Математические структуры и моделирование
2023. № 4 (68). С. 120–129

УДК 378.147:004.4
DOI 10.24147/2222-8772.2023.4.120-129

ОТ ЛАБОРАТОРНОГО СТЕНДА ДЛЯ ИЗУЧЕНИЯ ОСНОВ КОМПЬЮТЕРНЫХ СЕТЕЙ К ХАКЕРСПЕЙСУ ДЛЯ ИЗОБРЕТАТЕЛЕЙ И СОРЕВНОВАТЕЛЬНОМУ КИБЕРПОЛИГОНУ

С.В. Гусс
старший преподаватель, e-mail: sviat@v-guss.ru

Омский государственный университет им. Ф.М. Достоевского, Омск, Россия

Аннотация. Рассматривается проблема перехода от обычного лабораторного стенда для изучения основ функционирования компьютерных сетей к проектному хакерспейсу для изобретателей и соревновательному киберполигону для проведения различных мероприятий: хакатонов, чемпионатов, олимпиад. Рассматриваются конкретные примеры программного и аппаратного обеспечения для настройки и развёртывания необходимой инфраструктуры.

Ключевые слова: стенд, хакерспейс, киберполигон.

Введение

Цифровая трансформация образования, направленная на совершенствование цифровой образовательной среды должна способствовать формированию у студентов средних и высших учебных заведений ценностей и смыслов, мотивирующих обучающихся на саморазвитие и самообразование.

Не лишним будет вспомнить высказывание А. Эйнштейна, согласно которому «бессмысленно продолжать делать то же самое и ждать других результатов». Этой цитатой зададим пульс повествования и рассмотрим переход от традиционной учебно-лабораторной базы к системе, соответствующей реалиям современной жизни и отвечающей ожиданиям нового поколения. А более конкретно – поколению Z, согласно теории поколений Хоува – Штрауса. Поколению художников, стремящихся к изобретательству и креативу, не представляющих своей жизни без мобильных устройств и Интернета.

Вначале попробуем разобраться с тем, что такое лабораторный стенд, его цифровой двойник – виртуальный стенд и зачем, собственно, изобретать киберполигон. Также посмотрим, из чего всё это состоит, как и где используется.

Итак, что такое лабораторный стенд?

Лабораторный стенд – это физически доступный набор некоторого оборудования, инструментов и компонентов, используемых для проведения экспериментов, исследований или обучения конкретным навыкам. Стенды могут быть предназначены для различных целей, таких как изучение принципов работы различных устройств, тестирование новых технологий, обучение студентов и т. д.

Здесь сложностей с интерпретацией быть не должно. Термин устоявшийся. Лабораторные стенды используются в различных областях и служат главным образом для целей обучения. Особенно когда речь идёт о каких-то опасных и дорогостоящих объектах, к работе с которыми требуется особый допуск в связи с его степенью критичности и возможным ущербом. Стоит заметить, что лабораторный стенд не всегда соответствует реальному оборудованию или среде, а может имитировать их для развития каких-то элементарных, общих навыков. Сегодня всё чаще прибегают к технологиям виртуализации и созданию цифровых двойников.

И тут мы приходим к понятию виртуального лабораторного стенда.

Виртуальный лабораторный стенд – это программно-аппаратная система, которая имитирует реальный лабораторный стенд, обычно используемый для научных или технических исследований. Виртуальные лабораторные стенды позволяют проводить эксперименты и исследования без наличия физического оборудования, что снижает затраты на проведение экспериментов и в некоторых случаях помогает справиться со сложностью организации процесса. Они также обеспечивают большую безопасность и контроль в рамках экспериментов, так как нет риска получения травм или повреждения оборудования. Виртуальные стенды могут быть использованы для обучения, исследований, разработки и проверки новых идей или концепций.

В последнее время всё чаще можно услышать такое слово, как киберполигон, особенно в контексте обучения специалистов по направлениям кибербезопасности, главным образом когда речь идёт об анализе уязвимостей компьютерных сетей и организации тестов на проникновение за периметр сетевой инфраструктуры предприятия.

Киберполигон – это виртуальная среда, имитирующая реальную компьютерную сеть или систему в целях обучения, тестирования и оценки знаний и умений специалистов в области информационной безопасности. Киберполигон позволяет моделировать различные ситуации, связанные с сетевыми атаками, уязвимостями, несанкционированным доступом и другими угрозами, с которыми могут столкнуться специалисты в реальной жизни. Киберполигоны часто используются для проведения соревнований и конкурсов по кибербезопасности.

1. Лабораторные стенды

Самое очевидное решение для организации практических занятий – создание лабораторного стенда. Обучающиеся могут прикоснуться к реальному оборудованию, протестировать его, посмотреть на то, как устройства откликаются и реагируют на те или иные действия со стороны пользователя. В тех случаях, когда разместить в лаборатории реальное оборудование не представляется возможным ввиду ограничений по стоимости, размерам, среде функционирования и другим соображениям, создаются специальные макеты или симуляторы, по своим реакциям и взаимодействию с пользователем соответствующие реальному оборудованию.

Например, в лаборатории сетей и систем передачи информации можно разместить специальную стойку, или несколько стоек, с установленным в ней сетевым оборудованием, таким как концентраторы, коммутаторы, маршрутизаторы, межсетевые экраны, устройства обнаружения и предотвращения вторжений, серверы вир-

туализации для развёртывания программных реализаций сетевых устройств и т. д. Всё это хорошо, но для полноценного знакомства с полным спектром сетевых устройств придётся потратить немалую сумму плюс учесть расходы на поддержание всего этого в рабочем, стабильном состоянии.

Более современный подход – использование средств виртуализации и эмуляции реальных устройств. Для развёртывания базовой виртуальной сетевой инфраструктуры достаточно компьютеров со средними на сегодняшний день системными требованиями: 8–16 ГБ оперативной памяти, место на жёстком диске (лучше SSD) не менее 100 ГБ, 4–8-ядерный центральный процессор (x86 совместимый, поддерживающий виртуализацию, например Intel Core или AMD). Этого будет вполне достаточно для организации небольшой сети, в которой есть маршрутизатор, несколько коммутаторов и рабочих станций с установленными операционными системами Windows или GNU/Linux.

Одной сети, к тому же небольшой, не всегда достаточно для проведения исследований. Зачастую необходимо организовать несколько связанных друг с другом сетей, разбитых на зоны. Кроме того, серверы с работающими сетевыми службами и прикладными сервисами тоже могут потребовать больших вычислительных ресурсов для нормального функционирования. Таким образом, для более сложных сценариев уже потребуется производительный сервер виртуализации, чтобы серверам можно было выделить несколько процессорных ядер и достаточный объём оперативной памяти. Можно также воспользоваться услугами облачных провайдеров, взять в аренду необходимые вычислительные мощности и наращивать их объём в случае необходимости.

Отдельный вопрос, на который стоит обратить внимание, – наличие лицензии на использование официальных образов разворачиваемых систем (операционных, сетевых, прикладных). Речь идёт в основном об отечественных системах. Впрочем, там могут действовать определённые правила в рамках конкретного договора, особые условия для учебных заведений и т. д. Некоторые поставщики предлагают готовые решения и схемы развёртывания стендов для поддержки своих учебных курсов.

2. Киберполигоны

Поскольку киберполигоны в основном используются для проведения комплексных исследований или соревнований с большим количеством участников, то здесь уже точно не обойтись без мощных серверных решений. И самый оправданный вариант – использование существующих предложений от крупных поставщиков сетевого оборудования или программных решений, поскольку вся проблема заключается в поддержке такого решения и быстрой адаптации инфраструктуры под нужды возрастающего количества участников.

В случае когда киберполигон небольшой, не предполагает масштабного развёртывания и служит в основном для поддержки лабораторных и практических работ конкретной учебной дисциплины или нескольких похожих дисциплин, лучше использовать термин «миникиберполигон». В литературе и статьях термин практически не используется, но зато его часто можно услышать в рамках презентаций учебными заведениями каких-то своих локальных решений.

Учитывая тот факт, что тенденция сегодняшнего дня – виртуализация и разворачивание в облаке, то и киберполигон, чтобы быть максимально доступным, тоже зачастую разворачивается в облаке. По сути, такой полигон становится распределённой системой с возможностью подключения к ней не только удалённых пользователей, но и некоторой пользовательской системы, развернутой на локальных пользовательских ресурсах. Если в качестве пользователя выступает целая организация, то виртуальная сеть киберполигона может быть существенно расширена, особенно учитывая, что таких пользователей может быть, вообще говоря, немало.

3. Учебно-лабораторная база

Лаборатории, киберполигоны и всевозможные комплексы в рамках учебного процесса можно охарактеризовать одним, более ёмким понятием – учебно-лабораторная база по реализации образовательных программ [1].

Такая база, помимо развития базовых навыков у студентов, отработки учебных задач по различным направлениям обучения в области информационных технологий и кибербезопасности, может использоваться в качестве оценочных средств определения уровня сформированности компетенций [2].

Элементы такой базы должны соответствовать современным реалиям и давать возможность опробовать различные сценарии настройки оборудования и программных средств, проведения тестирований на проникновение и оперативное реагирование.

Киберполигон предоставляет следующие обучающие возможности [3]:

- выполнение лабораторных работ для отработки практических навыков (как индивидуальных, так и командных);
- испытание теоретических знаний опытными экспериментами;
- тестирование студентов для оценки уровня знаний.

4. Общедоступный киберполигон

Поскольку собрать свой киберполигон в учебном заведении не всегда возможно ввиду ограничений, связанных с недоступностью достаточно производительного оборудования, серверов, систем виртуализации, часто прибегают к использованию доступных, готовых решений и предложений от крупных компаний. Это профессиональные, комплексные системы, предоставляющие в том числе и профессиональное программное обеспечение для управления информацией и событиями безопасности (SIEM), настройки межсетевых экранов нового поколения (NGFW), для анализа сетевого трафика и обнаружения заражённых узлов и нарушений политик безопасности (NTA/NDR) и других систем (EDR, XDR, ISIM, Sandbox...).

Среди отечественных предложений можно выделить:

- **Национальный киберполигон** от Ростелеком для отработки практических навыков по кибербезопасности [4]. Здесь развёрнуты типовые инфраструк-

туры из различных отраслей (энергетика, нефтегазовый сектор, финансы, телеком). На момент написания статьи было доступно 7 отраслевых сегментов. Возможно построение киберполигонов на базе инфраструктуры заказчика, создание цифровых двойников сегментов. Рассчитан главным образом на подготовку специалистов конкретных предприятий.

- Киберполигон на базе решения **Ampire** в рамках консорциума «Цифровые технологии» (совместная экспозиция КНИТУ и Softline) [5]. Предоставляет специализированные программные системы для анализа следов злоумышленника и обнаружения атак, а также защиты информации. Подходит для обучения школьников и студентов, планирующих работать в сфере кибербезопасности. Используя шаблоны, можно моделировать типовые информационные системы и отрабатывать базовые сценарии.

- **Киберполигон Standoff 365** от Positive Technologies [6]. На базе полигона воссоздаются технологические и бизнес-процессы реальных компаний для исследования информационной инфраструктуры энергетических, финансовых компаний и корпоративных систем. На базе платформы проходят различные киберучения, соревнования и митапы.

Можно заметить, что киберполигон – это не просто стенд как набор технологий для развёртывания сетевой инфраструктуры. Это целый комплекс, выходящий на прикладной, проблемный уровень с готовыми схемами, шаблонами и сценариями, обобщающими практический опыт работы и исследований всевозможных случаев, подпадающих под сферу кибербезопасности, от социальной инженерии до защиты сетевого периметра.

Всё это примеры профессиональных решений. Существуют также частные решения, которые могут представлять интерес для тех, кто отважится развернуть полигон в лаборатории своего учебного заведения.

5. Частные полигоны учебных заведений

На прошедшем не так давно методическом семинаре «Вопросы преподавания и учебно-методического обеспечения реализации образовательного процесса по специальностям и направлениям подготовки в области информационной безопасности» (15 ноября 2023 г., СибГУТИ), был представлен ряд интересных решений: Миникиберполигон ЯрГУ и Кибергород на базе КГУ. Далее будет представлен небольшой обзор данных решений.

Миникиберполигон ЯрГУ

В рамках семинара проект был представлен Д.М. Муриным (Демидовский университет). Поскольку проект динамичный и детали реализации естественным образом могут меняться, то далее представлена общая идея и главным образом описание доступного для реализации программного и аппаратного обеспечения.

Стоит отметить, что данный проект поддержан грантом Потанина. Что доказывает необходимость построения таких систем и их актуальность.

Для реализации полигона используются серверы виртуализации SuperMicro и программно-аппаратный шлюз безопасности ViPNet.

Полный список средств:

- Средства криптографической защиты информации: ViPNet Администратор, ViPNet Координаторы, ViPNet Клиенты.
- Межсетевые экраны и средства обнаружения вторжений: Рубикон;
- Средства доверенной загрузки: Соболь, Аккорд;
- Системы активной защиты: Касперский, Dr. Web;
- Средства защиты информации от несанкционированного доступа: Dallas Lock, Secret Net;
- Аппаратный идентификатор: RuToken;
- Средства анализа защищённости: Xspider, MaxPatrol 8;
- Межсетевой экран для защиты веб-приложений: PT Application Firewall;
- Средства управления событиями безопасности: MaxPatrol SIEM, SIEM Комрад.

Аппаратно киберполигон поддерживается следующим оборудованием. Это 16 автоматизированных рабочих мест:

- 4 ядра / 8 потоков процессоры Intel i5;
- 32 ГБ оперативной памяти;
- 512 ГБ SSD;
- 2 ТБ жесткие диски.

На каждом рабочем месте установлено программное обеспечение:

- VMware Workstation Player или аналог;
- Виртуальная машина среды PNetLab (аналог EVE-NG);
- Клиент TightVNC.

Сервер (или комплекс серверов):

- 16-поточный процессор Intel;
- 256 ГБ оперативной памяти;

- 2 x 4 ТБ жесткие диски.

На сервере развёрнуты:

- 4 среды PNetLab (аналог EVE-NG);
- TightVNC (для трансляции рабочего стола преподавателя).

Помимо использования киберполигона в учебном классе, поддерживается дистанционное подключение, что немало важно в современных реалиях.

Кибергород на базе КГУ

В рамках семинара проект был представлен Л.С. Крыжевичем (Курский государственный университет). С проектом можно более подробно ознакомиться в работе [7].

Цель проекта – добавить интерактивности в мероприятия типа хакатонов и CTF и создать макет кибергорода. Не просто поставить проблему, а развернуть сценарий прямо на глазах у присутствующих. Создать эффект погружения.

Каждый объект имитируемого города базируется на технологиях Интернета вещей. Объектами можно управлять удалённо и интегрировать в общую цифровую экосистему.

Город представлен в виде трёхмерных моделей. Можно крушить, ломать, устраивать всевозможные ситуации (в том числе хакерские нападения), которые влияют на функционирование цифровой инфраструктуры и требуют немедленного реагирования.

6. Идея реализации киберполигона на базе хакерспейса

Проект «Академический хакерспейс»

Согласно данным ресурса Techopedia [8], хакерспейс – это:

- Место либо возможность (facility), т. е. предполагается как физическое (чаще), так и виртуальное присутствие и развёртывание;
- Место, где люди со схожими интересами работают над какими-то проектами, делятся знаниями, обсуждают и обкатывают идеи. Заводят полезные связи;
- Сообщество (community), в котором можно найти единомышленников.

Другие названия хакерспейса: опытная лаборатория (hacklab), изобретательский кружок (makerspace), хакерская тусовка (hackspace). Вольный перевод неустоявшихся терминов. Есть ещё понятие «фаблаб (fablab)» – мастерская.

В рамках проекта «Академический хакерспейс» [9] предлагаются следующие активности:

- Анализ и изучение имеющегося опыта (архитектуры микроконтроллеров, микропроцессоров, цифровой электроники и схемотехники, особенностей компонентных соединений, устройств, механизмов, интересных программных решений);
- Выявление возможностей (что можно сделать, из чего, для чего, как и как сделать ещё хитрее и ловче);
- Объяснение того, что происходит «за кадром» видимого и наблюдаемого (исходный код – машинная программа, идея – физические ограничения);
- Разработка идеологии хакерспейса как искусства инженерного мастерства. Методология, философия, социальное проявление.

Проект находится в самом начале своего зарождения, в фазе формирования идеи, высказывания и заявления о своём намерении, приурочен к году педагога и наставника, предполагает планомерное развитие. Пока предполагается, что проект будет функционировать в информационном пространстве, а сам хакерспейс будет разворачиваться виртуально. Формы, границы и правила находятся в процессе формирования и развития самой идеологии академического хакерспейса.

Миникиберполигон на базе хакерспейса

Хакерспейс можно рассматривать как базу с доступным инструментом, аппаратными и программными ресурсами. Если хакерспейс функционарует как фаблаб (небольшая мастерская, предоставляющая возможность изготовления необходимых изделий), то, скорее всего, это физически доступная база, на которой из компонентов можно собрать функциональное устройство, как вариант – модифицировать существующее.

Такая форма может быть использована для направления кибербезопасности, связанного с созданием устройств для тестов на проникновение. Речь идёт об устройствах Интернета вещей. Проникновение можно осуществлять не только за периметр предприятия, но и в частную сеть пользователя или просто на персональное устройство. Сегодня на рынке можно найти множество программируемых электронных устройств и компонентов для реализации подобных решений сетевой направленности [10]. Отлично, если в таком хакерспейсе имеется достаточно сетевого и серверного оборудования для имитации информационной инфраструктуры хотя бы небольшого офиса. Тогда можно проводить живые мероприятия с разбором сценариев атак, сооружением средств защиты и нападения.

Если же на базе хакерспейса реально организовать виртуальное пространство, то можно развернуть на базе имеющегося оборудования виртуализации киберполигон, доступный в том числе и извне.

Интересный сценарий – «киберполигон как крепость», которую можно атаковать снаружи. Допустим, развёрнут киберполигон. Настроены каналы доступа для участников к «воротам крепости». Нужно найти уязвимости и проникнуть за черту сетевого периметра, вывести систему из строя (отключить важные службы или сделать их работу недоступной для внешних пользователей).

Если хакерспейс функционирует на базе учебного заведения, то в его рамках студенты разных курсов и направлений подготовки могут общаться, делиться опытом и разрабатывать совместные проекты, что вполне соответствует духу проектного обучения, которое сейчас активно внедряется в учебные заведения как важная часть профессионального становления студентов.

7. Заключение

В статье был проведён анализ учебно-лабораторной базы, соответствующей потребностям обучения специалистов в области безопасности компьютерных сетей и телекоммуникаций. Представлены отличия лабораторных стендов и киберполигонов. Предложен вариант реализации киберполигона на базе хакерспейса.

Литература

1. Дружин О.В. [и др.] Научно-методологические подходы, принципы формирования учебно-лабораторной базы (киберполигонов, комплексов, лабораторий, учебно-тренировочных средств) по реализации образовательных программ в области информационной безопасности // Информационное противодействие угрозам терроризма. 2015. Т. 1, № 25. С. 150–153.
2. Монахов М.Ю., Тельный А.В., Мишин Д.В. О возможностях использования киберполигонов в качестве оценочных средств определения уровня сформированности компетенций // Информационное противодействие угрозам терроризма. 2015. Т. 1, № 25. С. 269–277.
3. Киреева Н.В. Особенности киберполигона как обучающей системы при подготовке специалистов по информационной безопасности // Актуальные проблемы высшего образования в области инфокоммуникационных технологий. 2023. С. 94.
4. КИБЕРМИР – Национальный киберполигон. URL: `https://cybermir.ru/` (дата обращения: 20.11.2023).
5. Учебно-тренировочная платформа для обучения методам обнаружения, анализа и устранения последствий компьютерных атак. URL: `https://softline.ru/solutions/security/kiberpoligon-ampire` (дата обращения: 20.11.2023).
6. Киберполигон. URL: `https://range.standoff365.com/` (дата обращения: 20.11.2023).
7. Крыжевич Л.С., Бабкин Г.В. Имитационная модель безопасного цифрового взаимодействия «Кибергород 2.0» // Фундаментальные проблемы информационной безопасности в условиях цифровой трансформации. 2019. С. 122–132.
8. What is Hackerspace? – Definition from Techopedia. URL: `https://www.techopedia.com/definition/29567/hackerspace` (дата обращения: 20.11.2023).
9. Академический хакерспейс // Academic Hackerspace. Stepik. URL: `https://stepik.org/course/180116` (дата обращения: 20.11.2023).
10. Гусс С.В. Гетерогенные сети с ячеистой топологией: технологии, моделирование, прототипирование сетевых устройств // Математические структуры и моделирование. 2023. № 3 (67). С. 71–87.

FROM A LABORATORY BENCH FOR STUDYING THE BASICS OF COMPUTER NETWORKS TO A HACKERSPACE FOR INVENTORS AND A COMPETITIVE CYBER TRAINING GROUND

S.V. Guss
Assistant Professor, e-mail: sviat@v-guss.ru

Dostoevsky Omsk State University, Omsk, Russia

Abstract. The article discusses the problem of transition from a traditional laboratory stand for studying the basics of computer networks to a project hackerspace for inventors and a competitive cyber training ground for holding various events: hackathons, championships. Specific examples of software and hardware for configuring and deploying equipment are discussed.

Keywords: stand, hackerspace, cyber ranges.

Дата поступления в редакцию: 20.11.2023