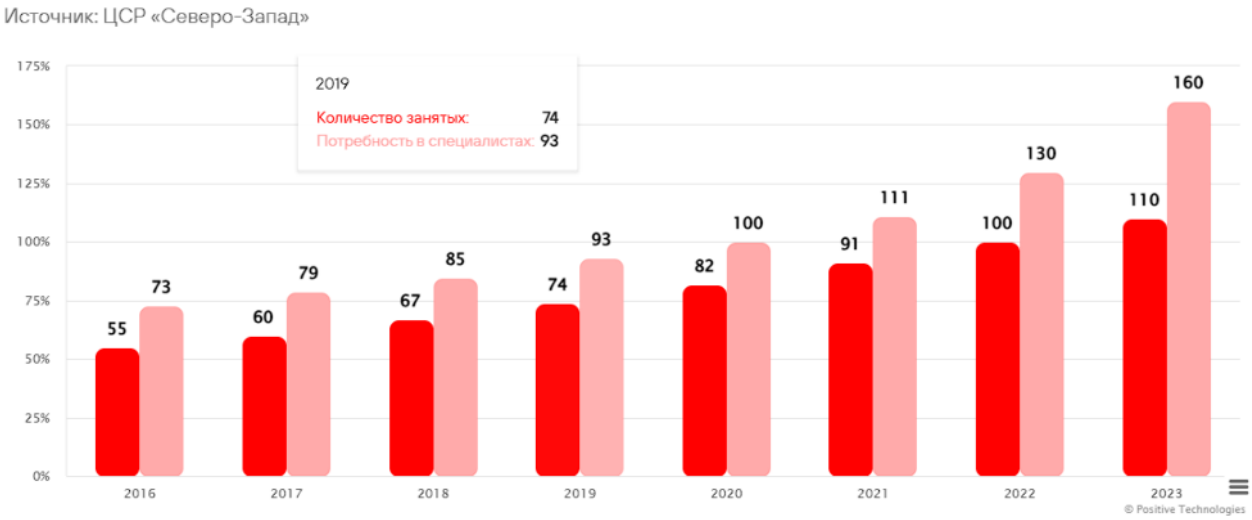
УДК 004.056

РАЗРАБОТКА ШАБЛОНА КИБЕРПОЛИГОНА AMPIRE ДЛЯ ПРЕДПРИЯТИЙ КУЗБАССА

Сергеев.С.С, студент гр. ИБс-211, IV курс
Научный руководитель: к.т.н., доцент Киренберг А.Г.
Кузбасский государственный технический университет имени Т.Ф. Горбачёва
г. Кемерово

Современный мир стремительно движется в сторону цифровизации, что



приводит к возрастанию атак на информационные системы. В нынешних реалиях приоритет отдается главному сегменту — Критические Информационные Инфраструктуры Государства. По данным Positive Technologies промышленность каждый год оказывается в тройке наиболее часто атакуемых отраслей.

Несмотря на то, что компании из различных областей промышленности, включая энергетику и угольную, продолжают увеличивать бюджеты на кибербезопасность и внедрять различные классы решений для ИБ, ситуация в отрасли коренным образом не меняется. Опыт вендоров ИБ показывает, что ИС многих предприятий, независимо от масштаба и набора средств, могут быть взломаны всего за несколько шагов.

Почему же предприятия не спешат повышать защищенность своего контура защиты? На этот вопрос нельзя ответить однозначно. Существует много факторов. Например, один из факторов является кадровый голод. По данным Positive Technologies к 2023 году дефицит кадров составляет пятьдесят тысяч специалистов. Это показывает график на рисунке 1.

Рисунок 1 — Количество и потребность занятых на рынке труда ИБ

Еще одним из факторов является недостаточный уровень компетентности среди потенциальных работников и выпускников вузов.

Давайте рассмотрим популярные площадки для отработки навыков по информационной безопасности:

1. **HackTheBox**. Зарубежная площадка для отработки навыков. Данная площадка предлагает широкий спектр знаний за определенную стоимость (для студентов 10 евро/месяц). Однако, не зная общих принципов ИБ и первичных навыков, будет сложно проходить обучение на данной площадке. **Не доступен для граждан РФ.**

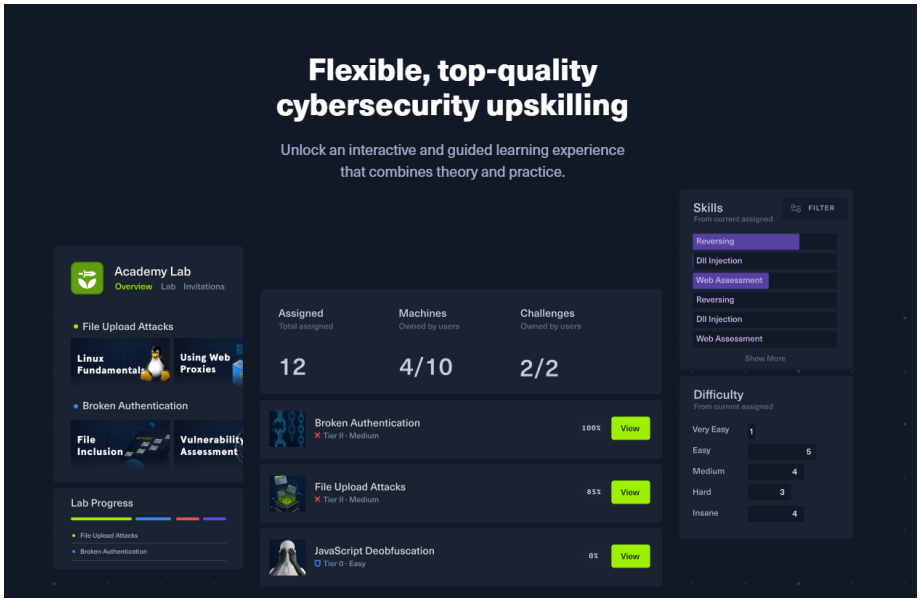


Рисунок 2 — Зарубежная площадка для отработки навыков ИБ

2. **Hacker Lab (Codeby games) Отечественная площадка**. В игровой форме предлагает освоить базовые навыки в разных областях информационной безопасности: OSINT, Форензика, Реверс, WEB, Active Directory и другие. В образовательных целях компания выпускает отдельные платные курсы на сайте своей академии. Стоимость курсов начинается от 55 тыс рублей, для студента данная сумма является неподъёмной.

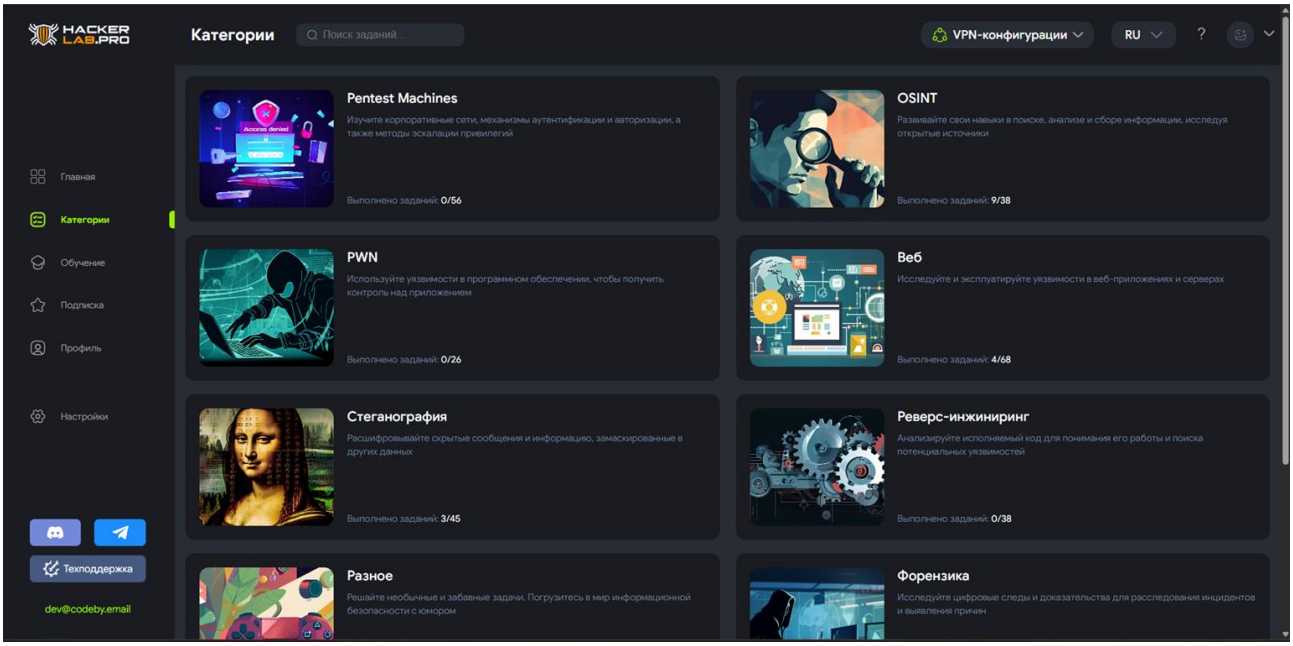


Рисунок 3 — Отечественный продукт для отработки навыков

В данной ситуации возникает логичный вопрос: где брать дополнительные знания кроме вуза?

Для решения данных проблем была сформулирована идея: совместно с компанией «Перспективный Мониторинг» создать собственный шаблон для КиберПолигона “Ampire”, моделирующего инфраструктуру предприятий топливно-энергетического комплекса (ТЭК) и объектов критической информационной инфраструктуры (КИИ). Суть идеи состоит в разработке универсального шаблона киберполигона с имитацией АСУ ТП (силами студентов кафедры ИБ) и компонентами защиты со стороны заказчика, который позволит устранить проблему недостатка ресурсов для отработки практических навыков и получения дополнительных знаний у студентов, интересующихся областью информационной безопасности, а также действующих специалистов по ИБ, работающих на предприятиях ТЭК и КИИ в Кемеровской области.

Проведя исследования в разработке сценариев защиты, требования к шаблону будет выглядеть следующим образом:

- Вся реализация предполагается на виртуальных машинах;
- В качестве ОС необходимо использовать Linux-системы (не проприетарные системы);
- Прикладное ПО должно быть свободно распространяемым или собственной разработки;
- Итоговый шаблон должен быть работоспособным после его включения, не должно быть никаких дополнительных настроек после запуска ВМ;
- Шаблон должен иметь сопроводительную документацию.

Обоснование структуры и понимания требований к шаблону разработки: реализация на виртуальных машинах позволяет снизить затраты на обо-

рудование, так как все виртуальные машины могут работать на одном физическом сервере. В данном случае будет использоваться гипервизор ESXi, который установлен на физический сервер на базе вуза. Linux-системы и прикладное ПО позволяю
т минимизировать или вовсе исключить финансовые затраты на покупку лицензий. Шаблон должен начинаться со схемы, это позволяет избежать проблемы при проектировании организации компонентов. Сопроводительная документация позволит людям впервые увидев киберполигон, быстро разобраться в структуре и функционале шаблона, что очень важно для новых пользователей. Участие компании «Перспективный мониторинг» заключается в том, что они предоставят системы защиты информации и окажут консультативную поддержку в разработке данного шаблона.

Организация готова поставить следующие продукты защиты:

1) ViPNet TIAS - Threat Intelligence Analytics System — программно-аппаратный комплекс, предназначенный для автоматического выявления инцидентов на основе анализа событий информационной безопасности.

2) ViPNet IDS NS - это сетевой сенсор обнаружения сетевых атак и вредоносного программного обеспечения в файлах, передаваемых в сетевом трафике, и предназначенный для интеграции в компьютерные сети с целью повышения уровня защищенности информационных систем, центров обработки данных, рабочих станций пользователей, серверов и коммуникационного оборудования.

Данные продукты позволят людям тренирующимся на шаблоне киберполигона получить реальные практические навыки в режиме работы SOC центра в формате 2 групп - Реагирования и Мониторинга. Студенты получат практические навыки с продуктами защиты, что позволит существенно поднять свою компетентность на уровень выше.

Вся инфраструктура будет реализована на виртуальных машинах

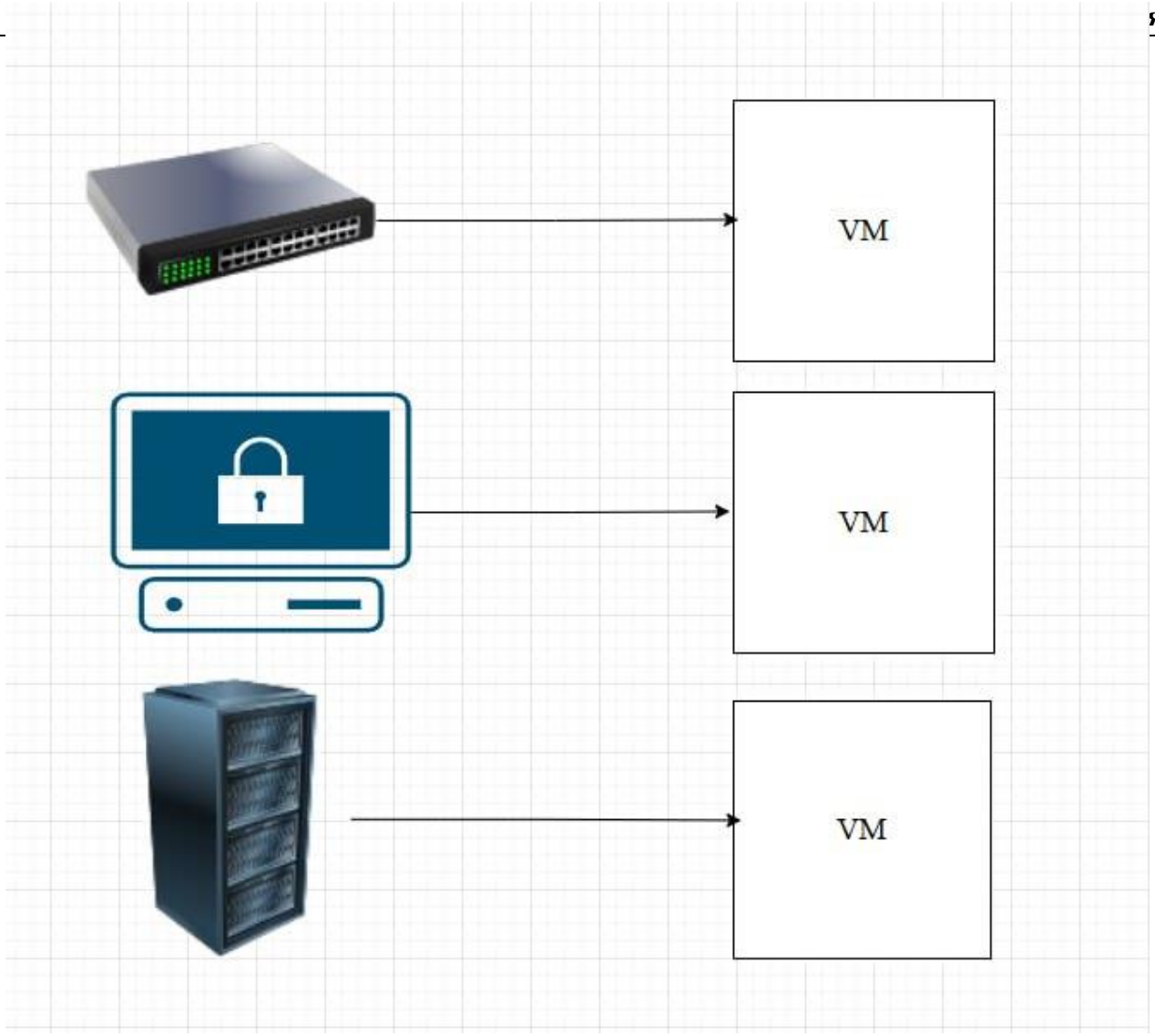


Рисунок 4 — виртуальные машины инфраструктуры

Подводя итог, можно сказать что данный шаблон киберполигона позволит студентам получить глубокие познания в этой области, а так же предприятиям отрабатывать реальные сценарии кибератак, обучать сотрудников навыкам предотвращения угроз. Он будет включать виртуализированную инфраструктуру, моделирующую корпоративные сети, и набор инструментов для анализа и реагирования на инциденты. Проект способствует повышению устойчивости предприятий к киберугрозам, снижению рисков утечек данных и финансовых потерь. Для студентов и специалистов ИБ это возможность получить практический опыт и повысить квалификацию. Разработка шаблона киберполигона укрепит региональную кибербезопасность и создаст основу для развития кадрового потенциала в сфере ИБ студентов Кузбасского Государственного технического университета.

Литература:

1) Рынок труда в информационной безопасности в России в 2024–2027 гг.: прогнозы, проблемы и перспективы [Электронный ресурс] URL: https://www.ptsecurity.com/ru-ru/research/analytics/rynok-truda-v-informaczionnoj-bezopasnosti-v-rossii-v-2024-2027-gg-prognozy-problemy-i-perspektivy/#id3
2) Промышленный сектор: нацеленность на остановку технологических процессов [Электронный ресурс] URL: https://pt-corp.storage.yandexcloud.net/upload/corporate/ru-ru/analytics/positive-research-2023-rus.pdf

3) Отечественная площадка для специалистов ИБ [Электронный ресурс] URL: https://codeby.school/training

4) Исследование рынка АСУ ТП в России [Электронный ресурс] URL: https://www.ptsecurity.com/ru-ru/research/analytics/issledovanie-rynka-asu-tp-v-rossii/?utm_source=tg_pt&utm_medium=post&utm_campaign=asutp&utm_content=12_02#id1

5) Зарубежная площадка для отработки навыков по ИБ [Электронный ресурс] URL: https://academy.hackthebox.com/academy-for-business

6) Система обнаружения компьютерных атак [Электронный ресурс] URL: https://infotecs.ru/products/vipnet-ids-ns/
7) Интеллектуальный анализ угроз информационной безопасности [Электронный ресурс] URL: https://infotecs.ru/products/vipnet-tias/