

Роль киберполигонов в вузах в борьбе с современными киберугрозами

Научный руководитель – Екатерина Денис Игоревич

Симакова Екатерина Андреевна

Студент (специалист)

Санкт-Петербургский университет Министерства внутренних дел Российской
Федерации, Санкт-Петербург, Россия

E-mail: ekaterina.simakova.2001@yandex.ru

В настоящее время наблюдается появление совершенно новых категорий угроз в сфере информационной безопасности [1]. Готовность к эффективному противостоянию этим угрозам требует постоянного обновления и расширения знаний в данной области.

Киберполигоны в учебных заведениях представляют собой часть национального киберполигона, развертываемого Минцифры России на всей территории страны. Эта инициатива является частью федерального проекта «Информационная безопасность», включенного в национальную программу «Цифровая экономика» [2]. Развертывание киберполигонов осуществляется совместно с участием экспертов из университетов и дочерней компании «Ростелекома» – «Ростелеком-Солар» [4].

В России сейчас работает пять киберполигонов: в Сибирском государственном университете телекоммуникаций и информатики, в ДВФУ на острове Русский, в НТУ «Сириус» в Сочи, в Санкт-Петербурге в ИТМО и университете «Бонч-Бруевича».

Национальный киберполигон — это крупная государственная инициатива, которую разрабатывает «Ростелеком». В 2021 году ИТМО совместно с компанией открыл опорный центр «Киберполигон». Он предназначен для того, чтобы отрабатывать процессы выявления и реагирования на компьютерные атаки.

Университет телекоммуникаций имени профессора М.А. Бонч-Бруевича в Санкт-Петербурге обладает киберполигоном, представляющим собой образовательную площадку, целью которой является моделирование и анализ хакерских атак. С помощью него студенты осваивают навыки работы с техническим оборудованием, изучают различные сценарии кибератак и проводят тренировки по обеспечению защиты информационной инфраструктуры от потенциальных хакерских воздействий [3].

Фундаментом для функционирования киберполигона является виртуальная среда, представляющая собой отображение инфраструктуры разнообразных организаций. В Университетах МВД в данный момент также разрабатывается программа по внедрению киберполигонов, которые можно будет использовать для обучения сотрудников МВД навыкам по информационной безопасности.

Киберполигоны сталкиваются с проблемой недостаточной реалистичности и актуальности обучающих сценариев. Внедрение передовых технологий, таких как искусственный интеллект и машинное обучение, может повысить эффективность киберполигонов.

Источники и литература

- 1) Буйневич М.В., Матвеев А.В., Смирнов А.С. Актуальные проблемы подготовки специалистов в области информационной безопасности МЧС России и конструктивные подходы к их решению // Научно аналитический журнал «Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России». 2022. №3. С. 1-17.

- 2) Матвеев А.В., Синещук М.Ю., Шестаков А.В., Гавкалюк Б.В. Методика технико-экономической оценки вариантов построения организационно-технической системы класса «Киберполигон» // ИВД. 2023. №6 (102). С. 121-137.
- 3) В ВУЗах Санкт-Петербурга открылся очередной киберполигон: <https://www.itbestsellers.ru/news/detail.php?ID=50799>
- 4) На базе Санкт-Петербургского университета Бонч-Бруевича открылся киберполигон: <https://digital.gov.ru/ru/events/41426/>