

заохочення позаштатних негласних працівників за надану інформацію, яка сприяла б виявленню, попередженню та розслідуванню злочинів, зокрема грабежів і розбоїв.

4) якісно підвищити рівень взаємодії у системі Національної поліції, щодо протидії грабежам та розбоям не тільки зі слідчими, але й дільничними інспекторами та патрульною поліцією.

Підсумовуючи викладене, зазначимо, що з урахуванням різкого загострення проблеми вчинення корисливо-насильницьких злочинів та безпосередньо грабежів та розбоїв, як найбільш тяжких з них необхідно постійно шукати нові підходи до вирішення даної проблеми, а починати це необхідно в першу чергу з підвищення якості підбору та підготовки працівників Національної поліції. Це, в свою чергу, зумовлює необхідність проведення комплексних досліджень у зазначеній сфері.

Одержано 11.11.2016

УДК 343

Ганна Михайлівна ШОРОХОВА,

*науковий співробітник науково-дослідної
лабораторії з проблем протидії злочинності*

Харківського національного університету внутрішніх справ

ДЕЯКІ ПИТАННЯ ПРАВОВОГО ТА ОРГАНІЗАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

Ми живемо в епоху інформаційного суспільства, коли комп'ютерні та телекомунікаційні технології охопили майже всі сфери життєдіяльності суспільства і держави. Але розвиток інформаційних технологій, поширення сфери використання глобальної комп'ютерної мережі Інтернет зумовили використання новітніх технологій у злочинних цілях.

На сьогодні комп'ютерні злочини – це одна з найдинамічніших груп суспільно небезпечних посягань. Швидко збільшуються показники поширення цих злочинів, а також постійно зростає їх суспільна небезпека. Це зумовлене прискореним розвитком науки й технологій у сфері комп'ютеризації, а також постійним розширенням сфери застосування комп'ютерних технологій.

Стрімкий розвиток інформаційних технологій викликали появу нових умов, які використовуються злочинцями для скоєння злочинів на національному, міжнародному і транснаціональному рівнях.

Розповсюдження комп'ютерних вірусів, шахрайства з пластиковими платіжними картками, крадіжки коштів з банківських рахунків,

викрадення комп'ютерної інформації та порушення правил експлуатації автоматизованих електронно-обчислювальних систем – це далеко не повний перелік подібних злочинів. Дану категорію злочинів називають по-різному: кіберзлочини, комп'ютерні злочини, злочини в сфері комп'ютерних технологій, злочини в сфері комп'ютерної інформації.

Кіберзлочинність – це злочинність у так званому «віртуальному просторі». Віртуальний простір можна визначити як простір, що моделюється за допомогою комп'ютера інформаційний, у якому перебувають відомості про особи, предмети, факти, подіях, явищах і процесах, представлені в математичному, символічному або будь-якому іншому виді й рухи, що перебувають у процесі, по локальних і глобальних комп'ютерних мережах, або відомості, що зберігаються в пам'яті будь-якого фізичного або віртуального устрою, а також іншого носія, спеціально призначеного для їхнього зберігання, обробки й передачі.

Кіберзлочинність, без перебільшення, стала одним з основних викликів, що постають перед сучасним суспільством. Тому не випадково в МВС України з 15 жовтня 2015 року здійснюються організаційно-штатні заходи щодо формування нового підрозділу – Департаменту кіберполіції, який повинен ефективно протидіяти поширенню кіберзлочинності в Україні.

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. 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. Адже Україна входить до десятки країн із найвищим рівнем поширення цього виду криміналу, а це дитяча порнографія, шахрайства, численні порушення авторських і суміжних прав із використанням комп'ютерних систем, несанкціоноване втручання в роботу комп'ютерних та телекомунікаційних мереж, виготовлення та розповсюдження шкідливих програм, викрадення ідентифікаційних даних осіб, електронне вимагання, що в переважній більшості носять транснаціональний організований характер тощо.

Щодня жертвами кіберзлочинності стають близько мільйона людей по всьому світу. Щороку жертви кіберзлочинів зазнають збитків на суму понад 290 мільярдів євро. При цьому велика кількість інтернет-злочинців залишається непокараною.

Через це боротьбу проти інтернет-злочинців потрібно вести на загальноєвропейському рівні. Саме з цією метою створено Європейський центр боротьби із кіберзлочинністю, який запрацював на початку 2013 року. Він є частиною Європолу – поліційної служби Євросоюзу – зі штаб-квартирою в Гаазі, Нідерланди. Фінансується Центр з бюджету Європолу.

Беручи до уваги значні обсяги збитків, кожна країна-член Євросоюзу намагається якимось боротися проти кіберзлочинності. Для протистояння кібершахраям в світі створюються спеціальні підрозділи і структури. Їхні повноваження постійно розширюються, а технічні можливості посилюються. Проте, поле діяльності правоохоронців кожної країни обмежене національними кордонами, тоді як всесвітня мережа кордонів не знає.

На даний момент нагально необхідним є створення єдиного ефективного міжнародного механізму протидії цьому виду злочинності. Потрібно вдосконалити систему взаємозв'язку та взаємодії правоохоронних органів України з правоохоронними органами інших держав, для вирішення проблем, які виникають на практиці при розслідуванні та попередженні кіберзлочинності. Важливим кроком – є залучення до цього процесу відповідних фахівців у сфері інформаційних технологій, наприклад, залучати професійних хакерів до підрозділів по розслідуванню кіберзлочинів для реалізації своїх функцій. Також потрібна підготовка висококваліфікованих працівників для національних підрозділів по боротьбі з кіберзлочинністю, а саме підготовка ІТ-спеціалістів широкого профілю – інженер-програмістів, системних адміністраторів, спеціалістів служб технічної підтримки, аналітиків комп'ютерного банку, аналітиків з комп'ютерних систем тощо.

Враховуючи ту обставину, що сучасні технології розвиваються швидше, ніж норми, які регулюють їх застосування, необхідно постійно знаходити шляхи вирішення нових задач, частіше пов'язаних із такими сферами, як захист даних, трансграничний доступ правоохоронних органів до даних і обмін інформацією між державними і приватними структурами. Успішне вирішення цієї проблеми залежить від якісного рівня правової основи співпраці, що потребує постійного моніторингу існуючої нормативної бази, постійного оновлення та доповнення, розробки нових стандартів у цій сфері. Особливе місце в процесі боротьби з кіберзлочинністю відіграє прийнята у 2001 році Радою Європи «Конвенція про кіберзлочинність», яка стала підґрунтям для уніфікації національного законодавства. Україна у 2005 році ратифікувала Конвенцію про кіберзлочинність, проте нормативно-правова основа боротьби зі злочинами у цій сфері

й дотепер залишається недосконалою. Зокрема в законодавстві досі залишаються невизначеними такі терміни як кіберзлочин, кіберзлочинність, кібератака, комп'ютерний тероризм. Таким чином, можна стверджувати, що здебільшого вітчизняне нормативно-правове поле у сфері кібербезпеки оперує термінами та поняттями, визначень яких фактично немає, або вони не узгоджені між різними нормативно-правовими актами.

Це говорить про те, що процес гармонізації українського та міжнародного законодавства ще не завершений та вітчизняна нормативно-правова база має бути вдосконалена. Насамперед, потрібно усунути прогалини та певні протиріччя в законодавстві України, чого можна досягти шляхом кодифікації законодавства у сфері боротьби з кіберзлочинністю з подальшою розробкою та ухваленням Інформаційного кодексу України.

Отже, підсумовуючи, можна сказати, що вітчизняні реалії протидії кіберзлочинності свідчать про низку важливих проблем, які заважають створенню ефективної системи протидії загрозам у кіберпросторі. До таких проблем належать передусім: термінологічна невизначеність, відсутність належної координації діяльності відповідних відомств, залежність України від програмних і технічних продуктів іноземного виробництва, складнощі з кадровим наповненням відповідних структурних підрозділів та міжнародне співробітництво України у боротьбі з кіберзлочинністю.

Одержано 12.10.2016