– створити міжвідомчу робочу групу для розроблення та координації спільних заходів протидії комп'ютерній злочинності між правоохоронними органами та операторами зв'язку, інтернет-провайдерами, контент-провайдерами, банківськими,фінансовими установами, державними та громадськими організаціями;

– створити міжвідомчу систему моніторингу оперативної обстановки у сфері інформаційно-телекомунікаційних технологій;

– розробити нормативно-правове забезпечення доступу правоохоронних органів до інформації про протиправні дії при використанні інформаційно-телекомунікаційних технологій;

– розробити та впровадити ефективні механізми реагування на комп'ютерні інциденти.

Одержано 31.10.2018

УДК 65.012.8+004

Олександр Володимирович МАНЖАЙ,
кандидат юридичних наук, доцент,
доцент кафедри кібербезпеки факультету № 4 (кіберполіції)
Харківського національного університету внутрішніх справ;
ORCID: https://orcid.org/0000-0001-5435-5921;
Віолетта Євгенівна ГАЛАУЗ,
слухач магістратури факультету № 6
Харківського національного університету внутрішніх справ

ШЛЯХИ ПІДГОТОВКИ ФАХІВЦІВ У СФЕРІ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

Складна суспільно-політична ситуація в Україні зумовлює потребу в інтенсифікації пошуку якісно нових підходів до підготовки фахівців у сфері протидії кіберзлочинності. Серед іншого потрібно поглибити міжнародне співробітництво за цим напрямом, а також модернізувати систему підготовки відповідних кадрів, підвищивши їх якість, та оптимізувавши витрати на їх підготовку.

Для цього можливі три варіанти дій (оперативний, тактичний та стратегічний). З урахуванням практики підготовки слухачів для підрозділів кіберполіції у 2016-2017 рр. на базі Харківського національного університету внутрішніх справ для усіх трьох варіантів структура курсів обов'язково має включати наступні дисципліни: «Кібербезпека», «Комп'ютерні технології», «Кримінальна розвідка», «Оперативно-технічні засоби і заходи», «Поліцейська діяльність у кіберсфері», «Правові засади захисту інтелектуальної власності», «Цифрова криміналістика». Зміст згаданих дисциплін має варіюватися в залежності від спеціалізації групи, яку готують (див., наприклад, Law Enforcement Training Strategy 2014).

Матеріально-технічна база підготовки спеціалістів має включати не лише мережу спеціалізованих комп'ютерних полігонів, але й низку спеціалізованих апаратно-програмних комплексів. Якісний

викладацький склад має розуміти як технічну, так і юридичну специфіку кіберзлочинності та методик протидії цьому негативному явищу.

Розглянемо описані потенційні плани підготовки фахівців більш докладно.

Оперативний план

Передбачається інтегративна ступенева модель підготовки фахівців. На першому етапі (цей етап вже впроваджується в Україні) здійснюється набір до патрульної поліції. Після визначеного строку роботи в патрульній поліції (наприклад, 1 рік) патрульні, які мають вищу освіту, одержують право пройти додаткові курси (6 місяців) зі спеціалізації «протидія кіберзлочинності» за умови попереднього конкурсного відбору.

Фахівці, які успішно склали іспити за підсумками курсів, мають право зайняти первинні посади у підрозділах кіберполіції.

У наступному кожні 3 роки означені фахівці мають проходити 3-місячні курси підвищення кваліфікації у відповідних установах.

Підготовку має здійснювати один з вищих навчальних закладів МВС України (по аналогії з Південним інститутом поліції у складі Університету м. Луївіль, Кентуккі, США).

Переваги:

– ступенева підготовка дозволяє відібрати найбільш мотивованих фахівців, які мають досвід роботи на первинних посадах поліції;

– скорочений термін підготовки фахівців дозволяє зекономити кошти.

Недоліки:

– швидкий розвиток комп'ютерних технологій передбачає постійну самоосвіту відповідних фахівців. Випадання патрульних з цього процесу на час служби в патрульній поліції не дозволяє говорити про підготовку висококваліфікованих фахівців у сфері високих технологій (у переважній більшості), які зможуть ефективно протидіяти дійсно кваліфікованому кіберзлочинцю;

– не можна впевнено говорити про підготовку ефективного фахівця, якщо він не має знань рівня «кваліфікований користувач» або «професіонал» у сфері комп'ютерної техніки.

Тактичний план

Підготовка фахівців у сфері протидії кіберзлочинності здійснюється через додаткову профільну адоптацію їх знань для роботи в правоохоронних органах. Вказаний план реалізується за допомогою початкової підготовки фахівців з технічною або юридичною освітою, яку вони здобули у цивільних вишах. Курс навчання – 6 місяців. Конкретні дисципліни залежатимуть від одержаних в університеті знань фахівця (юридичні або технічні науки).

Переваги:

– змога одержати кваліфікованого фахівця без додаткових затрат

бюджетних коштів (проте ця перевага нівелюється, якщо студент вчився за державним замовленням);

– скорочений термін підготовки фахівців дозволяє оперативніше змінювати зміст бази знань, яку вони мають набути.

Недоліки:

– підготовка означених фахівців у цивільних вишах викликає низку складнощів, основною з яких є те, що значна частина відповідних нормативних документів та методик протидії кіберзлочинності мають гриф обмеження доступу;

– заробітна платня фахівця відповідної кваліфікації у приватному секторі економіки у декілька разів перевищує аналогічний показник у МВС України, що робить нераціональною підготовку відповідних фахівців.

Стратегічний план

Підготовка фахівців здійснюється на базі вищих навчальних закладів системи МВС України. Термін навчання – 3-4 роки. Таку підготовку потрібно здійснювати на базі технічного напряму підготовки із можливістю на контрактній основі паралельного одержання вищої юридичної освіти. Вказане обумовлене тим, що технічному фахівцю і системним мисленням здебільшого набагато простіше набути юридичні знання, аніж технічно непідготовленому фахівцю у сфері права. Це доведено практикою.

Під час прийняття рішення про підготовку фахівців потрібно враховувати світові тенденції та аналітику. Наприклад, у «Стратегії Великобританії у сфері кібербезпеки» від 12 лютого 2013 року, публікованій Національним аудиторським агентством (National Audit Office) відзначається, що Великобританія гостро відчуває брак спеціалістів у сфері кібербезпеки та необхідність прийняття відповідних рішень вже зараз, оскільки на підготовку кваліфікованих фахівців потрібно декілька років.

Переваги:

– органічне поєднання технічних та юридичних знань, що є важливим для працівника підрозділів кіберполіції;

– систему підготовки можна здійснити на створеній базі вишів системи МВС України, курсант по закінченні вищого навчального закладу МВС України має дотримуватися умов контракту, що стримує його звільнення з Національної поліції України.

Недоліки:

– тривалий час підготовки фахівця;

– затрати на утримання вишів (нівелюється, якщо зважати на те, що держава все одно набирає на навчання громадян за державним замовленням).

Одержано 26.10.2018