4. Hybrid SDN Networks: A Survey of Existing Approaches / R. Amin, M. Reisslein, N. Shah. — Text : direct // IEEE Communications Surveys & Tutorials. — Vol. 20, Issue 4. — Fourthquarter, 2018.
5. Why use NETCONF/YANG when you can use SNMP and CLI? / Christos Rizos. — URL: https://www.snmpcenter.com/why-use-netconf/ (date of the application: 25.10.2016). — Text : electronic.

И. М. Пономарев, А. А. Селиверстов, Г. А. Пеннер, И. Р. Зулькарнеев
Тюменский государственный университет, г. Тюмень

УДК 004.056

ПРОЕКТИРОВАНИЕ КИБЕРПОЛИГОНА В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация. *В статье представлена концепция обучающего киберполигона в области информационной безопасности. Авторами проанализирован рынок существующих киберполигонов и сделан вывод о необходимости создания решения с возможностью обучения. Описаны требования, предъявляемые к проектируемому киберполигону, и его режимы работы. Разработана математическая модель рейтинговой системы для соревновательного режима. В завершении обозначены дальнейшие направления развития.*

Ключевые слова: *информационная безопасность, обучение, киберполигон, red team, blue team.*

Введение. По данным исследования Всероссийского научно-исследовательского института труда, проведенного в 2019 г., в Российской Федерации потребность в специалистах по информационной безопасности удовлетворена лишь наполовину, что говорит об их дефиците на рынке труда [1]. При этом, согласно информации «Лаборатории Касперского», количество инцидентов информационной безопасности в российских компаниях увеличилось в 4 раза за первые три месяца 2022 г. по отношению к показателю аналогичного периода 2021 г. [2]. Также Национальным координационным центром по компьютерным инцидентам 24 февраля уровень киберугрозы для России был оценен как «Критический» [3].

В связи с высказываниями выше возникает потребность в подготовке специалистов по информационной безопасности с практическими навыками работы реагирования на инциденты и нейтрализации уязвимостей — специалистов «Blue Team», а также тех, кто способен понимать действия злоумышленников во время атаки, проверять существующие информационные системы на наличие уязвимостей и имитировать действия злоумышленника — специалистов «Red Team».

Проблема исследования. Для отработки подобных навыков используются киберполигоны, которые представляют из себя систему моделирования компьютерных атак и защиты от них [4-5]. Задачей исследования является проектирование киберполигона в области информационной безопасности.

Материалы и методы. На российском рынке представлено 6 различных киберполигонов, которые были сравнены (табл. 1) по следующим критериям:

- Обучение — наличие функционала обучения либо базы знаний для пользователей.
- Blue Team — возможность отработки навыков защиты и реагирования на инциденты.
- Red Team — возможность отработки навыков нахождения и эксплуатации уязвимостей.
- Доступность — варианты получения доступа или участия в киберполигоне.
- Формат использования — возможные режимы работы киберполигона.

Таблица 1

Сравнительная таблица российских киберполигонов

Наименование киберполигона, разработчика	*Обучение*	*Blue Team*	*Red Team*	*Доступность*	*Формат использования*
1	*2*	*3*	*4*	*5*	*6*
Ampire (Перспективный мониторинг)	-	+	-	Покупка или аренда	Индивидуально в рамках учебного класса

Окончание табл. 1

1	*2*	*3*	*4*	*5*	*6*
BI.ZONE Cyber Polygon (BI.ZONE + СБЕР)	-	+	-	Только в рамках соревнований	Состязания команд на виртуальной инфраструктуре
Jet CyberCamp (Инфосистемы Джет)	+	+	-	Покупка или аренда	Индивидуально на облачной инфраструктуре
The Standoff (Positive Technologies)	-	+	+	Только в рамках соревнований	Состязания команд на физической и виртуальной инфраструктурах
«Киберполигон» (ООО «Киберполигон»)	-	+	+	Покупка или аренда	Состязания команд на виртуальной инфраструктуре
Национальный киберполигон (Ростелеком)	+	+	-	В рамках соревнований / покупка или аренда	Состязания команд на виртуальной инфраструктуре

Проанализировав полученные данные, авторы выделили следующие проблемы в существующих решениях:

1. Отсутствие обучающих материалов в рамках рассмотренных решений, которые последовательно бы обучали методикам, техникам и инструментарию используемых Red Team и Blue Team.

2. Ни одна из систем, кроме Ampire, не заявлена, как киберполигон с возможностью использования в образовательном процессе, но при этом она сосредоточена только на функционале Blue Team.

3. Системы концентрируются только на индивидуальном или только на командном формате.

В качестве решения данных проблем авторы предлагают концепцию образовательного киберполигона на виртуальной инфраструктуре, который включал бы в себя как теоретические знания в области

Red Team и Blue Team, так и их отработку на практике в индивидуальном и соревновательном режимах.

Проектируемый киберполигон должен обладать следующими возможностями:

- отработка атак (иными словами, тестирование на проникновение) на виртуальную инфраструктуру, имитирующую реальные цифровые сервисы с целью быстрого нахождения и эксплуатации уязвимостей и понимания действий злоумышленников;
- отработка различных подходов к реагированию на возникающие инциденты, которые генерируются как в автоматическом режиме, так и в ручном;
- обучение и тренировка студентов и начинающих специалистов в области ИБ, планирующих работать или работающих по направлениям Red Team или Blue Team;
- апробация различного инструментария и подходы в данных направлениях;
- реализация как индивидуального, так и командного подхода при решении кейсов ИБ;
- масштабируемость на крупное количество участников: от стандартного учебного класса с 15 студентами до командных соревнований на виртуальной инфраструктуре.

Разрабатываемый киберполигон будет состоять из:

- веб-интерфейса, как оболочки для взаимодействия с модулями системы;
- инфраструктуры сервисов, которые могут в зависимости от потребностей быть разными;
- различных подсистем, включающих в себя симуляцию атак, интернет-сервисов, пользовательскую активность, проверяющую систему и инструментарий туториалов.

Киберполигон будет иметь несколько режимов работы: режим обучения, тренировки и соревновательный режим, служащие для повышения уровня навыков в области практической информационной безопасности.

Режим обучения состоит из теоретических материалов, а также обучающих заданий, разбитых на категории по типу уязвимости

(веб, сетевые и локальные системные уязвимости, с возможностью расширения).

Пользователю предоставляется два типа заданий — «атака» и «защита». Для каждого задания пользователю создается индивидуальный виртуальный рабочий стол и индивидуальная виртуальная сетевая инфраструктура с уязвимыми сервисами и машинами, а также предоставляется подробный теоретический материал об уязвимостях и используемых в задании инструментах.

Для выполнения задания типа «атака» (рис. 1) пользователю будет предлагаться найти уязвимость в выделенной для него инфраструктуре. Кроме того, режим будет помогать пользователю, давать подсказки, а также ссылки на обучающий материал. Условием завершения задания является нахождение информации, указанной в задании, и отправка ее в систему. Отработка подобных навыков дает пользователю понимание действий злоумышленника.

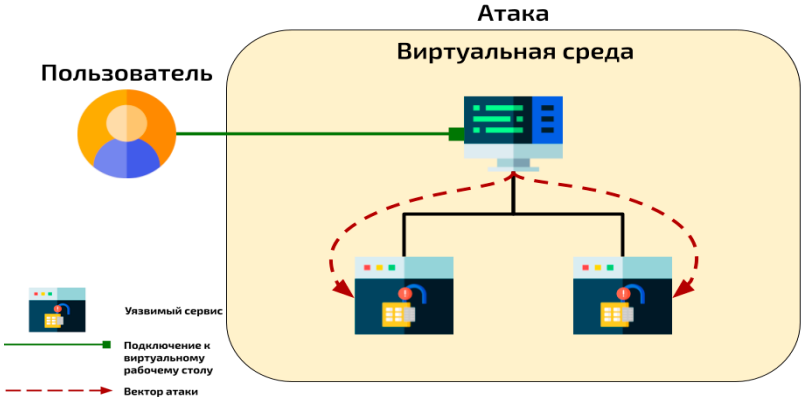

Рис. 1. Схема режима типа «атака»

Для выполнения задания типа «защита» (рис. 2) пользователю также выделяется индивидуальная инфраструктура, но спустя некоторое время на нее начинают идти автоматические атаки, реализующие утечки информации из уязвимых сервисов. При помощи встроенных в инфраструктуру инструментов мониторинга пользователь должен найти и нейтрализовать уязвимости системы и предотвратить

дальнейшие утечки информации. В этом ему способствуют обучающие материалы и подсказки системы. Условием завершения задания являются успешно заблокированные атаки. Таким образом, пользователь учится реагировать на инциденты.

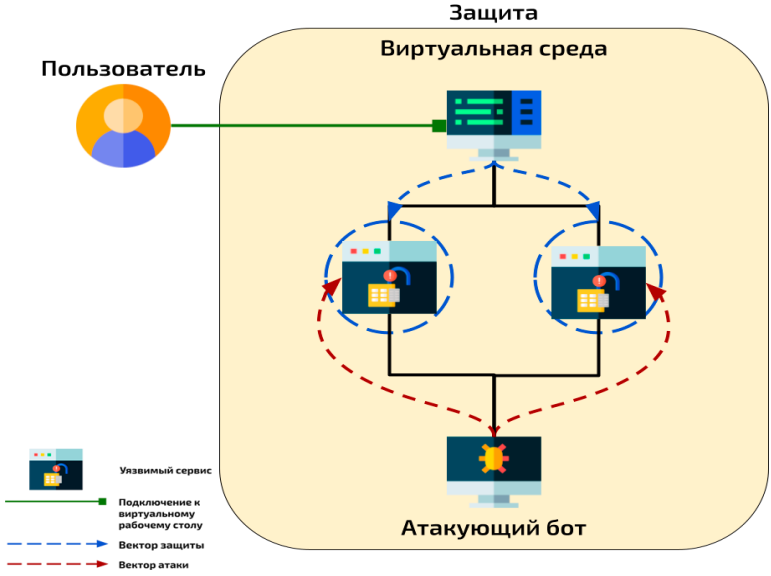

Рис. 2. Схема режима типа «защита»

С целью закрепления пройденного в обучающем режиме материала пользователь должен пройти режим тренировки. В тренировочном режиме используется инфраструктура и сервисы, аналогичные обучающему, однако без подсказок.

В тренировочном режиме типа «атака» целью является получение закрытой информации в уязвимом сервисе и ее отправка в проверяющую систему. Пользователю в зависимости от сложности задания необходимо найти не только одну уязвимость, но и обнаружить и эксплуатировать следующие уязвимости в сервисах, которые стали доступны пользователю при эксплуатации предыдущих.

В тренировочном режиме типа «защита» пользователь должен самостоятельно обнаружить источник утечки информации в уязвимых

сервисах, исправить уязвимость и поддержать работоспособность инфраструктуры на приемлемом уровне, который определяется исходя из задания. Проверку работоспособности режим делает автоматически, выполняя типичные пользовательские задачи на сервисе. По выполнению задания уровень работоспособности сервиса вычисляется соотношением успешных проверок к их общему количеству.

С целью отработки навыков в условиях, близких к реальным, будет использоваться соревновательный режим. Для каждой из команд, участвующих в этом режиме, предоставляется идентичная инфраструктура с уязвимыми сервисами, находящейся в единой сети с инфраструктурами других участников тренировки.

Цель команд — завладеть специально сокрытой информацией соперника, используя найденные вручную уязвимости в его сервисах, отправить ее в проверяющую систему для подсчета, не допустить утечку своей информации и при этом поддерживать сервисы в рабочем состоянии как можно дольше.

Сокрытая информация генерируется автоматически по алгоритму, имитирующему активность пользователей, которые размещают эту информацию на сервисах. За отправку полученной в ходе эксплуатации уязвимостей сокрытой информации соперника в проверяющую систему команде начисляются очки.

Так как данный модуль может масштабироваться на большее число участников, авторами была разработана гибкая система начисления очков командам, участвующим в соревновании. Изначально команды находятся в одинаковых условиях с равным счетом. За успешно проведенную атаку вычисляется число очков, которые будут начислены команде атакующих и отняты у команды защищающихся.

Для решения задачи более точного и гибкого подсчета очков авторами была модифицирована система подсчета рейтинга Эло под условия работы соревновательного режима (1).

$$D_A = \frac{S}{1+e^{\sqrt{A-V}}*K}, \quad (1)$$

где A — количество очков у атакующей команды соревновательного режима за задание, V — количество очков у защищающейся

команды соревновательного режима за задание, K — коэффициент для уменьшения дисперсии получаемых очков (2), S — коэффициент масштабирования очков (3).

$$K = \frac{\ln(\ln(H))}{12} \quad (2)$$

$$S = 50 * \sqrt{H}, \quad (3)$$

где H — уровень сложности проводимого соревнования.

Основываясь на метриках, эмпирическим путем авторы определили необходимые изменения. Были введены коэффициенты для уменьшения дисперсии получаемых очков и их масштабирования.

Конфигурационная переменная H показывает уровень сложности проводимого соревнования, который задается организаторами в блоке первоначальной настройки киберполигона и зависит от команд участников, количества сервисов и уровня сложности сервисов. H может принимать значения в интервале (0, 1) с шагом в 0.05 и влияет, сколько очков команда зарабатывает за атаку (чем выше сложность, тем больше волатильность рейтинга),

Итоговое число очков команды зависит от того, как долго ее инфраструктура находилась в рабочем состоянии. Подсчет времени будет производиться при помощи автоматических проверок работоспособности и исчисляться в процентном соотношении числа успешных проверок к общему количеству проверок.

Результаты. Авторами был исследован рынок киберполигонов в Российской Федерации и выделены проблемы, которые свойственны для этих систем. Выделены структурные элементы и требования к разработке киберполигона с возможными вариантами режимов его работы. Выработана математическая модель рейтинга соревновательного командного режима.

Заключение. Результатом данного исследования является доказательство необходимости создания обучающего киберполигона и представление его концепции, которая может использоваться как основа для разработки. При этом в дальнейших исследованиях для реализации данной концепции необходимо решить следующие проблемы:

• моделирование и создание методов автоматической генерации атак;

• реализация масштабируемости и гибкости в проектируемой инфраструктуре киберполигона;

• разработка интерактивного взаимодействия пользователя с базой знаний в процессе прохождения обучающего режима;

• оценка надежности и безопасности тренировочных и командных режимов.

СПИСОК ЛИТЕРАТУРЫ

1. НКЦКИ: существует угроза кибератак на российские информационные ресурсы. — Текст : электронный // Интернет-портал по информационной безопасности в сети. — 2022. — URL: https://safe-surf.ru/specialists/news/675925/ (дата обращения: 17.05.2022).
2. «Лаборатория Касперского»: количество киберинцидентов в российских компаниях увеличилось в 4 раза. — Текст : электронный // «Лаборатория Касперского» : [сайт]. — 2022. — URL: https://www.kaspersky.ru/about/press-releases/2022_laboratoriya-kasperskogo-kolichestvo-kiberincidentov-v-rossijskih-kompaniyah-uvelichilos-v-4-raza (дата обращения: 17.05.2022).
3. Перспективы развития и кадровое обеспечение области профессиональной деятельности «Информационная безопасность» : [презентация : результаты исследования, 7 октября 2019 г.]. — Текст : электронный // Министерство труда и социальной защиты Российской Федерации : официальный сайт. — 2019. — URL: https://spravochnik.rosmintrud.ru/storage/app/media/Infopmatsionnaya%20bezopacnoct.pdf (дата обращения: 17.05.2022).
4. Назарова О. Г. Информационная безопасность в период становления цифровой экономики в России / О. Г. Назарова, А. Д. Клименко. — Текст : электронный // Экономика. Социология. Право. — 2020. — № 2 (18). — URL: https://cyberleninka.ru/article/n/informatsionnaya-bezopasnost-v-period-stanovleniya-tsifrovoy-ekonomiki-v-rossii (дата обращения: 17.05.2022).
5. Ульянов А. Н. Качество плюс наглядность применение технологий виртуализации вычислительных ресурсов в информационно-образовательной среде. — Текст : электронный / А. Н. Ульянов, М. Г. Столяров, И. В. Стельмах // ВВО. — 2021. — № 6 (33). — URL: https://cyberleninka.ru/article/n/kachestvo-plyus-naglyadnost-primenenie-tehnologiy-virtualizatsii-vychislitelnyh-resursov-v-informatsionno-obrazovatelnoy-srede (дата обращения: 17.05.2022).