УДК 681.518

Бармін П.Є., Резніченко В.А.
Кіровоградський національний технічний університет

Становище кіберзлочинності в Україні

«Кіберзлочинність», «хакери», «комп'ютерний злом», «крадіжка машинного часу» - ці терміни вже перестали бути екзотикою для юристів. Проблеми протидії злочинам у сфері використання комп'ютерної техніки активно обговорюється науковцями, досить швидко розвивається практика застосування відповідних норм законодавства про кримінальну відповідальність.

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. В літературі найчастіше зустрічаються два терміни: кіберзлочини та комп'ютерні злочини. Оскільки вони використовуються для назви одних і тих самих суспільно-небезпечних діянь, то їх можна вважати синонімами та рівнозначними. У зв'язку з ратифікацією Україною Конвенції про кіберзлочинність 7 вересня 2005 року вважається за доцільне вживати термін кіберзлочини. Поняття "кіберзлочин" молоде і утворено сполученням двох слів: кібер і злочин. Термін "кібер" має на увазі поняття кіберпростору (у літературі частіше зустрічаються терміни "віртуальний простір", "віртуальний світ") та інформаційний простір, що моделюється за допомогою комп'ютера. Тобто кіберзлочини – це суспільно-небезпечні діяння, які так чи інакше пов'язані з кіберпростором та комп'ютерною інформацією, що моделюється комп'ютерами. Такі злочини характеризуються наступними особливостями: високою латентністю, складністю їх виявлення та розслідування, складністю доказу в суді подібних справ, транснаціональною складовою в основному з використанням інформаційної мережі Інтернет, високим збитком навіть від одиничного злочину.

Аналізуючи українські статистичні дані можна зробити висновок про те, що збиток, який завдає кіберзлочинність, сьогодні значно перевищує розмір збитків від традиційних видів злочинів. Кількість протиправних посягань на інформаційні ресурси держави зростає. Враховуючи щоденне збільшення обсягів інформації, що обробляється державними структурами, виникає необхідність їх захисту від протизаконних дій. В кінці минулого року в представленому PricewaterhouseCoopers огляді економічних злочинів значилося, що кіберзлочинність стала одним із п'яти найпоширеніших економічних злочинів в Україні, а збитки від онлайн-злочинів і махінацій на сьогодні

вже перевищили збитки від традиційних форм злочинності в Україні.

Сьогодні в Україні близько 18 млн. громадян є постійними користувачами мережі Інтернет. З кожним роком злочинів в інтернеті збільшується приблизно на 25-30%, але разом з тим збільшуються і можливості держави. В Україні вже були прецеденти, коли групи хакерів зупиняли діяльність сайтів держави і намагалися зламати бази даних. Тому влада вже сьогодні повинна подбати про кібербезпеку.

За даними спецслужб, за останній рік українські хакери вкрали з кредитних карт у всьому світі близько сотні мільйонів доларів. За кількістю спроб зараження комп'ютерними вірусами Україна випереджає країни не тільки Східної та Західної Європи, а також Центральної Азії і США, як показало дослідження «Лабораторії Касперського». Можна стверджувати, що 2011 рік ознаменував для України епоху розквіту професійного хакерства.

Українською проблемою є як недостатня кількість державних експертів в області комп'ютерно-технічної експертизи, так і складності з введенням в правове поле досліджень фахівців комерційних організацій. Середній термін проведення комп'ютерно-технічних експертиз становить від півроку і вище через високу завантаженість профільних державних установ. Для проведення розслідування таких злочинів необхідні кваліфіковані фахівці, що володіють не тільки технічними навичками, але й знаннями в галузі права.

На засіданні Ради міністрів закордонних справ ОБСЄ, глава українського МЗС Костянтин Грищенко пообіцяв, що Україна буде більш ефективно боротися з кіберзлочинністю в країні. «Україна приділятиме значну увагу консолідації зусиль ОБСЄ в боротьбі з сучасними викликами і загрозами безпеці, такими як тероризм, торгівля людьми, кіберзлочинність, організована транскордонна злочинність».

Боротися з подібними проблемами можна за допомогою інтеграційного підходу. Тому уряди багатьох країн йдуть сьогодні шляхом створення на державному рівні комплексних систем інформаційної безпеки шляхом об'єднання зусиль державних органів, представників бізнес-співтовариств і громадських організацій.

Таким чином, стрімкий розвиток інформаційних технологій є причиною прогресу кіберзлочинності. Вже сьогодні шкода, завдана віртуальними злочинцями в Україні, оцінюється в десятки мільйонів гривень. Країна прагне до світового лідерства за кількістю кіберзагроз. Міжнародні експерти відзначають, що в цьому році атаки кіберзлочинців стануть агресивнішими і будуть проводитися не тільки з метою заробітку або шпигунства, але і з метою демонстрації сили. Крім того, збільшиться кількість загроз для користувачів мобільних технологій.

Список використаних джерел

1. *Кіберзлочинність можна зупинити тільки разом.- Україна: бізнес-ревю №5-6 від 11.02.2013.*
2. *Комп'ютерна злочинність. – К.: Атіка, 2002.*
3. *Кримінальний кодекс України – К.: Атіка, 2006.*