Гвоздецька М.О., Ісмайлов К.Ю.
Одеський державний університет внутрішніх справ

Кримінологічна характеристика кіберзлочинності: сучасний стан, структура та специфіка вчинення

Активне застосування комп'ютерних технологій у всіх значимих сферах життя суспільства є невід'ємною характеристикою сучасного миру. В даний час цей вектор розвитку суспільного життя об'єктивно обумовлює і суттєве зростання кількості скоєних злочинів з використанням комп'ютерних технологій.

Суспільна небезпека злочинів у сфері комп'ютерної інформації полягає в тому, що неправомірний доступ або зміна комп'ютерної інформації може порушувати діяльність різних систем забезпечення держави: оборони, енергетики, транспорту та спричинити не тільки матеріальний збиток, але і людські жертви [1, с. 109].

Крім того, на сьогодні Україна знаходиться в стані інформаційної війни з Російською Федерацією, що потребує збільшення уваги до цієї категорії правопорушень, як зі сторони керівництва держави, правоохоронних органів, так і науковців. Так, на думку народного депутата України і радника глави МВС Антона Геращенко, тактикою Росії щодо дестабілізації ситуації в Україні є розвал України з середини через фінансування різного роду інформаційних видань, через створення атмосфери істерії, через створення невіри в те, що Україна може стати повноцінною державою та членом ЄС [2].

Не викликає сумнівів та обставина, що злочини, що здійснюються з використанням сучасних комп'ютерних технологій, мають істотну специфіку. Застосування технічних новинок для вчинення протиправних дій дозволяє злочинцям зазіхати на найбільш важливі охоронювані законом суспільні відносини в сфері прав та інтересів особистості, суспільства і безпеки держави.

Складність виявлення дій комп'ютерного злочинця полягає в його можливості скоювати злочини в кіберпросторі, у якого не має державних кордонів, що багаторазово збільшують ступінь її суспільної небезпеки.

Вважається, що часом вчинення злочину в сфері комп'ютерної інформації слід визнавати момент натискання керуючої клавіші комп'ютера, запуску кінцеву команду. При цьому не має істотного значення, через який проміжок часу настали передбачені небезпечні наслідки. Розділяє наслідки і діяння проміжок часу може бути мінімальним і складати кілька хвилин, витрачених комп'ютером на аналіз, прийняття і виконання завантаженої команди. Навпаки, за певних умов цей часовий проміжок може бути досить тривалим, оскільки, наприклад, у деякі шкідливі програми спочатку вноситься умова, при якому вони починають функціонувати не відразу, а через певний проміжок часу. Шкідливий код може почати руйнівну дію тільки після здійснення користувачем деяких маніпуляцій, наприклад, після запуску певної програми, або після закінчення деякого проміжку часу після роботи з програмою.

Тобто, кіберзлочини мають особливу кримінальну особливість у визначенні сукупності та повторності скоєння противоправних діянь.

Набагато складніше визначити місце вчинення комп'ютерного злочину. Більшість злочинів у сфері комп'ютерної інформації відбувається в комп'ютерних мережах. Це передбачає, що місце вчинення протиправного діяння і місце настання суспільно небезпечних наслідків можуть відділятися один від одного багатьма кілометрами і навіть перебувати на території різних держав [3, с. 14].

Суттєвим недоліком сучасного українського законодавства, який необхідно усунути якнайшвидше, є відсутність нормативного закріплення таких понять, як «злочин, що здійснюється з використанням комп'ютерних технологій», «комп'ютерні технології», «використання комп'ютерних технологій» та інші. Закріплені в чинному українському кримінальному законодавстві склади, які регламентують відповідальність за використання комп'ютерних технологій при вчиненні злочинів, не в усьому відповідають вимогам, що пред'являються міжнародним співтовариством для уніфікації на міжнародному рівні, зокрема, Конвенції Ради Європи «Про кіберзлочинність» [4].

Все це означає, що Україна зіткнеться з ситуацією, в якій значне зростання і повсюдне впровадження в усі аспекти життя суспільства сучасних комп'ютерних технологій, призведе до збільшення кількості комп'ютерної злочинності, на що правоохоронні органи зможуть адекватно відреагувати лише за умови належного правового та фінансового забезпечення своєї діяльності з протидії злочинності даного виду. Крім того, державі необхідно приділити увагу сучасній підготовці у вищих навчальних закладах фахівців з юриспруденції, спеціалістів з громадських зв'язків та зв'язків з засобами масової інформації, майбутніх представників журналістського корпусу, а також спеціалістів із захисту інформації [5, с. 215].

Отже, можна зробити висновок, що використання комп'ютерних технологій при скоєнні злочинів є особливим різновидом суспільно-небезпечної та протиправної діяльності, яка у даний час одержує усе більше поширення як у глобальному масштабі, так і в окремих країнах, в тому числі і в Україні.

Даному виду злочинів притаманні риси, що пояснюють зростання стрімкими темпами «популярність» в кримінальному середовищі: високий рівень латентності, пояснюється як всебічною комп'ютеризацією суспільному й особистому житті, так і транскордонним характером злочинної діяльності і пов'язаної з цим невловимістю комп'ютерних злочинців, а також порівняльна простота вчинення злочинів. Динамічність поширення комп'ютерних технологій та їх метаморфози зобов'язує законодавця і правоохоронні органи, що протидіють комп'ютерної злочинності, збільшувати швидкість реакції на появу нових способів протиправної діяльності з використанням комп'ютерних технологій. Найкращим способом протидії високотехнологічної злочинності, на мою думку, можна вважати реалізацію випереджаючого правового регулювання. Також слід додати, що відсутність єдиної міжнародної нормативної правової бази, істотні відмінності в національних законодавствах країн, об'єднаних ідеєю спільної боротьби з комп'ютерною злочинністю, та відсутність єдиного підходу до визначення понятійного апарату розглянутої сукупності суспільно небезпечних діянь суттєво ускладнюють ефективну протидію використанню комп'ютерних технологій при здійсненні злочинів.

На завершення хочеться додати, що існує нагальна, продиктована часом необхідність виділення злочинів, які вчиняються з використанням комп'ютерних технологій, в якості окремої групи протиправних діянь у кримінальному законі, адже потреба в цьому обумовлюється як зростаючою ступенем суспільної небезпеки діянь, так і особливостями їх об'єкта.

Список використаних джерел

1. *Старичков М.В. Умышленные преступления в сфере компьютерной информации: уголовно-правовая и криминологическая характеристики: дис. ... канд. юрид. наук: 12.00.08 . - Иркутск, 2008. - С. 269.*
2. *Геращенко пояснив, як Путін чинитиме з Україною [Електронний ресурс]: Режим доступу: http://gazeta.ua/articles/politics/_geraschenko-poyasniv-yak-putin-chinitime-z-ukrayinoyu/728866 .*
3. *Рассолов И.М. Киберпреступность: понятие, основные черты, формы проявления / И.М. Рассолов // Юридический мир. - 2008. - № 2. – 152 с.*
4. *Конвенція Ради Європи «Про кіберзлочинність» [Електронний ресурс]: Режим доступу: http://zakon2.rada.gov.ua/laws/show/994_575 .*
5. *Ісмайлов К.Ю. Прорахунки в інформаційно-правовій підготовці фахівців / К.Ю. Ісмайлов // Роль та місце правоохоронних органів у розбудові демократичної правової: Матеріали VIII Міжнародної науково-практичної конференції (м. Одеса, 25 березня 2016 р.). – Одеса: Одеський державний університет внутрішніх справ, 2016. – С. 215-216.*