

СЕКЦІЯ 4 КАДРОВЕ ЗАБЕЗПЕЧЕННЯ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ ТА ТОРГІВЛІ ЛЮДЬМИ

УДК 65.012.8+004

Вікторія Олександрівна КОВТУН,

курсант 1 курсу навчальної факультету № 4 (кіберполіції)

Харківського національного університету внутрішніх справ

АКТУАЛЬНІ ПИТАННЯ КАДРОВОГО ЗАБЕЗПЕЧЕННЯ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ ТА ТОРГІВЛІ ЛЮДЬМИ

Вступ і постановка проблеми. Корупція як негативне соціальне явище міцно увійшло в життя нашої держави. Володіння адміністративною владою відкриває широкі можливості для зловживання нею, будь то у формі протекціонізму, незаконного придбання різних соціальних благ і різного роду привілеїв, корупції тощо. Це впливає з самої суті адміністративної влади, анонімності, що характеризується, безособовістю, величезним впливом майже у всіх галузях суспільного життя, часто зрощенням з економічною владою, володінням інформацією з найбільш важливих проблем, що стоять перед суспільством, арсеналом примусових засобів. У зв'язку з реформування Міністерства внутрішніх справ України в частині створення Національної поліції України, виникла потреба у забезпеченні новостворених підрозділів (кіберполіції, кримінального аналізу, патрульної та дорожньої поліції тощо) кваліфікованими кадрами шляхом прийняттям на службу цивільних осіб з відповідним фахом або атестації осіб, які працювали в ОВС України.

Під час відбору кадрів необхідно приділяти важливу увагу дослідженню професійної придатності кандидата на службу. Вивчення досвіду розвинутих зарубіжних країн світу свідчить про те, що процедура дослідження професійної придатності поліцейських є досить складним процесом, який включає в себе низку соціально-психологічних методів, у тому числі співбесіду з кандидатом

Сьогодні комп'ютерні та телекомунікаційні технології охопили майже всі сфери життєдіяльності суспільства і держави. Але становлення інформаційного суспільства відбувається не без проблем, найсуттєвішою з яких слід вважати кіберзлочинність. Її спектр різноманітний – від створення комп'ютерних вірусів, вчинення крадіжок, різних видів шахрайства, комп'ютерних підробок до порушення авторських прав та розповсюдження дитячої порнографії. Зазвичай кіберзлочини мають корисливу спрямованість й відрізняються високим рівнем латентності й анонімності.

Відповідно до Закону «Про запобігання корупції», суб'єктами відповідальності за корупційні правопорушення в Україні є: особи,

уповноважені на виконання функцій держави або місцевого самоврядування (у тому числі Президент України, народні депутати, урядовці, судді); посадові особи юридичних осіб публічного права, які одержують заробітну плату за рахунок державного чи місцевого бюджету; особи, які надають публічні послуги (аудитори, нотаріуси, експерти, арбітражні керуючі, третейські судді тощо); посадові особи іноземних держав, міжнародних організацій; посадові особи і працівники юридичних осіб (у разі одержання ними неправомірної вигоди або надання ними такої вигоди особам, зазначеним вище) тощо. Досить широке коло суб'єктів правопорушення вимагає прискіпливого аналізу та контролю за діяльністю правоохоронних органів як в середини держави, так і за її межами.

Таким чином, корупція завжди залишалася однією з найсерйозніших проблем України. Після Революції гідності Україна залишалася найбільш корумпованою країною Європи: за результатами глобального Індексу сприйняття корупції 2016 (Corruption Perceptions Index) країна посідає 131 місце зі 176. Отже, Україна залишається корумпованою державою. Існуючий механізм протидії корупційним проявам в Україні є неефективним

До цього ж, сьогодні жертвами осіб, які вчиняють злочини у віртуальному просторі, можуть стати не лише окремі люди чи юридичні особи, а й цілі відомства і навіть держави. Зареєстровані випадки так званого кібертероризму, коли комп'ютер використовувався для блокування важливих систем життєзабезпечення та створення загрози для цілих груп населення. Для України, як однієї з найбільших європейських держав, де у повсякденне життя стрімко входять нові комунікативні технології, зокрема, ті, що розширюють можливості реалізації товарів і послуг за допомогою мережі Інтернет, проблема кіберзлочинності не обходить жодним чином.

Таким чином, для України проблема поширення кіберзлочинності сьогодні є вельми актуальною й такою, що вимагає невідкладного вирішення. Кіберзлочинність, без перебільшення, стала одним з основних викликів, що постають перед сучасним суспільством. Тому нагальними є питання щодо якісної підготовки фахівців-правоохоронців з протидії кіберзлочинності.

Кіберполіція в Україні є новою правоохоронною службою, професійна діяльність працівників якої є ще недостатньо вивченою в науковому плані. Підготовка працівників кіберполіції здійснюється у відомчих вищах МВС України двома шляхами: перепідготовка фахівців ІТ-сфери з наявною вищою освітою та підготовка курсантів за першим рівнем вищої освіти в умовах специфічного навчального середовища.

Обидва шляхи є перспективними і доцільними, але мають і певні недоліки. Так, щодо ІТ-фахівців, складно прогнозованою є їх професійна надійність, яка ґрунтується в основному на мотивації служіння і пошуку нових вражень, адже вони обрали професію із явно

нижчою оплатою праці, ніж це можливо для кваліфікованого спеціаліста у цивільних фірмах. Стійкість такої мотивації незначна, а отже прогноз стабільності і надійності їх праці – сумнівний. Професійна надійність курсантів ВНЗ МВС, принаймні перші роки після випуску, не викликає сумнівів. Але, їх професійна готовність явно поступається «дорослим» колегам, тобто їх необхідно доучувати вже на робочому місці. Для успіху цього процесу неабияке значення має те, як саме майбутні кіберполіцейські ставляться до важливих об'єктів і явищ соціально-професійного оточення: до громадян, законів, злочинців, своїх прав і обов'язків, врешті решт до себе самих. Ці ставлення, разом з іншими, утворюють цілісну систему ставлень курсанта, яка багато в чому визначає його професійне мислення, готовність до певної поведінки у професійній площині.

Цікавим є те, що у Європейський день протидії торгівлі людьми «Ла Страда-Україна» констатує: проблема залишається актуальною для України. Досі не були прийняті стандарти щодо здійснення послуг у сфері протидії торгівлі людьми, які були розроблені та подані до Міністерства соціальної політики групою експертів – представників державних, неурядових та міжнародних організацій ще в 2010 р.

Курс державної політики та зобов'язання, які взяла на себе Україна у сфері протидії торгівлі людьми, підписавши ряд міжнародних та національних документів, вимагають посилення діяльності у цій сфері, а також зміцнення кадрового потенціалу відповідальних структур. Натомість спостерігається ослаблення державного механізму протидії цьому явищу. Нові функції, які покладаються на Міністерство соціальної політики, зокрема щодо встановлення статусу особи постраждалої від торгівлі людьми, повноваження національного координатора державної політики у цій сфері та інші вимагають серйозного організаційного та кадрового забезпечення як на центральному, так і на обласному рівнях. В той же час згідно міжнародних стандартів, структурний підрозділ, відповідальний за протидію торгівлі людьми, повинен бути максимально високого рівня, що забезпечує можливість ефективно організувати координацію та взаємодію усіх задіяних структур та закладів.

Окрім того, Департамент по боротьбі з кіберзлочинністю і торгівлею людьми Міністерства внутрішніх справ було понижено до Управління боротьби з торгівлею людьми та злочинами проти моральності, а станом на сьогодні розслідування злочинів, пов'язаних з торгівлею людьми знаходиться у компетенції одного відділу у складі департаменту карного розшуку. На практиці всі ці зміни призводять до труднощів у роботі по боротьбі із злочинами, відволіканням працівників на іншу діяльність, як це було раніше.

Висновок. Резюмуючи все вище сказане, та з метою підвищення якості протидії комп'ютерній злочинності, необхідно також провести наступні організаційні заходи:

- 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