

Бутузов Віталій Миколайович –
головний науковий співробітник
Міжвідомчого НДЦ з проблем боротьби з
організованою злочинністю при РНБО
України, кандидат юридичних наук

До питання специфіки протидії комп'ютерній злочинності

У статті представлено характеристику сучасної комп'ютерної злочинності, висвітлюються проблемні питання специфіки протидії, характерні для нашої держави, шляхи їх вирішення.

Процес інформатизації сучасного суспільства привів до того, що інформація перетворилася у своєрідний стратегічний ресурс, який володіє цінністю, тобто має якості товару. Суспільні відносини вже не можуть існувати та нормально функціонувати без інформаційного обміну в інформаційно-телекомунікаційних системах. На сучасному етапі, внаслідок динамічного розвитку та застосування новітніх технологій, питання захисту суспільства від їхнього використання в злочинних цілях усе більше загострюється.

Слід констатувати, що відбулося різке набуття кримінального професіоналізму, збільшується кількість зухвалих за задумом і кваліфікованих за виконанням злочинів. Злочинні групи та співтовариства все частіше використовують у своїй діяльності новітні досягнення науки й техніки. Зокрема, комп'ютерні технології застосовуються для створення систем конспіративного зв'язку, проникнення в бази даних приватних організацій та державних відомств; комп'ютери й мережні технології стали інструментами вчинення злочинів, а інформаційні ресурси – об'єктами злочинних зазіхань [1].

Слід відмітити відповідну специфіку протидії комп'ютерній злочинності в багатьох країнах СНД, у тому числі й в Україні. Ця специфіка обумовлена наступними факторами [2]:

- відсутністю налагодженої системи правового та організаційно-технічного забезпечення законних інтересів громадян, держави та суспільства в галузі інформаційної безпеки;
- обмеженими можливостями бюджетного фінансування робіт по створенню правової, організаційної та технічної бази інформаційної безпеки;
- недостатнім усвідомленням можливих політичних, економічних, моральних та юридичних наслідків комп'ютерних злочинів;
- слабкістю координації дій по боротьбі з комп'ютерними злочинами правоохоронних органів, органів суду, прокуратури та невідповідністю їх кадрового складу до ефективного попередження, виявлення та розслідування таких діянь;
- серйозним відставанням вітчизняної індустрії розробки, впровадження засобів і технологій інформатизації та інформаційної безпеки від розвинутих країн світу.

Боротьба зі злочинністю в сучасних умовах міжнародних комп'ютерних мереж ускладнена з наступних причин:

- злочинні діяння можуть мати місце в кіберпросторі. Для виявлення та розслідування комп'ютерних злочинів, тобто будь-яких злочинів, вчинених з

використанням комп'ютерної чи телекомунікаційної мережі, потрібні конкретний спеціальний досвід і знання, процедури розслідування і відповідні юридичні повноваження;

- міжнародні комп'ютерні мережі, такі як Інтернет, є відкритим середовищем, що дає користувачам можливості чинити певні дії за межами кордонів держав, у яких вони перебувають. У той же час оперативні або слідчі дії правоохоронних органів повинні обмежуватися територією власної держави. Це означає, що боротьбу зі злочинністю у відкритих комп'ютерних мережах не можна здійснювати без належного міжнародного співробітництва;

- відкритість глобальних інформаційних мереж надає можливість користувачам вибирати таку юрисдикцію, яка відповідає їхнім цілям. Користувачі можуть вибирати ті країни, в яких певні діяння, здійснені в кіберпросторі, не визначаються як кримінальнокарані. Такі країни можуть створювати привабливі можливості для протиправних дій осіб з тих держав, де такі дії, згідно внутрішнього законодавства, підпадають під кримінальну відповідальність. Наявність “інформаційних притулків” – держав, що віддають пріоритет скороченню або запобіганню неправомірного використання комп'ютерних мереж, або в яких не розроблені ефективні процесуальні норми – стримує зусилля інших країн по боротьбі зі злочинністю з використанням інформаційно-телекомунікаційних технологій.

У контексті статті, корисним є наведення інформації, яка була оприлюднена на Конференції Ради Європи щодо співробітництва з протидії кіберзлочинності (01–02.04.2008 року, м. Страсбург, Французька Республіка). У її роботі брали участь представники Ради Європи, правоохоронних органів, наукових організацій, комерційних структур, що працюють у сфері високих технологій, а також міжнародних організацій з 60 країн світу. Метою Конференції було налагодження співробітництва, вивчення досвіду та обмін інформацією у сфері боротьби з кіберзлочинністю [3].

Учасниками Конференції сучасна комп'ютерна злочинність характеризується наступним чином:

- зростання кількості злочинів, що вчинюються з використанням персональних даних співробітників потужних корпорацій для подальшого втручання в автоматизовані центри обробки бухгалтерської, договірної та іншої інформації з метою її перекручування, копіювання або знищення;

- предметом комп'ютерного шахрайства стають права на об'єкти нерухомості. Інформаційні атаки здійснюються відносно інформації пенсійних та інвестиційних фондів від якої залежить котирування інструментів фондового ринку, змінюються індекси на валютних, торгових та фондових ринках. Встановлені факти таких атак на об'єкти, інформаційна інфраструктура яких забезпечує функціонування сфер, критичних для державного управління та економіки;

- поширення фактів використання злочинцями депозитних рахунків інших осіб, блокування інформації щодо роботи з клієнтами шляхом здійснення інформаційних атак на комп'ютери, системи, комп'ютерні мережі фінансових установ;

- інтеграція злочинців у злочинні організації, які спеціалізуються на привласненні інформації щодо реквізитів (персональних даних) сторонніх осіб за допомогою методів і засобів соціоінженерії та шкідливих програм для незаконного втручання до комп'ютерів, систем, комп'ютерних мереж і електрозв'язку. Змінилася тенденція щодо викрадання персональних даних, а саме більше стали викрадати дані відносно корпоративних клієнтів, а не окремих громадян. Наведені приклади діяльності злочинних організацій (названі Генеральним Секретарем Антифішингової робочої групи Пітером Кассіді, як “Транс юні”), що продають таку інформацію та

безпосередньо її використовують. У таких злочинних організаціях функції з питань добування, обробки, накопичення, реалізації такої інформації виконують різні особи.

Спеціалісти виділяють наступні причини та умови, що сприяють поширенню кіберзлочинності:

- боротьба з кіберзлочинністю для урядів багатьох країн не є пріоритетом, що не дозволяє визначити об'єктивний рівень небезпеки від комп'ютерних злочинів у багатьох державах;

- відставання, внаслідок стрімкого розвитку новітніх технологій, правових норм від умов використання цих технологій в економіці та суспільстві, у тому числі зі злочинною метою. Як приклад, високий ступінь анонімності у мережі Інтернет, що дає можливість отримувати великі злочинні доходи з мінімальним ризиком викриття, провокує до вчинення нових видів злочинів;

- брак конструктивного міжнародного співробітництва у протидії кіберзлочинності, наприклад, у багатьох державах, які ратифікували Конвенцію про кіберзлочинність, відсутні національні контактні пункти 24/7;

- відсутність у багатьох державах належної взаємодії між правоохоронними відомствами та приватним бізнесом (телекомунікаційними компаніями та компаніями, що надають послуги Інтернет) з питань надання необхідної інформації (доказів у електронному вигляді) та її збереження в комп'ютерних системах;

- технічна складність відстеження інформаційних загроз. Шкідливі програмні засоби стають усе більш непомітними. За інформацією Пітера Кассіді, дослідниками встановлено, що якщо у 2005 році відслідковувалося лише 85 % таких програм, то у 2006 році – вже 79 %.

З метою підвищення ефективності діяльності правоохоронних органів з протидії кіберзлочинності на Конференції було запропоновано:

- налагодити співробітництво в сфері протидії кіберзлочинності між урядовими структурами, правоохоронними органами, приватними організаціями, науковими організаціями як на внутрішньодержавному, так і міжнародному рівні;

- визначити пріоритетними напрямками у протидії кіберзлочинності підготовку кадрів, що здійснюють протидію кіберзлочинності, та обмін досвідом на міжрегіональному і міждержавному рівнях;

- забезпечити розробку та впровадження нових винаходів і результатів наукового прогресу в діяльність правоохоронних органів по забезпеченню інформаційної безпеки та боротьби з кіберзлочинністю;

- утворити у правоохоронній системі кожної держави спеціалізований підрозділ, особовий склад якого повинен мати спеціальні знання в галузі комп'ютерних та Інтернет технологій, економіки та юриспруденції, а також національний контактний пункт 24/7 згідно Конвенції про кіберзлочинність.

Аналіз сучасного стану боротьби зі злочинами у сфері високих технологій в Україні свідчить про те, що розглянуті на Конференції проблемні питання характерні й для нашої держави та потребують вжиття відповідних заходів з боку її владних структур.

Так, через відсутність протягом тривалого часу кримінологічно значущої інформації про комп'ютерну злочинність, протидія їй з боку правоохоронних органів не завжди носила системний характер. Тому першим етапом організаційних заходів по боротьбі з комп'ютерною злочинністю повинна бути інформаційно-аналітична робота. Перш за все, це створення системи обліку комп'ютерних злочинів, статистичної звітності, розробки порядку аналітичної діяльності органів, які здійснюють протидію таким злочинам, розробки нормативно-правових актів, що регламентують діяльність (взаємодію) спеціалізованих підрозділів з протидії правопорушенням у сфері інформаційно-телекомунікаційних технологій та розробки відповідних методик. Отримані в ході першого етапу організаційних заходів

боротьби з комп'ютерною злочинністю дані повинні бути покладені в основу більш повного та всебічного аналізу таких суспільно небезпечних проявів [4].

Необхідність використання правоохоронними органами певних технічних та програмних засобів для пошуку та фіксації фактичних даних про протиправні діяння у сфері використання електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж і мереж електрозв'язку обумовлює відповідне матеріально-технічне забезпечення вузькоспеціалізованих підрозділів по боротьбі з комп'ютерною злочинністю, здатних застосовувати сучасні методи оперативно-технічного документування злочинів даного виду.

Для боротьби з такою специфічною формою злочинності необхідні відповідно підготовлені спеціалісти вузькоспеціалізованих підрозділів правоохоронних органів, які здатні застосовувати сучасні методи оперативно-технічного документування та розкриття комп'ютерних злочинів. Тому, питання відповідної підготовки кадрів для правоохоронної системи є також першочерговим. Спеціальні знання, необхідні працівникам правоохоронних органів у протидії кіберзлочинності, можуть бути надзвичайно різноманітними та визначатися потребами конкретної служби чи підрозділу. Їх використання в оперативно-розшуковій, слідчій, експертній та управлінській діяльності органів внутрішніх справ буде корисним для прийняття рішень щодо запобігання, припинення, викриття, розслідування злочинів, забезпечення безпеки особи, суспільства і держави.

Враховуючи транснаціональний та міжнародний характер комп'ютерної злочинності, слід зазначити, що законотворчість у сфері інформаційно-телекомунікаційних технологій має бути направлена на розвиток законодавства, що регулює міждержавні та внутрішньодержавні відносини у цій сфері. Прийняття відповідних нормативно-правових актів має забезпечити взаємодію та координацію держав на міждержавному рівні та відомств на внутрішньодержавному рівні в протидії комп'ютерній злочинності. Міждержавна та міжвідомча координація діяльності підрозділів, що здійснюють протидію комп'ютерній злочинності, повинна бути визначена на рівні закону. Міжвідомча та внутрішньовідомча координація підрозділів та їх компетенція – на рівні законодавства, відомчих і міжвідомчих документів.

На етапі попередження у сфері боротьби з комп'ютерною злочинністю важливо змінити умови зовнішнього середовища таким чином, щоб по-перше, унеможливити кримінальне використання інформаційно-телекомунікаційних технологій та інформації, що циркулює в комп'ютерних системах і мережах; по-друге, забезпечити зміну ціннісних орієнтацій, тобто переорієнтовувати громадян на сформований та існуючий у суспільстві позитивний образ кіберзлочинця, який може вільно отримувати протиправні прибутки, на негативний образ, чим попереджувати людей від кримінальної поведінки у цій сфері.

Враховуючи тенденцію до збільшення кількості та зухвалості злочинів, що вчинюються з використанням інформаційно-телекомунікаційних технологій, слід зазначити, що протидіяти такому виду злочинності можуть тільки спеціалізовані структури, виключною компетенцією яких стала б боротьба зі злочинністю у цій сфері. Створення в Україні спеціалізованого підрозділу по боротьбі з комп'ютерними злочинами та надання йому відповідних повноважень, безумовно сприятиме підвищенню ефективності роботи правоохоронної та судової систем по забезпеченню інформаційної безпеки людини, суспільства та держави.

Враховуючи вищезазначене, а також спираючись на вітчизняний та міжнародний досвід, вважаємо за потрібне визначити найбільш доцільні, на наш погляд, шляхи вирішення проблемних питань боротьби з комп'ютерними злочинами в Україні:

– приведення національного законодавства у відповідність до вимог Конвенції ООН проти транснаціональної організованої злочинності та Конвенції Ради Європи про кіберзлочинність, подальше вдосконалення нормативно-правової бази, яка регулює боротьбу з комп'ютерною злочинністю (розширення можливостей правоохоронних органів з урахуванням транснаціонального характеру комп'ютерної злочинності, розроблення ефективного механізму взаємодії національних правоохоронних органів з компетентними органами інших країн);

– утворення спеціалізованого підрозділу, виключною компетенцією якого стала б боротьба з комп'ютерною злочинністю, що за умови надання цьому підрозділу відповідних повноважень та залучення відповідних кадрових і матеріально-технічних ресурсів сприятиме підвищенню ефективності роботи правоохоронної системи України у цій сфері;

– налагодження, на відповідній правовій основі, ефективної взаємодії з міжбанківськими інституціями, телекомунікаційними компаніями, зацікавленими центральними державними органами та правоохоронними органами інших країн з метою документування злочинних груп з міжнародними зв'язками.

Список використаних джерел

1. Сборник договорно-правовых, законодательных и иных нормативных актов “Правовое регулирование сотрудничества правоохранительных органов государств – участников СНГ в сфере обеспечения информационной безопасности”. – Москва, 2008.
2. Бутузов В.М. Злочини із застосуванням сучасних інформаційних технологій // Науково-практичний журнал “Боротьба з організованою злочинністю і корупцією” – 2003. – № 7. – С. 84–89.
3. Звіт “Про участь представників України у Конференції щодо співробітництва з протидії кіберзлочинності (Страсбург, 1–2 квітня 2008 року)”.
4. Бутузов В.М. “Особенности планирования заходов по запобіганню та протидії злочинам у сфері високих технологій” Матеріали міжвузівської науково-практичної конференції 14 грудня 2007 року: Боротьба зі злочинами у сфері комп'ютерної інформації: проблеми та шляхи їх вирішення – Донецьк: ДЮІ ЛУНВС, 2007.

The article is devoted to the description of the modern computer crime; the problems of the specificity of its counteraction in our country and the ways of their solution are examined.