

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>;*

Юрій Миколайович ОНИЩЕНКО,

*кандидат наук з державного управління,
доцент кафедри кібербезпеки факультету № 4
Харківського національного університету внутрішніх справ;
ORCID: <https://orcid.org/0000-0002-7755-3071>*

АКТУАЛЬНІ АСПЕКТИ ПІДГОТОВКИ КУРСАНТІВ ХАРКІВСЬКОГО НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ ВНУТРІШНІХ СПРАВ ЯК ФАХІВЦІВ КІБЕРБЕЗПЕКИ

Формування майбутніх фахівців кібербезпеки для Національної поліції є результатом тривалого процесу підготовки курсантів у Харківському національному університеті внутрішніх справ (ХНУВС). Одним з пріоритетних напрямів роботи ХНУВС є підготовка кваліфікованих фахівців для Національної поліції України, які орієнтовані на боротьбу зі складними у технічному плані злочинами. Курсанти вивчають новітні методи використання комп'ютерної техніки в оперативно-розшуковій діяльності, значна увага приділяється вивченню сучасних інформаційних технологій. Отриманні знання використовуються фахівцями з вищою освітою під час служби в оперативних підрозділах кіберполіції Національної поліції України та інших підрозділів Національної поліції України, що займаються протидією кіберзлочинності, злочинам у сфері торгівлі людьми та моральності, у міжнародній сфері та транснаціональній злочинності.

Викладачі ХНУВС постійно підтримують зв'язок з територіальними підрозділами слідства, кіберполіції, технічного захисту інформації Національної поліції України, а також з експертно-криміналістичними підрозділами МВС України. Працівники університету залучаються до проведення виїзних занять, підвищення кваліфікації, надання консультацій працівникам зазначених підрозділів, а також залучаються у якості спеціалістів при проведенні слідчих (розшукових) дій. Отриманий практичний досвід, підкріплений накопиченими специфічними теоретичними знаннями та уміннями, передається курсантам університету.

Загальна підготовленість курсантів до розслідування кіберзлочинів, злочинів у сфері торгівлі людьми, у міжнародній сфері та транснаціональній злочинності визначається вимогами оволодіння системою специфічних професійних знань та умінь, а також психологічними процесами, станом, досвідом і особистісними якостями майбутнього фахівця кібербезпеки. 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. Керівництво та науково-педагогічний склад ХНУВС прикладає багато зусиль для вирішення цього питання, але цього явно недостатньо. Питання підготовки фахівців з питань кібербезпеки в умовах сучасних викликів та розвитку глобального інформаційного простору потребує самої прискіпливої уваги Міністерства освіти і науки та МВС України та інших силових відомств.

На теперішній час актуальність підготовки фахівців кібербезпеки, особливо під час російської агресії, коли гостро відчувається потреба в таких спеціалістах, складно переоцінити, тому що кібербезпека – це одне з пріоритетних завдань держави, що визначено в основних нормативно-правових актах України. Структура готовності майбутніх фахівців з питань кібербезпеки до професійної діяльності включає в себе основоположні компоненти: теоретичні та методичні знання, професійні та прикладні уміння та навички; позитивну установку на виконання даного виду діяльності.

Засвоєння знань і умінь є необхідною передумовою для розвитку позитивного ставлення до майбутньої професійної діяльності випускника університету. У свою чергу позитивне ставлення

до виконання даної функції стимулює активність в оволодінні професійними знаннями і вміннями. Виключення будь-якого з вказаних компонентів або зниження рівня їх сформованості спричиняє зниження успішності, а відповідно і результативності професійної діяльності. Виходячи з результатів дослідження готовності курсантів до виконання службових обов'язків, можна виділити мотиваційну сферу як визначальний компонент у структурі готовності.

На жаль, за час навчання у ХНУВС курсанти не мають можливості в повній мері оволодіти професійною майстерністю, але її основи вони повинні опанувати. Професійна діяльність вимагає від курсантів глибоких теоретичних знань, практичних умінь і навичок не тільки в області кібербезпеки, але й у суміжних областях, без оволодіння якими не можна стати професійно підготовленим працівником поліції. Завдання університету полягає не тільки в тому, щоб озброїти курсантів теоретичними знаннями, але і навчити вчитися, тобто користуватися знаннями з практики.

Готовність до практичної діяльності на рівні професійної майстерності визначається низкою кваліфікаційних та професійних вимог. У порівнянні з навичками уміння в напрямку кібербезпеки мають велику змінність, носять усвідомлений характер виконання дій з переходом у наукову творчість. Зміна вимог до характеру умінь є відповіддю на зростання наукової інформації, швидку заміну старих знань новими. У цих умовах особливого значення набуває оволодіння людиною не стільки комп'ютерною технікою з відповідним програмним забезпеченням, скільки оперативною методикою виконання практичних завдань. Якщо такий підхід важливий у навчанні курсантів інших спеціальностей, то при підготовці фахівців з кібербезпеки він є необхідним. Адже фахівцям з кібербезпеки частіше, ніж іншим поліцейським доводиться оновлювати свої знання, переглядати методи роботи, опановувати нові вміння. Це складний процес, що включає інтелектуальний, емоційний і вольовий прояв особистості.

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 та студентів 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 недержавних інформаційних ресурсів.

Одержано 05.11.2017

УДК 351.74

Ігор Олегович СВЯТОКУМ,

*науковий співробітник науково-дослідної лабораторії
з проблем протидії злочинності*

Харківського національного університету внутрішніх справ;

ORCID: <https://orcid.org/0000-0003-4374-5494>

ПРОБЛЕМИ ОЦІНКИ ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ В КОНТЕКСТІ ПРОФЕСІЙНОЇ МОТИВАЦІЇ ЇЇ ПРАЦІВНИКІВ

Зміна підходу до оцінки ефективності роботи Національної поліції є одним із ключових елементів у її реформуванні та перетворенні на орган, що виконує передусім соціально-сервісну функцію. Важливість формування сучасної, прозорої та ефективної системи оцінки роботи поліції відображена у положеннях закону України «Про Національну поліцію», ч.3 ст.11 якого