УДК 378,004

Віталій Анатолійович СВІТЛИЧНИЙ,
кандидат технічних наук,
доцент кафедри кібербезпеки факультету № 4
Харківського національного університету внутрішніх справ;
ORCID: https://orcid.org/0000-0003-3381-3350

ВДОСКОНАЛЕННЯ ПІДГОТОВКИ КУРСАНТІВ ЗАКЛАДІВ ВИЩОЇ ОСВІТИ ІЗ СПЕЦИФІЧНИМИ УМОВАМИ НАВЧАННЯ ЯК ФАХІВЦІВ З КІБЕРБЕЗПЕКИ

З кожним роком проблема захисту інформації стає все більш актуальною і гострішою. На перший план виходить підготовка фахівців, які спроможні забезпечити інформаційну та кібербезпеку держави. На сучасному етапі розвитку науки і техніки кібербезпека перетворюється на одну з найактуальніших задач високотехнологічного суспільства. Внаслідок надзвичайно широкого використання сучасних інформаційних технологій в усіх сферах свого існування суспільство стало вразливим від незначних кібернетичних впливів, які все частіше стають ефективним інструментом на шляху досягнення мети щодо несилового контролю та управління як

об'єктами критичної інфраструктури держави, підприємств, так і окремо взятими громадянами, їх об'єднаннями.

З одного боку кібербезпека – це захищеність від наявних та потенційно небезпечних проявів інформаційного впливу, що створюють небезпеку для функціонування інформаційних ресурсів, систем, мереж, програмних і апаратних засобів, а також свідомості, підсвідомості, морально-психологічного стану людини, соціальних груп та суспільства в цілому.

З іншого, кібербезпека – це комплекс заходів та засобів, що спрямовані на захист комп'ютерів, цифрових даних і мереж їх передачі від несанкціонованого доступу та інших дій, пов'язаних з маніпулюваннями або крадіжкою, блокуванням, пошкодженням, руйнуванням та знищенням як випадкового, так і цілеспрямованого впливу. Тому об'єктом діяльності фахівця з кібербезпеки є процеси захисту інформації у всіх її видах.

Відомо, щороку всі українські університети випускають приблизно 1,5 тисячі бакалаврів спеціальності «Кібербезпека». Однак ці випускники не мають достатніх практичних навичок, їм потрібно 2-3 роки, щоб орієнтуватися в галузі та виконувати практичні завдання. Причина такої ситуації полягає в тому, що програми підготовки сьогоднішніх спеціалістів не дають тих навичок, які потрібні на робочому місці. Підготовка фахівців з кібербезпеки вимагає належної технологічної оснащеності вищого навчального закладу, залучення висококваліфікованих спеціалістів. Тому в Харківському національному університеті внутрішніх справ в серпні 2016 року створена кафедра кібербезпеки яка готує кіберполіцейських. Кафедра здійснює підготовку: бакалаврів з галузі знань 12 «Інформаційні технології», спеціальності 125 «Кібербезпека», спеціалізація Поліцейська діяльність у кіберсфері. Після закінчення ВНЗ фахівці з кібербезпеки можуть працювати на посадах слідчих і оперуповноважених підрозділів боротьби з кіберзлочинами, зі злочинами, пов'язаними з торгівлею людьми, а також в оперативно-технічних та інформаційно-аналітичних підрозділах та інших підрозділах Національної поліції України.

В процесі навчання курсанти отримають наступні знання та навички:

– здатність до використання інформаційних і комунікаційних технологій;

– здійснювати професійну діяльність на основі знань сучасних інформаційно-комунікаційних технологій, застосувати програмні засоби, навички роботи в телекомунікаційних та комп'ютерних мережах, використати спеціалізовані комп'ютерні програми в професійній діяльності;

– виконувати спеціальні дослідження технічних і програмно-апаратних засобів захисту обробки інформації;

– здійснювати проектування (розробку) систем, технологій і засобів кібербезпеки, використання національних стандартів криптографічного захисту інформації, протидію несанкціонованому

проникненню в інформаційні системи і мережі, вибір ефективних засобів та методів криптографічного захисту інформації в інформаційно-технічних системах;

– знання: основ криптології та криптографічного захисту інформації для забезпечення її конфіденційності та цілісності; національних стандартів криптографічного захисту інформації, захисту програм та даних програмно-апаратними засобами та оцінки якості прийнятих рішень, основних методів та способів захисту інформації відповідно до вимог сучасних стандартів кібербезпеки, застосовуючи системний підхід та отриманні знання;

– знання з основ законодавчої, нормативно-правової баз України та вимог відповідних стандартів, тому числі міжнародних; вміння готувати пропозиції до нормативних актів щодо забезпечення кібербезпеки;

– здатність впроваджувати та супроводжувати прикладне та системне програмного забезпечення операційних систем з метою захисту інформації в інформаційно-телекомунікаційних системах;

– прогнозувати, виявляти та оцінювати стан кібербезпеки об'єктів і систем;

– вміння визначати і усувати основні загрози кібербезпеки, будувати модель порушника, виявляти і усувати вразливості в основних компонентах відкритих інформаційно-телекомунікаційних системах, виявляти, переривати та попереджувати віддалені мережеві атаки за їх характерними ознаками, розробляти політику безпеки, проектувати і реалізовувати комплексну системи забезпечення кібербезпеки, тестувати і на основі результатів тестування робити обґрунтований вибір засобів захисту, здійснювати моніторинг мережевої безпеки адмініструвати відкриті інформаційно-телекомунікаційні системи.

Проте власне оволодіння системою знань і умінь є лише необхідною умовою для успішної діяльності та не впливає на активність її суб'єкта. Позиція молодого фахівця кібербезпеки багато в чому залежить від мотиваційної системи, ставлення до завдань, змісту і об'єкту його діяльності. Структура мотивації тісно пов'язана з суспільним розвитком особи і є могутнім суб'єктивним чинником ефективності життєдіяльності.

Окремої уваги потребує підготовка кіберполіцейських – аналітиків у сфері кібернетичної безпеки, на яких мають покладатись обов'язки щодо виявлення криміногенних чинників, що сприяють розповсюдженню комп'ютерних злочинів, відстеження основних тенденцій і прогнозування потенційних загроз. Незважаючи на важливість цієї категорії фахівців, такої відокремленої спеціальності в Україні взагалі немає, тому питання комплексної підготовки фахівців з питань кібербезпеки в умовах сучасних викликів та розвитку глобального кіберпростору потребує самої прискіпливої уваги МВС та Міністерства освіти і науки України.

Висновок. На нашу думку, з метою більш якісної підготовки фахівців з кібербезпеки потрібно враховувати академічні та професійні

вимоги до спеціалістів в галузі програмування, комп'ютерних наук та інформаційно-комунікаційних технологій, а також у супутніх галузях. Тому курсантів потрібно навчити нестандартно мислити, добре володіти іноземною мовою, щоб спілкуватися зі своїми колегами з інших країн для ознайомлення з зарубіжним досвідом в галузі боротьби з кіберзлочинністю. При цьому значну увагу потрібно надавати вивченню та практичному застосуванню технологій кібербезпеки при користуванні та розробці систем аналітичних досліджень, керування базами даних та знань, мережевих додатків та інтернет-сервісів, протоколів передачі та шифрування даних. Крім того потрібно ознайомлювати курсантів з методиками сертифікації, експертизи та проведення спеціальних досліджень (в тому числі з використанням паралельних та квантових обчислювальних середовищ) засобів і систем кібернетичного захисту інформаційних ресурсів. Необхідно ввести або значно розширити вузькоспеціалізовані курси, присвячені методам виявлення, блокування загроз та отримання доказів несанкціонованого доступу до інформації з відповідним ступенем секретності державних та комерційних інформаційних ресурсів. Крім того для якісної підготовки фахівців із кібербезпеки необхідно розробити такі навчальні програми, що ґрунтувалися б на класичному навчанні та вимогах сертифікатів міжнародних професійних асоціацій, перш за все сертифікація спеціалістів з інформаційної безпеки, наприклад Certified Information Systems Security Professional (CISSP).

Одержано 03.10.2018