Научная статья
УДК 004.456

МОДЕЛИРОВАНИЕ СЦЕНАРИЕВ КИБЕРАТАК В КИБЕРПОЛИГОНАХ

✉**Метельков Александр Николаевич.**
Санкт-Петербургский университет ГПС МЧС России, Санкт-Петербург, Россия
✉***metelkov5178@mail.ru***

Аннотация. Цель статьи состоит в исследовании возможностей современной технологии и концепции киберполигонов для решения практических задач, направленных на повышение устойчивости и безопасности компьютерных систем за счет повышения качества подготовки специалистов. В условиях резкого возрастания числа компьютерных атак на информационную инфраструктуру становится весьма актуальным внедрение современных информационных технологий в подготовку специалистов. В развитых странах мира в обучении современным практикам обеспечения информационной безопасности активно применяются киберполигоны. Технология киберполигонов на основе моделирования киберугроз в безопасной среде в течение почти двух десятилетий ее использования в ведущих университетах мира подтвердила свою эффективность для защиты систем и сетей. Методы моделирования эффективно используются для конструирования компьютерной атаки и обучения по разным сценариям. Практика показала особую значимость технологий моделирования кибератак в подготовке персонала современным методам защиты информации. В результате исследования и обобщения зарубежного опыта применения практико-ориентированного подхода с использованием киберполигонов, автор приходит к выводу о целесообразности их внедрения в образовательный процесс ведущих отраслевых и ведомственных высших образовательных учреждений в целях повышения эффективности закрепления знаний, получения навыков в сфере информационной безопасности, формирования компетенций, позволяющих вести дальнейшие масштабные преобразования в области цифровизации государственного управления.

Ключевые слова: киберполигон, обучение, моделирование, кибеугрозы, компьютерная атака

Для цитирования: Метельков А.Н. Моделирование сценариев кибератак в киберполигонах // Науч.-аналит. журн. «Вестник С.-Петерб. ун-та ГПС МЧС России». 2023. № 2. С. 161–176.

Scientific article

MODELING CYBERATTACK SCENARIOS IN CYBERPOLYGONS

✉**Metelkov Alexander N.**
Saint-Petersburg university of State fire service of EMERCOM of Russia, Saint-Petersburg, Russia
✉***metelkov5178@mail.ru***

Abstract. The purpose of the article is to study the possibilities of modern technology and the concept of cyberpolygons for solving practical problems aimed at improving the stability and security of computer systems by improving the quality of training. In the context of a sharp increase in the number of computer attacks on the information infrastructure, it becomes very important to introduce modern information technologies into the training of specialists. In the developed countries of the world, cyberpolygons are actively used in teaching modern information security practices. Cyberpolygon technology based on simulation of cyber threats in a secure environment has been proven to be effective for the protection of systems and networks for almost two decades of its use in the world's leading universities. Practice has shown the particular importance

in the training of personnel in modern methods of protection against computer attacks. As a result of research and generalization of foreign experience in applying a practice-oriented approach using cyberpolygons, the author comes to the conclusion that it is expedient to introduce them into the educational process of leading industry and departmental higher educational institutions in order to increase the effectiveness of consolidating knowledge, gaining skills in the field of information security, and developing competencies , allowing for further large-scale transformations in the field of digitalization of public administration.

Keywords: cyberpolygon, training, modeling, cyberthreats, computer attack

For citation: Metelkov A.N. Modeling cyberattack scenarios in cyberpolygons // Scientific and analytical journal «Vestnik Saint-Petersburg university of State fire service of EMERCOM of Russia». 2023. № 2. P. 161–176.

Введение

На протяжении последних месяцев Национальный координационный центр по компьютерным инцидентам фиксирует резкий рост компьютерных атак. Основными целями беспрецедентной по масштабам киберкомпании против России в связи с проведением спецоперации на Украине является выведение из строя информационной инфраструктуры.

В киберпространстве из-за информационной асимметрии нападение в форме компьютерных атак в целом имеет преимущество перед обороной. Атакующий в основном свободен в выборе времени и способов скомпрометировать информационную систему, в то время как защитник вынужден непрерывно защищать активы от всех возможных актуальных векторов атак. Атаковать компьютерные системы намного проще и дешевле, чем обнаруживать кибератаки и защищаться от них. Первая линия защиты от киберугроз и киберпреступлений заключается в готовности к реагированию на информационные инциденты посредством обучения способам обеспечения кибербезопасности. Обучение может иметь две формы: первая предназначена для специалистов по безопасности и направлена на улучшение понимания последних актуальных угроз, повышение уровня навыков защиты от них и смягчения их последствий. Вторая форма обучения, которая раньше привлекала меньше внимания, направлена на повышение осведомленности о кибербезопасности среди специалистов, не связанных с безопасностью, и широкой общественности. Для проведения учебных программ требуются специальные испытательные стенды и инфраструктура, которые помогают реализовать и выполнять учебные сценарии и предоставляют обучаемым игровую площадку [1–3]. Киберполигон (Cyber ranges, CR) [4, 5], с одной стороны, рассматривают как среду, предназначенную для предоставления испытательных стендов [6], с другой, как платформу для разработки, доставки и использования интерактивных сред моделирования [7–12]. Платформа может быть задумана как группа технологий, используемых для создания и использования среды моделирования. Сторонники второго подхода полагают, что подавляющее большинство существующих киберполигонов государственного и частного секторов предлагают дополнительные возможности. Кроме того, в преобладающих случаях использования киберпространства требуется одна или несколько возможностей, выходящих за рамки среды моделирования. Следовательно, как считают сторонники второго подхода, киберполигон следует определить как платформу, а не как среду моделирования. Среда моделирования – это представление информационно-телекоммуникационных и операционных технологий, мобильных и физических систем, приложений и инфраструктуры организации, включая моделирование атак, пользователей и их действий, а также любых других интернет-сервисов, общедоступных или сторонних сервисов, которые могут использоваться в смоделированной среде. Киберполигон включает в себя комбинацию основных технологий для реализации и использования среды моделирования и дополнительных компонентов, которые необходимы для достижения конкретных вариантов его применения.

Сценарии во многом зависят от приложения и архитектуры сети и адаптируются к целям обучения. Сценарий планируется с использованием последовательности действий, которые осуществляются последовательностью взаимосвязанных шагов обучающихся согласно определенной временной шкале. Для решения учебной задачи обучающиеся должны оценить ситуацию, расследовать и разрешить инцидент. Инженер по управлению (ENG) наблюдает за процессом автоматизации с помощью программного обеспечения (ПО) и осуществляет управление сценарием инцидента. Группа управления и реагирования на инциденты (INC), дежурный менеджер (MOD) и локальная команда операторов (LOT) могут быть активными участниками смоделированного учебного сценария. В процессе тренировок, упражнений или на учениях по кибербезопасности участник для управления определенными ситуациями взаимодействует с киберполигоном [13]. Обычно обучение сосредотачивается на сокращении времени реагирования на инциденты, оценке качества принятия решений и преодолении внезапно возникших трудностей. Связь между целями обучения и оптимальным сценарием остается основополагающей при оценке положительного значения киберполигонов.

Большая часть обучения безопасности и повышение квалификации проводится в режиме онлайн и очных учебных курсов в сравнительно небольшое время на практических занятиях и тренировках. Использование киберполигона меняет ситуацию, поскольку может обеспечить удобный и более экономичный способ практико-ориентированного обучения, а также связанной с ним оценки и сертификации обучения. Технология киберполигона позволяет концентрировать усилия на подготовке высококвалифицированного персонала, способного идти в ногу с развивающимися технологиями и возрастающими рисками кибербезопасности.

Киберполигоны в обеспечении устойчивости сетей и систем

В связи с цифровой трансформацией и переходом к взаимосвязанным интеллектуальным информационным технологиям в сфере государственного управления, предоставления услуг и производства возросли масштабы угроз компьютерных атак. Территориальные органы и организации МЧС России сталкиваются с проблемами, связанными с обеспечением устойчивости и безопасности информационных сетей и систем, увеличением скорости развития угроз и уязвимостей, а также с предотвращением, обнаружением и устранением инцидентов кибербезопасности в сфере управления, координации, контроля и реагирования в области гражданской обороны, защиты населения и территорий от чрезвычайных ситуаций, обеспечения пожарной безопасности и безопасности людей на водных объектах. Примером этому являются взломы «хакерами» серверов радиостанций и телекомпаний 22 и 28 февраля 2023 г. в ряде регионов страны с распространением ложных сведений о воздушной тревоге, которые были опровергнуты МЧС России. Действия киберпреступников благодаря оперативности технических специалистов были пресечены.

В целях повышения устойчивости и безопасности функционирования ведомственных информационных ресурсов возникла необходимость обеспечения их устойчивости за счет повышения готовности и времени реагирования на киберинциденты. Знания, навыки и способности сотрудников МЧС России должны совершенствоваться в соответствии с развитием цифровых технологий и цифровой трансформацией всех сфер жизнедеятельности общества, включая обеспечение различных видов безопасности. Современные технологии обучения часто не предусматривают практических занятий и упражнений. Следовательно, методы и технологии обучения должны адаптироваться к новым требованиям цифровой трансформации и прогресса.

Изучение зарубежного опыта показывает, что обучение может включать следующие темы: политики, обеспечивающие соблюдение кибер- и кибер-физических систем; синергетическую кибербезопасность (от эффективного использования оборудования

и применения безопасности в системных архитектурах до эффективных пользовательских интерфейсов и четкой документации); разработку и развертывание процедур для защиты информационных активов на ИТ-системах от компьютерных атак; угрозы сетевой безопасности, уязвимости и анализ протоколов; создание защищенных распределенных систем; основы кибероперациий; анализ оперативной информации и отчетность. Непрерывное обучение может охватывать наставничество, сопровождение, участие в конференциях, вебинарах или ротациях, которые рекомендуется проводить до 40 ч в год.

Киберполигоны – это искусственно сконструированные виртуальные среды, которые имитируют реалистичные сети и системы и могут применяться для обучения, тестирования, проведения учений или исследований в киберпространстве. Киберполигоны – это виртуальные среды, имитирующие информационные технологии, инфраструктуры операционных технологий, критические инциденты безопасности в информационных системах и используемые в обучении информационной безопасности, тренировках и учениях по кибербезопасности. Основное преимущество использования киберполигона заключается в возможности протестировать в безопасной и изолированной виртуальной среде ситуации и стратегии обороны/нападения от кибератак. Киберполигоны нередко используются в открытом доступе для исследований, обучения, кибертренировок. Обзор киберполигонов сделан в работе [14]. Киберполигоны автоматически не включают промышленные автоматизированные системы управления (Industrial Control System, ICS), однако во многих из них интегрированы компоненты или подсистемы, представляющие операционные технологии.

На практике существуют и другие подходы к обучению, но либо с использованием других технологий (физические устройства, виртуальная реальность), либо с другой целью: обучение, техническое тестирование системы, оценка низкоуровневых процессов. Понятием киберполигон охватывают «инфраструктуру для отработки практических навыков специалистов в области информационной безопасности и информационных технологий, а также для тестирования программного и аппаратного обеспечения путем моделирования компьютерных атак и отработки реакций на них» [15]. Например, для анализа угроз кибербезопасности в сетях беспилотных летательных аппаратов применяют симулятор с открытым исходным кодом UAVSim поверх фреймворка моделирования OMNetþ. Такие симуляторы обеспечивают реалистичную работу в сети, включая организацию очередей. Эмуляторы реализуются в виде ПО с использованием виртуальных машин и обеспечивают большую гибкость в конфигурировании и масштабировании систем, чем физические модели. Имитационные модели [16] предоставляют необходимый инструментарий для исследования и понимания запутанных взаимодействий, включая воздействия антропогенных субъектов. Во многих областях для исследований в сфере кибербезопасности можно получить важные сведения, используя имитационные модели. Ландшафт кибербезопасности расширяется с постоянным появлением новых угроз и принятием контрмер, что требует периодического изменения и добавления в шаблоны новых сценариев реализации компьютерных атак.

В архитектуре киберполигона выделяют прикладной уровень обеспечения его работы, пользовательский интерфейс, инфраструктуру оркестровки сервисов, реализуемую методами физической эмуляции, виртуализации, контейнеризации и применения облачных технологий. Прикладной модуль включает симуляцию интернет-сервисов, пользовательской активности и атак, управление компетенциями, сбор данных и их анализ, оценку и отчетность, разработку сценариев и контента, инструментарий тренеров.

Виртуальная оценка сложных концепций управления и контроля требует использования разнородных сред моделирования. Проблемы разработки заключаются в интеграции нескольких механизмов моделирования с различной семантикой, сценариев моделирования и управления сложными взаимодействиями между ними (рис.). Для координации механизмов моделирования существующим средам моделирования, которые могут предоставлять время выполнения служебным программам, не хватает

всеобъемлющего подхода к интеграции, связывающим функциональную совместимость гетерогенных моделей предметной области при их взаимодействии.

Киберополигон, как показало изучение зарубежного и отечественного опыта, повышает эффективность обучения пользователей и уровень информационной безопасности объектов информатизации в процессе киберучений, способствует повышению квалификации персонала в вопросах информационной безопасности. Традиционный подход к практическому обучению кибербезопасности заключается в использовании специального ПО для создания обучающей среды посредством изоляции физической компьютерной инфраструктуры. Такие инфраструктуры с точки зрения создания и обслуживания затратны и неэффективны из-за необходимости масштабирования для обслуживания большого количества обучаемых.

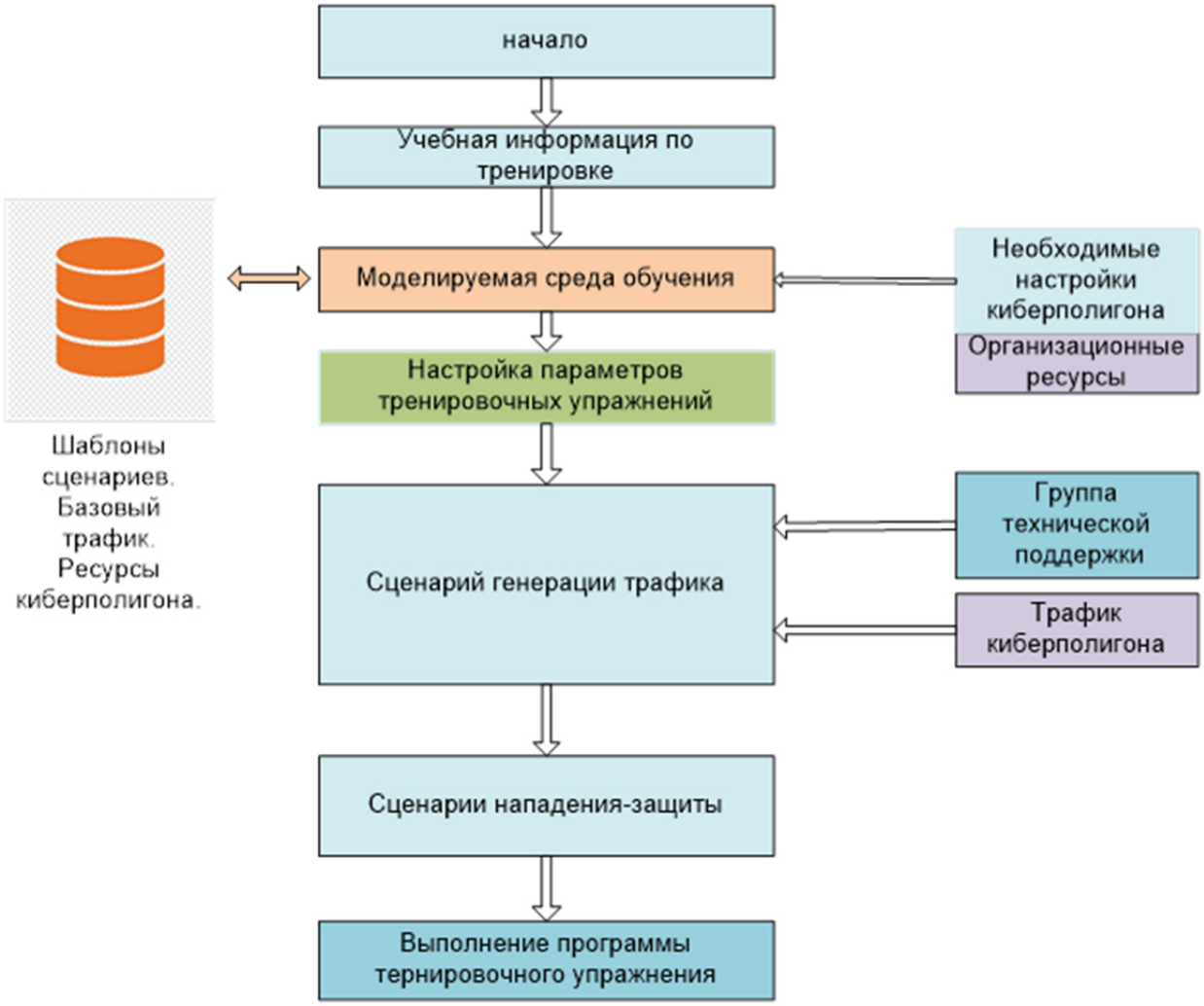

Рис. **Моделирование сценариев в киберполигоне**

Использование технологии виртуализации устраняет эти недостатки. Инфраструктура киберполигона обеспечивает углубление знаний и совершенствование навыков в обнаружении компьютерных атак, расследовании инцидентов, принятии упреждающих мер по их нейтрализации, проведении киберучений и тренировок, координации взаимодействия. Инфраструктура также позволяет тестировать ПО, аппаратные средства, осуществлять учебные мероприятия по поиску уязвимостей и тестированию ПО на защищённость.

В ходе киберучений могут выявляться новые угрозы и уязвимости, повышается уровень персонала служб мониторинга и противодействия инцидентам информационной

безопасности. Проверяется эффективность действий Центра управления безопасности (Security Operations Center) по осуществлению оперативного мониторинга IT-среды и предотвращения киберинцидентов при обнаружении подозрительной активности и принятии необходимых мер.

При этом создать собственный киберполигон и поддерживать его в актуальном состоянии – наукоемкая и ресурсозатратная задача. В связи с влиянием этого фактора за рубежом тематика киберполигонов с 2006 г. вышла на государственный уровень [17, с. 153; 18].

В киберполигонах реализуются различные способы формирования тестовых сред в виде виртуальных машин и «песочниц» (Sandbox), обеспечивающих изоляцию среды. В программно-аппаратных средствах киберполигонов могут отсутствовать или, наоборот, быть заложены возможности предотвращения вредоносных действий, происходящих в приложениях. Поскольку тестовые среды реализованы по-разному, они имеют различные программы, файлы и операционные системы. В то время как виртуальные машины занимают большой объем памяти и обеспечивают полную изоляцию, «песочницам» для работы необходимы относительно небольшие ресурсы памяти, и они обеспечивают гибкую изоляцию. В большинстве зарубежных киберполигонов используются виртуальные машины, а в некоторых одновременно реализованы виртуальные машины и «песочницы». Причина, по которой киберполигоны не полагаются исключительно на «песочницы», заключается в более безопасном тестировании вредоносных программ внутри виртуальных машин, чем в «песочницах». Поскольку «песочницы» обеспечивают гибкую изоляцию, их возможностей недостаточно для тестирования сложных вредоносных программ, и вредоносное ПО может воздействовать на периферийные устройства. Выработка рекомендаций позволяет углубить понимание жизненного цикла киберугроз, выбрать технологии и передовые методы для защиты данных. Рекомендации описывают возможный характер воздействия конкретных кибератак на информационные системы и ресурсы, определяют инструменты, методы и процедуры, которые злоумышленники используют для их развертывания.

Учебные вводные формируют у обучающихся представление о возникающих проблемах в ландшафте угроз, инициируют исследование вредоносных программ, эксплойтов нулевого дня, целевых систем и критических уязвимостей. Среди тактик выделяют целевой фишинг для получения первоначального доступа к локальной сети, развертывание программ-вымогателей для шифрования данных, подключение к не требующему аутентификации для начального доступа программируемому логическому контроллеру с доступом в интернет, эксплуатацию используемых портов и стандартных протоколов уровня приложений для связи с контроллерами и загрузки измененной логики управления и др.

Обеспечение устойчивости функционирования государственных и частных систем и сетей в условиях возрастания реальных и потенциальных угроз кибератак на критически важную, потенциально опасную и общественно значимую инфраструктуру может быть реализовано методом моделирования сценариев киберучений как комплекса взаимосвязанных и взаимозависимых действий или операций государственных и частных структур в киберпространстве. Обеспечение такой устойчивости обладает некоторыми уникальными характеристиками, без знания которых трудно представить использование кибервозможностей в стратегии и планах государства, общества, личности, организаций и предприятий.

По мере усиления зависимости критической инфраструктуры от информационных технологий возрастает ее уязвимость для внешних и внутренних кибератак. Среди таких атак могут быть и кибертеррористические. Опасения в целом ряде развитых и развивающихся государств по поводу кибербезопасности усилились сразу же после возникновения пандемии коронавируса, что побудило многих пользователей перенести часть своей деятельности в интернет.

Компьютерные атаки в настоящее время могут осуществляться на целый ряд целей (APT, advanced persistent threats). Они имеют сложные организацию и процесс реализации вектора атак в виде многошаговых скоординированных распределенных действий с использованием средств компьютерной автоматизации [19]. В ландшафте киберугроз возникает необходимость создания интеллектуальных средств защиты, позволяющих обнаруживать сложные целевые атаки еще на ранних стадиях их реализации с использованием индикаторов компрометации (IOC, Indicator of Compromise) и атак (IOA, Indicator of Attack). Подобные индикаторы позволяют описывать вредоносные объекты, действия или подозрительное поведение системы. При совпадении с индикаторами события кибербезопасности программа относит его к признакам компьютерной атаки. При сопоставлении IOC с IOA проводится «моделирование вектора атаки на различных этапах ее жизненного цикла: обнаружение уже совершенных вредоносных действий злоумышленника, определение значимости и устранение последствий, формирование рекомендаций для предотвращения» [20, с. 2] инцидентов.

Масштаб и взаимосвязанность системных рисков создают проблемы для менеджеров по рискам, которые вместе с другими заинтересованными сторонами разделяют задачу защиты растущей кибернетической и физической инфраструктуры. Масштаб и взаимосвязанность системного риска означает, что часто ни одна организация не имеет достаточной информации, чтобы полностью охарактеризовать риск, и ни одна организация не может управлять им в одиночку. Управление системным риском требует широкого обмена информацией и сотрудничества. Взаимосвязанные системы, состоящие из оборудования, ПО, данных, операционных технологий, физических элементов и других компонентов, лежат в основе инфраструктуры любого современного развитого государства. Источником системного риска может стать зависимость от информационных и коммуникационных технологий, поддерживающих разнообразные приложения. Компоненты в этих системах могут быть скомпрометированы преднамеренными или непреднамеренными уязвимостями, которые могут иметь каскадное воздействие на функции обеспечения безопасности жизнедеятельности и государственного управления. Кроме того, враждебные национальные государства могут субсидировать захват стратегических рынков, навязывая зависимость от ненадежных поставщиков, вытесняя конкурентов из бизнеса и иным образом создавая системные риски на рынках и в цепочках поставок в ряде отраслей и секторов. Системные риски могут быть вызваны передачей ненадлежащего риска. Для минимизации риска, например, в США в процессе семинаров FEMA Region III по кибербезопасности осуществляется презентация национального плана реагирования на киберинциденты, проводятся командно-штабные (настольные) учения и тренировки. В США применяется федеральная виртуальная учебная среда (FedVTE) – бесплатная онлайн-система обучения кибербезопасности по запросу, управляемая Министерством внутренней безопасности США (DHS) и доступная для сотрудников федерального правительства и местных, племенных и территориальных (SLTT) органов власти и управления, государственных подрядчиков, и содержит модули наблюдения, управления рисками и анализа вредоносных программ.

Координация взаимодействия государственных и заинтересованных субъектов посредством формализации обмена данными, формирование системы администрирования и контроля до инцидента повышают качество информационного обмена и готовность к реагированию на киберинциденты.

Анализ научных публикаций и отчетов по киберучениям показывает, что будущее информационной безопасности сосредоточено на учете корреляции множественных инцидентов и коммуникаций, координации и сотрудничестве в реагировании на киберинциденты государственными и частными заинтересованными сторонами. На каждом учебном мероприятии определяются задачи и выделяются критерии оценки эффективности обучения (табл.).

Таблица

Задачи и критерии обучения

Задача обучения	Критерии оценки эффективности
Получение навыков внедрения конфигурации безопасности в конкретной системе	Количество успешных атак, выполненных командами злоумышленников на эту систему
Мониторинг безопасности систем	Количество обнаруженных атак от общего количества выполненных атак
Обработка/реагирование на инциденты	Время восстановления после успешной атаки
Приобретение навыков анализирования логов и проведения экспертизы	Определение количества атак
Выполнение сканирования и перечисления	Количество обнаруженных открытых портов/сервисов по сравнению с общим количеством открытых предварительно настроенных портов
Выполнение DDOS	Время простоя атакуемого сервиса по сравнению с длительностью атаки
«Заметание следов» и установка бэкдора	Количество успешных обращений к цели системы сохраняются до конца учений

В США на федеральном уровне на основе итогов стратегических учений Министерством внутренней безопасности разрабатываются Национальные киберучения и Программа планирования для поддержки планов реагирования на кибербезопасность. Ежегодно с 2010 г. на платформе Cyber Range центра киберзащиты и его вычислительных ресурсов Вооруженными силами Эстонии в г. Таллинне проводятся крупномасштабные киберучения Locked Shields (LS). Платформа имеет технические возможности для отработки действий специалистов в области защиты информационных систем и критической инфраструктуры от кибератак. Для LS разворачивается тренировочная сеть в составе около пяти тысяч виртуальных машин, разнообразных клиентов, серверов и сетевых компонентов. В частности, во время учения в 2019 г. была реализована система управления условной водонапорной станцией, а также реальная сеть мобильной телефонии со своим провайдером. Виртуальные и реальные системы являются легитимными целями противника («красной команды»). В рамках киберучения всем «синим командам» для создания корректных стартовых условий учебная сеть, обозначенная как «Геймнет» (Gamenet), делилась на сегменты, каждый из которых обороняла одна «синяя команда». Доступ в учебную сеть в основном предоставлялся через VPN-соединение, поэтому не имело значения, где во время учения физически находилась «синяя команда».

Для достижения целей учений сценарии можно комбинировать. Иногда они строятся очень сложно, чтобы использовать особенности инфраструктуры организации и предложить участникам возможность выполнять упражнения в контролируемой среде «с боевой стрельбой», также известные как «синие против красных». Традиционная красная команда обычно возглавляется опытными специалистами по безопасности. Хотя командные учения красных и синих долгое время были важным инструментом безопасности, они имеют два основных недостатка. К таким недостаткам можно отнести потребность в большом количестве ручных операций и значительных ресурсов, что ограничивает возможности проводить тестирование. В результате в промежутках между тестированием могут появиться незамеченные уязвимости, и защитники не будут информированы об истинном состоянии своей среды безопасности. В современных системах киберполигонов деятельность красной команды часто осуществляется с разной степенью автоматизации и реализма с участием человека или без него. В продвинутых платформах для упражнений используются

технологии на основе агентов, позволяющие вводить трафик реального использования и специально созданные или сложные векторы атак на основе матрицы MITRE ATT@CK. Инъекции (учебные вводные) могут быть запланированы или отдаваться в ходе тренировки по запросу, контролироваться автоматически заложенным сценарием или инструктором, ведущим упражнение.

Проведение киберучений является исследовательской основой для анализа угроз и последующей выработки мер защиты от кибератак, информирования участников и других заинтересованных лиц и организаций об актуальных угрозах и их возможных последствиях. В результате учений повышается готовность обучающихся принимать упреждающие меры безопасности с использованием современных методов и средств средства обнаружения и предотвращения компьютерных атак.

Для достижения учебных целей [21] важным элементом подготовки киберучений и тренировок является моделирование учебной обстановки [22]. Кибербезопасность становится все более важной областью университетского образования. Очевидно, что существует широкий спрос на образовательные программы для повышения квалификации и наращивания потенциала, но кибербезопасность требует целостного и междисциплинарного подхода. Таким образом, перед учреждениями и педагогами стоит задача создать эффективное предложение и соответствующий опыт для учащихся. Киберполигон может восполнить этот пробел в обучении. Для этой цели его можно использовать в качестве инструмента обучения и для удовлетворения различных требований и потребностей целевых групп. Для этого разрабатывается методология, которая объединит новые и существующие подходы и методы исследований в области преподавания и обучения с предлагаемыми потенциальными стратегиями обучения. Киберполигон позволяет учебным заведениям предоставлять реальное и ориентированное на практику образование в области кибербезопасности, применяя проблемные, многоточечные и ориентированные на общение уроки, а также способствует приобретению междисциплинарных компетенций и навыков обучающихся. В частности, позволяет обучающимся развивать совместные и саморефлексивные подходы, а также улучшать свое понимание и осведомленность о кибербезопасности посредством проблемного и независимого изучения контента. Благодаря интеграции киберпространства и гармонизации образования и обучения могут быть достигнуты различные потребности и цели целевых групп (обучающихся и преподавателей). Для МЧС России это означает, что сотрудники, курсанты и студенты будут лучше подготовлены к сегодняшним и завтрашним вызовам в области кибербезопасности. Преподаватели могут предоставлять учебный контент, адаптированный к целевой группе, ориентированный на уровень знаний и специфичный для темы, что минимизирует рабочую нагрузку и подготовку преподавателей, предоставляя сценарий в абстрактной форме. С использованием киберполигона можно комбинировать различные концепции обучения (теоретические упражнения, совместные практические примеры, интерактивный учебный контент) и облегчать разработку возможных решений по нейтрализации компьютерных атак и обеспечения безопасности цифровой информационной инфраструктуры МЧС России в киберпространстве и его сегментах.

Для киберобразования и обучения в соответствии с существующими требованиями и нормами в сфере информационной безопасности и защиты информации необходимо моделирование реалистичной учебной среды. Возможности обучения и тренинги в реальных сетях весьма ограничены, что связано с затратами, человеческими ресурсами и влиянием на операционную деятельность организаций. Для создания подходящей реалистичной среды, которая позволяет проводить полезное обучение и тренировку широкое распространение получили методы моделирования различных сценариев кибератак в процессе состязательной атаки и защиты.

При разработке моделей сети выделяют следующие основные черты реальных сетей: «…наличие статической и динамической маршрутизации; возможность фильтрации

на любом сетевом узле; поддержка преобразований адресов источника и получателя (SNAT и DNAT); соответствие уязвимости любым локальным и сетевым сервисам» [23, с. 166].

В основе моделей систем защиты информации лежат теории вероятностей и случайных процессов, графов, автоматов и сетей Петри, нечетких множеств, теории игр и конфликтов, катастроф, а также эволюционное моделирование, формально-эвристический и энтропийный подходы [24].

Моделирование эффективно используется для понимания атаки и обучения по разным сценариям. Например, в работе [8] предложен метод моделирования кибербезопасности путем разработки базового компонента и составной модели, называемых соответственно абстрактной моделью блока кибербезопасности (ACSUM) и абстрактной моделью моделирования кибербезопасности (ACSIM). Предлагаемые модели основаны на формализме DEVS (Discrete EVent Systems), «теории моделирования дискретно-событийных систем» [25], обеспечивающей математическую основу для компьютерного моделирования и симуляции, объединяющую различные подходы к симуляции, описывающие формулировку модели, выполнение имитационной модели и процесс ее построения с ключевыми действиями по абстракции модели и упрощению модели, а также организацию библиотек моделей. Особое внимание уделяется интеграции дискретно-событийного и непрерывного подходов к моделированию, а также к дискретно-событийному моделированию непрерывных процессов. Обсуждается выполнение моделирования на параллельных и распределенных машинах и концепции реализации имитационной модели на основе стандарта архитектуры высокого уровня (HLA) Министерства обороны США.

Общая методология позволяет использовать модульные модели, отделяя модели от входных и выходных интерфейсов. В случае изменения сценария необходимо лишь изменить структуру связи, а не дизайн модели. DEVS-формализм был разработан Зиглером (B. Zeigler) в 1976 г. в работе «Теория моделирования и симуляции» (Theory of Modeling and Simulation). DEVS позволяет представить все системы, в которых поведение ввода/вывода может быть описано последовательностью событий с условием, что состояние имеет конечное число изменений в любой конечный интервал времени. Модель DEVS обрабатывает траекторию входного события и в соответствии с этой траекторией и своими начальными условиями определяет выходную траекторию события. Возможно использование DEVS независимо от типа системы, элементов (например, хостов, сетей, приложений) или механизмов обнаружения. DEVS предоставляет метод моделирования для дискретных четных систем. Существует два типа моделей DEVS: атомарная модель и связанная модель. С помощью этих двух моделей можно создавать иерархические и модульные модели. Атомарная модель M представлена следующей формализацией:

$$M=< X, S, Y, \delta_{int}, \delta_{ext}, \lambda, t_a >,$$

где X – множество входных событий; S – множество состояний; Y – множество выходных событий; δ_{int} – внутренняя функция перехода; $S \rightarrow S$; δ_{ext} – внешняя функция перехода; $Q \times X \rightarrow S$; λ – выходная функция; $S \rightarrow Y$; t_a – функция опережения по времени, где $Q=\{(s,e) \mid s \in S, 0 \leqslant e \leqslant t_a(s)\}$, где e – время, прошедшее с момента последнего перехода. Связанная модель определяет структуры связи между атомарными моделями. Связанная модель N представлена следующим формализмом:

$$N=(X, Y, D, Md \mid d \in D, EIC, EOC, IC, Select),$$

где X – набор входов через интерфейсы; Y – набор выходов через интерфейсы; D – набор имен компонентов; Md – модели DEVS, названные одним из элементов D; EIC – связи между внешними входами и входами компонентов; EOC – это соединения между выходами компонента и внешними выходами; IC – это соединения между входами и выходами компонента; Select – это функция разрешения конфликтов, определяющая приоритет выполнения компонентов.

Разработка сценариев атак упорядочивает их поведение с помощью ACSUM, а затем моделируется ACSIM, комбинируя и абстрагируя ACSUM с точки зрения безопасности. Концепции ACSUM и ACSIM позволяют администраторам безопасности моделировать многочисленные проблемы кибербезопасности. С этой целью на национальном и институциональном уровнях создаются специальные подразделения, формируется организационная, методическая и технологическая платформа для проведения тренингов и учений по кибербезопасности. Особенностью критической инфраструктуры является ее функционирование посредством киберпространства, что формирует условия для оказания дистанционного деструктивного воздействия на важные объекты. Некоторыми из таких объектов из любой точки планеты возможно не только управлять, но и переводить их в деструктивный режим функционирования, вплоть до физического разрушения.

Моделирование учебных угроз подразумевает выработку вводных для обучаемых, отражающих угрозы для информационных систем и информационно-телекоммуникационной инфраструктуры, на основании которых участники учений принимают решения по нейтрализации актуальных угроз. Модель угроз безопасности информации согласно ГОСТ Р 53114–2008 «Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения» представляет собой физическое, математическое, описательное представление свойств или характеристик угроз безопасности информации [26]. Наиболее семантически точным, на взгляд автора, является определение моделирования как процесса «замещения одного объекта другим с целью получения информации о важнейших свойствах объекта-оригинала с помощью объекта-модели» [27, с. 12].

Модель угроз разрабатывается в соответствии с требованиями законодательства и регуляторов по защите информации и, как правило, оформляется в виде документа, определяющего основные исходные условия для проверки соответствия системы защиты информационной системы заданным требованиям. Модель может включать специально организованный вектор угроз безопасности информации, воздействующих на характерные уязвимости информационных систем и исходящих от источников угроз, имеющих антропогенный и техногенный характер. Модели, при необходимости подлежат адаптации по итогам проведения киберучений и тренировок. При разработке модели угроз безопасности информации для автоматизированных (информационных) систем используются нормативная база и методики Федеральной службы безопасности (ФСБ) России и Федеральной службы по техническому и экспертному контролю (ФСТЭК) России (Гостехкомиссии). Результаты моделирования отражаются в модели угроз безопасности информации – формализованном описании актуальных угроз. Такая модель формируется для информационных ресурсов и компонентов систем и сетей, включенных в состав моделируемых угроз. Негативные последствия реализации (возникновения) угроз безопасности информации, оценка актуальности, возможные объекты воздействия кибератак, возможности и способы их осуществления отражены в Методике оценки угроз безопасности информации (утв. ФСТЭК России 5 февраля 2021 г.).

Моделирование основано на формализации логической последовательности: «множество выявленных уязвимостей ПО; множество релевантных угроз; множество наиболее вероятных сценариев реализации угроз; возможные киберфизические последствия количественной оценки рисков нарушения кибербезопасности» [28] с учетом требований нормативных документов регуляторов – ФСБ России и ФСТЭК России.

Целью моделирования угроз является выявление условий и факторов, приводящих или способных привести к нарушению конфиденциальности, целостности, доступности, неотказуемости, подотчетности, аутентичности и достоверности информации и (или) средств её обработки, а также к нарушению или прекращению функционирования систем и сетей. В качестве угроз безопасности информации при моделировании рассматриваются неправомерные действия и (или) воздействия на ресурсы или компоненты систем или сетей, в результате которых возможно нарушение безопасности информации и (или) нарушение

или прекращение функционирования систем и сетей, повлекшее наступление негативных последствий.

Большинство современных систем являются территориально-распределенными, что теоретически увеличивает количество актуальных угроз, ввиду сложности инфраструктуры, особенностей информационной технологии, общедоступных незащищенных каналов связи. Моделирование имитационных кибератак в территориально-распределенных информационных системах позволяет побуждать участников сообщать о предполагаемых или подтвержденных киберинцидентах, в том числе о случаях, когда затронутая организация может быть заинтересована в государственной помощи в устранении последствий действий нарушителя (противника), восстановлении операций и рекомендациях для дальнейшего обеспечения информационной безопасности.

Киберполигоны и экосистема вокруг них – «горячая тема» при рассмотрении кибербезопасности, повышении киберустойчивости, проведении исследований или экспериментов с модификациями инфраструктуры [29]. В динамической технологии киберполигона может быть реализовано моделирование поведения, может имитироваться влияние реальных взаимодействий пользователя с системой [30].

Установлено, что проведение киберучений является исследовательской платформой для анализа угроз и последующей выработки мер защиты от компьютерных атак, информирования участников и других заинтересованных лиц и организаций о последних угрозах и их последствиях, тенденциях в развитии угроз для того, чтобы они могли принимать упреждающие меры для повышения безопасности своих сред, совершенствования мер защиты, методов и средств средства обнаружения и предотвращения кибератак.

Заключение

Создание организационно-технологической и методологической инфраструктуры киберполигона формирует основу для проведения киберучений и тренировок, совершенствования уровня практической подготовки в выявлении и расследовании инцидентов информационной безопасности и компьютерных атак, улучшения взаимодействия между подразделениями, внедрения превентивных мер по предупреждению компьютерных атак у обучающихся, а также по тестированию ПО на защищённость и проведению соревнований по поиску уязвимостей [31, 32].

Для нейтрализации и локализации кибератак, обеспечения устойчивости и безопасности информационной инфраструктуры организациям необходимо обнаруживать и быстро корректировать состояние безопасности в отношении вновь обнаруженных атак на их расширяющейся поверхности, то есть общем числе потенциально уязвимых объектов в компьютерной системе. Для этого необходимо постоянно обучать персонал. Одним из эффективных современных способов обучения является внедрение в практику образовательных учреждений технологии киберполигонов.

Статья подготовлена в рамках выполнения в 2023 г. прикладных научных исследований Санкт-Петербургского университета ГПС МЧС России по заказу МЧС России, регистрационный номер ЕГИСУ НИОКТР № 123030100017-2 и № 123030100009-7 от 1 марта 2023 г.

Список источников

1. Ait cyber range: Flexible cyber security environment for exercises, training and research: In Proc. of the 1st European Interdisciplinary Cybersecurity Conference (EICC’20) / M. Leitner [et al.]. Rennes, France, 2020. P. 1–6.

2. Cyber ranges and testbeds for education, training, and research / N. Chouliaras [et al.] // Applied Sciences. 2021. № 11 (4). P. 1809–1831.

3. Brilingaite A., Bukauskas L., Kutka E. Development of an educational platform for cyber defence training: In Proc. of the 16th European Conference on Cyber Warfare and Security (ECCWS'17). Dublin, Ireland, 2017. P. 73–81. Academic Conferences International Limited.

4. Kypo cyber range: Design and use cases: In Proc. of the 12th International Conference on Software Technologies (ICSOFT'17) / J.Vykopal [et al.]. Madrid, Spain. 2017. P. 310–321. SciTePress.

5. Karjalainen M., Kokkonen T. Comprehensive cyber arena; the next generation cyber range: In Proc. of the 4th IEEE European Symposium on Security and Privacy Workshops (EuroS&PW'20). Genoa, Italy. 2020. P. 11–16. IEEE.

6. Yamin M.M., Katt B., Gkioulos V. Cyber ranges and security testbeds: Scenarios, functions, tools and architecture. Comput. Secur. 2020. № 88. P. 101636.

7. Jiyeon KIM, Hyung-Jong Kim. Defining Security Primitives for Eliciting Flexible Attack Scenarios Through CAPEC Analysis // Information Security Applications. WISA 2014. Lecture Notes in Computer Science. Springer, Cham. 2015. Vol. 8909. P. 370–382.

8. Sarjoughian H. Introduction to DEVS modeling &simulation with JAVA: Developing component-based simulation models // Arizona State University. 2005.

9. Ingalls Ricki G. Introduction to simulation: in Proc. of the 40th Conference on Winter Simulation. Winter Simulation Conference. 2008.

10. Whitley John N. Attribution of attack trees. Computers&Electrical Engineering. 2011. № 37 (4). P. 624–628.

11. Saini Vineet, Qiang Duan, Vamsi Paruchuri. Threat modeling using attack trees // Journal of Computing Sciences in Colleges. 2008. № 23 (4). P. 124–131.

12. Have it your way: Generating customized log datasets with a model-driven simulation testbed / M. Landauer [et al]. Transactions on Reliability. 2021. № 70 (1). S. 402–415. IEEE.

13. Обучение методам обнаружения компьютерных атак на базе киберполигона кафедры «Информационной безопасности» РТУ (МИРЭА) / А.П. Коваленко [и др.] // Методы и технические средства обеспечения безопасности информации. 2021. № 30. С. 39–44.

14. Davies J., Margat S. Review of cyberproving grounds and test benches (№ DSTO-GD-0771) // Cyber Electronic Warfare Division, Defense Science and Technology Organization DSTO, Edinburgh, AU 5111. Australia. 2013.

15. Правила предоставления субсидий из федерального бюджета на введение в эксплуатацию и обеспечение функционирования киберполигона для обучения и тренировки специалистов и экспертов разного профиля, руководителей в области информационной безопасности и информационных технологий современным практикам обеспечения безопасности (с изм. и доп. от 27 февр. 2021 г.; утв. постановлением Правительства Рос. Федерации от 12 окт. 2019 г. № 1320). Доступ из справ.-правового портала «Гарант».

16. Жуков М.М., Баркалов Ю.М., Телков А.Ю. Методологический подход к имитационному моделированию при исследовании практической эффективности систем защиты от сетевых кибератак // Вестник Воронежского института МВД России. 2022. № 1. С. 24–39.

17. Цифровые технологии и проблемы информационной безопасности / под ред. Е.В. Стельмашонок, И.Н. Васильевой. СПб.: Изд-во СПбГЭУ, 2021. 163 с.

18. Ferette L. European Union Agency for Cybersecurity. The 2015 report on national and international cyber security exercises: survey, analysis and recommendations, European Network and Information Security Agency. 2015.

19. A targeted attack for enhancing resiliency of intelligent intrusion detection modules in energy cyber physical systems: In 19th International Conference on Intelligent System Application to Power Systems (ISAP) / El. Hariri M. [et al.]. 2017. P. 1–6. IEEE.

20. Васильев В.И., Кириллова А.Д., Вульфин А.М. Когнитивное моделирование вектора кибератак на основе меташаблонов CAPEC // Вопросы кибербезопасности. 2021. № 2 (42).

21. Lessons learned from complex hands-on defence exercises in a cyber range: In Proc. of the 47th IEEE Frontiers in Education Conference (FIE'17) / J. Vykopal [et al.]. Indianapolis, Indiana, USA. 2017. P. 1–8. IEEE.

22. AIT Cyber Range: Flexible Cyber Security Environment for Exercises, Training and Research / Leitner Maria [et al.] // Proceedings of the European Interdisciplinary Cybersecurity Conference. 2020. P. 49.

23. Абрамов Е.С., Андреев А.В., Мордвин Д.В. Применение графов атак для моделирования вредоносных сетевых воздействий // Известия Южного федерального университета. Технические науки. 2012. № 126 (1). С. 165–174.

24. Курилов Ф.М. Моделирование систем защиты информации. Приложение теории графов // Технические науки: теория и практика: материалы III Междунар. науч. конф. Чита: Изд-во Молодой ученый, 2016. С. 6–9.

25. Zeigler Bernard P., Herbert Praehofer, Tag Gon Kim. Theory of modeling and simulation. 2nd edition, Academic Press, 2000 // Theory of Modeling and Simulation: Integrating Discrete Event and Continuous Complex Dynamic Systems.

26. ГОСТ Р 53114–2008. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. URL: htth:// base.garant.ru (дата обращения: 24.04.2023).

27. Бутырский Е.Ю., Матвеев А.В. Математическое моделирования систем и процессов. СПб.: Стратегия будущего, 2022. 733 с.

28. Метельков А.Н. Киберучения: зарубежный опыт защиты критической инфраструктуры // Правовая информатика. 2022. № 1. С. 51–60.

29. The Current State of The Art and Future of European Cyber Range Ecosystem / C. Virág [et al.]. 2021 IEEE International Conference on Cyber Security and Resilience (CSR), Rhodes, Greece. 2021. P. 390–395.

30. User Behavior Simulation in ICS Cyber Ranges: 19th Annual International Conference on Privacy / C. Liu [et al.]. Security&Trust (PST), Fredericton, NB, Canada. 2022. P. 1–5.

31. Матвеев А.В., Метельков А.Н., Шестаков А.В. Риски кибератак: ликвидация последствий проявлений кибертерроризма и чрезвычайных ситуаций // Вестник Воронежского института ФСИН России. 2023. № 1. С. 98–106. EDN AYXLTO.

32. Методика технико-экономической оценки вариантов построения организационно-технической системы класса «киберполигон» / А.В. Матвеев [и др.] // Инженерный вестник Дона. 2023. № 6. URL: http://www.ivdon.ru/ru/magazine/archive/n6y2023/8474/.

References

1. Ait cyber range: Flexible cyber security environment for exercises, training and research: In Proc. of the 1st European Interdisciplinary Cybersecurity Conference (EICC'20) / M. Leitner [et al.]. Rennes, France, 2020. P. 1–6.

2. Cyber ranges and testbeds for education, training, and research / N. Chouliaras [et al.] // Applied Sciences. 2021. № 11 (4). P. 1809–1831.

3. Brilingaite A., Bukauskas L., Kutka E. Development of an educational platform for cyber defence training: In Proc. of the 16th European Conference on Cyber Warfare and Security (ECCWS'17). Dublin, Ireland, 2017. P. 73–81. Academic Conferences International Limited.

4. Kypo cyber range: Design and use cases: In Proc. of the 12th International Conference on Software Technologies (ICSOFT'17) / J.Vykopal [et al.]. Madrid, Spain. 2017. P. 310–321. SciTePress.

5. Karjalainen M., Kokkonen T. Comprehensive cyber arena; the next generation cyber range: In Proc. of the 4th IEEE European Symposium on Security and Privacy Workshops (EuroS&PW'20). Genoa, Italy. 2020. P. 11–16. IEEE.

6. Yamin M.M., Katt B., Gkioulos V. Cyber ranges and security testbeds: Scenarios, functions, tools and architecture. Comput. Secur. 2020. № 88. P. 101636.

7. Jiyeon KIM, Hyung-Jong Kim. Defining Security Primitives for Eliciting Flexible Attack Scenarios Through CAPEC Analysis // Information Security Applications. WISA 2014. Lecture Notes in Computer Science. Springer, Cham. 2015. Vol. 8909. P. 370–382.

8. Sarjoughian H. Introduction to DEVS modeling &simulation with JAVA: Developing component-based simulation models // Arizona State University. 2005.

9. Ingalls Ricki G. Introduction to simulation: in Proc. of the 40th Conference on Winter Simulation. Winter Simulation Conference. 2008.

10. Whitley John N. Attribution of attack trees. Computers&Electrical Engineering. 2011. № 37 (4). P. 624–628.

11. Saini Vineet, Qiang Duan, Vamsi Paruchuri. Threat modeling using attack trees // Journal of Computing Sciences in Colleges. 2008. № 23 (4). P. 124–131.

12. Have it your way: Generating customized log datasets with a model-driven simulation testbed / M. Landauer [et al]. Transactions on Reliability. 2021. № 70 (1). S. 402–415. IEEE.

13. Obuchenie metodam obnaruzheniya komp'yuternyh atak na baze kiberpoligona kafedry «Informacionnoj bezopasnosti» RTU (MIREA) / A.P. Kovalenko [i dr.] // Metody i tekhnicheskie sredstva obespecheniya bezopasnosti informacii. 2021. № 30. S. 39–44.

14. Davies J., Margat S. Review of cyberproving grounds and test benches (№ DSTO-GD-0771) // Cyber Electronic Warfare Division, Defense Science and Technology Organization DSTO, Edinburgh, AU 5111. Australia. 2013.

15. Pravila predostavleniya subsidij iz federal'nogo byudzheta na vvedenie v ekspluataciyu i obespechenie funkcionirovaniya kiberpoligona dlya obucheniya i trenirovki specialistov i ekspertov raznogo profilya, rukovoditelej v oblasti informacionnoj bezopasnosti i informacionnyh tekhnologij sovremennym praktikam obespecheniya bezopasnosti (s izm. i dop. ot 27 fevr. 2021 g.; utv. postanovleniem Pravitel'stva Ros. Federacii ot 12 okt. 2019 g. № 1320). Dostup iz sprav.-pravovogo portala «Garant».

16. Zhukov M.M., Barkalov Yu.M., Telkov A.Yu. Metodologicheskij podhod k imitacionnomu modelirovaniyu pri issledovanii prakticheskoj effektivnosti sistem zashchity ot setevyh kiberatak // Vestnik Voronezhskogo instituta MVD Rossii. 2022. № 1. S. 24–39.

17. Cifrovye tekhnologii i problemy informacionnoj bezopasnosti / pod red. E.V. Stel'mashonok, I.N. Vasil'evoj. SPb.: Izd-vo SPbGEU, 2021. 163 s.

18. Ferette L. European Union Agency for Cybersecurity. The 2015 report on national and international cyber security exercises: survey, analysis and recommendations, European Network and Information Security Agency. 2015.

19. A targeted attack for enhancing resiliency of intelligent intrusion detection modules in energy cyber physical systems: In 19th International Conference on Intelligent System Application to Power Systems (ISAP) / El. Hariri M. [et al.]. 2017. P. 1–6. IEEE.

20. Vasil'ev V.I., Kirillova A.D., Vul'fin A.M. Kognitivnoe modelirovanie vektora kiberatak na osnove metashablonov CAPEC // Voprosy kiberbezopasnosti. 2021. № 2 (42).

21. Lessons learned from complex hands-on defence exercises in a cyber range: In Proc. of the 47th IEEE Frontiers in Education Conference (FIE’17) / J. Vykopal [et al.]. Indianapolis, Indiana, USA. 2017. P. 1–8. IEEE.

22. AIT Cyber Range: Flexible Cyber Security Environment for Exercises, Training and Research / Leitner Maria [et al.] // Proceedings of the European Interdisciplinary Cybersecurity Conference. 2020. P. 49.

23. Abramov E.S., Andreev A.V., Mordvin D.V. Primenenie grafov atak dlya modelirovaniya vredonosnyh setevyh vozdejstvij // Izvestiya Yuzhnogo federal'nogo universiteta. Tekhnicheskie nauki. 2012. № 126 (1). S. 165–174.

24. Kurilov F.M. Modelirovanie sistem zashchity informacii. Prilozhenie teorii grafov // Tekhnicheskie nauki: teoriya i praktika: materialy III Mezhdunar. nauch. konf. Chita: Izd-vo Molodoj uchenyj, 2016. S. 6–9.

25. Zeigler Bernard P., Herbert Praehofer, Tag Gon Kim. Theory of modeling and simulation. 2nd edition, Academic Press, 2000 // Theory of Modeling and Simulation: Integrating Discrete Event and Continuous Complex Dynamic Systems.

26. GOST R 53114–2008. Zashchita informacii. Obespechenie informacionnoj bezopasnosti v organizacii. Osnovnye terminy i opredeleniya. URL: htth:// base.garant.ru (data obrashcheniya: 24.04.2023).

27. Butyrskij E.Yu., Matveev A.V. Matematicheskoe modelirovaniya sistem i processov. SPb.: Strategiya budushchego, 2022. 733 s.

28. Metel'kov A.N. Kiberucheniya: zarubezhnyj opyt zashchity kriticheskoj infrastruktury // Pravovaya informatika. 2022. № 1. S. 51–60.

29. The Current State of The Art and Future of European Cyber Range Ecosystem / C. Virág [et al.]. 2021 IEEE International Conference on Cyber Security and Resilience (CSR), Rhodes, Greece. 2021. P. 390–395.

30. User Behavior Simulation in ICS Cyber Ranges: 19th Annual International Conference on Privacy / C. Liu [et al.]. Security&Trust (PST), Fredericton, NB, Canada. 2022. P. 1–5.

31. Matveev A.V., Metel'kov A.N., Shestakov A.V. Riski kiberatak: likvidaciya posledstvij proyavlenij kiberterrorizma i chrezvychajnyh situacij // Vestnik Voronezhskogo instituta FSIN Rossii. 2023. № 1. S. 98–106. EDN AYXLTO.

32. Metodika tekhniko-ekonomicheskoj ocenki variantov postroeniya organizacionno-tekhnicheskoj sistemy klassa «kiberpoligon» / A.V. Matveev [i dr.] // Inzhenernyj vestnik Dona. 2023. № 6. URL: http://www.ivdon.ru/ru/magazine/archive/n6y2023/8474/.

Информация о статье:
Статья поступила в редакцию: 06.06.2023; одобрена после рецензирования: 16.06.2023;
принята к публикации: 20.06.2023
Information about the article:
The article was submitted to the editorial office: 06.06.2023; approved after review: 16.06.2023;
accepted for publication: 20.06.2023

Сведения об авторах:
Метельков Александр Николаевич, доцент кафедры прикладной математики и информационных технологий Санкт-Петербургского университета ГПС МЧС России (196105, Санкт-Петербург, Московский пр., д. 149), кандидат юридических наук, e-mail: metelkov5178@mail.ru, https://orcid.org/0000-0002-6113-8981

Information about authors:
Metelkov Alexander N., associate professor of the department of applied mathematics and information technologies, Saint-Petersburg university of State fire service of EMERCOM of Russia (196105, Saint-Petersburg, Moskovsky ave., 149), candidate of law, e-mail: metelkov5178@mail.ru, https: //orcid.org/0000-0002-6113-8981