Жуков А.О., викладач
Житомирський військовий інститут імені С. П. Корольова

РОЛЬ НАВЧАЛЬНИХ КІБЕРПОЛІГОНІВ У ПІДГОТОВЦІ ФАХІВЦІВ У СФЕРІ КІБЕРБЕЗПЕКИ

Відкрита збройна агресія рф проти нашої держави супроводжується активними кібератаками на українську інформаційну інфраструктуру. За даними Держспецзв'язку, проти України від початку повномасштабного вторгнення здійснено втричі більше кібератак, ніж за аналогічний період минулого року.

Для адекватного реагування на нові виклики виникає гостра проблема у посиленні кіберзахисту, удосконалення технологій та підготовці висококваліфікованих спеціалістів, що володіють знаннями та практичними навичками вирішувати реальні завдання у сфері кібербезпеки.

Одним з перспективних напрямів технологічного досягнення такої мети є проектування, розробка та застосування навчально-лабораторних комплексів – кіберполігонів. Кіберполігон – це спеціальне середовище, яке являє собою сукупність спеціалізованого апаратно-програмного забезпечення, об'єднаного мережними комунікаціями, що може бути інтегрованим до мережі Інтернет, та призначене для підвищення рівня технічної підготовки персоналу при вирішенні ними спеціальних завдань (протидії кібертероризму, кіберзлочинності, забезпечення кібероборони тощо) та випробування новітніх технологій гарантування кібербезпеки [1, с. 152].

На теперішній час з урахуванням аналізу передового досвіду застосування сучасних навчально-лабораторних комплексів на базі Житомирського військового інституту імені С. П. Корольова розгорнутий та ефективно функціонує унікальний навчально-тренувальний комплекс Кіберполігон [2] для проведення науково-практичних досліджень, відпрацювання навчальних заходів з протидії гібридних впливів у кіберпросторі, якісної підготовки фахівців із кібербезпеки.

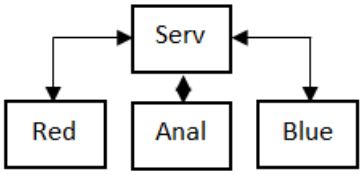

Рисунок 1 – Топологія кіберполігону

Технічно структура Кіберполігону складається з 4 функціонально-пов'язаних компонентів: комплекту кібероборони (кібербезпеки, кіберзахисту) та кіберрозвідки (тестування на кіберзахищеність), серверної інфраструктури для створення мережевої моделі, моніторингу та аналізу всіх виконуваних дій (рис. 1). Програмним ядром є новітній дистрибутив операційної системи Kali Linux. Функціональне призначення програмної та апаратної складових визначається безпосередніми класами задач і специфіки кожного із компонентів Кіберполігону.

Особливістю впровадження кіберполігону у навчальний процес є можливість готувати спеціалістів з інформаційної безпеки в умовах максимально наближених до реальних, удосконалення практичних навичок курсантами (студентами) у вигляді командних (групових) змагань, зокрема таких як національні змагання з кібербезпеки UA30CTF, Національний оборонний хакатон (National Defence Hackathon) тощо.

Наявність такого Кіберполігону надає можливість підвищення кваліфікації кіберспеціалістів, проведення наукових досліджень, ознайомлення з особливостями протидії кібернетичним загрозам та впливам в кіберпросторі, висококваліфіковану підготовку військових та цивільних фахівців у галузі кібербезпеки, надає можливість проведення з їх використанням кібернавчань і тренувань з елементами відпрацювання дій в умовах інформаційних та кібервпливів, участі у національних та міжнародних змаганнях і навчаннях, удосконалення системи підготовки та підвищення кваліфікації військових фахівців у галузі інформаційної та кібербезпеки з впровадженням комплексних підходів і стандартів НАТО.

Список використаних джерел та літератури

1. Грищук Р. В. Кіберполігон як навчальне середовище з метою підготовки персоналу для боротьби з кіберзлочинністю. Кібербезпека в Україні: правові та організаційні питання : матеріали Всеукр. наук.-практ. конф. Одеса: Одеський держ. ун-т внутр. спр., 2017. С. 152- 153.
2. Навчальний кіберполігон відкрили в Житомирському військовому інституті.URL:https://censor.net/ua/photo_news/3222663/navchalnyyi_kiberpoligon_vidkryly_v_jytomyrskomu_viyiskovomu_instytuti_fotoreportaj.