

лить вже у поточному 2017 році впровадити технологію FIND в Національній поліції і надавати доступ до комунікаційної системи Інтерполу всім підрозділам поліції, що мають потребу використовувати банки даних Інтерполу у повсякденній роботі.

У зв'язку із цим відзначаємо неабияку актуальність питання щодо навчання поліцейських-практиків роботі з інформаційними ресурсами Інтерполу, що у свою чергу, на наш погляд, вимагає уваги і з боку навчальних закладів, які здійснюють підготовку відповідних фахівців.

Одержано 31.10.2017

УДК 343.9 : 004 : 343.3/7

Олександр Сергійович ПИРОЖЕНКО,

кандидат юридичних наук, доцент, професор кафедри соціально-економічних дисциплін Комунального закладу «Харківська гуманітарно-педагогічна академія» Харківської обласної ради, адвокат

ДО ПИТАННЯ ПРО НАПЯМИ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

На сучасному етапі розвитку людської цивілізації інформаційна сфера є системоутворюючим фактором життя суспільства, безпосереднім чинником економічного зростання. Розвиток інформаційних та телекомунікаційних технологій сприяє розширенню можливостей управління різними процесами, що впливає на забезпечення соціально-економічної стабільності й обороноздатності країни.

Комплексне і широкомасштабне використання персональних комп'ютерів, інформаційно-обчислювальних мереж і комп'ютеризованих комунікаційних систем призвело до появи нового стратегічно важливого ресурсу, що потребує всебічної охорони, – інформації. У зв'язку з цим інформаційна безпека є однією зі складових національної безпеки держави.

Одним із негативних наслідків науково-технічного прогресу безумовно стало виникнення нових видів суспільно небезпечних діянь – «кіберзлочинів», які проявляються у багатьох сферах життєдіяльності людини (від викрадення коштів з банківського рахунку потерпілого до отримання контролю над транспортним засобом чи повітряним судном).

У науковій юридичній літературі справедливо відмічається, що основною проблемою боротьби зі злочинністю в мережі Інтернет є транснаціональність самої мережі і відсутність механізмів контролю. Відтак, світова спільнота перебуває у пос-

тійному пошуку дієвих способів та засобів протидії кіберзлочинності, іноді нехтуючи природними правами і свободами конкретної людини з метою «забезпечення загального блага».

Відмітимо, що функції з протидії кіберзлочинам покладають на поліцію, органи державної безпеки, спеціальні служби захисту інформації тощо. При цьому нерідко створюються спеціальні підрозділи, головним завданням яких є:

- моніторинг кіберпростору з метою виявлення кіберзлочинів, вірусів або шкідливого програмного забезпечення;

- здійснення оперативно-розшукових та розвідувальних заходів з метою фіксування протиправної діяльності кіберзлочинців;

- розслідування кіберзлочинів, надання методичної та практичної допомоги іншим галузевим службам і правоохоронним органам у межах своєї компетенції;

- накопичення, узагальнення та аналіз інформації про кіберзлочинність;

- профілактику кіберзлочинів за допомогою громадськості та засобів масової інформації тощо [1, с. 109].

Ефективність виконання згаданими вище органами завдань у сфері інформаційної безпеки істотно залежить від якості підготовки персоналу. В цьому вагоме слово повинні промовляти заклади із специфічними умовами навчання, які здійснюють підготовку фахівців по боротьбі з кіберзлочинністю. Погоджуючись з колегами з Національної академії прокуратури України слід відмітити, що, окрім підготовки поліцейських, важливою складовою у протидії злочинам, що вчинюються з використанням інформаційних та інформаційно-телекомунікаційних технологій, є відповідна підготовка прокурорів (державних обвинувачів) та суддів [2].

Важливим елементом у системі заходів боротьби з кіберзлочинністю є створення захищеної інформаційної інфраструктури. Своєчасне удосконалення комплексів програмно-технічних засобів, організаційних систем та нормативних баз забезпечить швидку організацію взаємодії інформаційних потоків, якісне функціонування та всебічний розвиток засобів інформаційної взаємодії та інформаційного простору. Цікавим прикладом такої взаємодії є проект протидії кіберзлочинності, що з 2013 року реалізовується спільними зусиллями Національної асоціації банків України, Національного банку України, Департаменту кіберполіції та банками-членами НАБУ. Головна мета проекту – створення Єдиної інформаційної бази банків

для запобігання кібершахрайству на загальнодержавному рівні [3].

Досягнення позитивних результатів у сфері протидії кіберзлочинності є абсолютно неможливим без відповідної профілактичної роботи серед населення та інформування суспільства про нові види кіберзагроз. При цьому вказані функції повинні реалізовуватися не тільки правоохоронними органами, а й громадськими організаціями масштабу Transparency International, Greenpeace, Amnesty International тощо.

Наостанок відмітимо, що кіберзлочинність – проблема ХХІ століття, яка невпинно зростає та поглинає все більше фінансових ресурсів. Незважаючи на заходи, що вживаються окремими особами, як фізичними, так і юридичними, державою, це явище продовжує існувати та розширює масштаби своєї діяльності, збільшуючи прибутки правопорушників. Тому на сьогодні особливо важливим питанням є усвідомлення глибини даної проблеми, прогнозування подальших напрямів її розвитку та дія на випередження.

Список використаних джерел:

1. Марков В. В. До питання щодо зарубіжного досвіду протидії кіберзлочинності. *Право і безпека*. 2015. № 2. С. 107-113.
2. До питання протидії кіберзлочинності в Україні. URL: http://www.akademia.gp.gov.ua/userfiles/file/Academia2016/Akt_schema/123441234524.pdf. (дата звернення: 28.10.2017).
3. Протидія кіберзлочинності. URL: <https://nabu.ua/ua/protidiya-kiberzlochinnosti.html> (дата звернення: 28.10.2017).

Одержано 30.10.2017

УДК 342.98

Віктор Миколайович ПЛЕТЕНЕЦЬ,

кандидат юридичних наук, доцент кафедри криміналістики, судової медицини та психіатрії факультету підготовки фахівців для органів досудового розслідування Дніпропетровського державного університету внутрішніх справ

Катерина Вікторівна КАРАБУТА,

курсант КМ-443 факультету підготовки фахівців для підрозділів кримінальної поліції Дніпропетровського державного університету внутрішніх справ

**ШАХРАЙСТВО У КІБЕРПРОСТОРІ:
ОКРЕМІ АСПЕКТИ ПРОТИДІЇ**

На сучасному етапі розвитку інформаційних технологій шахрайство посідає особливе місце. Це пов'язано з тим, що з