Охрімчук В.В., к.т.н., професор,
Гуменюк І.В., к.т.н., доцент
Кошева І.Г.
Житомирський військовий інститут імені С. П. Корольова

РОЛЬ І МІСЦЕ ПІДГОТОВКИ ФАХІВЦІВ ІЗ КІБЕРБЕЗПЕКИ ДЛЯ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ ДЕРЖАВИ

Під час російсько-української війни, яка розпочалась з анексії Криму в 2014 році, інформаційно-комунікаційні системи (ІКС) України ставали об'єктами атак з боку російської федерації (рф). Так, наприклад 23 грудня 2015 року російським зловмисникам вдалось успішно атакувати комп'ютерні системи управління "Прикарпаттяобленерго" та вимкнули близько 30 підстанцій, залишивши близько 230 тисяч мешканців без світла протягом однієї-шести годин. Вона стала першою у світі підтвердженою кібератакою, спрямованою на виведення з ладу енергосистеми. Найбільшою за останні роки є атака на підприємства України вірусу Petya у 2017 році, внаслідок якої було призупинено роботу третини всіх українських банків, більш ніж 100 великих підприємств і організацій були вимушені призупинити свою роботу. Країни-члени організації розвідувального альянсу FVEY (Five Eyes) покладають відповідальність за цю атаку на рф.

Від початку повномасштабного воєнного вторгнення рф в Україну Урядова команда реагування на комп'ютерні надзвичайні події CERT-UA зареєструвала та дослідила понад 1500 кібератак. Більшість із них – з боку рф. Серед головних цілей ворожих хакерів – шпіонаж (отримання розвідданих щодо логістики, озброєння, планів та операцій Сил безпеки та оборони), спроби виведення з ладу об'єктів критичної інформаційної інфраструктури, позбавлення доступу громадян до державних послуг та сервісів, банківського обслуговування тощо, а також – інформаційно-психологічні операції та дезінформаційні "вкиди" з метою підриву довіри до спроможностей органів державної влади, Сил безпеки та оборони, поширення панічних настроїв серед населення.

Таким чином, для забезпечення відповідного (належного) рівня національної безпеки України в умовах, які склалися, якісна та своєчасна підготовка фахівців із кібербезпеки, постійне нарощення ситуаційної обізнаності, передовий досвід країн-членів Альянсу НАТО та впровадження його в освітні компоненти є беззаперечно актуальним, своєчасним та необхідним завданням, у тому числі і для відбиття збройної агресії рф та отримання інформаційної переваги над противником.

Підготовка фахівців із кібербезпеки вимагає належної технологічної оснащеності вищого військового навчального закладу, залучення висококваліфікованих спеціалістів. Одним із пріоритетних напрямків реалізації якісної підготовки є врахування передового досвіду, отриманого під час курсової підготовки педагогів із фундаментальних знань та набуття технологічних навичок та умінь мережної академії CISCO. Зокрема, використання провідного мережного устаткування та відповідного програмного забезпечення є базовою складовою щодо підготовки відповідного рівня фахівців. Так, на базі кафедри спроєктовано та впроваджено в експлуатацію унікальне апаратно-програмне середовище забезпечення кібербезпеки ІКС – Кіберполігон, який не має аналогів серед закладів вищої освіти України.

Основну увагу під час підготовки варто приділяти гібридності інформаційної та кібервійни з боку рф, особливості скоєння кібератак та деталізованому аналізу кіберінцидентів. Це дозволить спланувати надійний захист ІКС під час майбутніх кібердій. Необхідними компонентами у забезпеченні національної безпеки України на кожному із мандатних рівнів (організацій, державних установ, об'єктів критичної інфраструктури, військових та силових структур) є знання технологій оцінювання захищеності ІКС чи локальних мереж шляхом часткового моделювання дій зовнішніх зловмисників з проникнення у неї (pentesting) та вміння їх застосовувати; налаштовувати та використовувати відомі та надійні сервіси безпеки на програмному та/або апаратному рівнях тощо. Підтримання відповідного кваліфікаційного рівня науково-педагогічного складу шляхом проходження щорічних особистих стажувань, участі у міжнародних кіберзмаганнях, постійного нарощення кіберобізнаності та кібергігієни викладачами кафедри є також невід'ємною складовою у досягненні поставленого завдання.

Враховуючи пріоритетність та актуальність забезпечення національної безпеки України, збереження територіальної цілісності та недоторканості під час відбиття повномасштабного вторгнення рф, якісна підготовка фахівців із кібербезпеки вимагає постійного нарощення досвіду, знань та технологічного опанування провідного мережного устаткування та оперативного використання здобутих результатів навчання. У такому контексті досягається інформаційна перевага над противником, успішна та своєчасна протидія усім потенційно можливим кіберзагрозам з боку рф.

Отже, підготовка фахівців із кібербезпеки є одним із важливих напрямків забезпечення національної безпеки держави.