Методические основы киберучений и CTF-соревнований

En **Methodological Foundations of Cyber Exercises and CTF Competitions**

A. V. Dorofeev,
Director
ad@cnpo.ru
Echelon Training Center

A. S. Markov,
PhD (Eng., Grand Doctor), Full Professor
a.markov@bmstu.ru
Bauman Moscow State Technical University

The aim of the publication is to show the formation of cyber exercises, including CTF competitions, as an effective form of training professionals in the field of information security. The publication concludes that cyber exercises are part of the information security discipline. An overview of the standards and methodological documents relevant to conducting cyber exercises is given. Taxonomies, on the basis of which cyber exercises scenarios are formed, are shown. The comparison of the MITRE ATT&CK taxonomy and the FSTEC methodological document on information security threats assessment is presented. The possibility of using the Russian methodological documents for the developing cyberthreat scenarios is demonstrated. An example of the scenario and the CTF competition stand is illustrated. The conclusion is made about the formation of cyber exercise services in Russia as models of infrastructure, platform and software.

Keywords: cybersecurity, cyber exercises, command and staff exercises, CTF competition, cyber range, threat simulation, drills, training, education, professional standards, information security, Capture the Flag (CTF)

Цель публикации состоит в том, чтобы показать становление киберучений, в том числе CTF-соревнований, как эффективной формы подготовки профессионалов в области информационной безопасности. При этом продемонстрирована возможность использования российских методических документов по оценке компьютерных угроз для организации учений в области кибербезопасности. Определено, что последние являются частью дисциплины информационной безопасности, имеющей свои терминологический аппарат, цели, задачи, объект и предмет, классификации. Дан обзор стандартов и методических документов, релевантных проведению киберучений. Приведены таксономии, на базе которых формируются сценарии киберучений. Представлено краткое сравнение таксономии MITRE ATT&CK и методического документа ФСТЭК России по оценке угроз информационной безопасности. Продемонстрирована возможность применения российских методических документов ФСТЭК России для разработки сценариев киберучений. Проиллюстрирован пример сценария и стенда CTF-соревнования. Сделан вывод о формировании услуг по киберучениям в нашей стране как моделей инфраструктуры, платформы и приложений.

Ключевые слова: кибербезопасность, киберучения, командно-штабные учения, CTF-соревнования, киберполигон, имитация угроз, тренинг, обучение, образование, профессиональные стандарты, информационная безопасность, компетенции, захват флага

Александр Владимирович Дорофеев,
директор
ad@cnpo.ru
Учебный центр «Эшелон»

Алексей Сергеевич Марков,
доктор технических наук, профессор
a.markov@bmstu.ru
МГТУ им. Н. Э. Баумана

Введение

Принято считать, что основы обучения путем имитации (*simulation*) реальных кризисных ситуаций (к которым можно отнести целенаправленные компьютерные атаки) были заложены американским философом Джоном Дьюи в 1938 году [1]. Однако в военной области такой подход, получивший название учений (*exercises*), использовался намного ранее: все знают изречение графа Святой Римской империи, фельдмаршала русской и австрийской армии, а также пьемонтских войск, генералиссимуса Русских Сил Александра Васильевича Суворова – «тяжело в учении, легко в бою», зафиксированное в положении о боевой подготовке войскам в 1794 году.

Со всеобщей компьютеризацией, апробацией дистанционной работы и внедрением пакетов компьютерного моделирования тематических сред (например, объектов критической информационной инфраструктуры) и пр. прикладные возможности имитации реальных ситуаций с целью обучения принципиально изменились. Перенесение моделирования кризисных ситуаций в область информационной безопасности обусловило становление новой дисцип-

лины – киберсоревнований и киберучений (рис. 1). При создании и внедрении киберучений методисты, как правило, опираются на систематики в области информационной безопасности американского происхождения, в частности, разрабатываемые NIST и MITRE. В данной публикации авторы привели пример проведения киберучений, опираясь на оригинальную методику оценки угроз ФСТЭК России[1].

Базовые определения киберучений

В настоящее время терминологический аппарат киберучений еще находится на стадии становления, и истоки его, конечно, лежат в военной области. Так, MITRE Cyber Exercise Playbook [2] фактически относит учения к имитации военной кибероперации (включающей планирование, подготовку и выполнение), которая проводится с целью обучения и оценки организации с упором на программу обеспечения информационной безопасности. В документе NIST SP 800-84 (*Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*) [3] отмечается, что учения должны представлять имитацию чрезвычайной ситуации, разработанной для проверки плана ИТ, в первую очередь – ролей и обязанностей персонала. Исследования МСЭ по кибербезопасности трактуют цели киберучения как совершенствование скоординированных действий по реагированию на инциденты в компьютерной сфере в вопросах борьбы с киберугрозами [4]. Согласно ISO 22398 (*Guidelines for Exercises*), учения могут использоваться для проверки документов, уточнения и обучения персонала ролям и обязанностям, улучшения координации и коммуникаций, улучшения индивидуальных показателей и пр. Что касается перспективного стандарта ISO/IEC TR 27109 (*Cybersecurity Education and Training*), то термин там пока не состоялся.

Развернутое определение дано в документе Европейской организации по кибербезопасности (ECSO) [5], где киберучения трактуются как запланированное мероприятие, в ходе которого организация имитирует кибератаки, инциденты информационной безопасности или другие виды нарушений с целью проверки кибервозможностей организации, начиная от способности вовремя обнаружить инцидент безопасности и заканчивая способностью адекватно реагировать на таковой и минимизировать любые связанные с ним последствия.

Следует отметить ряд особенностей киберучений, таких как:

- проведение имитации чрезвычайной ситуации в области информационной безопасности;
- проверка актуальных и реализуемых (а не гипотетических) угроз, уязвимостей и компьютерных атак в области информационной безопасности;
- использование комплексной учебной программы, включающей игровой сценарий, который может быть развит в процессе игры;
- совершенствование как осведомленности персонала, их ролей и обязанностей, координации действий, так и способности принимать решения в нестандартных ситуациях.

Относительно последнего пункта интересно отметить, что обучение требует отработки принятия решений на основе полученных знаний по Расмуссену [6], например, в ситуации, которая не прописана в руководствах по управлению инцидентами и реагированию на компьютерные атаки.

Как известно, личный состав киберучений представлен рядом команд, как правило, следующих: *Red team* – нападающие, *Blue team* – защищающиеся, *Green team* – администраторы, *Yellow team* – разработчики, *White team* – организаторы, *Orange team* – аналитики (рис. 2).

Рис. 1. ***Киберучения как междисциплинарная деятельность***

Задачи и ожидания от киберучений определяются конкретными целями и возможностями, например, следующими:

- обучить технический персонал применению средств защиты информации;
- повысить осведомленность в области кибербезопасности;
- в ходе процедуры реагирования на инцидент отработать процесс принятия необходимых управленческих решений;
- отработать процессы коммуникаций в команде защищающихся;
- проверить адекватность принятых в организации регламентов по реагированию на инциденты и т. д.

Киберполигон (*cyber range*), как правило, включает следующие сегменты:

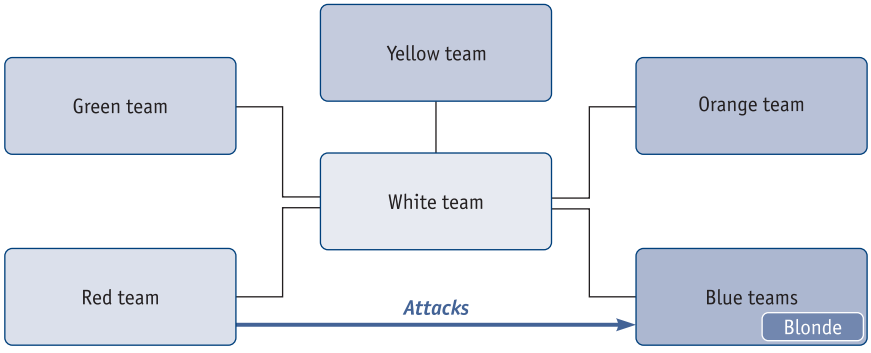

Рис. 2. ***Примеры киберкоманд***

[1] *Методика оценки угроз безопасности информации. Методический документ. ФСТЭК России. – 2021. – 87 с.*

- базовый сегмент: производительные серверы, которые могут обеспечить одновременное функционирование десятков и сотен виртуальных серверов, а также система виртуализации;
- виртуальная инфраструктура для защиты и нападения: сетевое оборудование, серверы и рабочие станции, средства защиты информации;
- вспомогательная инфраструктура;
- система скоринга (судейская система).

Нормативные и методические документы

Нормативные документы позволяют ответить на следующие вопросы:

1) в каких случаях киберучения необходимы;

2) как их проводить?

Что касается первого вопроса, то следует указать на обязательность повышения квалификации сотрудников организаций и на рекомендации по проведению аудита информационной безопасности (в первую очередь, проведения теста на проникновение путем имитации реальных атак). Как известно, в большинстве стран мира эти моменты регулируются государством. В России требования по аудиту информационной безопасности (в том числе теста на проникновение) в явном виде определены регуляторами безопасности банковской сферы (стандарт Банка России) и критической информационной инфраструктуры (приказы ФСТЭК России).

Обязательность и периодичность переподготовки и повышения квалификации сотрудников вытекают из Постановлений Правительства РФ (№ № 79 ПП РФ, 171 ПП РФ, 313 ПП РФ) и уточнены рекомендациями и регламентами регуляторов в области информационной безопасности.

Указанное обусловливает синтез нового класса обучения специалистов по информационной безопасности в реальной среде киберугроз, а именно, в рамках участия в киберучениях.

Вопросы проведения киберучений наиболее концептуально описаны в указанном ранее документе MITRE [2]. К нему следует добавить международный стандарт ISO 22390, касающийся в целом учений в области ИТ, а также французскую публикацию, посвященную учениям в сфере непрерывности бизнеса [7]. Указанные материалы по-своему классифицируют киберучения с целью формирования задач, ожиданий, команд и пр.

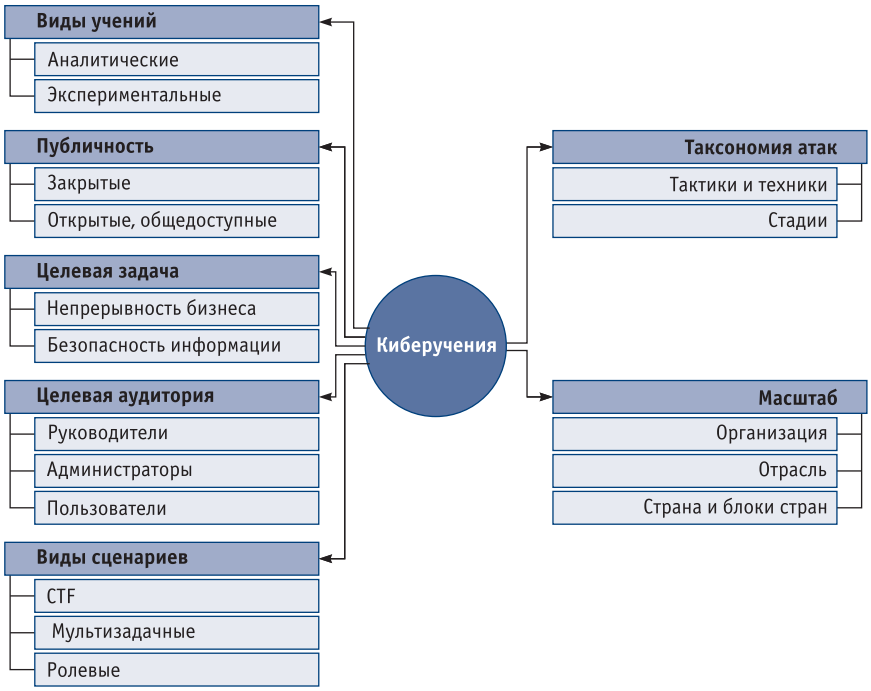

Рис. 3. ***Классификация киберучений***

Классификация киберучений

Авторы предлагают классификацию киберучений по следующим показателям (рис. 3) [8]:

- виды учений и степень абстракции (теоретические, реальные);
- уровень публичности (закрытые, открытые);
- целевой показатель (конфиденциальность, непрерывность бизнеса, целостность, доступность и пр.);
- целевая аудитория (руководство, администраторы, пользователи, а также поставщики, производители и пр.);
- виды сценариев (CTF-соревнования, мультизадачные, ролевые);
- подклассы атак (целевые этапы, методы, средства, среды, а также атаки, характерные для какой-либо кибергруппы, и пр.);
- масштаб (организация, отрасль, страна, союзные государства и пр.).

Основополагающими в приведенной классификации представляются виды учений, к которым можно отнести следующие [3, 9, 10]:

1) штабные учения (*discussion based*):

- настольные (*table top*);
- штабные игры (*games*);
- мастер-классы (*workshop*);
- семинары;

2) функциональные (*operations based*):

- проверка управления, контроля и координации;
- отработка навыков (*drill*);
- полномасштабные учения;

3) смешанные.

Что касается масштабирования и тематической направленности, то большинство описанных в литературе киберучений посвящены отраслям критической информационной инфраструктуры (КИИ) или кибервойнам.

Примеры киберучений

По известным причинам в первую очередь следует назвать характеристики зарубежных киберучений. Например, в эстонских ежегодных киберучениях NATO Locked Shields в 2021 году приняло непосредственное участие более 2000 профессионалов по кибербезопасности из

30 стран мира. Учредителями учений было сорганизовано 22 киберкоманды Blue Team. Техническая среда включала более 5000 виртуальных хостов. Команда Red Team исследовала возможность взлома военных целей и значимых объектов КИИ ЕС, таких как автоматизированные системы управления выработкой электроэнергии, группировкой космических спутников, ПВО, очисткой воды, военной тактической радиосвязью, мобильной связью и пр.

Другим показательным примером могут служить американские киберучения Cyber Storm, проводимые раз в два года [11]. В 2020 году в указанных учениях также приняло участие более 2000 специалистов по кибербезопасности, в том числе сотрудники от более чем 90 индустриальных партнеров (коммерческих ИБ-фирм), спецагенты от 30 федеральных министерств США, а также представители 13 союзных государств. На учениях отрабатывались навыки одновременного противодействия сразу двум независимым кибергруппировкам «враждебных стран», осуществляющим параллельные APT-атаки на ресурсы девяти секторов экономики США.

Что касается распределения киберучений в Европе по отраслям КИИ, то в [12] представлена соответствующая статистика (рис. 4).

В России наиболее популярны киберучения класса CTF-соревнований (Capture the Flag, «захват флага» как аналог пионерской «Зарницы» в СССР) [13–19]. Истоки компьютерных CTF-соревнований сформированы еще в 1996 на известной конференции Defcon. В России в данном ключе наиболее известна деятельность ассоциации АРСИБ, которая проводит CTF-соревнования уже более десяти лет и поддерживает более 25 проектов студенческих CTF-движений[2], включая летнюю CTF-школу [18]. Кроме того, в качестве примера можно назвать CTF-киберучения «Эшелонированная оборона», проведенные по инициативе патриотического молодежного движения России под патронажем Минобороны России. Эти соревнования включали 3 уровня участников: старшеклассники, студенты и курсанты. В 2019 году в них участвовали 147 человек в составе 25 команд, а в 2020 году соревнования включали уже более 100 команд.

Отметим характерные черты CTF-соревнований:

- командам участников предлагается набор заданий по тестированию защищенности информационных систем, форензике, поиску и анализу информации, подбору паролей и эксплуатации комбинаций уязвимостей, криптографии, стеганографии и т. п.;
- результатом успешного прохождения задания является набор символов (флаг). В роли которого может выступать, например, пароль администратора, доступное только определенному пользователю содержимое файла, расшифрованное значение и т. п.;
- флаги регистрируются в специальной судейской системе, которая автоматически ведет подсчет баллов каждой команды.

Опираясь на публикации Национального киберполигона России, созданного «Ростелекомом» в рамках программы «Цифровая экономика России», можно отметить, что крупномасштабные учения в сфере безопасности КИИ РФ уже затронули сегменты энергетической и банковской отраслей; также заявлены кибериссследования нефтегазовой, телекоммуникационной, транспортной и металлургической отраслей[3] (рис. 5) [20].

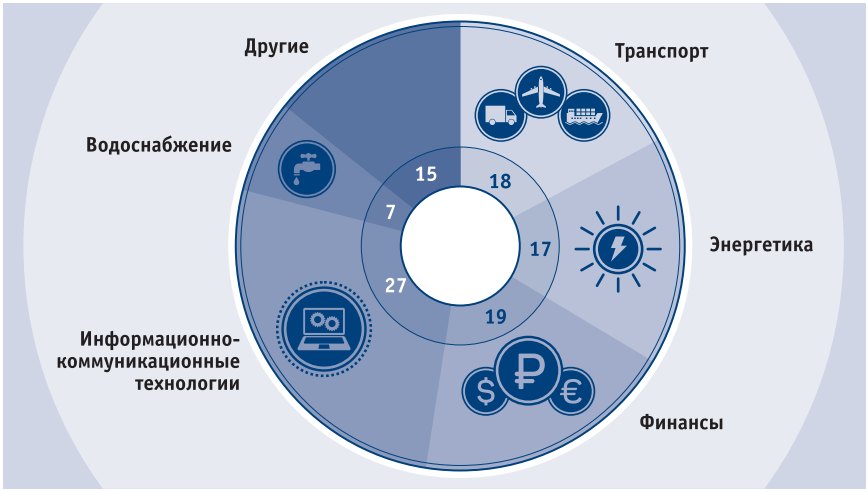

Рис. 4. ***Распределение учений по отраслям КИИ в ЕС***

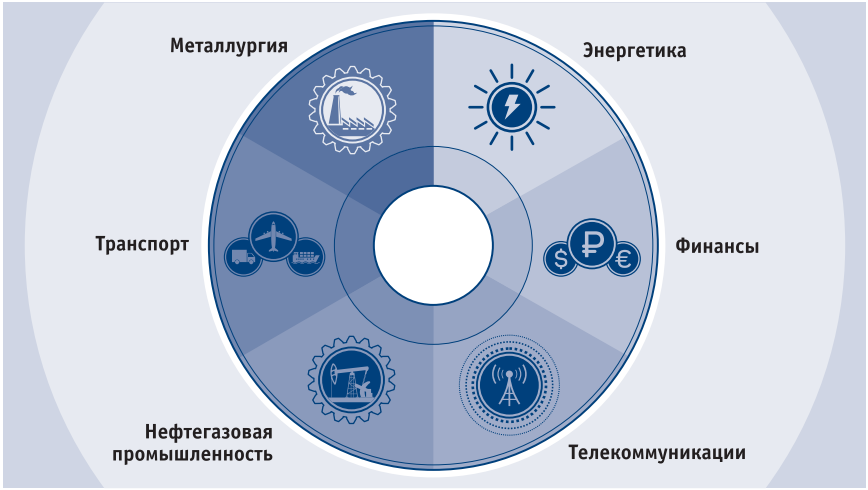

Рис. 5. ***Распределение учений по отраслям КИИ в России***

[2] *http://aciso.ru/aciso-projects/3861/.*
[3] *https://www.vest-news.ru/news/162124.*

Таким образом, касательно российского рынка киберучений можно утверждать, что последние уже могут быть представлены как сервис, например:

- *киберучения как инфраструктура* – здесь в качестве примера можно привести Национальный киберполигон России;
- *киберучения как платформа* – примером может служить коробочный продукт Ampire, разработанный группой компаний «Инфотекс»;
- *киберучения как продукт* – к этому классу может быть отнесена продукция десятков компаний России, производящих широкий спектр средств защиты информации, задействованных в учениях (как правило, речь идет о линейке SIEM-систем, систем обнаружения вторжений (СОВ), средств анализа защищенности и межсетевых экранов).

Таксономии сценариев киберучений

Отметим, что центральным моментом киберучений является их сценарий, содержащий задания. Например, типовой сценарий для проведения киберучений в организации может быть следующим [8, 21]:

- подключение к комьюнити сотрудников организации;
- фишинговая рассылка с ПО для удаленного администрирования;
- подбрасывание USB-носителя с ПО для удаленного администрирования;
- сетевые атаки на ИТ-инфраструктуру, доступную извне;
- скрытая передача данных из сети с использованием стандартных протоколов, например, DNS;
- попытки физического получения конфиденциальной информации у сотрудников с помощью методов социальной инженерии.

Отраслевые учения могут быть организованы для отражения атаки какой-либо кибергруппировки, например, APT Tonto и TA428[4], если задача состоит в защите интеллектуальной собственности, или хакерских групп Cobalt и Carbanak – в случае банковских учений. В этом плане для разработки сценария киберучения удобно использовать атрибутивные характеристики APT-атак, представляемые MITRE [22].

Набор заданий (сценарий) формируется либо экспертным путем (из опыта организаторов), либо привязывается к систематикам компьютерных атак, к которым, по мнению авторов, можно отнести следующие:

- NIST Cyber Framework (зрелость компании и/или этапы);
- Lockheed Martin Cyber Kill Chain (фазы кибератаки);
- MITRE ATT&CK (постповедение атакующих).

Так, в [23] подробно рассмотрены вопросы формирования различного рода киберучений относительно NIST Cyber Framework. Изюминкой проекта является учет зрелости компаний, задействованных в обучении. Это позволяет установить приоритеты как по видам учений (теоретические, практические), так и по сложности и содержанию заданий вплоть до их итерации для достижения поставленных целей по отработке навыков и закрепления знаний [24].

До недавнего времени наиболее цитируемой в литературе являлась 7-этапная модель Cyber Kill Chain. В этом случае киберучения организуются в соответствии с фазами кибероперациий [25, 26].

Современные изыскания, касающиеся определения и демонстрации сценариев, посвящены использованию поведенческих методов проведенных атак (рассматривается постинцидент). В данном случае сценарий соотносят с таксономией MITRE ATT&CK. В текущий момент вариант таксономии включает 14 тактик (целевых этапов) и 144 техники (способов выполнения атаки).

Авторы предлагают подобный подход, но касающийся построения сценария на основе модели угроз, принятой в России. Текущая методика оценки угроз ФСТЭК России включает 10 целевых этапов атаки, используемых для построения сценариев реализации угроз безопасности информации:

- Т1. Сбор информации;
- Т2. Получение первоначального доступа;
- Т3. Внедрение и исполнение вредоносного ПО;
- Т4. Закрепление доступа;
- Т5. Управление вредоносным ПО;
- Т6. Повышение привилегий;
- Т7. Сокрытие действий;
- Т8. Распространение доступа к смежным системам;
- Т9. Сбор и вывод из системы информации;
- Т10. Несанкционированное воздействие или доступ (целевое воздействие).

Указанные целевые этапы включают 145 способов их реализации.

Несложно сравнить указанный подход с систематикой ATT&CK. Из-за лимитированного объема публикации авторы ограничились сравнением одного целевого этапа («тактики») – Т4 (табл. 1).

Пример организации киберполигона и киберучений начального уровня

Рассмотрим опыт использования названных таксономий при организации киберучений. В качестве примера приведем специальный киберполигон в АНО «Учебный центр «Эшелон», используемый для проведения практических занятий по тестированию на проникновение, мониторингу информационной безопасности и обнаружению вторжений. Киберполигон позволяет моделировать кибератаки на компьютерные сети предприятий и обучать специалистов на должном уровне. На рис. 6 представлена схема сети киберполигона для тренинга начального уровня.

Так, для первоначального обучения сформирована виртуальная ИТ-инфраструктура, в которой в качестве целей используются серверы, размещенные в DMZ-сегменте, с запущенными http/ftp/ssh-сервисами и типовые рабочие станции на базе ОС Windows и Linux, размещенные в локальном сегменте сети. Компьютер атакующего создан на базе

[4] *https://www.kommersant.ru/doc/4802201/.*

специализированного дистрибутива Kali Linux и размещен во внешнем сегменте сети. В рамках тренинга начального уровня предполагается освоение базовых инструментов для проведения компьютерных атак, таких как фреймворк Metasploit Framework, комплекс анализа защищенности «Сканер-ВС» и другие актуальные утилиты. Из средств защиты информации применяются межсетевой экран PFSense и решения, разрабатываемые НПО «Эшелон»: KOMRAD Enterprise SIEM, «Сканер-ВС» и варианты СОВ (см. рис. 6).

С помощью механизма NAT во внешнем сегменте определены необходимые сервисы (табл. 2).

В рамках обучения слушатели выполняют имитацию ряда типовых атак, после чего разбираются с тем, как их можно обнаружить, создав соответствующие правила для реальных SIEM-систем и СОВ. В табл. 3 представлены атаки и цели, сопоставленные с классификацией атакующих воздействий по материалам MITRE ATT&CK и ФСТЭК России.

Следующая ступень обучения предполагает развитие киберполигона в направлении расширения набора сервисов в качестве целей атакующих (Active Directory, DNS, электронная почта, различные СУБД и т. п.), а также расширения инструментария нападающих (Metasploit Framework, PowerShell Empire и пр.).

Таблица 1. ***Пример сравнения целевых этапов атак по методикам ФСТЭК России и MITRE ATT&CK***

T4. Закрепление доступа	
ID ФСТЭК России	MITRE ATT@CK
T4.1. Несанкционированное создание учетных записей	T1136 T1212
T4.2. Использование штатных средств удаленного доступа ОС	T1133 T1021
T4.3. Скрытая установка и запуск средств удаленного доступа ОС	T1133 T1021 T1219
T4.4. Маскирование подключенных устройств под легитимные	Близко к T1036
T4.5. Внесение соответствующих записей в компоненты автозапуска	T1542 T1053 T1547 T1037
T4.6. Компрометация прошивок устройств	T1542.001 T1495
T4.7. Резервное копирование вредоносного кода в скрытые области	Отсутствует

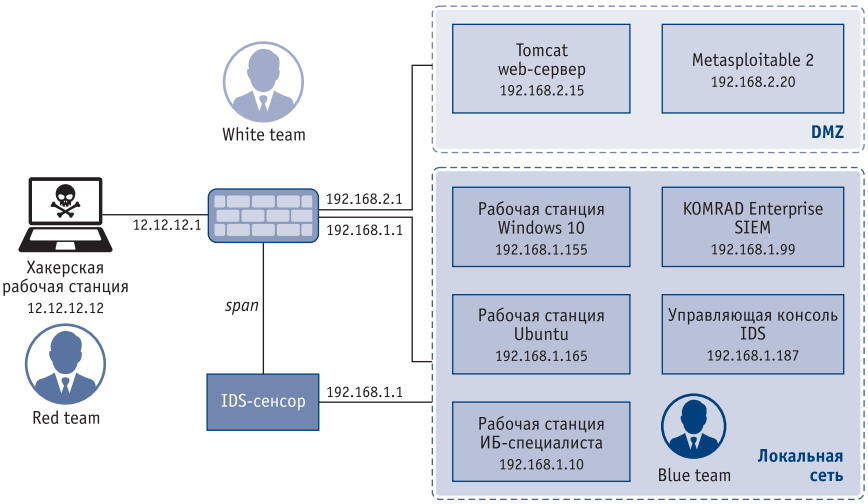

Рис. 6. ***Пример схемы киберполигона начального уровня***

Таблица 2. ***Пример настройки служб киберполигона***

Сервер в DMZ	Порт/служба	Сервер	Порт
192.168.2.15	21/ftp	12.12.12.1	21
192.168.2.15	22/ssh	12.12.12.1	22
192.168.2.15	8080/http	12.12.12.1	8080
192.168.2.20	21/ftp	12.12.12.1	2121

Заключение

Приведенный обзор позволяет сделать ряд кратких выводов.

1. Киберучения – это актуальная форма обучения, ориентированная на реальные инциденты. Важной чертой киберучений является полная согласованность со ставшим обыденным в период пандемии дистанционным обучением. При этом в настоящее время наиболее популярными в вузовской среде являются CTF-соревнования.

2. В мире сложилось понимание формирования сценариев киберучений, которые в настоящее время опираются на развивающиеся систематики атак, в первую очередь, MITRE ATT&CK. Однако в работе показано, что сценарии могут опираться на модели угроз, в том числе российскую методику.

3. Современный киберполигон характеризуется свойством масштабирования в зависимости от решаемых задач. Основным техническим элементом киберполигона является развивающаяся SIEM-система, позволяющая группам защиты информации (Blue Teams) создавать и исследовать в режиме реального времени правила выявления и реагирования на компьютерные атаки, в том числе нестандартные.

4. Можно утверждать, что рынок киберучений в мире и в России сложился, что позволяет говорить о киберучениях как об услуге (киберуче-

Таблица 3. ***Атаки и цели по классификации MITRE и ФСТЭК России***

№	Атака (задача Red team)	Цели нападающего	Цель: IP	Цель: сервис	ФСТЭК России	MITRE	Обнаружение (задача Blue team)
1	Сетевая разведка	Определение сервисов, доступных для дальнейших атак	12.12.12.1	Все доступные	Т1.4	T1595.001	● Создать правило для СОВ. ● Создать фильтр для SIEM и директиву корреляции. ● Настроить в PFSense передачу событий по syslog в SIEM. ● Создать плагин для PFSense для парсинга событий
2	Подбор паролей к консоли управления web-сервера	Получение доступа к консоли управления для обеспечения возможности загрузки вредоносного ПО (ВПО) (webshell)	192.168.2.15	HTTP (8080)	Т2.10	T1110	● Создать правило для СОВ. ● Настроить журналирование web-сервера Tomcat. ● Настроить rsyslog для удаленной передачи событий. ● Создать плагин для парсинга журналов Tomcat. ● Создать директиву для определения подбора паролей по протоколу HTTP
3	Подбор паролей к FTP-серверу	Получение доступа к данным, хранящимся на FTP-сервере	192.168.2.15	FTP (21)	Т2.10	T1110	● Создать правило для СОВ. ● Настроить журналирование FTP. ● Создать директиву корреляции
4	Подбор паролей к SSH-серверу	Получение доступа к серверу	192.168.2.15	SSH (22)	Т2.10	T1110	● Создать правило для СОВ. ● Настроить журналирование SSH. ● Создать директиву корреляции
5	Подбор паролей к хэшам из /etc/shadow	Получение учетных записей для перемещения внутри инфраструктуры	192.168.2.15	–	Т2.10	T1110	● Настроить мониторинг auditd-доступа к файлу. ● Настроить мониторинг передачи по сети содержимого файла. ● Создать директиву корреляции
6	Попытка эксплуатации уязвимости в VSFTPD	Получение доступа к серверу	192.168.2.20	FTP (21)	Т2.5	T1190 T1211	● Создать правило для СОВ. ● Настроить мониторинг открытия порта. ● Создать директиву корреляции
7	Подготовка и размещение web-shell	Получение доступа к операционной системе	192.168.2.15	HTTP (8080)	Т3.1	T1059 T1204	● Создать правило для СОВ (хэш-зловреда). ● Настроить мониторинг открытия порта. ● Создать директиву корреляции
8	Размещение ВПО на web-сервере/портале для атак на пользователей (.deb и .exe)	Осуществление фишинговой атаки, нацеленной на пользователей сети	192.168.2.20		Т3.1	T1059 T1204	● Настроить мониторинг содержимого директории. ● Создать директиву корреляции
9	Запуск ВПО на Windows-компьютере	Сбор данных: скриншоты/keylogger/поиск текстовых документов	192.168.1.155		Т3.1	T1059 T1204	● Создать правило для СОВ (хэш-зловреда) ● Настроить локальный мониторинг (sysmon, osquery). ● Создать директиву корреляции
10	Получение хэшей паролей пользователей	Последующий подбор	192.168.1.155		Т1.9	–	● Настроить локальный мониторинг (sysmon, osquery). ● Создать директиву корреляции
11	Подбор паролей по полученным хэшам	Получение учетных записей для расширения зоны влияния	192.168.1.155		Т2.10	T1110	–
12	Запуск ВПО на Linux-компьютере	Сбор данных: поиск текстовых документов	192.168.165		Т3.1	T1059 T1204	● Создать правило для СОВ (хэш-зловреда). ● Настроить локальный мониторинг (sysmon, osquery). ● Создать директиву корреляции
13	Передача полученных данных вовне	Получение информации	192.168.1.155 192.168.165		Т9.6	T1048	● Создать правило для СОВ. ● Создать директиву корреляции

ния как инфраструктура, киберучения как платформа и киберучения как продукт). В этом плане имеется широкий спектр проприетарных (платных) продуктов и продуктов с открытым кодом для проведения или организации учений. Многие компании-производители средств защиты информации (SIEM, IDS/IPS, VA, FW) развивают бесплатные программы, ориентированные на российские вузы. ■

ЛИТЕРАТУРА

1. *Dewey J. Education and Experience. Kappa Delta Pi, 1938. 91 p.*
2. *Kick J. Cyber Exercise Playbook. MP140714 // Wiesbaden, Germany. MITRE. 2014. 50 p.*
3. *Grance T. et al. NIST SP 800-84 Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities. 2006. 97 p.*
4. *Исследование МСЭ-D потенциальных направлений развития региона СНГ в период 2022–2025 – кибербезопасность // RPM-CIS21/INF/5-R. ITU WTDC, 2021. – Версия 1.0. – 52 с.*
5. *Understanding Cyber Ranges: From Hype to Reality. – WG5 PAPER. SWG 5.1. – Cyber Range Environments and Technical Exercises // European Cyber Security Organisation, Brussels, Belgium. 2020. 31 p.*
6. *Rasmussen J. Skills, rules, and knowledge; signals, signs, and symbols, and other distinctions in human performance models // IEEE Transactions on Systems, Man, and Cybernetics, 1983. V. SMC-13, № 3. P. 257–266. DOI: 10.1109/TSMC.1983.6313160.*
7. *Organising a cyber crisis management exercise, by ed. G. Poupard and V. Vallee // CCA. 2021. 128 p.*
8. *Dorofeev A. V., Markov A. S. Conducting Cyber Exercises Based on the Information Security Threat Model // CEUR Workshop Proceedings. 2021. V. 3057. P. 1–10.*
9. *Homeland Security Exercise and Evaluation Program // FEMA. 2020, 6 p.*
10. *Петренко А. А., Петренко С. А. Киберучения: методические рекомендации ENISA // Вопросы кибербезопасности. – 2015. – № 3 (11). – С. 2–14.*
11. *Метельков А. Н. Киберучения: зарубежный опыт защиты критической инфраструктуры // Правовая информатика. – 2022. – № 1. – С. 20–30.*
12. *Diez E. G. et al. Cyber Exercises Taxonomy // Spanish National Institute for Cyber-security. 2015. 56 p.*
13. *Бородай Р. Р., Киреев А. П., Новиков В. И., Братишко Н. М. Детальный разбор тасков по CTF: Forensics // Точная наука. – 2019. – № 66. – С. 33–38.*
14. *Бурлака И. М., Компаниец Р. И. Обзор способов решения задач из раздела «forensics» на соревнованиях по информационной безопасности, проводимых в формате CTF // Методы и технические средства обеспечения безопасности информации. – 2020. – № 29. – С. 70–71.*
15. *Воробьев А. М., Ястребов А. В., Бирюков Д. Н. Опыт организации и проведения межвузовских соревнований по информационной безопасности в формате CTF // Методы и технические средства обеспечения безопасности информации. – 2020. – № 29. – С. 122–124.*
16. *Литвиненко А. В. Использование программных средств обеспечение безопасности linux-сервера в рамках соревнований CTF // Вопросы кибербезопасности. – 2013. – № 3 (3). – С. 33–35.*
17. *Мансуров А. В. CTF-ориентированная парадигма изучения практических вопросов информационной безопасности // Символ науки. – 2016. – № 8-2 (20). – С. 69–73.*
18. *Минин В. В. Россия в CTF-движении // Information Security. – 2012. – № 4. – С. 7.*
19. *Петренко А. С., Петренко С. А. Первые межгосударственные киберучения стран СНГ: «Кибер-антитеррор-2016» // Защита информации. Инсайд. – 2016. – № 5 (71). – С. 57–63.*
20. *Архангельский О. Д., Кузнецов А. В., Сютов Д. В., Никонёнок М. П. Опыт проведения киберучений на национальном киберполигоне // Автоматизация в промышленности. – 2021. – № 11. – С. 26–32.*
21. *Dorofeev A. V., Markov A. S., Rautkin Y. V. Ethical Hacking Training. CEUR Workshop Proceedings. 2019. V. 2522. P. 47–56.*
22. *Марков А. С. Проблемы атрибуции и регулирования международной информационной безопасности // Сб. докладов участников Четырнадцатого международного форума «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности». – 2020. – С. 88–93.*
23. *Aoyama T. et al. On the Complexity of Cybersecurity Exercises Proportional to Preparedness // J. of Disaster Research. 2017, V. 12, № 5. P. 1081–1090. DOI: 10.20965/jdr.2017.p1081.*
24. *Petersen R. et al. Workforce Framework for Cybersecurity (NICE Framework). NIST Special Publication 800-181 Revision 1. NIST. 2020. 27 p. DOI: 10.6028/NIST.SP.800-181r1.*
25. *Choet S. Cyber Kill Chain based Threat Taxonomy and its Application on Cyber Common Operational Picture // Proc.: 2018 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (Cyber SA). 2018. P. 1–8. DOI: 10.1109/CyberSA.2018.8551383.*
26. *Mokhor V., Tsurkan V., Pokrovska V. Analysis of Cyber Exercises Approaches // CEUR Workshop Proceedings. 2021. V. 2859. P. 61–70.*

НОВОСТИ

Представители госорганов видят серьезные риски в случайных утечках информации

«Ростелеком-Солар» подвел итоги исследования «Случайные утечки информации в госорганах». Опросив госслужащих из всех регионов РФ, аналитики компании выяснили: более 90 % представителей госаппарата видит в этом серьезные риски. Из них более половины полагает, что эти риски даже выше, чем вследствие умышленных «сливов» конфиденциальных данных.

Почти в 60 % случаев из госорганов непреднамеренно утекают служебные документы и внутренняя конфиденциальная переписка вследствие их пересылки госслужащими на личную электронную почту. А почти в каждом пятом случае источником потенциальных утечек названы обсуждения с третьими лицами позиции руководства по рабочим вопросам и содержания внутренних служебных документов.

Чаще всего (в 51% случаев) чувствительная информация случайно покидает периметр государственных организаций через различные интернет-каналы, особенно посредством служебной электронной почты (более 23 % случаев) и мессенджеров (17 %).

Более чем в половине случаев виновниками неумышленных утечек в госорганах становятся руководители среднего звена, в 36 % случаев – рядовые служащие, и лишь каждая десятая неумышленная утечка происходит по вине руководителя высшего звена.

Основной причиной случайных утечек в госорганах 55 % участников исследования считают нехватку знаний в области информационной безопасности. Еще треть опрошенных полагает, что во всем виновата перегруженность многочисленными задачами, что порождает ошибки в обращении с чувствительной информацией, а чуть более 10 % придерживаются мнения, что причиной утечек является простая невнимательность.

В исследовании приняло участие более 100 представителей государственных органов и организаций.

https://rt-solar.ru