світове співтовариство в цілому, і кожна держава окремо, створить для захисту міжнародних і національних інтересів.

Кузьменко Б.В., професор кафедри комп'ютерно-інтегрованих технологій Міжрегіональної академії управління персоналом, доктор технічних наук, професор;
Заіка Ю. О.,
начальник кафедри цивільного права і процесу НАВС, д.ю.н., професор

СУЧАСНИЙ СТАН КРИМІНАЛЬНОЇ ЗЛОЧИННОСТІ В ГАЛУЗІ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В УКРАЇНІ

Комп'ютерний геній і лиходійство прогнозовано виявилися цілком сумісними, класичний арсенал злочинного світу виявився затребуваним і у сучасному кіберпросторі. Зламування, крадіжки, здирництво, шантаж, психологічне насильство, «кримінальні» можливості сьогоднішнього Інтернету вже сьогодні «оцінені» українськими і міжнародними терористичними організаціями. Паролі, явки, конспіративні зустрічі членів терористичних та радикальних угрупувань успішно перемістилися у віртуальний світ, спантеличили спецслужби практично всього цивілізованого світу. Специфіка комп'ютерних злочинів робить їх важкорозкриваними, вони: вчиняються в одну мить, високолатентні; добувати докази надзвичайно складно, робити це слід по гарячих слідах, те, що може бути доказом, недовго зберігається в реєстраційних системах. Сучасні інформаційні технології дають можливість злочинцям, терористам швидко і ефективно об'єднуватися в угрупування, залишатися непоміченими, здійснювати атаки на елементи національних інфраструктур. Перехід зловмисників на віртуальне становище потребує надзвичайно потужних наукоємних методів протидії, з десятками і сотнями кроків на випередження. Інтернет затягнув у

свої тенета десятки і сотні мільйонів користувачів нечуваними масштабами свободи, безвізовим подоланням кордонів, відсутністю цензури, довільним ступенем анонімності. Просунутий хакер залишає обмаль слідів, його вирахувати вкрай складно, часто неможливо.

Кримінальну відповідальність за комп'ютерні злочини в Україні запроваджено 1994 року, кількість таких правопорушень щорічно зростає на чверть, Кримінальний Кодекс України (ККУ) постійно поповнюється новими статтями, у 2001 році Україна приєдналася до Конвенції про кіберзлочинність, у 2006 році ратифіковано Додатковий протокол до цього документу. Рівень інформатизації українського суспільства залишається не найвищому рівні, але вітчизняні хакери добре набили руку на діях, які підпадають під статтю ККУ з «Несанкціонованого втручання в роботу комп'ютерних систем», 2007 року СБУ розслідувала 150 відповідних кримінальних справ, засуджено 36 осіб. В Україні в рамках адаптації нормативної бази до міжнародних стандартів слід збалансувати права і обов'язки операторів і провайдерів телекомунікацій. Особливий інтерес для України, в контексті виборів до ВРУ, становить досвід захисту баз даних від стороннього втручання. Важливе значення для організації захисту інформації в Україні має вирішення проблем в аспектах організаційно-технічному, а також організаційно-правовому та організаційно-управлінському. У контексті проблематики слід звернути увагу на стан .правового регулювання питань організації захисту інформації, який в Україні зумовлюється такими чинниками: а) складність системи правового регулювання в інформаційній сфері, зокрема у сфері захисту таємниць (крім державної), конфіденційної інформації та відкритої інформації, важливої для особи, суспільства та держави; б) недостатність наукового забезпечення розробки нормативно-правових актів і нормативних документів з питань проведення досліджень, розроблення та виробництва засобів забезпечення організації захисту інформації; в) недосконалість організації системи сертифікації інженерно-технічних, у тому числі програмно-

математичних засобів захисту інформації; г) недосконаліть системи атестації на відповідність вимогам технічного захисту інформації державних об'єктів, робота яких пов'язана з інформацією, що підлягає захисту; д) недостатня узгодженість чинних в Україні нормативно-правових актів та нормативних документів з питань технічного захисту інформації з відповідними міжнародними договорами України, у тому числі щодо боротьби з комп'ютерною злочинністю.

Опалинський Ю.В., начальник ННІЗН НАВС, к.ю.н., доцент

ПРАВОВИЙ РЕЖИМ ІНФОРМАЦІЇ, ЯКА МІСТИТЬ БАНКІВСЬКУ ТАЄМНИЦЮ: ПІДСТАВИ ТА ПРАВИЛА ЇЇ РОЗКРИТТЯ, ВИЗНАЧЕНІ ЗАКОНОДАВСТВОМ

Аналіз чинного законодавства дає підстави дійти висновку, що банківська таємниця належить до такого виду інформації з обмеженим доступом, як таємна інформація або виступає різновидом комерційної таємниці.

Згідно зі ст. 1076 ЦКУ банк гарантує таємницю банківського рахунка, операцій за рахунком і відомостей про клієнта. Відомості про операції та рахунки можуть бути надані тільки самим клієнтам або їхнім представникам. Іншим особам, у тому числі органам державної влади, їхнім посадовим і службовим особам, такі відомості можуть бути надані виключно у випадках та в порядку, встановлених Законом України «Про банки і банківську діяльність» (далі-Закону), в якому питанням банківської таємниці та конфіденційності інформації присвячена гл. 10.

Зокрема, у ст. 60 цього Закону поняття «банківська таємниця» визначено як інформація щодо діяльності та фінансового стану клієнта, яка стала відомою банку в процесі обслуговування клієнта та взаємовідносин з ним чи третім особам при наданні послуг банку і розголошення якої може завдати матеріальну чи моральну шкоди клієнту.