УДК 341:[343.346.8:004]

Роман Русланович ОРЛОВ,
курсант 2 курсу факультету № 4
Харківського національного університету внутрішніх справ

Юрій Миколайович ОНИЩЕНКО,
кандидат наук з державного управління, доцент,
доцент кафедри інформаційних технологій та кібербезпеки факультету
№ 4 Харківського національного університету внутрішніх справ

БОРОТЬБА З КІБЕРЗЛОЧИННІСТЮ НА МІЖНАРОДНОМУ РІВНІ

Дослідники, що займаються проблемою кіберзлочинності, пропонують різні класифікації кіберзлочинів. Кіберзлочини поділяють на види залежно від об'єкта і предмета посягання. Найпоширеніший варіант – це розподіл на комп'ютерні злочини і злочини, що здійснюються за допомогою комп'ютерів, комп'ютерних мереж та інших пристроїв доступу до кіберпростору. Цю класифікацію використовує Організація Об'єднаних Націй, поділяючи цей вид злочинної діяльності на кіберзлочини в «широкому» та «вузькому» розумінні. В даному контексті комп'ютерні злочини – це злочини, основним об'єктом посягання яких є конфіденційність, цілісність, доступність і безпечне функціонування комп'ютерних даних і систем. Решта кіберзлочинів, крім комп'ютерних систем, зазіхають на інші об'єкти (в якості основних): безпека суспільства і людини (кібертероризм), майно та майнові права (крадіжки, шахрайства, скоєні за допомогою комп'ютерних систем або в кіберпросторі), авторські права (плагіат і піратство).

Що стосується джерел кіберзлочинів, то фахівці поділяють осіб і організації, які здійснюють атаки, на кілька категорій. Однак, між цими категоріями не існує досить чітких меж. Наприклад, багато експертів говорять про можливість залучення в терористичні дії хакерів-одинаків і груп хакерів, які не мають уявлення про те, до якого результату можуть призвести їхні дії. Отже, розподіл на групи можна вважати умовним.

З упевненістю можна сказати, що всі провідні міжнародні організації визнають небезпеку кіберзлочинності та її транскордонний характер, обмеженість одностороннього підходу до вирішення цієї проблеми і

необхідність міжнародного співробітництва, як в прийнятті необхідних технічних заходів, так і у виробленні міжнародного законодавства. ОЕСР, Рада Європи, Європейський союз, ООН і Інтерпол – всі ці організації відіграють важливу роль в координації міжнародних зусиль, побудові міжнародної співпраці в боротьбі зі злочинами в сфері високих технологій.

Проблема кіберзлочинності та кібертероризму є відносно новою для міжнародної спільноти. Саме тому на даному етапі будь-які серйозні висновки про її стан і подальші перспективи зробити досить складно. Зрозумілим є те, що дане явище, яке виникло лише кілька десятиліть тому, охоплює все нові сфери діяльності, зростає швидкими темпами і вимагає прийняття адекватних і своєчасних заходів реагування, як на національному, так і на міжнародному рівні. Якщо проводити оцінку заходів, які були вжиті світовою спільнотою для боротьби з кіберзлочинністю, починаючи з середини 80-х рр. минулого століття, то можна з упевненістю сказати, що на сьогоднішній день ми маємо досить міцну для подальших кроків опору.

Фундаментом міжнародної співпраці у сфері боротьби з кіберзлочинністю є ратифікована Україною у 2005 році Конвенція про кіберзлочинність. Так, на виконання вимог статті 35 Будапештської Конвенції в Україні створено сектор національного контактного пункту реагування на кіберзлочини, що є структурним підрозділом Департаменту кіберполіції Національної поліції України. Сектор є підрозділом для здійснення контактів цілодобово впродовж тижня з метою надання негайної допомоги для розслідування або переслідування стосовно кримінальних правопорушень, пов'язаних з комп'ютерними системами і даними, або з метою збирання доказів у електронній формі, що стосуються кримінального правопорушення.

Україна, як активний учасник боротьби з кіберзлочинністю бере участь у:

- проведенні спільних навчань суб'єктів сектору безпеки і оборони в рамках заходів колективної оборони;
- проектах Європейського Союзу та НАТО з метою посилення спроможності України у сфері кібербезпеки;
- заходах із зміцнення довіри при використанні кіберпростору, що проводяться під егідою Організації з безпеки і співробітництва в Європі;

– у спільних проектах Ради Європи і Європейського Союзу щодо підвищення обізнаності і навчання співробітників правоохоронних органів у сфері кібербезпеки.

Отже, результативна міжнародна співпраця в боротьбі зі злочинністю у сфері використання комп'ютерних технологій можлива за умови подальшого удосконалення правового, організаційного і наукового забезпечення.

Одержано 09.05.2020