УДК 65.012.8

Марков В. В.,
кандидат юридичних наук, старший науковий співробітник, начальник факультету підготовки фахівців для підрозділів боротьби з кіберзлочинністю та торгівлею людьми Харківського національного університету внутрішніх справ

ОСОБЛИВОСТІ ВПРОВАДЖЕННЯ ЗАРУБІЖНОГО ДОСВІДУ БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ В НАВЧАЛЬНИЙ ПРОЦЕС

Анотація. У статті проаналізовано стан та перспективи впровадження зарубіжного досвіду боротьби з кіберзлочинністю до навчального процесу відомчих навчальних закладів системи МВС України на прикладі Харківського національного університету внутрішніх справ. Розкрито останні досягнення університету у сфері впровадження зарубіжного досвіду, його взаємодію з Радою Європи, ОБСЄ, Організацією ІСІТАР, Ла-Страда тощо. Акцентовано увагу на потребі у впровадженні спеціалізованих навчальних курсів, програмного та апаратного забезпечення. Звертається увага на потребі залучення анонімної допомоги громадян у протидії кіберзлочинності, а також упровадженні досвіду США з протидії дитячій порнографії. Описано проект, запроваджений у Харківському національному університеті внутрішніх справ, у рамках якого відбувається одночасне поєднання курсантами виконання завдань з охорони правопорядку, відпрацювання навичок правоохоронця на спеціальних навчально-тренувальних полігонах, розробка власного програмного забезпечення.

Ключові слова: боротьба з кіберзлочинністю, зарубіжний досвід, правоохоронні органи, підготовка фахівців.

Постановка проблеми. Сучасний розвиток інформаційних технологій є розподіленим процесом, який відбувається паралельно по всьому світу та водночас характеризується наявністю певних центрів тяжіння, які акумулюють наукові думки та практичні напрацювання в цій сфері. На теперішній час такими центрами можна назвати США, потужні країни Європейського Союзу, КНР, Японію, Індію, Австралію. Відповідно, здебільшого саме в цих країнах відбувається найшвидше впровадження передових технологій у правоохоронну діяльність, зокрема з питань протидії кіберзлочинності.

Враховуючи викладене, вважається актуальним для правоохоронних органів України впровадження зарубіжного досвіду вказаних країн не лише безпосередньо в практичну діяльність, але й у навчальний процес курсантів, студентів, слухачів вищих навчальних закладів, які здійснюють підготовку фахівців у сфері боротьби з кіберзлочинністю. Більш того, впровадження такого досвіду повинно носити випереджаючий характер. Мінімальною вимогою має стати, аби найновіші досягнення у сфері боротьби з кіберзлочинністю паралельно впроваджувалися як у навчальний процес, так і в практичну діяльність. Програма максимум – аби такі технології спочатку відпрацьовувалися під час навчання. Поки ці технології дійдуть до «практиків», вищі навчальні заклади вже зможуть випустити підготовлених фахівців у цій сфері. Відтак вони не потребуватимуть додаткового навчання.

Питаннями впровадження зарубіжного досвіду боротьби з кіберзлочинністю у навчальний процес курсантів вищих навчальних закладів МВС України займалися О.М. Бандурка, А.В. Вінаков, А.В. Войціховський, О.М. Головко, С.М. Гусаров, М.Ю. Літвінов, О.В. Манжай, В.В. Носов, Л.А. Осипенко, І.М. Рязанцева, М.М. Перепелиця, В.В. Тулупов, В.Г. Хахановський та багато інших авторів.

Стаття має **на меті** проаналізувати стан та перспективи впровадження зарубіжного досвіду боротьби з кіберзлочинністю до навчального процесу відомчих навчальних закладів системи МВС України на прикладі Харківського національного університету внутрішніх справ.

Виклад основного матеріалу. 25 січня 2012 року наказом МВС України № 60 «Про оптимізацію узагальнення та поширення передового досвіду МВС України» Харківський національний університет внутрішніх справ було визначено відповідальним за роботу із загального вивчення та розповсюдження матеріалів передового досвіду в органах внутрішніх справ і внутрішніх військах МВС України [1, с. 170]. Таким чином, відбулося формальне закріплення статусу університету як однієї з провідних установ, яка здійснює накопичення та апробацію передового вітчизняного та зарубіжного досвіду у сфері протидії злочинності взагалі, та кіберзлочинності зокрема.

У контексті досліджуваної проблематики потрібно відмітити останні здобутки університету щодо впровадження зарубіжного досвіду у навчальний процес курсантів.

2014 року Харківський національний університет внутрішніх справ було включено до Стратегії Ради Європи «Підготовка правоохоронних органів» в частині навчання фахівців з протидії кіберзлочинності в Україні.

У цьому ж році в рамках взаємодії з Організацією безпеки та співробітництва в Європі Харківський національний університет внутрішніх справ отримав матеріали, які сприяють впровадженню нових технологій у навчальний процес. За результатами цієї взаємодії на факультеті підготовки фахівців для підрозділів боротьби з кіберзлочинністю та торгівлею людьми у навчальний процес впроваджено матеріали з цифрової криміналістики за такими темами: операційні системи та комп'ютерне обладнання; криміналістика даних в режимі реального часу; аналіз шкідливих програм; основні принципи та відповідні процедури пошуку та вилучення цифрових доказів; основні відомості про Linux; використання сервісів Google як засобів тестування безпеки інформаційних ресурсів мережі; огляд сфери кіберзлочинів; основи комп'ютерних мереж у контексті боротьби з кіберзлочинністю; пошук слідів при атаках на сервер комп'ютерної мережі; ідентифікація та геолокація підозрюваного; пошук слідів комп'ютерних засобів у режимі реального часу; боротьба з дитячою порнографією; валідація, отримання даних, хешування та стерилізація у цифровій криміналістиці.

Також у 2014 році представники університету вивчили досвід правоохоронних органів США у дослідженні бортових комп'ютерів автомобілів; мобільних пристроїв та чипів, а також досвід боротьби з дитячою порнографією, та використання знань з інформаційної безпеки у попередженні кіберзлочинів за програмою ІСІТАР Міністерства юстиції США. Раніше пред-

ставники університету у складі офіційної делегації МВС України відвідали з навчальним візитом Технологічний університет Труа (Франція) [2].

В.Г. Хахановський, аналізуючи перспективи автоматизації процесу розслідування, обґрунтовує необхідність широкого впровадження у слідчі та оперативні підрозділи ОВС України системи «I2», яка є світовим лідером серед програм для візуального аналізу даних у процесі розслідування, та використовується аналітиками і слідчими всього світу [3, с. 15]. На сьогодні Харківський національний університет внутрішніх справ продовжує переговори з компанією IBM щодо передачі університету цього програмного забезпечення для впровадження у навчальний процес.

Також бачиться корисним впровадження зарубіжного досвіду використання анонімної допомоги громадян для протидії злочинності. Наприклад, у США за надання допомоги поліції, у тому числі на анонімній основі, населення може розраховувати на отримання винагороди, яка залежить від цінності наданої інформації і розкритого злочину. Особі, яка повідомила відомості про злочин, гарантується повна анонімність. У час першого ж телефонного контакту їм привласнюється певний кодовий номер, яким користуються і при подальшому спілкуванні з цими громадянами. Якщо отримані відомості виявилися корисними для поліції (сприяли арешту, засудженню, поверненню викраденого майна, розшуку зниклої особи і тому подібне), при черговій телефонній розмові з громадянином оговорюється сума винагороди, а також спосіб і місце її передачі. Для отримання винагороди інформатор зацікавлений в успішному завершенні розслідування. Це є стимулом до постійних контактів з поліцією, в процесі яких не лише уточнюються первинні відомості, але і виявляються додаткові подробиці. Виплата винагороди зазвичай здійснюється через банк або якесь торгове підприємство, де, назвавши свій кодовий номер і суму винагороди, інформатор отримує конверт із грошима [4, с. 69].

Повертаючись до впровадження досвіду із використання анонімної допомоги громадян для протидії кіберзлочинності у Харківському національному університеті внутрішніх справ, варто відзначити, що у другому півріччі 2014 року університет взяв на себе підтримку гарячої лінії www.internetbezpeka.org.ua. За допомогою цієї лінії кожен громадянин України може повідомити про наявність дитячої порнографії в інтернет-просторі. За останні 6 місяців на гарячу лінію надійшло 19 повідомлень про вчинення правопорушень, які мають ознаки розповсюдження дитячої порнографії. Усі вони були уважно опрацьовані та передані правоохоронним органам за належністю.

Гаряча лінія є моніторинговим інструментом для збирання (шляхом отримання повідомлень від громадян) інформації про факти розповсюдження дитячої порнографії в Інтернеті з метою подальшого блокування цього негативного контенту.

Кожен користувач Інтернету може повідомити про випадки дитячої порнографії в Інтернеті, надіславши інформацію за допомогою форми на Головній сторінці сайту. Перевірка повідомлень буде здійснюватися 1–2 рази на тиждень експертом центру «Ла Страда–Україна». Користувачі Інтернетом мають змогу надсилати інформацію про факти дитячої порнографії в Інтернеті анонімно. Якщо ж користувач бажає отримати відповідь на своє повідомлення та дізнатися про подальшу роботу фахівців лінії з отриманою інформацією, він може залишити свої контакти.

Створення такої лінії є втіленням у життя однієї з рекомендацій Третього всесвітнього конгресу по боротьбі із комерційною сексуальною експлуатацією дітей та підлітків (2008 р.), воно відповідає принципам Факультативного протоколу по боротьбі із торгівлею дітьми, дитячою проституцією та дитячою порнографією, який доповнює Конвенцію ООН про права дитини, Конвенції Ради Європи про кіберзлочинність, Закону України про Загальнонаціональну програму «Національний план дій на виконання Конвенції ООН про права дитини до 2016 року». Програмне забезпечення лінії створене у відповідності до діючих зразків подібних ліній, що працюють в європейських країнах [5].

Як відзначають Д.Г. Мулявка та Т.А. Рекуненко, ефективна міжнародна взаємодія вимагає швидкого обміну інформацією між державами і оперативного виконання прохання про надання інформації, що зараз майже неможливо. Широке використання в даному випадку комп'ютерних мереж або інших засобів комунікації могло б значно прискорити процес отримання, обробки і застосування необхідної інформації [6, с. 143].

У зв'язку з наведеним вбачаємо необхідність упровадження американського досвіду щодо обміну інформацією про факти виготовлення та розповсюдження дитячої порнографії. З цією метою було б корисним отримати доступ до сервісу secure.icaccops.com, який акумулює дані про IP-адреси, з яких відбувається описана протиправна діяльність. Це завдання також сьогодні намагається вирішити Харківський національний університет внутрішніх справ. Доступ до цього ресурсу полегшить роботу функціонуючого в університеті з 2013 року Навчально-тренувального центру боротьби з кіберзлочинністю та моніторингу кіберпростору на громадських засадах (http://cybercop.in.ua/). До речі, завдяки роботі означеного центру в університеті реалізовано унікальний проект навчання. У рамках функціонування вказаного проекту відбувається одночасне поєднання курсантами виконання завдань з охорони правопорядку, відпрацювання навичок правоохоронця на спеціальних навчально-тренувальних полігонах, розробка власного програмного забезпечення. Вказаний процес реалізується у безпосередній взаємодії з територіальними підрозділами органів внутрішніх справ, про що було складено відповідні договори.

Подібний проект реалізовано в університеті Пердью «The Purdue University Cyber Forensics Lab» (штат Індіана, США), а також UCD Centre for Cybersecurity & Cybercrime Investigation – у провідному європейському виші з надання освіти у сфері протидії кіберзлочинності Дублінському університетському коледжі (University College Dublin). Разом із тим, реалізований у Харківському національному університеті внутрішніх справ проект вигідно відрізняється тим, що курсанти залучаються до роботи правоохоронних органів не лише під час провадження відповідних експертних досліджень, але й для виявлення, попередження, розкриття правопорушень та розшуку осіб.

Для реалізації проекту в університеті було спроектовано навчально-тренувальний полігон боротьби з кіберзлочинністю та моніторингу кіберпростору, та спеціалізоване програмне забезпечення (автоматизований банк даних «Невід») для супроводження його діяльності. Автоматизований банк даних «Невід» призначений для накопичення інформації про розміщення протиправного контенту в мережі Інтернет (інформаційна система «Правопорушення») і розшуку осіб (інформаційна система «Розшук»), та відповідних заходів щодо цього з боку органів внутрішніх справ.

На теперішній час курсанти, які навчаються на факультеті підготовки фахівців для підрозділів боротьби з кіберзлочинністю та торгівлею людьми за напрямком «Системи технічного захисту інформації», програмують відповідні модулі «Невід», ті з них, хто навчається за напрямком «Правознавство», здійснюють пошук інформації в комп'ютерних мережах за пріоритетними напрямками, визначеними МВС України. За домовле-

ністю з керівництвом Управління боротьби з кіберзлочинністю МВС України «Невід» після доопрацювання буде інтегровано як окремий модуль до розроблюваного автоматизованого робочого місця працівника Управління боротьби з кіберзлочинністю, після чого до його наповнення будуть залучені курсанти решти вишів системи МВС.

Висновки. Таким чином, у рамках підготовки фахівців для підрозділів, задіяних у боротьбі з кіберзлочинністю, в університетах потрібно постійно використовувати нові ідеї та підходи, а також упроваджувати передовий зарубіжний досвід. Адже інновації, як відомо, – це запорука розвитку правоохоронного відомства, інструмент, який стає реальною зброєю у боротьбі зі злочинністю. Саме тому на важливості використання інновацій у роботі міліції постійно наголошує керівництво Міністерства внутрішніх справ, особливо у контексті реформування правоохоронної системи України.

Література:

1. Волинець В.В. Теоретичні та практичні засади впровадження позитивного досвіду в діяльність органів внутрішніх справ / В.В. Волинець // Боротьба з організованою злочинністю і корупцією (теорія і практика). – 2012. – № 2 (28). – С. 167–178.
2. Курсанти вивчають зарубіжний досвід протидії кіберзлочинності [Електронний ресурс]. – Режим доступу: http://univd.edu.ua/news_n/?id_doc_n=200&lang=uk.
3. Хахановський В.Г. Теорія і практика криміналістичної інформатики: автореф. дис. … д-ра. юрид. наук: спец. 12.00.09 «Кримінальний процес та криміналістка; судова експертиза; оперативно-розшукова діяльність» / В.Г. Хахановський. – Київ, 2011. – 30 с.
4. Рукавишников Г.А. Об использовании анонимной помощи граждан правоохранительными органами зарубежных государств / Г.А. Рукавишников / Вестник Казанского юридического института МВД России. – 2012. – № 8. – С. 67–70.
5. Прес-Реліз (електронна гаряча лінія www.internetbezpeka.org.ua) [Електронний ресурс]. – Режим доступу: http://gurt.org.ua/uploads/news/2009/11/20/pres-reliz.doc.
6. Мулявка Д.Г. Информационно-аналитическая деятельность налоговой милиции по противодействию налоговой преступности / Д.Г. Мулявка, Т.А. Рекуненко // Криминологический журнал Байкальского государственного университета экономики и права. – 2013. – № 2. – С. 140–145.

Марков В. В. Особенности внедрения зарубежного опыта борьбы с киберпреступностью в учебный процесс

Аннотация. В статье проанализировано состояние и перспективы внедрения зарубежного опыта борьбы с киберпреступностью в учебный процесс ведомственных учебных заведений системы МВД Украины на примере Харьковского национального университета внутренних дел. Раскрыты последние достижения университета в сфере внедрения зарубежного опыта, его взаимодействие с Советом Европы, ОБСЕ, Организацией ICITAP, Ла-Страда и тому подобное. Акцентировано внимание на потребности во внедрении специализированных учебных курсов, программного и аппаратного обеспечения. Обращается внимание на потребности привлечения анонимной помощи граждан для противодействия киберпреступности, а также внедрении опыта США по противодействию детской порнографии. Описан внедренный в Харьковском национальном университете внутренних дел проект, в рамках которого происходит одновременное сочетание курсантами выполнения заданий по охране правопорядка, отработке навыков правоохранителя на специальных учебно-тренировочных полигонах, разработка собственного программного обеспечения.

Ключевые слова: борьба с киберпреступностью, зарубежный опыт, правоохранительные органы, подготовка специалистов.

Markov V. Peculiarities of implementation of foreign cybercrime combating experience into educational process

Summary. The article analyses status and prospects of implementation of foreign cybercrime combating experience into educational process of leading higher educational institutions through example of Kharkiv National University of Internal Affairs. It highlights achievements of University in field of foreign experience implementation, cooperation of the University with the Council of Europe, OSCE, ICITAP, La Strada etc. The article emphasizes importance of introducing new training courses as well as the importance of new soft and hardware. A lot of attention is paid to necessity of citizens' anonymous help in cybercrime combating and implementation of the US experience in child pornography counteraction. The article also describes project implemented in Kharkiv National University of Internal Affairs that allows cadets to combine tasks of enforcing rule of law, developing law enforcement skills in special training areas, using self-developed software.

Key words: cybercrime combating, foreign experience, law enforcement, training experts.