ПОЛИТЕХ
Санкт-Петербургский политехнический университет Петра Великого

Виртуальный киберполигон для практико-ориентированных образовательных игровых технологий в области информационной безопасности

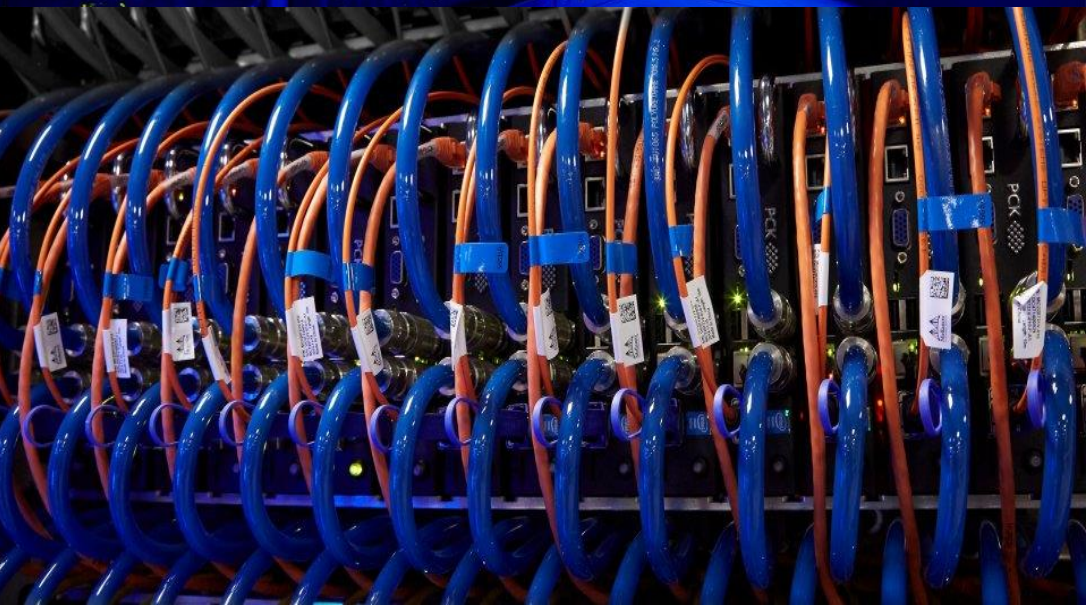
Доцент института кибербезопасности и защиты информации СПБПУ, к.т.н.

Павленко Евгений Юрьевич

Санкт-Петербург
2021

ПОЛИТЕХ
Санкт-Петербургский политехнический университет Петра Великого

Использование виртуального киберполигона



Описание подхода

- С использованием собственного оборудования ИКиЗИ и суперкомпьютерного центра «Политехнический» создается виртуальный киберполигон, обеспечивающий одновременную работу с ним большого числа студентов
- Полигон представляет собой виртуальную среду, имитирующую информационную инфраструктуру реальных компьютерных и киберфизических систем
- Использование виртуального киберполигона позволяет студентам удаленно и в игровой форме получать практические знания и навыки по обеспечению кибербезопасности
- Имитация реальных систем позволяет наглядно демонстрировать возможные вектора кибератак на них, последствия от кибератак, а также эффект от использования различных средств кибербезопасности

ПОЛИТЕХ
Санкт-Петербургский политехнический университет Петра Великого

Общая схема обучения на киберполигоне

Студенты: атакующие

Студенты: аналитики

Студенты: защитники

Реальные атаки

Анализ и оценка

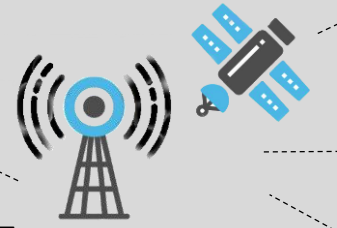
Защита

СКЦ «Политехнический»

Виртуальная IT-инфраструктура реальных отраслей

Транспорт

Экономика



Телекоммуникации и связь

Нефтедобыча

Строительство и техническая экспертиза

Здравоохранение

Металлургия

Юриспруденция и правовая экспертиза

Моделирование любых внешних условий: **технологические санкции**, отключение от сети Интернет…

Выпускники

- Имеют практические навыки построения систем кибербезопасности
- Готовы отражать и предотвращать реальные кибератаки
- Умеют работать с интеллектуальными средствами защиты

Результаты

- Развитие и совершенствование отечественных средств защиты
- Устойчивость функционирования в условиях внешних воздействий и технологических санкций

ПОЛИТЕХ
Санкт-Петербургский политехнический университет Петра Великого

Преимущества виртуального киберполигона

СТУДЕНТЫ

- Автоматизированная генерация отчетов о выполненной работе
- Работа с виртуальной информационной инфраструктурой реальных систем
- Широкий выбор используемых средств кибербезопасности и возможность их гибкой настройки

ВИРТУАЛЬНЫЕ ЛАБОРАТОРИИ

- Множество цифровых лабораторий в рамках одного виртуального полигона
- Имитация информационной инфраструктуры промышленных и киберфизических систем
- Имитация вредоносных объектов и средств обеспечения кибербезопасности

ПОТЕНЦИАЛЬНЫЕ РАБОТОДАТЕЛИ

ПРЕПОДАВАТЕЛИ

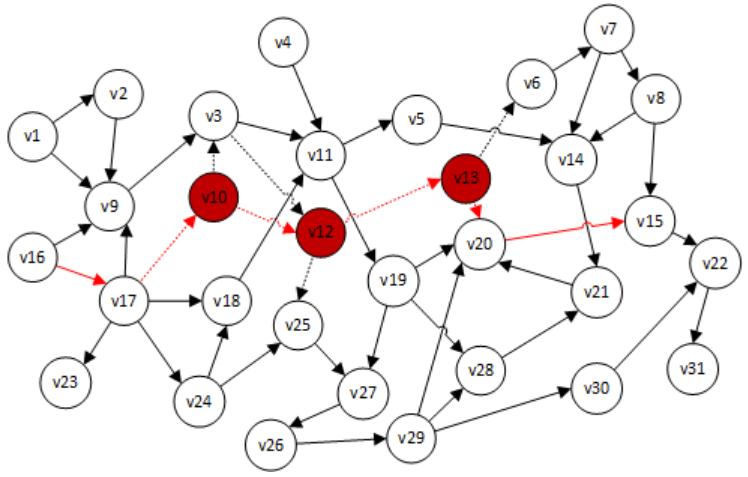
- Генерация индивидуальных лабораторных работ
- Автоматизированная проверка лабораторных работ
- Интеллектуальные средства оценки и проверки на плагиат
- Автоматическая генерация новых вариантов лабораторных работ

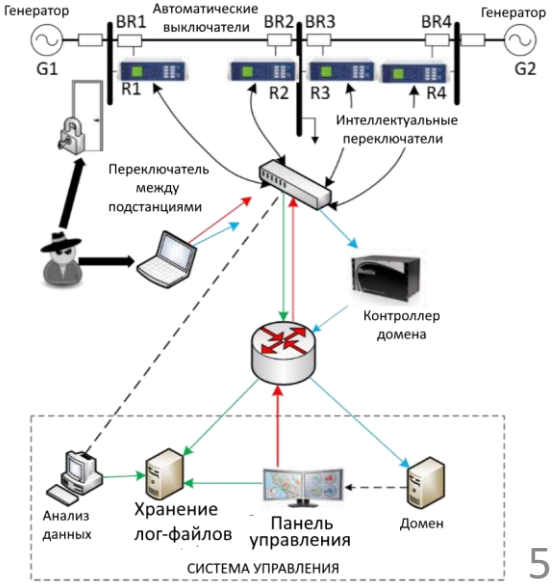
ПОЛИТЕХ
Санкт-Петербургский политехнический университет Петра Великого

Наработки ИКиЗИ в части создания виртуального киберполигона (1)

ИНТЕЛЛЕКТУАЛЬНАЯ СЕТЬ ЭНЕРГОСНАБЖЕНИЯ SMART GRID

- Имитация информационной инфраструктуры интеллектуальных сетей энергоснабжения Smart Grid (сетевые устройства, «умные» измерители, переключатели, концентраторы, компоненты управления)
- Моделирование кибератак на Smart Grid (внедрение ложных данных, изменение настроек системы, удаленное отключение компонентов системы)
- Лабораторные работы, связанные с обнаружением кибератак на Smart Grid и автоматической саморегуляцией структуры сети для нейтрализации кибератак:
  - Использование методов искусственного интеллекта для обнаружения кибератак
  - Настройка средств защиты: систем обнаружения вторжений, антивирусных средств, межсетевых экранов
  - Разработка сценариев и моделей защиты в соответствии с типами кибератак



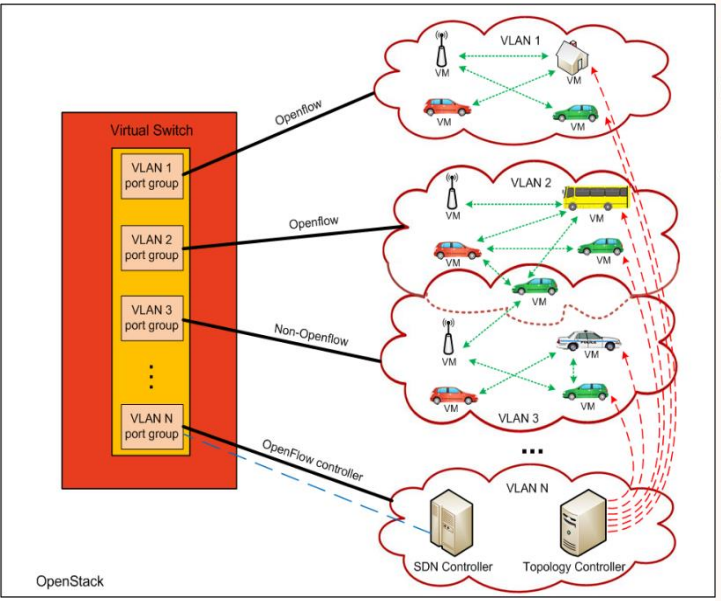


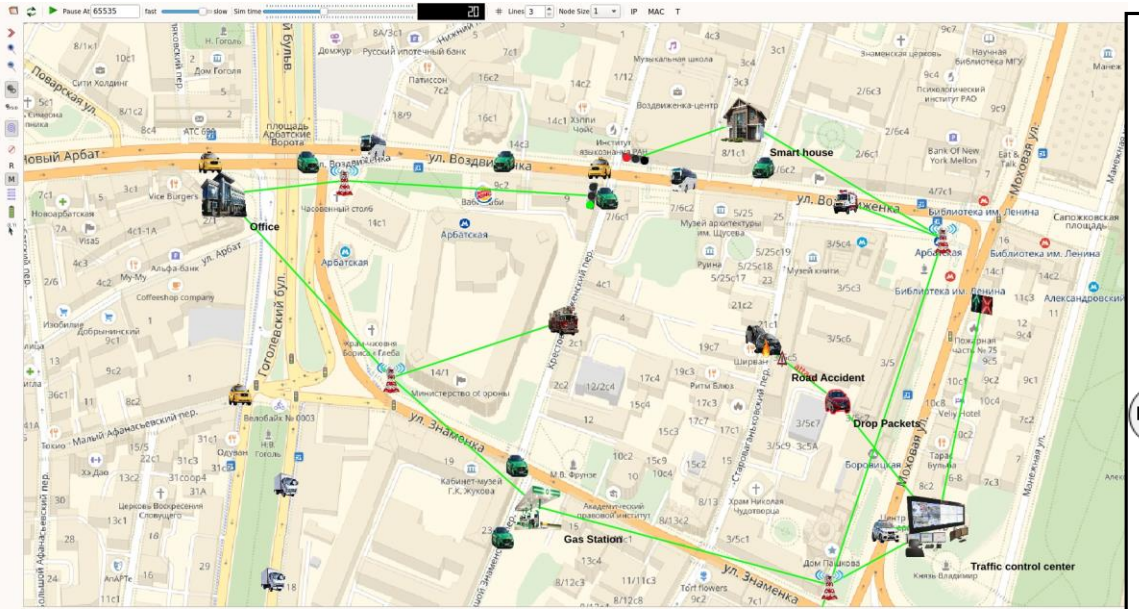
ПОЛИТЕХ
Санкт-Петербургский политехнический университет Петра Великого

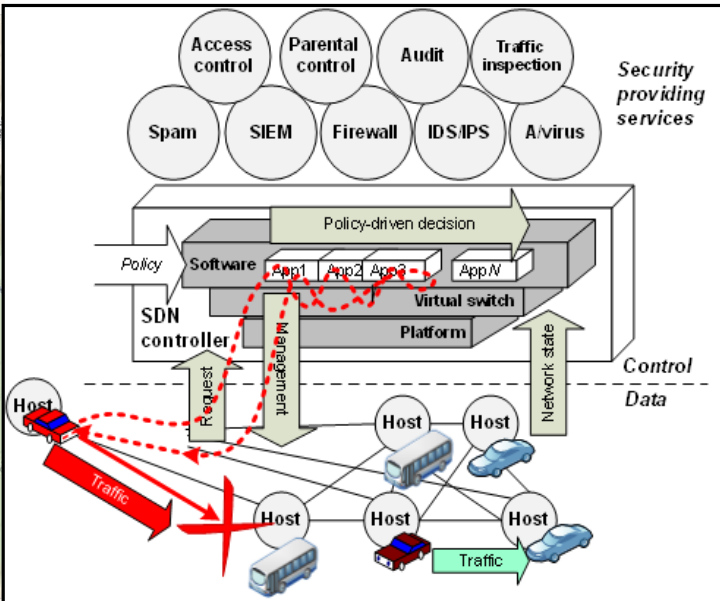
Наработки ИКиЗИ в части создания виртуального киберполигона (2)

ИНТЕЛЛЕКТУАЛЬНАЯ СЕТЬ БЕСПИЛОТНОГО ТРАНСПОРТА (VANET)

- Имитация сети беспилотных автомобилей с использованием СКЦ «Политехнический»
- Интеллектуальная случайная генерация кибератак на сеть, вызывающих дорожно-транспортные происшествия и перебои в работе городского транспорта
- Лабораторные работы, связанные с обнаружением кибератак на сети беспилотного транспорта и построением систем защиты:
  - Настройка контроллеров программно-конфигурируемых сетей, разработка программных политик безопасности для них
  - Работа с механизмами контроля доступа, системами обнаружения вторжений и межсетевыми экранами
  - Обнаружение вредоносного программного обеспечения





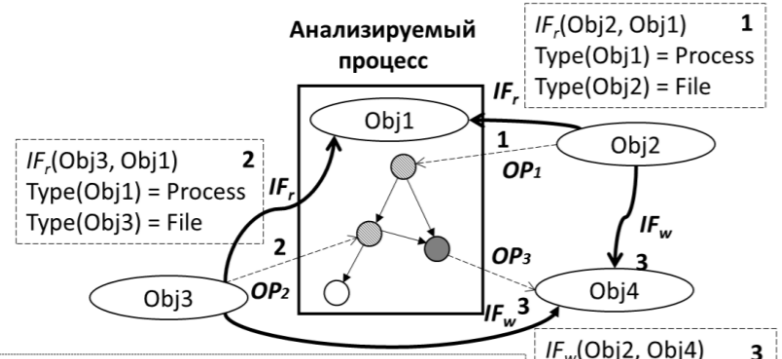


ПОЛИТЕХ
Санкт-Петербургский политехнический университет Петра Великого

Наработки ИКиЗИ в части создания виртуального киберполигона (3)

ИНТЕЛЛЕКТУАЛЬНЫЙ АНАЛИЗ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ НА ПРЕДМЕТ ВРЕДОНОСНОГО ПОВЕДЕНИЯ

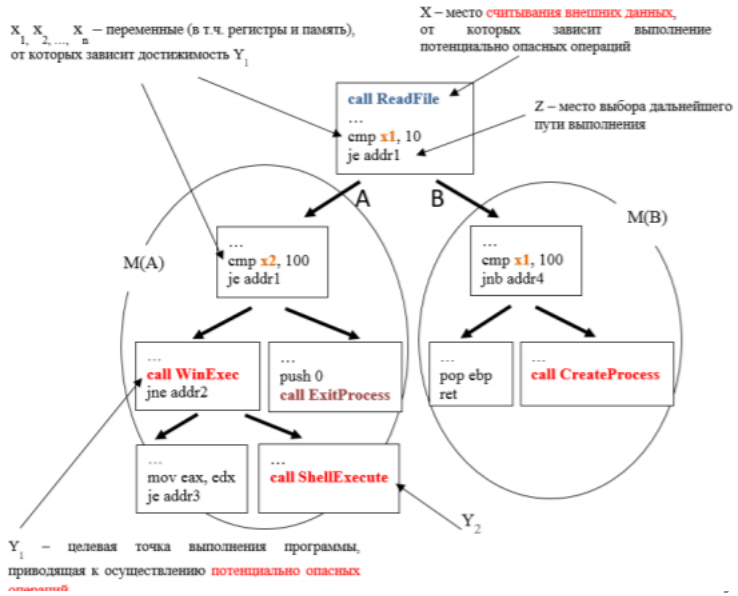
- Интеллектуальная генерация образцов вредоносного программного обеспечения (ВПО)
- Загрузка в виртуальную лабораторию набора образцов, среди которых образцы как легитимного ПО, так и ВПО



Пример анализируемой трассы выполнения:
*ReadFile(**File1**, Buf1, 0x10, nBytes1, NULL); // **OP1***
*ReadFile(**File2**, Buf1+nBytes1, 0x20, nBytes2, NULL); // **OP2***
*send(**Socket**, Buf1, nBytes1+nBytes2, 0); // **OP3***

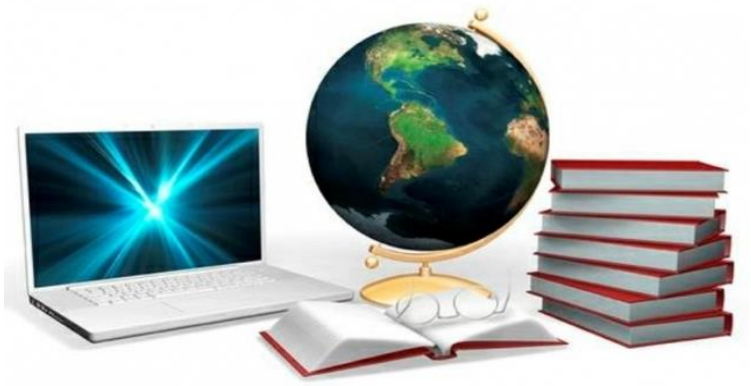
OP – операции с внешними объектами, выполняемые анализируемым процессом
IF – информационные потоки, порожденные при выполнении операций

- Лабораторные работы, связанные с применением reverse engineering и методов искусственного интеллекта для автоматического распознавания ВПО:
  - Статический и динамический анализ программного обеспечения
  - Разработка модулей для интеграции с антивирусными средствами
  - Максимизация покрытия анализируемого кода
  - Использование машинного обучения для выявления аномального поведения программ



ПОЛИТЕХ
Санкт-Петербургский политехнический университет Петра Великого

Эффекты от внедрения виртуального киберполигона



- ✓ Предоставление качественного образования в области кибербезопасности, сочетающего теорию и практику
- ✓ Организация гибкого регулярного доступа к цифровым лабораториям
- ✓ Широкий спектр объектов защиты, имитирующих инфраструктуру реальных объектов
- ✓ Получение студентами практических навыков по построению систем защиты удаленно и в игровой форме
- ✓ Работа с наиболее распространенными технологиями и средствами обеспечения кибербезопасности, получение опыта в их конфигурации
- ✓ Отсутствие предвзятости при генерации и проверке лабораторных работ
- ✓ Широкие возможности для трудоустройства посредством предоставления потенциальным работодателям «цифрового резюме» студентов

ПОЛИТЕХ
Санкт-Петербургский политехнический университет Петра Великого

СПАСИБО ЗА ВНИМАНИЕ

Доцент ИКиЗИ СПБПУ, к.т.н.

Павленко Евгений Юрьевич

Санкт-Петербург
2021