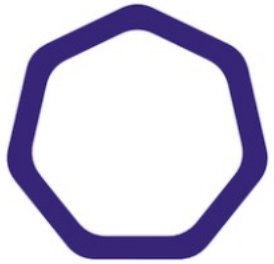


Эшелон
комплексная безопасность

Актуальные вопросы проведения киберучений (как нового класса обучения в области информационной безопасности)

Конференция «Теория и практика обеспечения информационной безопасности»,
Москва, МТУСИ, 2021, 3 декабря 2021 г.

Алексей Марков,
д.т.н., CISSP, CEH

План

1. Что такое киберучения?
2. Нормативные и методические документы
3. Классификация киберучений
4. Типовые сценарии учений и систематики

5. Примеры зарубежных киберучения

6. Опыт российского CTF-учения «Кибер Патриот»

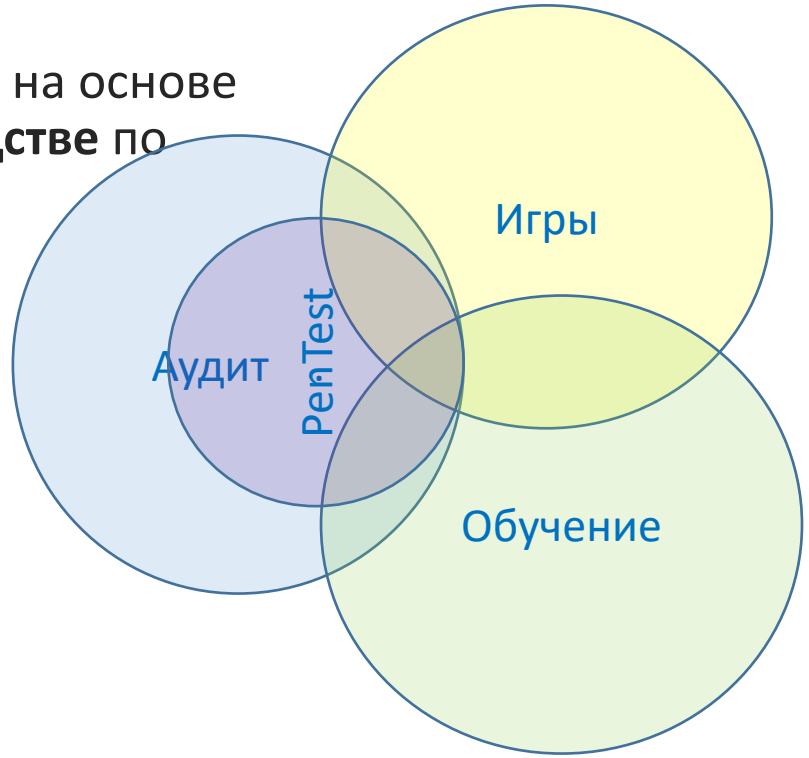
7. Пример технологической платформы для проведения киберучений: SIEM, IDS, VA и др.

8. Краткие выводы

Определения

Киберучения (Cyber exercises)
– **смоделированная** кибероперация (включающая планирование, подготовку и выполнение), которая проводится с целью обучения и оценки (US CJCSM)
– запланированное мероприятие, в ходе которого **имитируется чрезвычайная ситуация (кибератаки)** для оценки готовности участников к инцидентам ИБ, извлечения уроков и рекомендаций, повышения осведомленности, обучения и пр. (ISO/NIST/..)

- Проводятся на основе **сценария**, требующего принятия решений на основе **знаний***, например, в ситуации, которая **не прописана в руководстве** по урегулированию инцидентов (атак)
- Представляет комплексную программу обучения

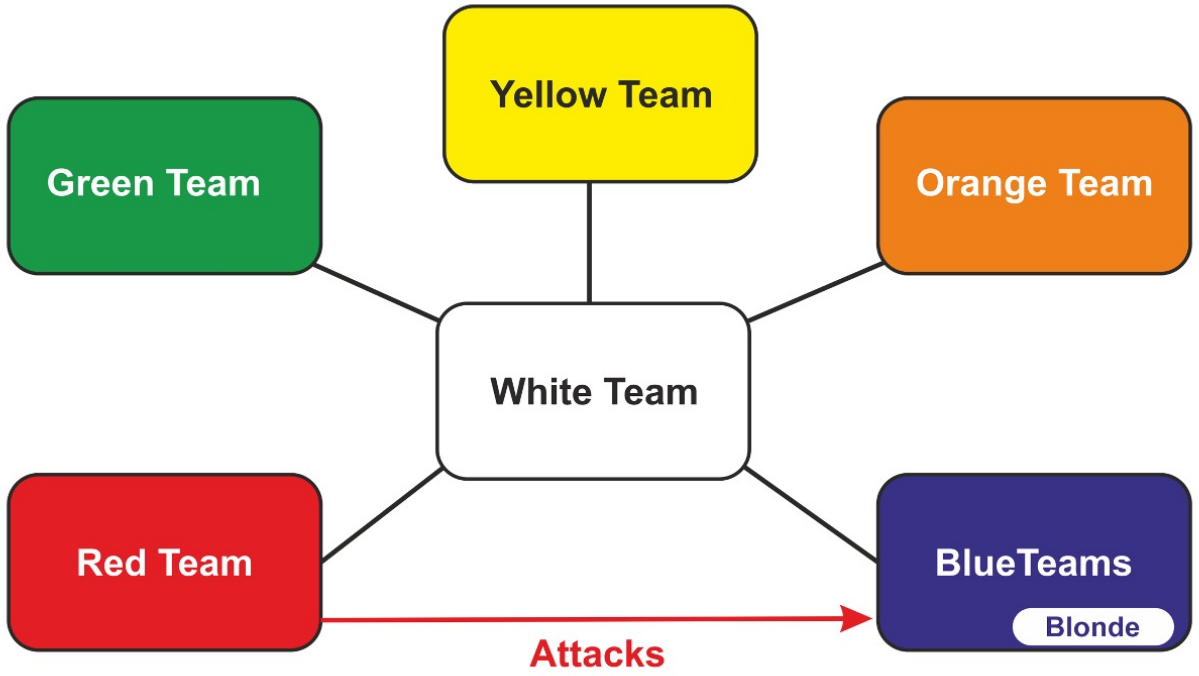


Другие понятия

- Киберполигон (cyber range)
- Тест на проникновение (pentest), red-timing
- CTF-соревнования и ролевые игры

Участники киберучений

- Red team – нападающие
- Blue team – защищающиеся
- Green team – администраторы
- White team – организаторы
- Yellow team - исследователи



Задачи и ожидания киберучений

см. методические документы (в зависимости от видов учений)

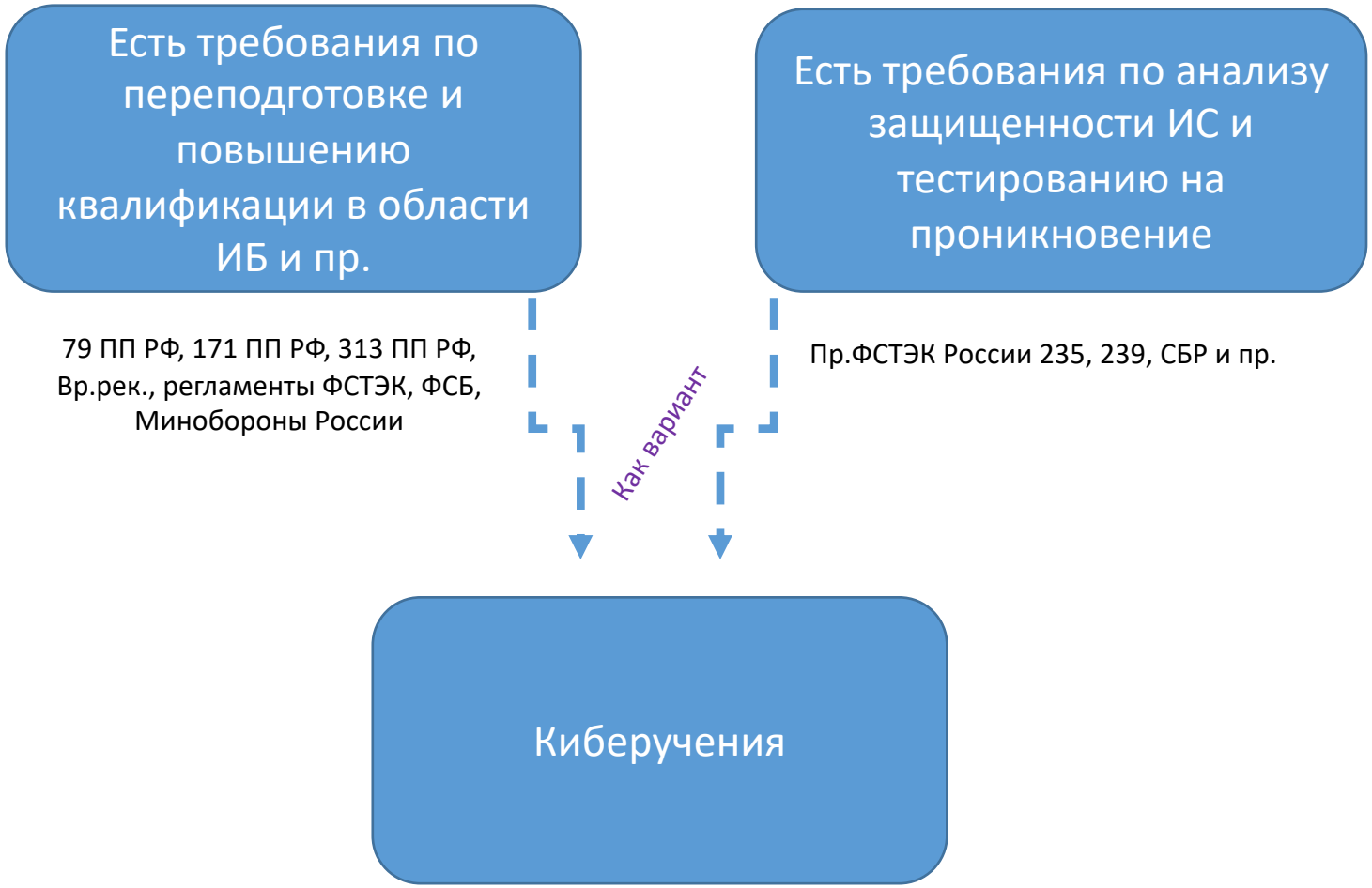
- Обучить технический персонал применению средств защиты информации
- Повысить осведомленность в области кибербезопасности
- Отработать процесс принятия управленческих решений в ходе процедуры реагирования на инцидент
- Отработать процессы коммуникаций в команде защищающихся
- Проверить адекватность принятых в организации регламентов по реагированию на инциденты

Инфраструктура для проведения киберучений

- Базовая платформа (ядро):
  - производительные серверы, которые могут обеспечить одновременные функционирование десятков и сотен виртуальных серверов;
  - система виртуализации.
- Виртуальная инфраструктура для защиты и нападения:
  - сетевое оборудование;
  - серверы и рабочие станции;
  - средства защиты информации.
- Вспомогательная инфраструктура
- Судейская система (система скоринга)

Нормативные и методические документы

- Необходимость
- Как проводить



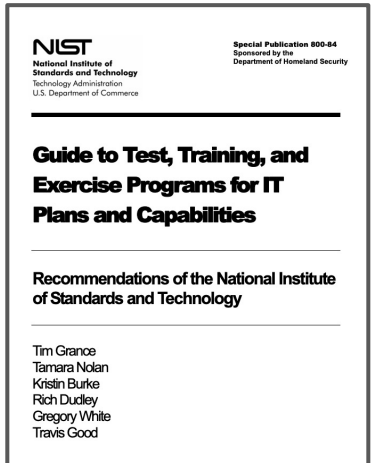
Методические документы и учебники

Киберучения и киберполигоны

- MITRE Cyber Exercise Playbook, 2014, 50p

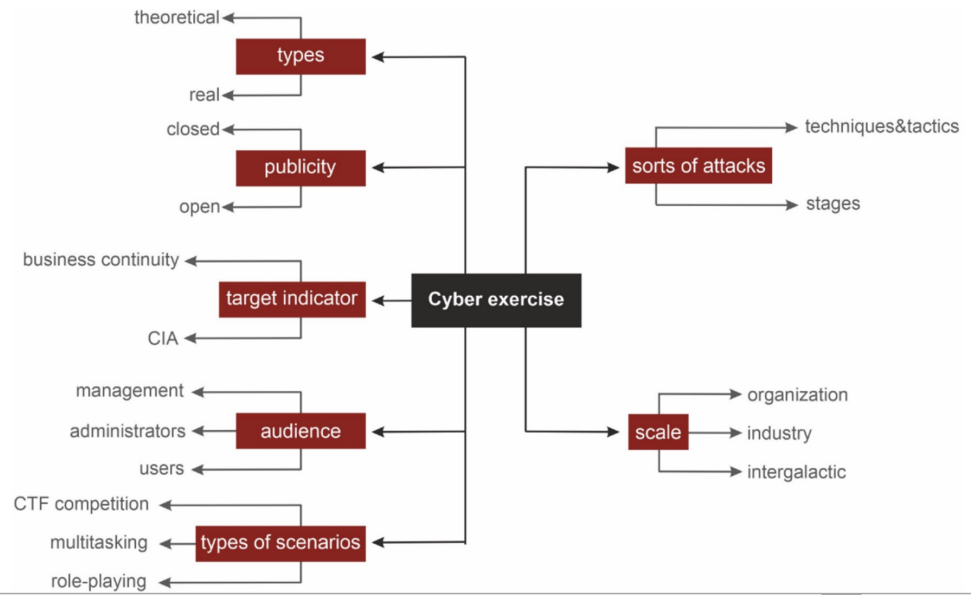
ИТ-учения и тренинги

- ISO 22390: 2013 – SS. Guidelines for exercises and testing, 40 p.
- NIST SP 800-84 Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities, 2006. 97 p.



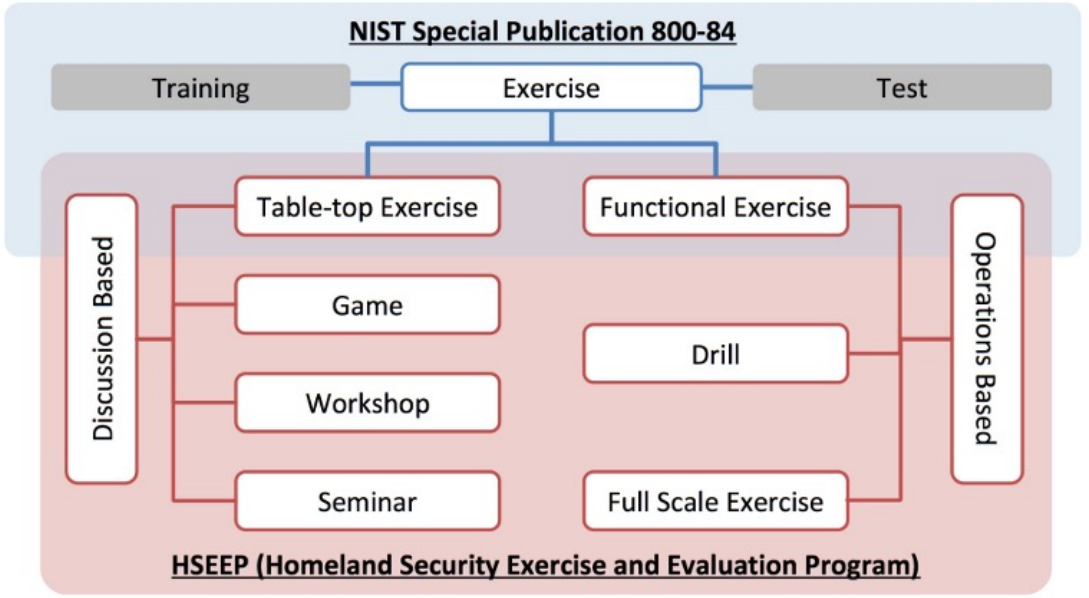
Классификации

- Виды учений и степень абстракции (теоретические, реальные)
- Уровень публичности (закрытые, открытые)
- Целевой показатель (непрерывность бизнеса, ЦДК, ..)
- Целевая аудитория (руководство, администраторы, пользователи)
- Виды сценариев (CTF-игра, мультизадачные, ролевые)
- Техники и тактики исследуемых атак
- Масштаб (организация, отрасль, ..)
- Прикладная сфера (КИИ)



Виды учений

- Штабные учения (discussion based)
  - Настольные (Table Top)
  - Штабные игры (Games)
  - Мастер-классы (Workshop)
  - Семинары
- Практические/технические (operations based)
  - Проверка управления, контроля и координации
  - Отработка навыков (Drill)
  - Полномасштабные учения
- Смешанные



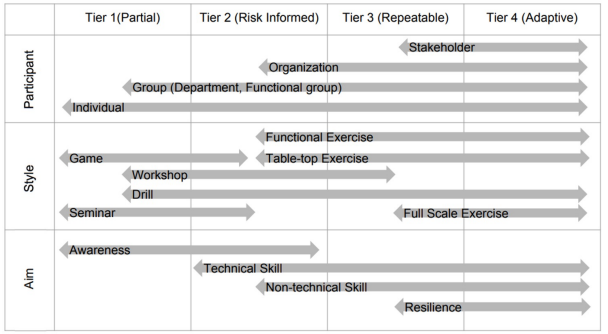
Пример: CTF-игры как вид киберучений

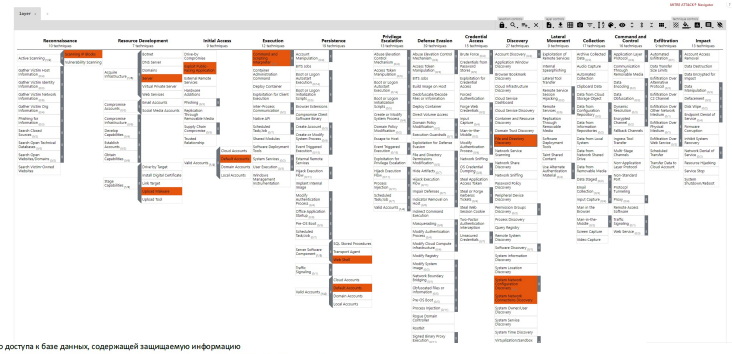
1996 г. Defcon

- Командам участников предлагается набор заданий по тестированию защищенности информационных систем, форензике, поиску и анализу информации, криптографии и т.п.
- Результатом успешного прохождения задания является набор символов (флаг). Например, флагом может быть пароль администратора, содержимое файла, доступное только определенному пользователю, расшифрованное значение и т.п.
- Флаги регистрируются в специальной судейской системе, которая автоматически ведет подсчет баллов каждой команды

Систематики ИБ для формирования сценариев

- NIST Framework (зрелость компании и/или этапы)
- LM Cyber Kill Chain (фазы кибератаки)
- MITRE ATT&CK (пост поведение атакующих)
- ФСТЭК России: Методика оценки угроз безопасности информации (перечень угроз)





Пример сценария для проведения киберучений в организации

- Сетевые атаки на ИТ-инфраструктуру, доступную извне
- Фишинговая рассылка с ПО для удаленного администрирования
- Подключение неавторизованного компьютера в корпоративную сеть
- Подбрасывание USB-носителя с ПО для удаленного администрирования
- Скрытая передача данных из сети с использованием стандартных протоколов, например по DNS
- Попытки физического получения конфиденциальной информации у сотрудников с помощью методов социальной инженерии

Пример сценария отраслевых или межгосударственных учений

- Противодействие кибергрупперовке

(например, Carbanak или Cobalt)

Наиболее известные за рубежом киберучения

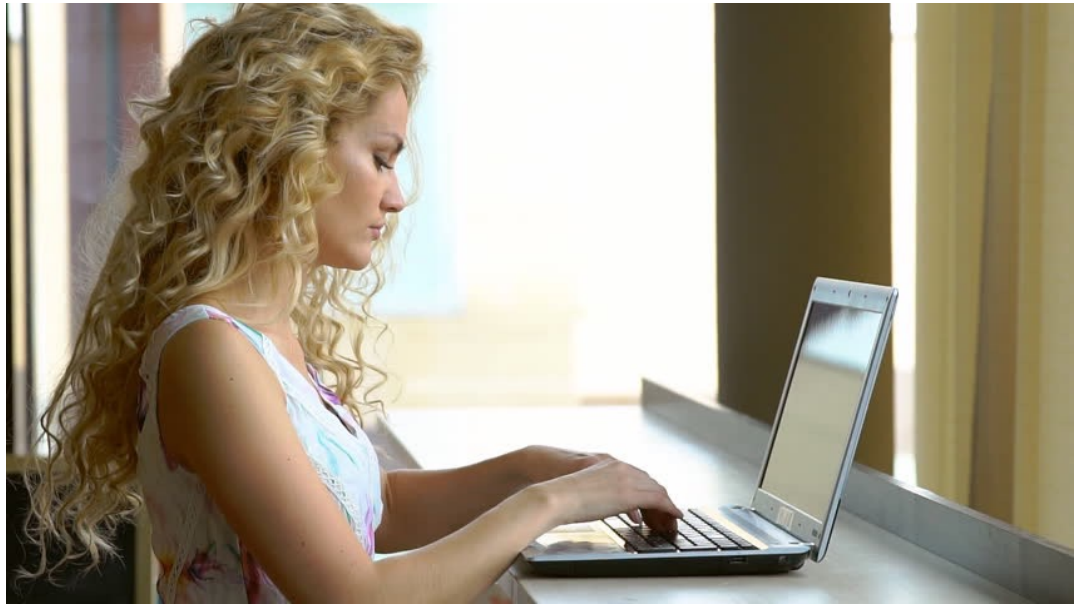
- Locked Shields (NATO Cooperative Cyber Defense Centre of Excellence)
- Crossed Swords (NATO Cooperative Cyber Defense Centre of Excellence)
- Cyber Coalition (NATO Cooperative Cyber Defense Centre of Excellence)
- Cyber Europe (European Union Agency for Network and Information Security)
- Cyber Guard (U.S. Cyber Command)
- Cyber Storm (U.S. Cybersecurity and Infrastructure Security Agency)

CCDCOE
NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia

enisa
European Network and Information Security Agency

Locked Shields : Проведения учений: ситуация, приближенная к реальной

- для нападающих защищаемая инфраструктура – «белый» ящик
- предустановлены бэкдоры
- в каждой защищаемой инфраструктуре есть пользователь с ролью «blonde», открывающий все вложения и переходящий по всем ссылкам
- уязвимости в основном в прикладном ПО



«blonde»

LOCKED SHIELDS

CCDCOE
NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia

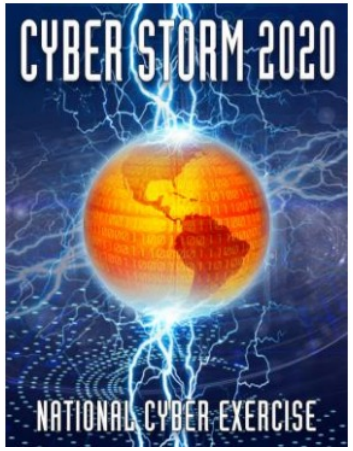
Locked Shields: Игровая инфраструктура: Gamenet

- 2013: 400 виртуальных узлов
- 2019: 4000 виртуальных узлов
- 2021: 5000 виртуальных узлов
- Разработчик: Cybexer (Эстония)

LOCKED SHIELDS

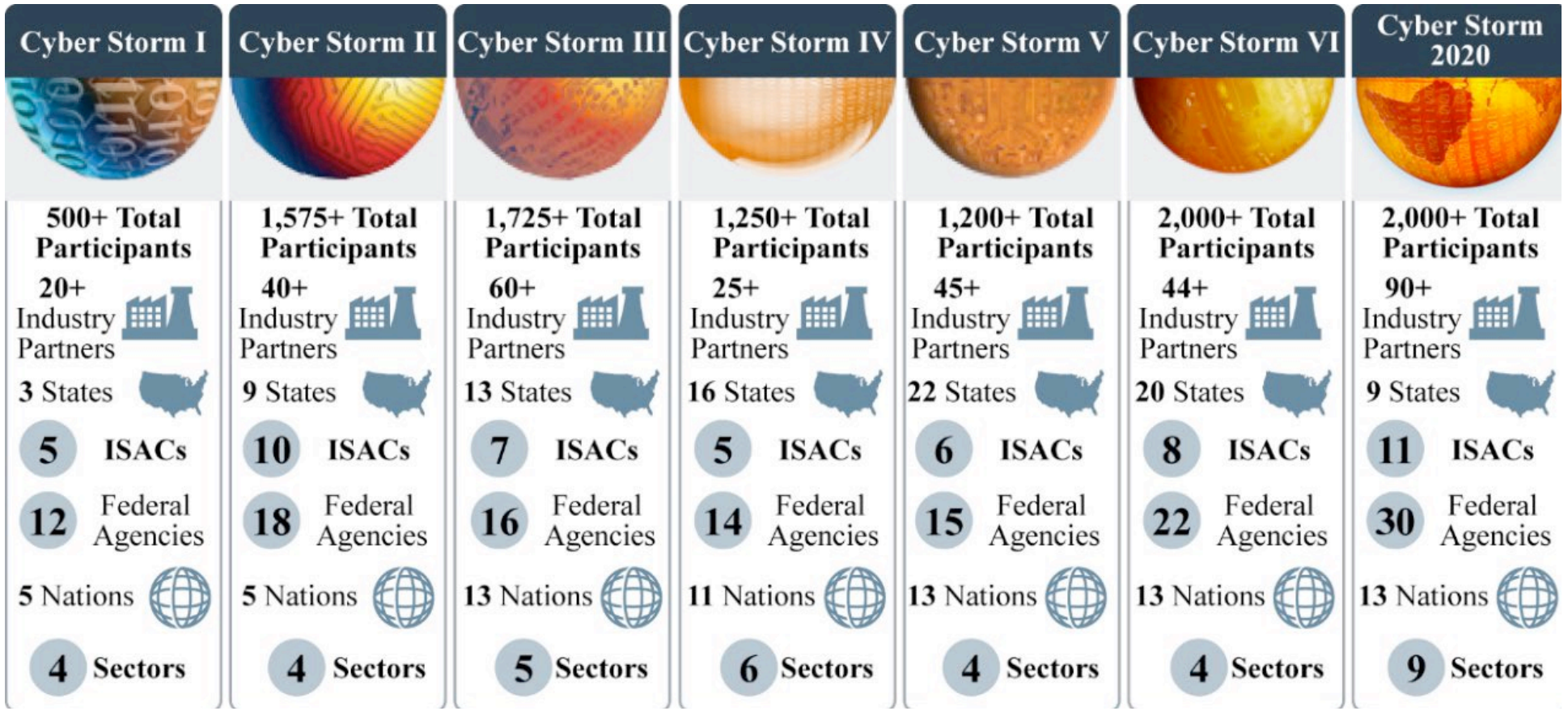
CCDCOE
NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia

Cyber Storm 2020: участники



- 2000 участников, среди которых представители:
  - государственных учреждений;
  - критической информационной инфраструктуры: телекоммуникации, энергетика, финансы, здравоохранение, транспорт, ИТ и др.

Киберучения Cyber Storm



Российские киберучения и полигоны

Киберучения как сервис

- CEaaI

- CEaaP

AMPIRE

- CEaaS Компании разработчики полной линейки (SIEM, VA, SIEM..)

BI.ZONE Cyber Polygon

АРСИБ
АССОЦИАЦИЯ РУКОВОДИТЕЛЕЙ СЛУЖБ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

RuCTF

The Standoff

Эшелонированная оборона

Эшелонированная оборона

Организаторы

Под эгидой Минобороны России объединились ведущие профильные компании и учебные заведения в сфере информационной безопасности и киберспорта

Организаторы

Департамент информационных Систем Минобороны России

Восьмое управление Генерального штаба Вооружённых сил

Военный инновационный технополис «ЭРА»

Основные технические организаторы

Эшелон
учебный центр

НТЦ
ВУЛКАН

генеральный спонсор:
ПСБ

Проведенные мероприятие в 2019

7 декабря 2019 года на территории парка «Патриот» состоялась торжественная церемония открытия практических соревнований по кибербезопасности.

В открытии приняли участие представители Государственной Думы, Минобороны, РАНХиГС, руководство ПАО «Промсвязьбанк», Юнармии.

Соревнования были проведены с активным привлечением инфраструктуры РАНХиГС, что позволило протестировать географическую разнесенность команд в ходе мероприятия.

Соревнования прошли по 3 номинациям:

«Специалисты» - **7 команд по 7 человек**;

«Начинающие» - **6 команд по 7 человек**;

«Юниоры» - **8 команд по 7 человек**.

Всего в соревнованиях приняли участие **147 человек** из **7 городов России**.

Особенность соревнований заключалась в том, что они прошли в онлайн-режиме, все участники соревнований находились на своих площадках в своих городах.

Почетный гость Вячеслав Александрович ФЕТИСОВ отметил, что данные соревнования являются хорошим заделом на проведение более масштабных как командных, так и индивидуальных состязаний и подчеркнул важность мероприятия для выявления талантливой молодежи

первый заместитель председателя Комитета Государственной Думы по физической культуре, спорту, туризму и делам молодежи В.А.ФЕТИСОВ

Декабрь 2019

Август 2020

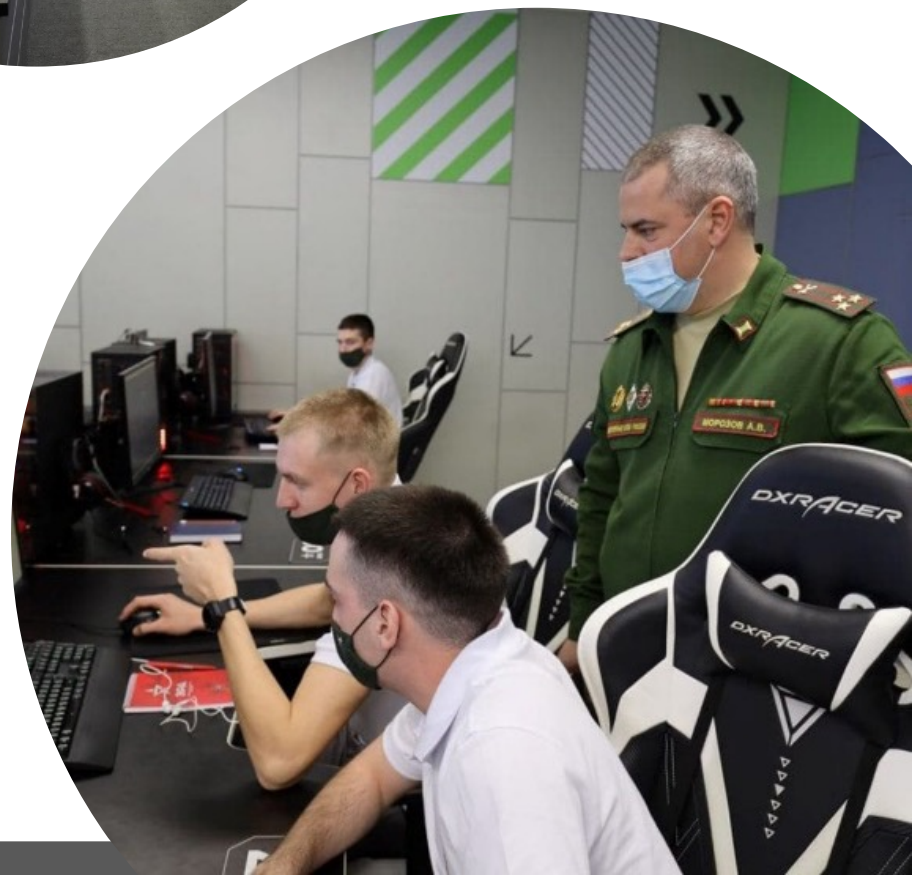

Мастер-класс по тестированию защищенности
КИБЕРПАТРИОТ


КИБЕРПАТРИОТ

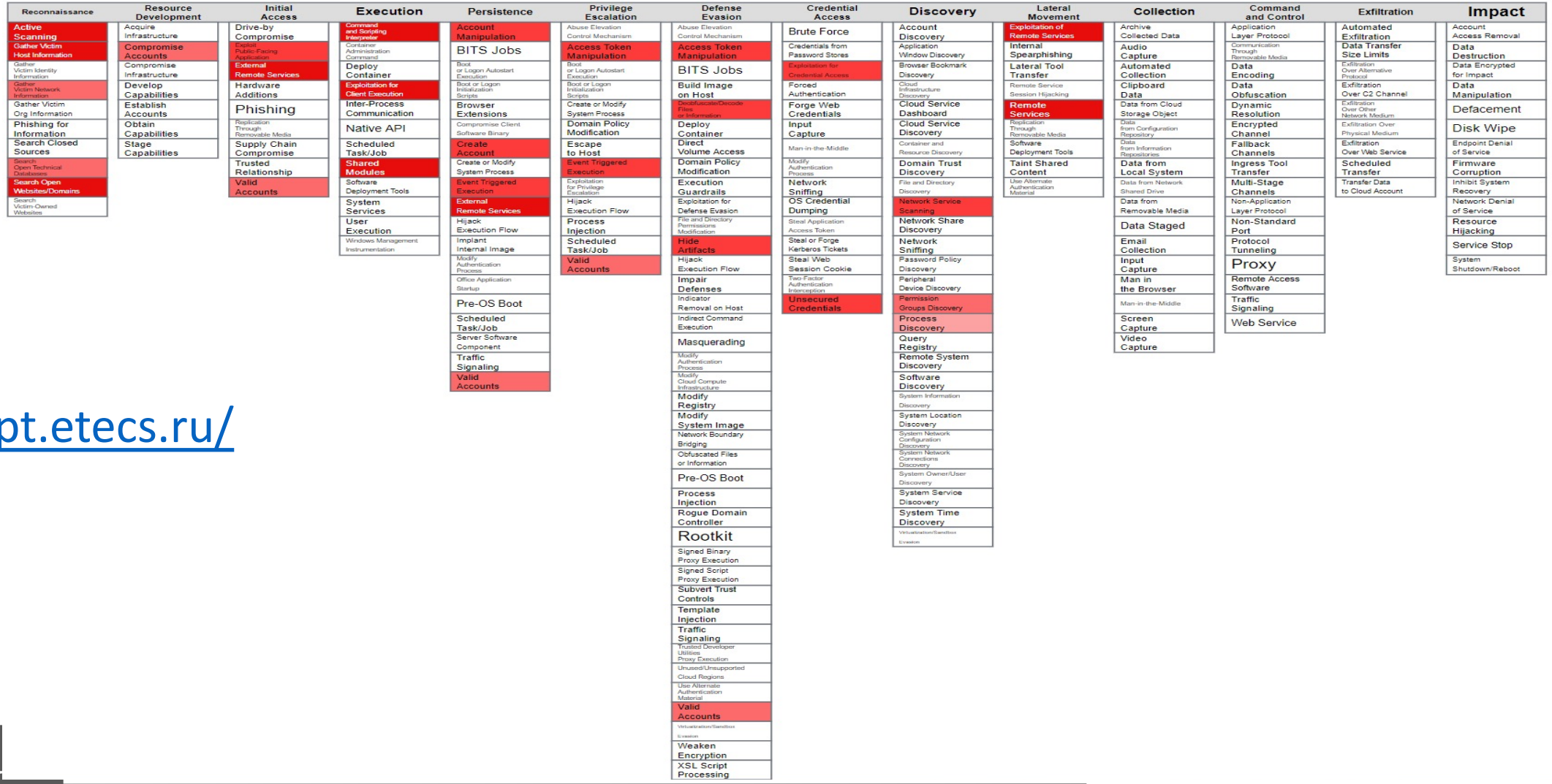

КИБЕРПАТРИОТ
АКС
ПСБ

Эшелонированная оборона 2020

- Более 100 команд и 3 уровня участников: юниоры, специалисты и курсанты
- Участники из 27 городов России
- Финал проводился из ВИТ ЭРА



Сопоставление типов заданий с матрицей MITRE ATT@CK



https://apt.etecs.ru/

География участников

Всего участвовало команд: 112

Вузы, принявшие участие

- ВКА им. А.Ф. Можайского
- Краснодарское высшее военное училище
- Военная академия связи
- Военный университет радиоэлектроники
- ФГАУ ВИТ «ЭРА»
- Академия ФСО России
- РТУ МИРЭА
- МГТУ им. Баумана
- НИУ МЭИ
- МАИ
- НИЯУ МИФИ
- Череповецкий государственный университет
- Курганский государственный технологический университет
- Крымский федеральный университет имени В.И.Вернадского
- Государственный университет "Дубна"
- ВИ МВД России
- Астраханский Государственный Технический Университет
- Университет ИТМО
- Ярославский государственный университет им. П. Г. Демидова
- Пермский государственный национальный исследовательский университет
- и многие другие

Призеры:

В категории «Специалисты»:

1. Университет ИТМО, г. Санкт-Петербург;
2. Академия ФСО России, г. Орёл;
3. КУБГТУ, г. Краснодар.

В категории «Курсанты»:

1. ВКА имени А.Ф. Можайского, г. Санкт-Петербург;
2. ВКА имени А.Ф. Можайского, г. Санкт-Петербург (команда 2);
3. Краснодарское высшее военное училище, г. Краснодар.

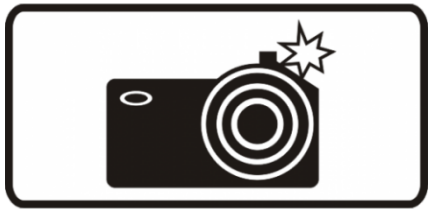
В категории «Юниоры»:

1. Сборная из школ Калининграда, Санкт-Петербурга и Ростова-на-Дону;
2. СУНЦ УрФУ, г. Екатеринбург;
3. Школа №1770, г. Москва

Киберучения бессмысленны, если отсутствуют СЗИ следующих классов: FW, IDS, VA и SIEM

МЭ и СОВ «РУБИКОН»

1. Межсетевой экран



2. Система обнаружения вторжений

3. Маршрутизатор

KOMRAD Enterprise SIEM 4.0

Гибкая и производительная система централизованного управления событиями информационной безопасности, совместимая с отечественными средствами защиты информации.

Система анализа защищенности Сканер-ВС 6.0

- Сканирование портов и определение версий сервисов
- Инвентаризация установленного программного обеспечения
- Сканирование уязвимостей
- Подбор паролей
- Анализ конфигурации

Краткие выводы

- Киберучения – актуальная форма обучения, ориентированная на реальный инциденты
- Сочетается с дистанционным обучением
- Популярные учения в вузовской среде – CTF-учения
- В мире и России сложились систематики формирования сценариев
- Представлены различные уровни организации учений: от «полигонов под ключ» до создания собственных с нуля
- Имеется широкий спектр проприетарных (платных) инструментариев и инструментариев с открытым кодом для проведения или организации учений
- Имеется бесплатный инструментарий, ориентированный на вузы

Литература

- *Dorofeev A.V., Markov A.S.* Conducting Cyber Exercises Based on the Information Security Threat Model // CEUR Workshop Proceedings, 2021, vol. 3057, pp. 1–10. URL: http://ceur-ws.org/Vol-3057/paper1.pdf

СПАСИБО ЗА ВНИМАНИЕ!

Марков Алексей Сергеевич
a.markov@npo-echelon.ru