsk, Belarus, ORCID: https://orcid.org/0009-0007-8654-9692, e-mail: filipov_andrew@mail.ru