Система моделирования киберугроз и управления инцидентами ИБ в ИТ-инфраструктурах (киберполигон Purple Ground)

УДК 519.876.5

Вследствие увеличения количества киберугроз возрастает потребность в подготовке специалистов по информационной безопасности (ИБ), в привитии им практических навыков выявления событий ИБ и управления компьютерными инцидентами в целях минимизации неблагоприятного воздействия кибератак на системы (сервисы, сети). В статье показана актуальность проведения тренировок с использованием систем моделирования воздействий кибератак на реалистичные ИТ-инфраструктуры. Представлен вариант построения киберполигона в виртуальной среде гипервизора, реализованного на открытом ПО.

Ключевые слова: реалистичная ИТ-инфраструктура, киберполигон, обучение, специалист ИБ

Владимир Николаевич Богданов,
кандидат технических наук,
Лауреат Госпремии РФ
v.bogdanov@center-inform.ru

Александр Петрович Вихлянцев,
a.vihlyantsev@center-inform.ru

Петр Сергеевич Вихлянцев,
кандидат технических наук, доцент
p.vikhliantcev@center-inform.ru

Александр Дмитриевич Анисимов
a.anisimov@center-inform.ru

Александр Николаевич Герасимов
a.gerasimov@center-inform.ru

Евгений Александрович Шмырин
e.shmyrin@center-inform.ru

Илья Николаевич Костюлин
i.kostyulin@center-inform.ru

Николай Николаевич Сердюков,
кандидат технических наук
n.serdiukov@center-inform.ru

АО «ЦентрИнформ»

Введение

С развитием информационных и телекоммуникационных систем возрастают киберугрозы, связанные с целенаправленными воздействиями программными средствами на ИТ-инфраструктуры с целью нарушения конфиденциальности, целостности или доступности информации.

С расширением интернет-сервисов и информационных систем количество кибератак растет угрожающими темпами. Кибератаки все более усложняются, воздействуя на потребителей, предприятия и государственные учреждения.

Так, в 2021 году в результате атаки на крупнейшего производителя мяса в США компанию JBS, она была вынуждена выплатить 11 млн долл. за возможность разблокировать свою ИТ-инфраструктуру. В том же году хакеры остановили крупнейший в США нефтепровод Colonial Pipeline. Руководство выплатило злоумышленникам 5 млн долл.

В 2022 году на российские компании было совершено 911 тыс. хакерских атак, что вдвое больше, чем годом ранее. По данным центра мони-

En System for Cyber Threats Simulation and Cybersecurity Incidents Elimination in Information Infrastructures (Cyber Range Purple Ground)

***V. N. Bogdanov**, PhD (Eng.)*
v.bogdanov@center-inform.ru

A. P. Vikhliantcev
a.vihlyantsev@center-inform.ru

***P. S. Vikhliantcev**,*
PhD (Eng.), Associate Professor
p.vikhliantcev@center-inform.ru

A. D. Anisimov
a.anisimov@center-inform.ru

A. N. Gerasimov
a.gerasimov@center-inform.ru

E. A. Smyrin
e.shmyrin@center-inform.ru

I. N. Kostulin
i.kostyulin@center-inform.ru

***N. N. Serdiukov**, PhD (Eng.)*
n.serdiukov@center-inform.ru

JSC CenterInform

Due to the growing cyber threats, the need is increasing to train information security (IS) experts to instill in them practical skills in identifying IS events and managing computer accidents in order to minimize the damage from them. The relevance is shown of training in systems that simulate cyber attack effects on realistic IT infrastructures is shown. An example of cyber range construction in a virtual environment of an open source-based hypervisor software is presented.

Keywords: realistic IT infrastructures, cyber range, training, IS specialist

торинга кибербезопасности IZ:SOC компании «Информзащита», в 2–3 раза по сравнению с 2021 годом возросло количество кибератак на российский государственный сектор [1], который был целью множества преступных группировок (как вымогателей, так и APT), в числе которых Cloud Atlas, Tonto, Gamaredon, MuddyWater, Mustang Panda. Злоумышленники использовали вредоносные программы почти в каждой второй атаке на госучреждения. Наиболее популярными типами кибератак оказались шифровальщики (56 %) и вредоносные программы для удаленного управления (29 %) [2].

Поскольку количество кибератак продолжает увеличиваться, а сами они становятся все более изощренными, потребность в квалифицированных специалистах по информационной безопасности (ИБ) также растет.

По данным исследования компании Cyberbit, дефицит кадров в области информационной безопасности испытывают компании по всему миру [3]. Только в США существует около 460 тыс. таких вакансий, на заполнение которых компании тратят в среднем на 21 % больше времени, чем применительно к другим позициям в ИТ-блоках. В ходе исследований многие участники опроса признались, что не чувствуют себя готовыми к оперативному реагированию на инциденты ИБ и лишь 45 % опрошенных считают, что их команды достаточно квалифицированы.

По расчетам ФСТЭК России, общая потребность только федеральных органов исполнительной власти, органов местного самоуправления и подведомственных организаций к 2025 году составит более 7200 человек, а всего в стране может потребоваться до 30 тыс. высококвалифицированных специалистов по обнаружению, предупреждению и ликвидации компьютерных атак [4].

Актуальность создания специальной учебно-тренировочной базы

Традиционные способы обучения ИБ-специалистов не позволяют достаточно эффективно готовить персонал к своевременному реагированию на быстро меняющиеся киберугрозы. Программы обучения, ориентированные на отражение известных кибератак, быстро устаревают из-за появления новых сценариев последних. Работа в учебном классе под руководством преподавателей малоэффективна для привития обучаемым практических навыков по выявлению событий ИБ и управлению инцидентами ИБ.

Под понятиями «событие ИБ» и «инцидент ИБ» будем понимать следующие определения, установленные стандартами [5, 6]:

- «событие ИБ» – идентифицированное появление определенного состояния актива организации (системы, сервиса или сети), указывающего на возможное нарушение политики ИБ или нарушение в работе средств защиты, или возникновение ранее неизвестной ситуации, которая может иметь отношение к ИБ;
- «инцидент ИБ» – появление одного или нескольких нежелательных или неожиданных событий ИБ, имеющих значительную вероятность компрометации бизнес-операций и указывающих на свершившуюся, предпринимаемую или вероятную реализацию угрозы ИБ для активов организации.

Практические занятия в процессе прохождения обучаемыми производственной практики на «боевых» информационных системах весьма ограничены, а на значимых объектах критической информационной инфраструктуры (КИИ) зачастую невозможны. Особую проблему представляет привитие обучаемым навыков командной работы.

Индивидуальные практические навыки и навыки командной работы по обнаружению кибератак и реагированию на инциденты ИБ могут нарабатываться в ходе кибертренировок с использованием специальной учебно-тренировочной базы – киберполигона – без задействования «боевых» информационных систем.

Под кибертренировкой будем понимать процесс практической подготовки, освоения и привития навыков учащимся путем моделирования кибератак на реалистичные ИТ-инфраструктуры и отработки реакции на инциденты ИБ.

На киберполигоне необходимо имитировать реалистичные ИТ-инфраструктуры, многократно изменять сценарии кибератак и на их основе отрабатывать практические навыки у обучаемых по управлению инцидентами ИБ. Создание такой специальной учебно-тренировочной базы является актуальной практической задачей.

Каким должен быть киберполигон?

Главные требования, предъявляемые к киберполигону, следующие:

- в арсенале киберполигона необходимо иметь шаблоны виртуальных ИТ-инфраструктур (цифровых двойников) и пополняемый набор сценариев кибератак различных уровней сложности;
- программную платформу киберполигона целесообразно реализовать на технологиях Open Source, что позволит упростить обслуживание, повысить гибкость ее адаптации и доработки;
- техническое решение киберполигона должно быть гибким и обладать возможностью настройки под заказчика;
- для управления кибертренировками необходимо иметь функционал автоматического наблюдения за ходом тренировки (скоринга и статистики);
- к разработке киберполигона необходимо привлекать опытных специалистов, имеющих опыт проведения пентестов и киберучений, а также опыт анализа защищенности ИТ-инфраструктур.

Зарубежные учебно-тренировочные инструменты

Практика разработки и применения киберполигонов наиболее развита в США и Израиле. К наиболее известным американским коммерческим решениям можно отнести следующие:

- киберполигон Accenture, созданный для нефтегазовой отрасли и развитый для других отраслей;

- решение Range Force, реализованное на базе облачных технологий и направленное на отработку групповых навыков;
- масштабируемое решение U. S. Cyber Range на базе облачных технологий, разработанное компанией Virginia Tech и ориентированное как на коммерческих клиентов, так и на учебные заведения.

Отдельного внимания заслуживают университетские киберполигоны, созданные в целях подготовки студентов по различным специальностям в области ИБ. Наиболее известными из них являются Raytheon Cyber Operations, Development and Evaluation (CODE) Center (Массачусетс), Regent University Cyber Range (Вирджиния) и Nashville Cyber Range (Теннесси). Некоторые университетские киберполигоны достигли высокого уровня и стали применяться в разных отраслях промышленности и государственных структурах.

Основатели израильской компании KERNELiOS после посещения существующих колледжей и анализа учебных программ по кибербезопасности пришли к пониманию того, что нет никакой связи между тем, что студенты изучают на различных курсах, и знаниями, которые требуются экспертам по кибербезопасности. Исходя из этого, компанией разработано ПО Simulator для проведения киберучений и тренировок.

Другую израильскую платформу – Cyberbit[1] – используют для управления действиями обучаемых по подготовке команд SOC и развития их практических навыков. Платформа Cyberbit предоставляет практическую киберлабораторию и каталог смоделированных кибератак. Киберучения проводятся с имитацией реальных сетей и средств защиты информации, включающих продукты SIEM, firewall и EDR.

Обучающая израильская платформа Cympire[2] предлагает студентам инструмент для простой или инновационной настройки и создания учебного контента. Платформу можно использовать на занятиях под руководством инструктора, а также, по запросу студентов, получать удаленный доступ к ней в нерабочее время.

Коробочное решение французского тренингового центра BlueCyForce, построенного для министерства обороны этой страны, реализовано с использованием технологии гибридного сетевого моделирования (*Hybrid Network Simulation*, HNS) путем комбинирования реального и виртуального оборудования с распределением нагрузки моделирования на несколько серверов с возможностью их связи по сети Интернет. При этом функционал известных коробочных решений весьма ограничен, так как не предусматривает их настройку под конкретного заказчика.

Опыт зарубежных специалистов, несомненно, представляет интерес для российских исследователей и разработчиков киберполигонов. Однако в условиях санкционных ограничений практическое использование в России зарубежных решений затруднено и представляется нецелесообразным.

Российские решения

В настоящее время созданию современной учебно-материальной базы в Российской Федерации уделяется особое внимание. В рамках федеральной программы «Цифровая экономика» Правительством РФ выделены значительные средства на разработку «Национального киберполигона» и на кибертренировки [7].

В основу национального киберполигона положена программная платформа «Кибермир», включающая полунатурное моделирование (*hardware-in-the-loop*, HIL) типовых инфраструктур (офисной, электросети и финансовой организации), имеется скоринговая система. В рамках гибридного подхода киберфизическая система частично моделируется с помощью реального оборудования, а частично – с помощью математических моделей. «Кибермир» функционирует с декабря 2020 года, отвечает большинству требований, предъявляемых к киберполигону, но имеет технические ограничения по адаптации под потребности отдельных заказчиков.

Регулярно проводятся киберучения на базе киберполигона Standoff365[3], включающего в свой состав инфраструктуры энергетических компаний, ИТ-компаний, банков. Для наглядности презентаций киберполигон дополняется макетами линий передачи электроэнергии, электроподстанций, транспорта, зданий и т. п. Доступ к киберполигону осуществляется на бесплатной основе через VPN-подключение. При регистрации на сайте участники получают имя для входа (login), пароль и адрес электронной почты. Для участия в киберучениях подается заявка, и участник получает список IP-адресов. В учениях принимают участие только команды нападающих, в будущем планируется участие команд защиты.

Киберполигон Ampire[4] имитирует кибератаки на шаблонные инфраструктуры, представляющие набор виртуальных машин, моделирующих работу типовой сети организации. Преподаватель запускает и останавливает сценарии атак, выполняет отдельные этапы. Работу команды мониторинга преподаватель оценивает по создаваемым обучаемыми карточкам инцидентов и выдает рекомендаций обучаемым в мессенджере.

Киберполигон КНИТУ Softline[5] создан в 2022 году в Казанском национальном исследовательском технологическом университете (КНИТУ) совместно с компанией Softline в рамках Консорциума «Цифровые технологии». Киберполигон создан на базе российского решения Ampire и ориентирован на обучение студентов техникам отражения атак на инфраструктуры сетей SCADA химической отрасли.

[1] *https://www.cyberbit.com/.*
[2] *https://cympire.com/.*
[3] *https://range.standoff365.com/.*
[4] *https://amonitoring.ru/product/ampire/.*
[5] *https://yandex.ru/video/preview/10349422257430888800/.*

Киберполигон Purple Ground

Архитектура киберполигона

Система моделирования киберугроз и ликвидации инцидентов кибербезопасности в информационных инфраструктурах (киберполигон Purple Ground)[6] от АО «Центр-Информ» представляет собой учебную базу для проведения занятий со специалистами команды мониторинга *Security Operation Center* (SOC), команды защиты BlueTeam – по реагированию на инциденты ИБ, их расследованию и устранению последствий, а также команды атакующих RedTeam – по выявлению уязвимостей и их последующей эксплуатации (рис. 1).

Киберполигон Purple Ground представляет собой программно-аппаратный комплекс позволяющий:

- имитировать виртуальные сетевые ИТ-инфраструктуры с использованием программного конструктора;
- имитировать информационные потоки с помощью программного модуля генерации белого трафика;
- в автоматизированном режиме симулировать компьютерные атаки с помощью программного модуля хакерской активности или в ручном режиме специалистом RedTeam путем подключения или web-доступа к атакуемой ИТ-инфраструктуре;
- организовывать виртуальные рабочие места руководителей, администратора, специалистов SOC и BlueTeam для отработки практических навыков по обнаружению компьютерных атак и реагированию на инциденты ИБ;
- организовывать и проводить кибертренировки в целях отработки обучаемыми практических навыков защиты ИТ-инфраструктур от внешнего и внутреннего нарушителя.

Программное обеспечение киберполигона Purple Ground является российской разработкой. Оно построено с использованием технологий Open Source, включает базовые средства защиты информации Security Onion и имеет возможности подключения проприетарных решений заказчика. Использование открытого ПО позволяет избежать зависимости от сторонних поставщиков и гарантирует гибкость адаптации и доработки решения согласно требованиям заказчика.

В команде разработчиков киберполигона работают опытные специалисты ООО «Авилликс», имеющие опыт участия в киберучениях, проведения тестов на проникновение и анализа защищенности. Интерфейсная часть разработана с участием специалистов ООО «Айди Ист».

Архитектура киберполигона Purple Ground приведена на рис. 2.

Программная платформа содержит серверную часть (ядро), набор программных модулей и клиентскую часть. Серверная часть включает системный сервер для моделирования киберугроз и ликвидации инцидентов ИБ в информационных инфраструктурах (Cyber Range Server), сервер баз данных (Cyber Range DB) и web-сервер.

Набор программных модулей включает генератор сетевого трафика (Network Activity Generator), модуль имитации хакерской активности (Hacker Activity Generator), модуль скоринга и статистики (Scoring and Statistics), генератор отчетов (Report Generator).

Клиентская часть состоит из следующих программных модулей: АРМ администратора киберполигона (Cyber Range Admin), АРМ инструк-

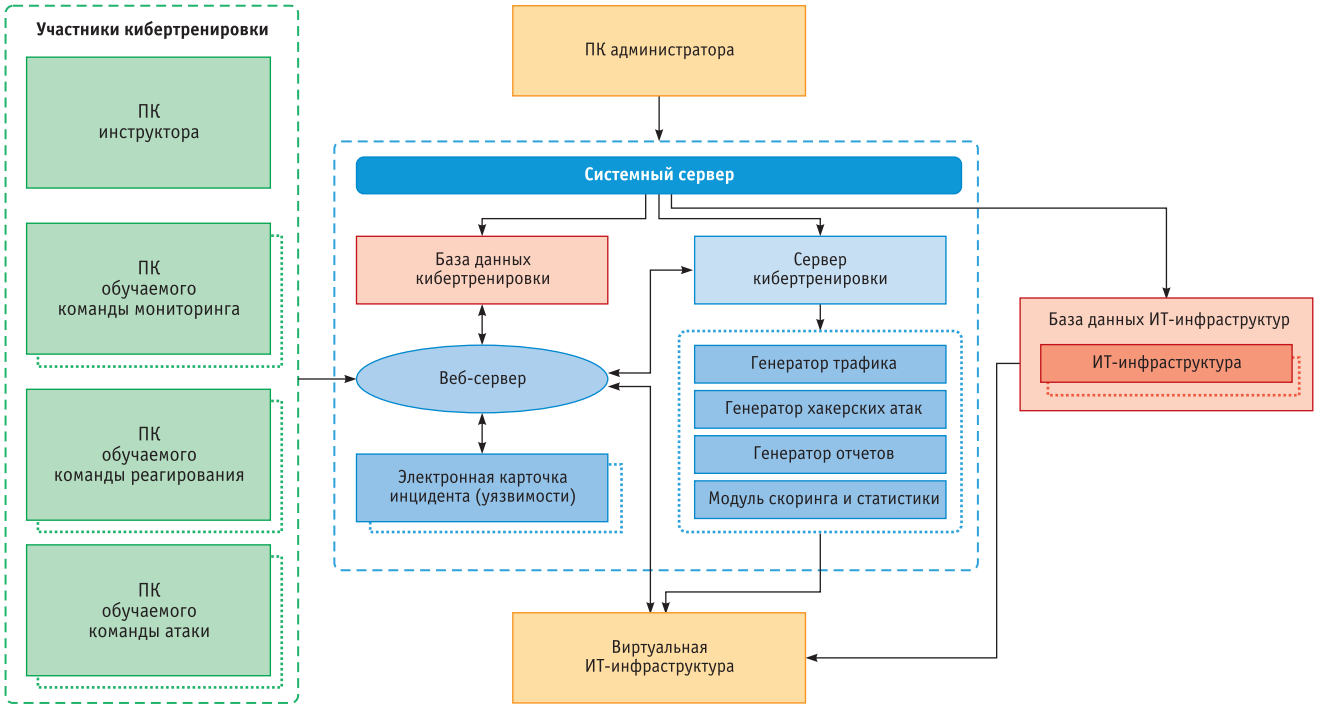

Рис. 1. ***Система моделирования киберугроз и ликвидации инцидентов кибербезопасности в информационных инфраструктурах (киберполигон Purple Ground)***

[6] *https://center-inform.ru/products_and_solutions/software_and_equipment/Cyber-Range/8866413/.*

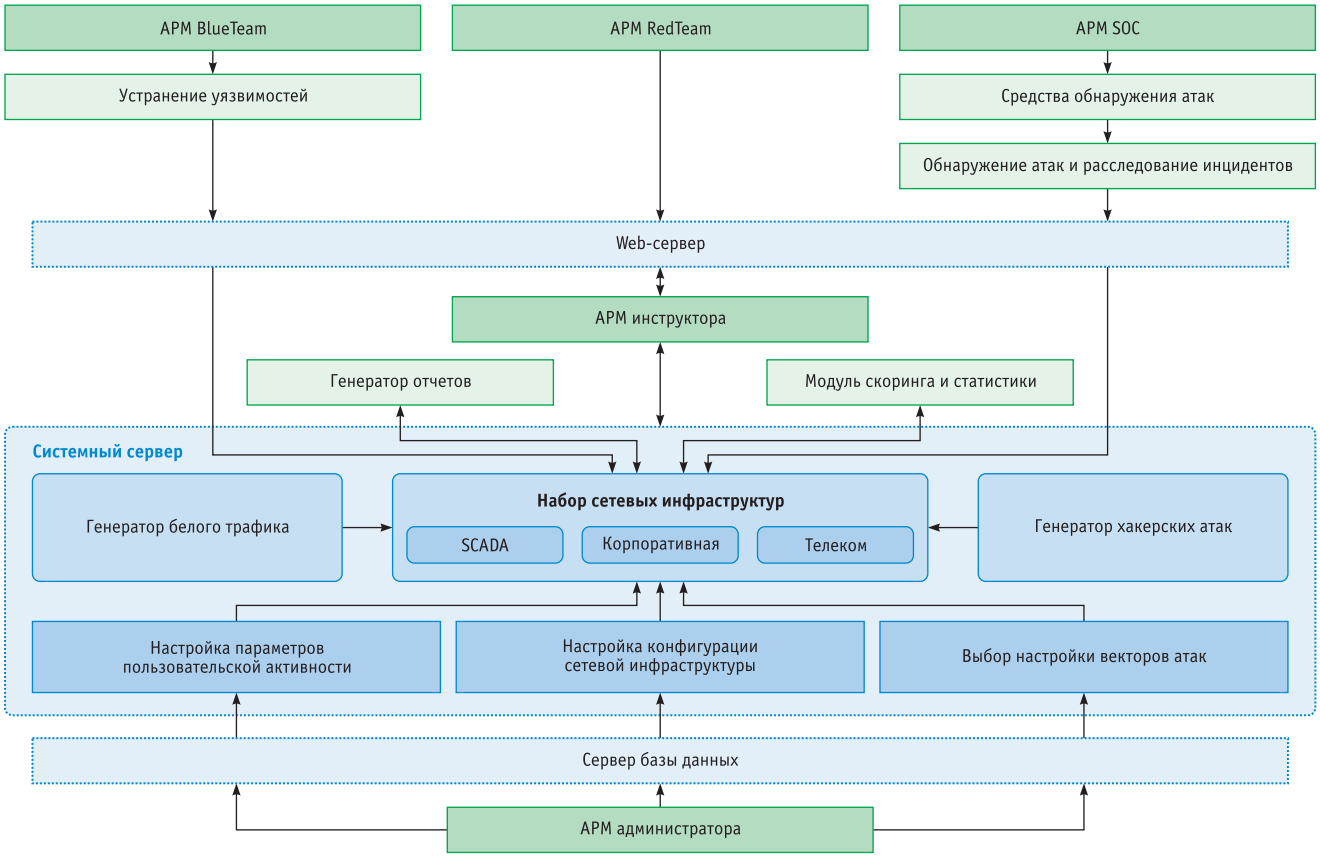

Рис. 2. ***Архитектура киберполигона Purple Ground***

тора (Instructor Workplace), АРМ специалиста SOC (SOC Client) и АРМ специалиста BlueTeam (BlueTeam Client). Количество клиентских автоматизированных мест определяется исходя из потребностей заказчика.

Аппаратная часть киберполигона состоит из серверного оборудования, персональных компьютеров (ноутбуков) пользователей, средств отображения и вспомогательного сетевого оборудования. Оборудование позволяет реализовать базовые виртуальные шаблоны учебных инфраструктур (около 40 хостов) с возможностью обучения группы из 10–15 человек. При необходимости одновременной тренировки нескольких групп состав оборудования потребуется увеличить.

Киберполигон имитирует реалистичную виртуальную ИТ-инфраструктуру и среду ее функционирования в виртуальной программной среде (корпоративная информационная сеть организации, АСУ производственными и технологическими процессами и т. п.). Вариант имитируемой офисной сети с элементами SCADA показан на рис. 3.

Виртуальная среда реализована на адаптированном под задачи киберполигона гипервизоре Proxmox Virtual Environment, backend – на языке программирования Python (фреймворк Django), frontend – на языке Java (фреймворк Vue.js), атакующий модуль – на языках Python, PowerShell, Bash, Ruby. В качестве СУБД выбрано PostgreSQL, обработчик событий включает базу данных TinyDB и набор скриптов.

Базовая версия киберполигона включает следующий набор сценариев атак:

- проникновение во внутреннюю сеть и вывод чувствительных данных в обход средств защиты (Data Compressed Exfiltration);
- внешнее проникновение во внутреннюю сеть и вывод критичных данных с применением вредоносного программного обеспечения (Remote File Copy);
- атака, направленная на остановку и вывод из строя критичных серверов (Server Corruption);
- векторы атак на протоколы передачи данных и устройства внутри АСУ ТП (атака на сеть SCADA);
- скрытное передвижение по сети и захват промышленных систем (EIS Takeover – Advanced);
- атака через уязвимость, не имеющую идентификатора CVE (No 0-day).

Киберполигон имеет встроенные СЗИ для предотвращения вторжений и анализа инцидентов из дистрибутива Security Onion:

- средство предотвращения вторжений на базе хоста (HIDS) – Wazuh;
- средство предотвращения вторжений на базе сети (NIDS) – Snort/Suricata;
- захват пакетов – netsniff-ng;
- межсетевой экран – pfSense;
- отображение событий – Squert/Sguil;
- стек ELK (ElasticEearch, LogStash, Kibana).

Возможно подключение проприетарных решений WAF (Imperva, Wallarm, F5, Barracuda, Fortinet), межсетевых экранов (Palo Alto, Cisco, Fortinet, Checkpoint, Juniper), антивирусов (Kaspersky, McAfee, TrendMicro), систем мониторинга информационной безопасности типа IDS/IPS (TrendMicro, Cisco, McAfee).

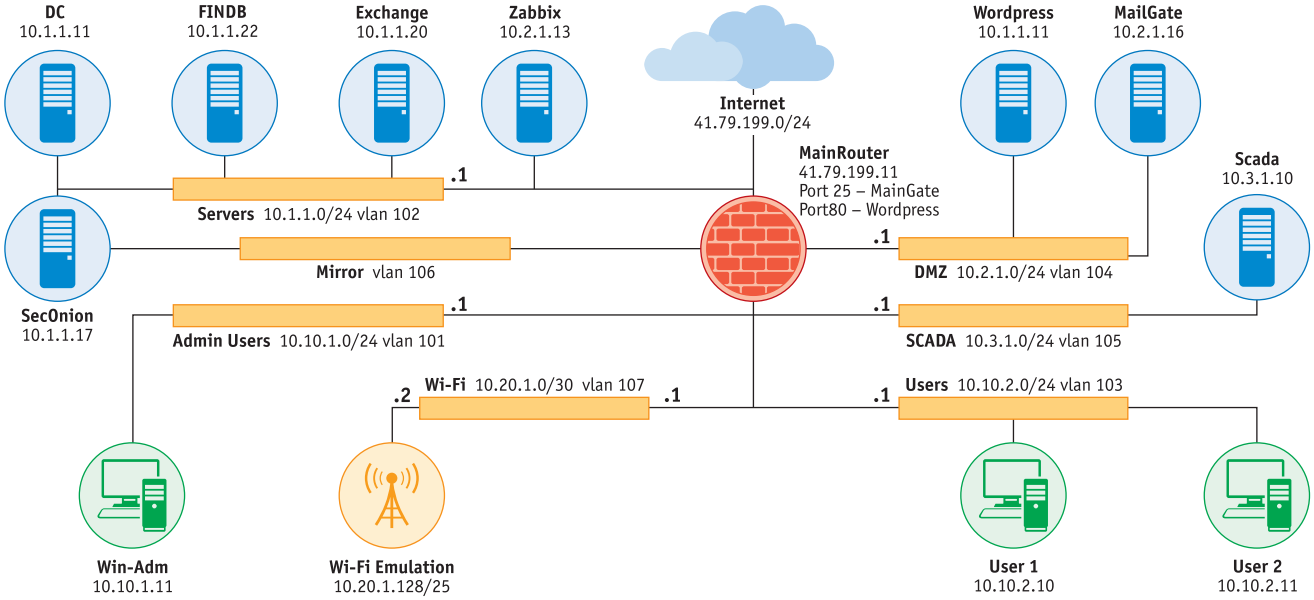

Рис. 3. ***Офисная сеть с элементами SCADA (вариант)***

Организация и проведение кибертренировок

Кибертренировки предполагают отработку обучаемыми взаимосвязанных процессов мониторинга ИБ и управления инцидентами ИБ [8]. Из числа обучаемых формируется, по меньшей мере, две команды: команда мониторинга (команда SOC) и команда реагирования на инциденты (команда BlueTeam), также может формироваться команда атакующих (команда RedTeam).

Кибертренировки можно проводить как путем запуска скриптов, генерируемых модулем имитации хакерской активности, так и путем атаки командой RedTeam. В качестве инструмента выявления уязвимостей атакующие могут использовать сетевой картограф Nmap из дистрибутива Kali Linux [9], публичные (открытые) эксплойты или иные инструменты (сканеры) для проникновения в защищаемую систему (ресурс). Пример сценария кибертренировки иллюстрируется на рис. 4.

Обучение специалистов защиты включает практическую отработку следующих типовых задач:

- обнаружение событий ИБ и идентификация инцидента ИБ;
- реагирование на инцидент ИБ;
- восстановление ИТ-инфраструктуры после инцидента ИБ;
- анализ причин возникшего инцидента и составление отчета об инциденте ИБ.

В основу обучения положен способ и система кибертренировок, направленные на формирование у обучаемых практических навыков командной работы по обнаружению событий ИБ и реагированию на инциденты ИБ в соответствии со стандартами [5, 6].

Инструктор инициирует кибертренировку посредством прямого или удаленного доступа к виртуальной программной среде, предоставляет доступ обучаемым к виртуальной программной среде, имитирует сценарии кибератаки на элементы виртуальной ИТ-инфраструктуры. Интерфейс рабочего места инструктора показан на рис. 5.

Обучаемые из команды мониторинга обнаруживают события ИБ и идентифицируют инциденты ИБ путем выявления соответствующих признаков инцидентов, таких как:

- сообщения от СЗИ, аномалии в сетевом трафике;
- подозрительные процессы на рабочих станциях и серверах виртуальной ИТ-инфраструктуры;
- отклонения в протоколах обмена SMTP, DNS, HTTP(S) и др.

Сведения о каждом обнаруженном инциденте обучаемые фиксиру-

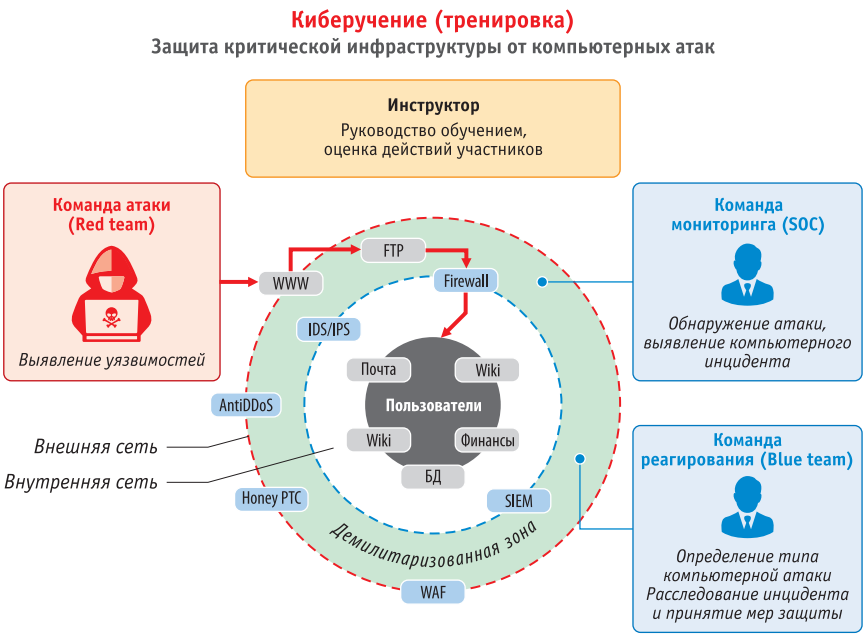

Рис. 4. ***Сценарий тренировки (вариант)***

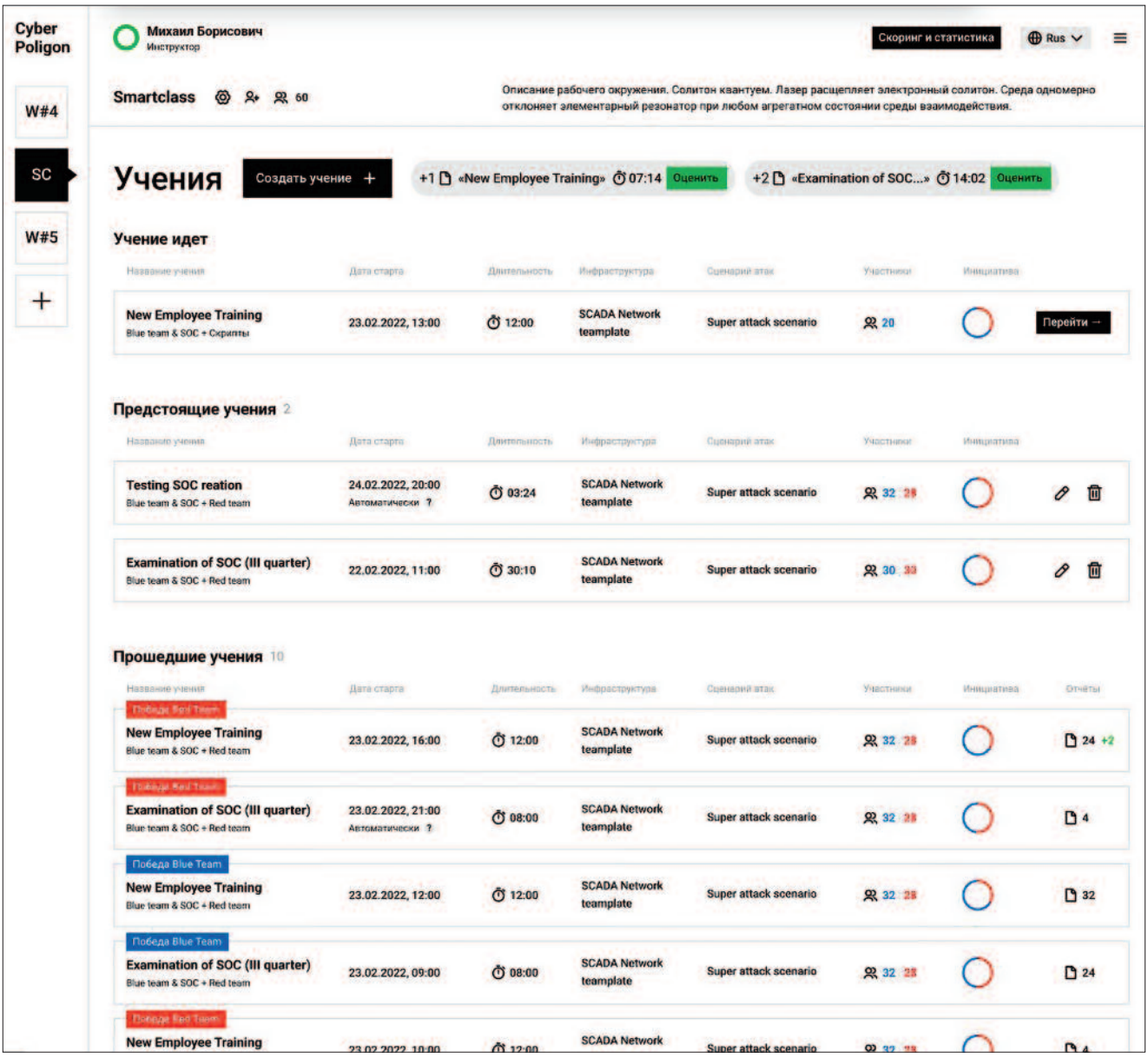

Рис. 5. ***Интерфейс инструктора кибертренировки***

ют в электронной карточке инцидента.

Обучаемые из команды реагирования расследуют инциденты ИБ, дополняют электронную карточку инцидента результатами расследования с указанием мер реагирования, минимизирующих последствия инцидента, и реализуют меры реагирования. Интерфейс специалиста команды BlueTeam показан на рис. 6.

Инструктор наблюдает за действиями обучаемых и оценивает участников с использованием программного модуля скоринга и статистики.

Задачи атакующей команде ставит инструктор на этапе планирования кибертренировки. Здесь можно руководствоваться опытом постановки задач, практикуемым на CTF-чемпионатах. Атакующая команда формирует электронные карточки уязвимостей, в которых фиксируются сведения о выявленных уязвимостях и результатах их эксплуатации.

В качестве примера работы команды RedTeam рассмотрим фишинговую атаку как наиболее частый вид APT-атаки на финансовые компании [10]. Атакующий из команды RedTeam проводит фишинговую рассылку скриптов, изготовленных на базе PowerShell. Пользователь финансового департамента открывает вложение и запускает скрипт, в котором реализована функция обхода антивируса, встроенного в Windows 10. Скрипт проводит разведку, обращаясь к контроллеру домена, и обнаруживает, что пользователь является локальным администратором SQL Server. Подключившись с помощью *winrm* к SQL Server, скрипт получает доступ к аутентификационным данным администратора домена.

Задачи команд мониторинга и реагирования при такой атаке состоят в следующем:

1) обнаружить фишинговые письма и предотвратить их распространение ;

2) определить пользователей, которые успели прочитать содержимое фишингового письма и запустили вредоносный скрипт;

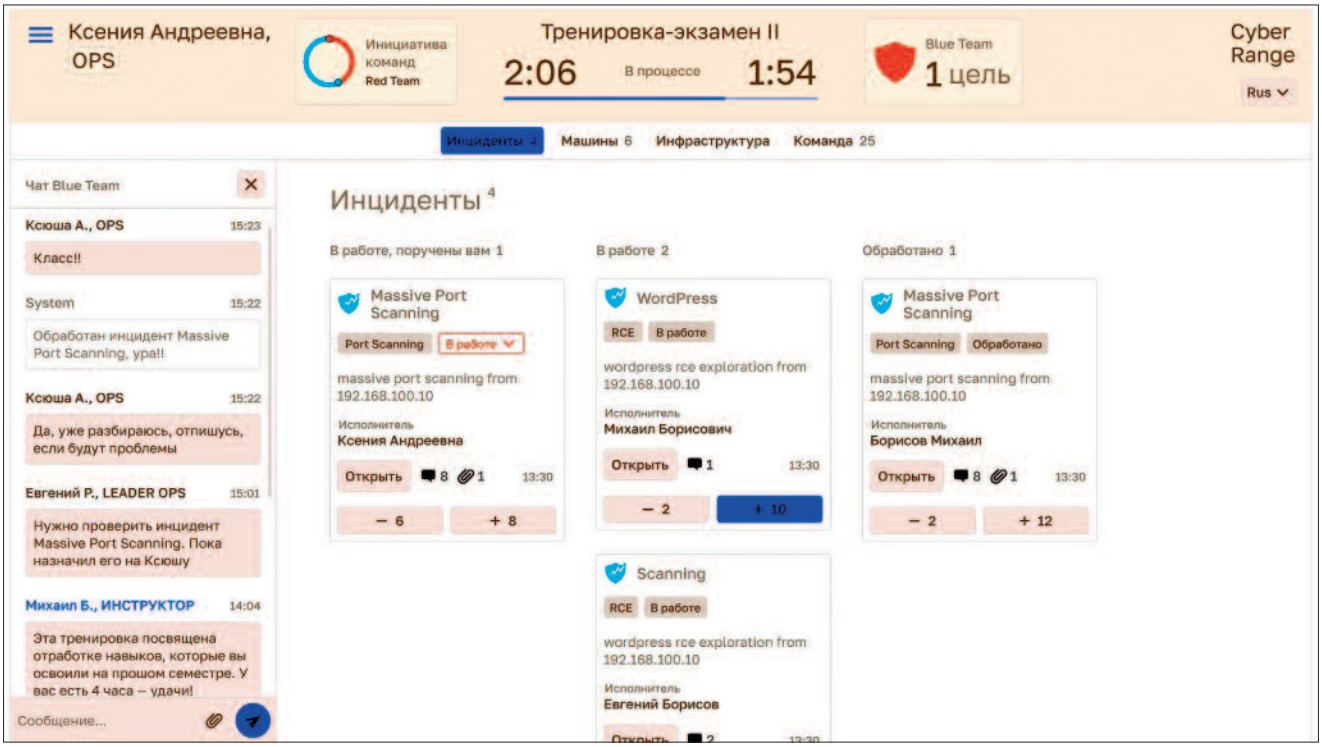

Рис. 6. ***Интерфейс специалиста команды BlueTeam***

3) предотвратить открытие фишингового письма для тех пользователей, которые не успели запустить вредоносный скрипт;

4) расследовать инцидент и установить последствия работы вредоносного скрипта внутри сети;

5) предотвратить развитие атаки и защитить контроллер домена.

Итоги кибертренировки и оценки участникам

Индивидуальные практические навыки каждого обучаемого оценивают по своевременности, полноте и достоверности сведений, указанных им в электронной карточке инцидента. Так, оценивая команду SOC, учитывают временные затраты на корректное обнаружение инцидента ИБ, а оценивая BlueTeam – время, затраченное на реагирование на обнаруженный инцидент ИБ.

Команды оцениваются в зависимости от степени достижения поставленных целей кибертренировки и выполнения отдельных задач. Итоговая оценка складывается из частных: времени реакции на события ИБ, количества правильно обнаруженных и классифицированных инцидентов, количества корректно устраненных уязвимостей и др.

Индивидуальная оценка за кибертренировку j-го обучаемого из команды SOC может рассчитывается по формуле

$$m_{SOC}^{(j)} = \frac{1}{IN_{\text{обн.}}^{(j)}} \sum_{i=1}^{IN_{\text{обн.}}^{(j)}} m_{\text{карт.}}^{(i,j)},$$

где: $IN_{\text{обн.}}^{(j)}$ – количество инцидентов (событий ИБ), обнаруженных и зафиксированных j-м учеником в электронных карточках инцидентов;

$m_{\text{карт.}}^{(i,j)}$ – оценка, выставленная за электронную карточку i-го инцидента (события ИБ).

Оценка за электронную карточку i-го инцидента может рассчитываться по формуле

$$m_{\text{карт.}}^{(i,j)} = \xi_{t}^{(i,j)} \cdot \xi_{\text{дост.}}^{(i,j)} \cdot \xi_{\text{полн.}}^{(i,j)},$$

где: $\xi_{t}^{(i,j)}, \xi_{\text{дост.}}^{(i,j)}, \xi_{\text{полн.}}^{(i,j)}$ – коэффициенты своевременности заполнения карточки, достоверности и полноты информации об инциденте (событии ИБ) соответственно.

Оценка команды SOC может рассчитываться по формуле

$$M_{SOC} = \frac{\sum_{j=1}^{N_{SOC}} m_{SOC}^{(j)}}{N_{SOC}},$$

где: N_{SOC} – количество обучаемых в команде мониторинга.

Индивидуальная оценка за кибертренировку j-го обучаемого из команды реагирования может рассчитываться по формуле

$$m_{\text{BLUE}}^{j} = \frac{IN_{\text{устр.}}^{(j)}}{IN_{\text{обн.}}^{(j)}} \left(1 - \frac{IN_{\text{не устр.}}^{(j)}}{IN_{\text{обн.}}^{(j)}}\right),$$

где: $IN_{\text{обн.}}^{(j)}, IN_{\text{устр.}}^{(j)}, IN_{\text{не устр.}}^{(j)}$ – количество обнаруженных инцидентов, переданных для устранения j-му обучаемому из команды реагирования, устраненных или не устраненных инцидентов соответственно.

Оценка команды BlueTeam может рассчитываться по формуле

$$M_{\text{BLUE}} = \frac{IN_{\text{устр.}}}{IN_{\text{обн.}}} \left(1 - \frac{IN_{\text{не устр.}}^{(j)}}{IN_{\text{обн.}}^{(j)}}\right) K_{\text{И}},$$

где: $K_{\text{И}}$ – коэффициент исправной работы виртуальной ИТ-инфраструктуры.

Индивидуальные и командные оценки могут рассчитываться в относительных единицах в интервале от 0 до 1 или в баллах от 0 до 100.

При оценивании инструктор использует генератор отчетов и модуль скоринга и статистики, которые отслеживают процесс кибертренировки в автоматическом режиме, сравнивают и оценивают обучаемых, со-

ставляют рейтинг. Посредством шаблонов формируют отчет с данными о проведенной кибертренировке.

Оценки могут быть повышены за меньшее по сравнению с нормативным время обнаружения (реагирования) на инциденты либо снижены путем вычитания штрафных баллов за превышение норматива и (или) за свехнормативные простои в работе ИТ-инфраструктуры, вызванные хакерскими атаками (инцидентами).

Допускается корректирование командных оценок из-за сокращенного (увеличенного) численного состава команды относительно оптимального состава.

Нормативные временные показатели, допустимая продолжительность простоев и оптимальная численность команды определяются инструктором кибертренировки по определенной методике или исходя из практического опыта.

Атакующих оценивают по времени, затраченному на выявление уязвимостей и выполнение пентестов, а также по полноте и достоверности сведений, указанных в электронной карточке уязвимостей.

Выводы

Академическое обучение специалистов ИБ необходимо подкреплять практическими кибертренировками и киберучениями в специализированных центрах, которые способны имитировать реальные ИТ-инфраструктуры во всей их сложности и многообразии.

Компании по всему миру активно работают над созданием специализированных инструментов, позволяющих имитировать критическую инфраструктуру и симулировать кибератаки на такие объекты. Использование иностранных решений несет в себе риски, связанные с санкционным давлением отдельных стран на участников рынка ИБ.

Создание и развитие отечественной учебно-тренировочной базы в форме киберполигонов для специалистов ИБ является приоритетной практической задачей.

Эффективное использование киберполигона является необходимым условием успешного обучения и должно сочетаться с разработкой методик обучения специалистов различного уровня подготовки и специализации. ■

ЛИТЕРАТУРА

1. Курашева А., Устинова А. Хакеры атаковали госорганы в три раза чаще в 2022 году // Ведомости, 16.01.2023 [Электронный ресурс]. – URL: https://www.vedomosti.ru/technology/articles/2023/01/16/959104-hakeri-atakovali-gosorgani-chasche (дата обращения: 27.03.2023).

2. Число кибератак в России и в мире // Tadviser, 31.03.2023 [Электронный ресурс]. – URL: https://www.tadviser.ru/index.php/Статья:Число_кибератак_в_России_и_в_мире (дата обращения: 06.04.2023).

3. Дефицит ИБ-специалистов на рынке усугубляют устаревшие программы по их обучению // C-News, 19.01.2022 [Электронный ресурс]. – URL: https://www.cnews.ru/news/top/2022-01-18_defitsit_ib-spetsialistov (дата обращения: 06.04.2023).

4. Марченко А. В. Подготовка специалистов по защите информации // Доклад на Объединенном форуме федеральных учебно-методических объединений в системе высшего образования и среднего профессионального образования по УГСН «Информационная безопасность» и Ассоциации защиты информации «Перспективные образовательные программы подготовки специалистов в области информационной безопасности». – М.: МГТУ, 08.02.2023.

5. ГОСТ Р ИСО/МЭК ТО 18044–2007 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности». – М.: Стандартинформ. – 2009.

6. ISO/IEC 27035:2011 «Information technology. Security techniques. Information security incident management».

7. Королёв И. Власти потратят 1,9 миллиарда на тренировки по кибербезопасности // C-News, 06.06.2022 [Электронный ресурс]. – URL: https://www.cnews.ru/news/top/2022-09-06_vlasti_potratyat_19_milliarda (дата обращения: 27.03.2023).

8. Милославская Н. Г., Сенаторов М. Ю., Толстой А. И. Проверка и оценка деятельности по управлению информационной безопасностью: учеб. пос. для вузов. – 2-е изд., испр. – М.: Горячая линия – Телеком. – 2022. – С. 24.

9. Парасрам Ш., Замм А. и др. Kali Linux. Тестирование на проникновение и безопасность. – СПб.: Питер. – 2022. – 448 с.

10. APT-атаки на кредитно-финансовую сферу в России: обзор тактик и техник // Защита информации. Инсайд. – 2019. – № 6 (90). – С. 50–55.