УДК 355.40: 004.621: 355.405.1 **Самчишин О.В., Умінський В.В.**

ПРОЕКТ КІБЕРНЕТИЧНОГО ПОЛІГОНУ ДЛЯ ПІДГОТОВКИ ВИСОКОКВАЛІФІКОВАНИХ ФАХІВЦІВ У ГАЛУЗІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

Запропоновано проект кібернетичного полігону для відпрацювання питань захисту національних інформаційних ресурсів. У статті розглянуто спектр питань, які необхідно вирішити при підготовці висококваліфікованих фахівців у галузі інформаційної безпеки держави.

Ключові слова: кібернетичний полігон, кіберпростір, кіберзброя, кібербезпека, кіберзахист.

Постановка проблеми. Активне впровадження сучасних інформаційно-комунікаційних технологій для управління військами та зброєю потребує приділення особливої уваги безпеці інформаційно-телекомунікаційних систем військового призначення. Сьогодні кіберпростір стає новим театром воєнних дій, який відкриває широкі можливості щодо порушення життєво необхідних функцій об'єктів критичної інфраструктури будь-якої держави світу без використання літаків, танків та інших "класичних" зразків озброєння, при цьому не піддаючи ризику життя власних солдат. Прикладом тому є локальні воєнні конфлікти, які виникли останнім часом в Іраку, Росії, Грузії, Афганістані, Тунісі, Алжирі, Лівії, Йорданії, Ємені, Єгипті, Сирії, Марокко, Бахрейні, Ірані тощо. І це далеко не повний перелік країн, в яких відбувається збройна боротьба із застосуванням кіберзброї.

Зазначені вище факти формують широкий спектр сучасних небезпек та загроз національним інтересам України у сфері оборони, що зумовлює нагальну потребу коригування її державної воєнної політики у галузі інформаційної безпеки, а також дієвої стратегії стосовно реформування Збройних Сил. Реалізація такої стратегії можлива виключно на основі глибокого аналізу тенденцій розвитку збройної боротьби сучасності та прогнозування її розвитку на майбутнє з метою удосконалення діючих підходів щодо оборонного планування в області кібербезпеки.

Одним з перспективних підходів до проведення такого аналізу є створення кібернетичного полігону, що за своїм змістом є фактично моделлю розподіленої мережі управління військами та зброєю.

Аналіз останніх досліджень і публікацій. У провідних країнах світу протягом останнього десятиліття спостерігається активне створення, інтенсивне нарощування і динамічне розгортання спеціалізованих підрозділів в області кібербезпеки [1]. Так військові командування і спеціалізовані підрозділи кібербезпеки для ведення високотехнологічних війн вже мають більше 30 держав, включаючи армії Китаю, США, Німеччини, Ізраїлю, Франції, Англії, Росії, Індії, Ірану, Пакистану, Південної і Північної Кореї. На сьогодні вже створено мережу колективної кібербезпеки Північноатлантичного альянсу. Наприклад, у 2008 році в Таллінні був відкритий Центр кіберзахисту НАТО, одним із завдань якого є моделювання онлайн-кібервійн для проведення постійних тренінгів фахівців у галузі інформаційної безпеки [2-6]. Нині завершуються роботи над проектом «Національний кіберполігон» (National Cyber Range) в США [7], проводяться показові віртуальні навчання на британському кібернетичному полігоні [8].

Тому задача створення проекту кібернетичного полігону *є актуальною* і на початковому етапі зводиться до визначення завдань, складових і його структури з метою підготовки висококваліфікованих фахівців у галузі інформаційної безпеки держави**.**

Виклад основного матеріалу. Військові експерти з кібербезпеки [9] вважають, що максимуму уваги слід приділяти питанням удосконалення електронної обороноздатності й посиленню кібернетичної розвідки. У зв'язку зі збільшенням випадків проведення кібератак на військові мережі вони прогнозують активізацію превентивних дій в кіберпросторі. Реалізація визначених питань дозволить військовим командуванням і спеціалізованим підрозділам кібербезпеки перейти від збору інформації до розробки широкого спектру кіберзброї наступального характеру, яка стане активно використовуватись поряд з

традиційними методами ведення війни. Розширення наступального потенціалу в кіберпросторі стає для збройних сил важливим етапом у зміні тактики ведення бойових дій.

Тому кібернетичний полігон доцільно створити з метою відпрацювання технологій виявлення кібератак та протидії ним, ліквідації наслідків застосування кіберзброї та відновлення нормальних режимів функціонування мереж управління військами та зброєю. Не менш важливе значення при цьому має підготовка фахівців, здатних здійснювати кібердудари у відповідь на несанкціоновані дії атакуючої сторони.

Кібернетичний полігон - це сукупність апаратно-програмних засобів, об'єднаних єдиною розподіленою локальною мережею з виходом до мережі Інтернет, призначений для випробувань військових систем кібернетичного впливу та захисту, проведення заходів з технічної підготовки висококваліфікованих фахівців і досліджень у галузі інформаційної безпеки держави. На такому полігоні спеціалісти з інформаційної безпеки зможуть відпрацьовувати варіанти захисту інформаційних мереж, національних електронних ресурсів від кіберзброї та моделювати проведення кібератак у відповідь на несанкціоновані дії.

З визначення кібернетичного полігону сформульовано спектр основних завдань, які необхідно вирішувати:

- розробка спеціалізованого програмного забезпечення кібернетичного впливу та захисту від несанкціонованого доступу до інформаційно-телекомунікаційних систем;
- розробка лабораторного середовища для проведення спецдосліджень в галузі технічних та програмних засобів кіберзахисту та відповідних методик захисту об'єктів критичної інфраструктури;
- визначення оптимального способу нейтралізації загроз в кіберпросторі з урахуванням наявних апаратно-програмних засобів технічного захисту інформації;
- моделювання процесів нападу та захисту інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури;
- оцінювання рівня захищеності електронних ресурсів та апаратно-програмних засобів інформаційно-телекомунікаційних систем;
- аналіз ефективності кібернетичного впливу на інформаційно-телекомунікаційних системи об'єктів критичної інфраструктури протидіючої сторони.

Реалізація зазначених завдань можлива на кібернетичному полігоні, проект якого подано на рис. 1.

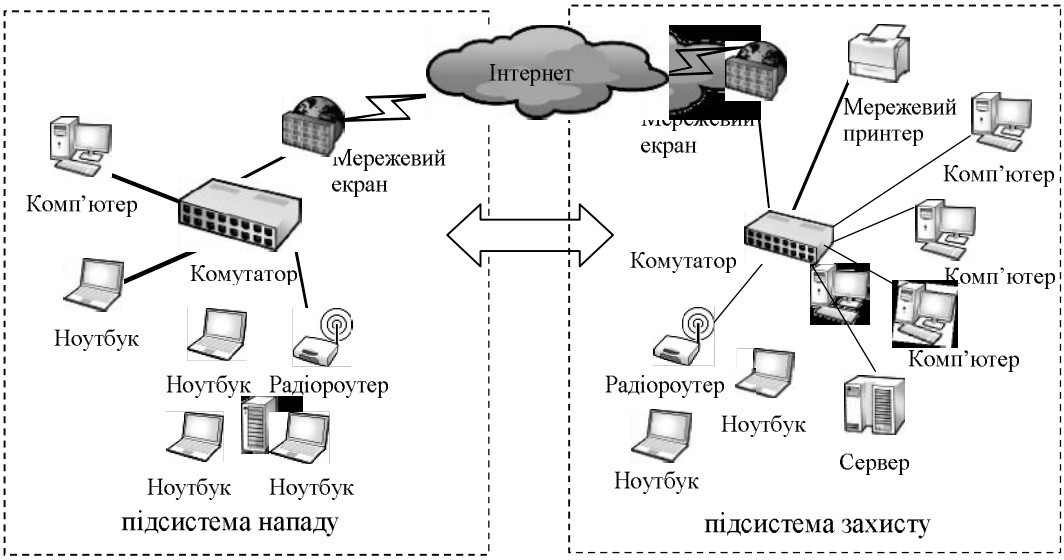

Рис. 1. Проект кібернетичного полігону

На рис. 1 до проекту кібернетичного полігону запропоновано включити дві підсистеми – нападу та захисту. Програмно-апаратні ресурси підсистеми нападу повинні забезпечувати можливість проведення кібератак різного типу, використовуючи відповідні мережеві

протоколи, вразливості системного та прикладного програмного забезпечення, недосконалості антивірусного програмного забезпечення. Наприклад: сканування портів, відмова в обслуговуванні, прослуховування та перехват потоку інформації в каналах мережі, псевдосанкціоноване проникнення в підсистему захисту, знищення, спотворення, крадіжка інформації, блокування доступу до неї в підсистемі захисту за допомогою засобів спеціального програмного впливу тощо. Технічні пристрої і спеціалізоване програмне забезпечення повинні забезпечити надійний захист системних ресурсів та інформації, що циркулює та зберігається на комп'ютерах в локальній мережі підсистеми захисту.

У рамках проекту кібернетичного полігону спеціалісти з інформаційної безпеки (кожний окремо або у складі визначених команд) зможуть відпрацьовувати спеціальні прийоми кібернападу та захисту від нього, не наносячи шкоди існуючій електронній інфраструктурі держави.

Висновки. Якісно організоване інформаційне вторгнення в локальні мережі об'єктів критичної інфраструктури будь-якої держави світу в змозі нанести більші збитки, ніж "класична" військова операція. Тому потреба створення в складі силових відомств нашої країни спеціалізованих підрозділів з кібербезпеки для забезпечення захисту від діяльності кіберзлочинців, вивчення способів і тактик ведення кібервійн є очевидною.

Запропонований проект кібернетичного полігону на першому етапі дозволить проводити підготовку висококваліфікованих фахівців спеціалізованих підрозділів у галузі інформаційної безпеки держави, які зможуть відпрацьовувати такі основні питання, як моделювання кібератак, виявлення вразливих місць систем захисту локальних мереж, відтворення комп'ютерних мереж військового призначення з метою перевірки рівня їх захищеності тощо.

ЛІТЕРАТУРА

1. Хорошко В.А. Информационная безопасность Украины. основные проблемы и перспективы / В.А. Хорошко // Захист інформації. Спеціальний випуск (40) / Державний університет інформаційно-комунікаційних технологій. - К. : ДУІКТ, 2008. - 131 с. стр. 6-9.
2. Даник Ю. Г. Деякі підходи до формування системи підготовки кадрів для системи кібернетичної безпеки України / Ю. Г. Даник, Ю. М. Супрунов // Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем : збірник наукових праць. Вип. 5 / Житомирський військовий інститут імені С.П. Корольова Національного авіаційного університету. - Ж. : ЖВІ НАУ, 2011. - 232 с. стр 5-22.
3. Lappin, Yaakov (18 May 2011). "Prime minister announces new cyber defense taskforce". Jerusalem Post [Электронный ресурс]. - Режим доступу: http://www.jpost.com/Defense/Article.aspx.
4. Williams, Dan (18 May 2011). "Eye on tech exports, Israel launches cyber" [Электронный ресурс]. - Режим доступу : http://www.reuters.com/article/2011/05/18/israel-security-cyber.
5. Yu, Eileen (27 May 2011). "China dispatches online army" [Электронный ресурс]. - Режим доступу: http://www.zdnetasia.com/china-dispatches-online-army-62300502.htm.
6. China Confirms Existence of Elite Cyber-Warfare Outfit the "Blue Army" [Электронный ресурс]. - Режим доступу : http://www.foxnews.com/scitech/2011/05/26/china-confirms-existence-blue-army-elite-cyber-warfare-outfit.
7. DARPA построит национальный киберполигон [Электронный ресурс]. - Режим доступу: http://vpk.name/news/54138_darpa_postroit_nacionalnyii_ kiberpoligon.html.
8. На британском "киберполигоне" провели показательные виртуальные учения [Электронный ресурс]. - Режим доступу: http://hitech.newsru.com/article/27dec2010/northrop.
9. Дергачев В. Геополитика мировой кибервойны. - Вестник аналитики - 2011. - №1. - [Электронный ресурс]. - Режим доступу: http://dergachev.ru/geop/index.html.

Надійшла: 25.01.2012

Рецензент: д.т.н., проф. Хорошко В.О.