УДК 343.974:343.237

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

Організована та комп'ютерна злочинність: тенденції, проблеми, шляхи вирішення

У статті висвітлено зв'язок між організованою та комп'ютерною злочинністю. Представлено основні тенденції, проблеми та шляхи вирішення питання протидії цим явищам.

Ключові слова: організована злочинність, комп'ютерна злочинність, інформаційні притулки, ТОЗ-Конвенція, Конвенція про кіберзлочинність.

В останні роки зв'язок між такими явищами як "організована злочинність" та "комп'ютерна злочинність" постійно зміцнюється. Характеризуючи ці явища слід відмітити, що сьогодні відбувається інтеграція окремих злочинців-фахівців у галузі ІТ у злочинні групи, а груп – в організації. Такі злочинні об'єднання стають структурованими за професійними ознаками, де окремі функції виконують різні особи. Зазначені об'єднання можуть мати і тимчасовий характер, наприклад для здійснення однієї незаконної операції. У свою чергу, як злочинні співтовариства наймають кваліфікованих фахівців у галузі фінансів, права, у тому числі і міжнародного, для проведення операцій з "відмивання" коштів із використанням різноманітних схем, так і організована злочинність використовує фахівців з ІТ-галузі. Останнім часом прослідковується тенденція до обміну "передовим" досвідом використання новітніх технологій між організованими злочинними групами.

Як показує практика, комп'ютерна злочинність, зазвичай, базується на тих територіях, де з боку держави не створено відповідних умов для забезпечення протидії злочинності, тобто в державах з обмеженими можливостями протидії новітнім загрозам. Так, відкритість глобальних інформаційних мереж надає можливість злочинцям вибирати таку юрисдикцію, яка відповідає їхнім злочинним цілям. А саме, правопорушники можуть вибирати ті країни, де існують привабливі умови для протиправних дій, які згідно з внутрішнім законодавством не підпадають під кримінальну відповідальність, або на тій території відсутні спеціалізовані підрозділи по боротьбі з комп'ютерною злочинністю. У свою чергу, наявність таких "інформаційних притулків" – держав, в яких не розроблені ефективні процесуальні норми – стримує зусилля інших країн по боротьбі з цим видом злочинності. Міжнародні експерти вважають що більшість транснаціональних злочинних угрупувань та організацій знаходиться в державах з перехідною економікою та державах, що перебувають на шляху розвитку ("третього світу"). Таким чином, держави з достатнім рівнем розвитку сфери інформаційних технологій та низькою можливістю протидіяти злочинам у цій сфері, стають притулками для транснаціональної злочинності.

Вже не викликає сумнів той факт, що анонімність дій в інформаційних мережах досягається різними способами, а саме: використанням доступу до мереж через Інтернет-клуби, використання ананімайзерів, проксісерверів, що дозволяє, в свою чергу, задавати необхідні шляхи маршрутизації. Через використання

багаточисленних сервісів анонімізації користувачів мережі Інтернет, правоохоронцям практично неможливо встановити особу злочинця. При роботі з даними сервісами об'єкт атаки встановлює віртуальну IP-адресу, яка не співпадає з реальною адресою особи, яка здійснює атаку.

Навіть у традиційних системах підпільних банків (за типом "Havala" в Індії, "Fei chi'en" у Китаї та "Hundi" у Пакистані) відбуваються технологічні зміни з можливостями переказувати кошти у будь-яку частину світу за допомогою глобальних інформаційних мереж. Інформаційні технології дозволяють здійснювати рух коштів поза банківської системи яка регулюється національним законодавством. Слід враховувати використання злочинними співтовариствами віртуальних банків та різних системи електронних грошей, що функціонують у глобальних інформаційних мережах. Такими системами, наприклад, є: WebMoney, CyberPlat, PayPal, тощо. Вони вважаються одним із видів електронних платіжних систем, але не є зареєстрованими згідно діючого законодавства країн, на території яких використовуються. Крім того, що вони використовуються для здійснення платежів при купівлі товарів та послуг в Інтернет-магазинах або за використання інших Інтернет-ресурсів, їх використовують для анонімних розрахунків. Конвертацію реальних грошей у віртуальні та навпаки, можливо здійснити через банки або через обмінні пункти цих систем. Усі рахунки в таких системах є анонімними, відслідкувати подальший шлях перерахованих таким чином грошових коштів майже неможливо.

Крім створення умов конспірації, розвиток інформаційно-телекомунікаційних технологій надав нові можливості як для удосконалення традиційних, так і появи нових видів злочинів.

Професійним стало використання інформаційних мереж для шахрайства. Наприклад, на початку цього десятиріччя були поширені випадки шахрайства, яке отримало назву "Нігерійські листи". Шахраїв, які використовували схему "шахрайство із передоплатою" (ще відому як "шахрайство 419" – за назвою параграфу Нігерійського Кримінального кодексу), можливо вважати на свій час винахідливими та інноваційними. Атрибутом сучасності стало використання мережі Інтернет при розповсюдженні дитячої порнографії, торгівлі наркотиками, "класичному" вимаганні та вимаганні, що обумовлене загрозою знищення інформаційних даних та комунікаційних систем.

Організована злочинність має на меті отримання надприбутку і може розглядатися як ведення бізнесу злочинними засобами. По оцінках ФСБ Росії, кожна друга російська фірма займається промисловим шпигунством, а конкуренти ведуть проти неї ту ж діяльність. За експертними оцінками, на частку економічного шпигунства доводиться 60 % втрат підприємства від несумлінної конкуренції [1].

Окремим видом злочинного бізнесу вже тривалий час є викрадення персональних даних. Щорічно збитки від витоку персональних або конфіденційних даних ростуть на 20–25 %. По оцінках аналітичного центру InfoWatch, в 2006 році одна лише економіка США втратила більше 60–65 млрд дол. унаслідок витоку приватних відомостей… Можна стверджувати, що загальносвітовий збиток від цих інцидентів становить близько 500 млрд дол. Не врахованою залишається загроза витоку конфіденційної інформації. Виходячи із власного досвіду розслідування інсайдерських інцидентів, аналітичний центр InfoWatch за підсумками року оцінює сукупні втрати світової економіки через витік комерційних секретів у 175 млрд дол. Таким чином, обидва види витоків обходяться щорічно майже в 700 млрд дол. [2].

Питання протидії організованій та комп'ютерній злочинності стає занадто гостро при розгляді такої загрози, як міжнародний тероризм, адже інформаційні впливи можуть стати найпотужнішою зброєю, застосування якої стосовно систем управління енергетикою, транспортом, фінансами й іншими критичними технологіями може бути катастрофічним. Потужність такого впливу порівнюють із

засобами масового ураження, враховуючи що витрати, які необхідні для здійснення такого впливу, мінімальні, а джерело нападу важко ідентифікувати [3].

Щодо імовірності руйнування міжнародних фінансових ринків. Ураховуючи взаємозв'язок всесвітньої фінансової системи, можливо через дестабілізацію роботи фінансових інститутів в окремій державі вплинути на фінансові коливання в інших країнах. Вважають, що "самою привабливою метою для тероризму нового покоління варто визнати ділові центри обробки інформації, насамперед комп'ютеризовані банківські установи. Терористичний удар за допомогою надвисокочастотного випромінювання по великому банку здатний викликати системну кризу всієї фінансової системи розвинених країн, оскільки він позбавляє суспільство довіри до сучасних технологій грошового ринку" [4].

Неодноразово в засобах масової інформації наголошувалося на тому факті, що криза у Південно-Східній Азії була штучно викликана. За однією версією – це була інформаційно-психологічна атака проти національних валют держав Азіатсько-Тихоокеанського регіону – Малайзії, Індонезії, Сінгапуру та Філіппін. За іншою – хакерська атака на одну з фондових бірж, унаслідок чого відбувся "обвал" фондового ринку цих країн, а потім (ефект доміно) падіння китайського фондового індексу Shanghai Composite, гонконгського Hang Seng та японського Nikkei. Зазначена акція вплинула на фінансові ринки не тільки держав зазначеного регіону, а всього світу.

В свою чергу, "…. наслідки азійської кризи найбільш руйнівно позначились на Росії, яка знаходилась далеко від епіцентру кризи, але обтяженої власними політичними та соціально-економічними негараздами, незавершеністю та прорахунками реформ, стагнацією виробництва, незбалансованістю бюджету, внутрішньою та зовнішньою заборгованістю, що критично зросла. Як відмічалося світовими ЗМІ, з посиланнями на дані міжнародних фінансових інститутів, по падінню з початку 1998 року цін на фондових ринках Росія обігнала Індонезію, яка найбільш постраждала з п'яти держав Південно-Східної Азії, де азійська криза зародилася та розповсюдилася" [5].

Активізація організованої злочинності у сфері інформаційних технологій, що відбулася в останні роки через політичні, економічні, інноваційні та соціальні зміни глобального характеру, потребує нових, у тому числі міжнародно-правових, підходів до їх нейтралізації. Правові норми, що спрямовані на протидію організованій злочинності, передбачені низкою міжнародно-правових актів, насамперед Конвенцій, які вимагають від держав, які їх підписали, відповідних розслідувань, судових розглядів, притягнення винних до відповідальності, а також практичної реалізації правового співробітництва з іншими державами.

Важливе значення для діяльності державних органів щодо протидії організованій та комп'ютерній злочинності має Конвенція Організації Об'єднаних Націй проти транснаціональної організованої злочинності (ратифікована у 2004 році) та Конвенція Ради Європи про кіберзлочинність (ратифікована у 2005 році), а також протоколи, що їх доповнюють.

Метою Конвенції Організації Об'єднаних Націй проти транснаціональної організованої злочинності (далі – ТОЗ-Конвенція) є сприяння співробітництву справі більш ефективного попередження транснаціональної організованої злочинності та боротьби з нею.

В рамках теми запропонованої статті, доцільно було б навести основні положення ТОЗ-Конвенції. Так, під терміном "організована злочинна група" розуміється структурно оформлена група в складі трьох або більше осіб, що існує протягом визначеного періоду часу і діє узгоджено з метою здійснення одного або декількох серйозних злочинів чи злочинів, визнаних такими відповідно до цієї Конвенції, для того, щоб одержати, прямо чи опосередковано, фінансову або іншу матеріальну вигоду. Під "серйозним злочином" визначено злочин, що карається

позбавленням волі на максимальний строк не менше чотирьох років або більш суворою мірою покарання.

Згідно статті 3, зазначена Конвенція застосовується до попередження, розслідування і кримінального переслідування у зв'язку з серйозними злочинами, якщо ці злочини носять транснаціональний характер і вчинені за участю організованої злочинної групи. Злочин має транснаціональний характер, якщо він учинений у більш ніж одній державі; учинений в одній державі, але істотна частина його підготовки, планування, керівництва або контролю має місце в іншій державі; учинений в одній державі, але за участю організованої злочинної групи, яка здійснює злочинну діяльність у більш ніж одній державі; або учинений в одній державі, але його істотні наслідки мають місце в іншій державі.

Центральне місце в міжнародних актах займає принцип міжнародного співробітництва в боротьбі з організованою злочинністю в усіх її проявах, послідовне втілення якого в життя відкриває широкі можливості протидії цьому явищу. В свою чергу, в Конвенції передбачено можливість укладання двосторонніх або багатосторонніх угод чи домовленостей, в силу яких у зв'язку зі справами, є предметом розслідування, кримінального переслідування або судового розгляду в одній або декількох державах, заінтересовані компетентні органи можуть створювати органи з проведення спільних розслідувань. За відсутності таких угод або домовленостей спільні розслідування можуть проводитися за угодою в кожному окремому випадку.

Співробітництво між правоохоронними органами, як і інші заходи, здійснюється у вигляді сприяння ефективній координації між компетентними органами, установами; обміну інформацією про конкретні засоби і методи, що застосовуються організованими злочинними групами; обміну інформацією і координації адміністративних та інших заходів, що здійснюються у відповідних випадках з метою завчасного виявлення злочинів, що охоплюються цією Конвенцією.

Відповідно до Конвенції, держави-учасниці розглядають можливість щодо:

– проведення консультацій з науково-дослідними колами, аналізу тенденцій розвитку організованої злочинності на своїй території, умов, у яких існує організована злочинність, а також вивчення залучених до вчинення злочинів професійних груп і технологій;

– розширення аналітичних знань про організовану злочинну діяльність та обміну цими знаннями для чого необхідно розробляти та використовувати загальні визначення, стандарти і методологію;

– здійснення контролю за політикою і практичними заходами щодо боротьби проти організованої злочинності, а також проведення оцінки їхньої ефективності та дієвості.

Крім того, державам-учасницям рекомендується у необхідних межах здійснювати, розробляти чи вдосконалювати конкретні програми підготовки персоналу правоохоронних органів, у тому числі працівників прокуратури, слідчих і співробітників митних органів, а також інших співробітників, що відповідають за попередження, виявлення і припинення злочинів. Такі програми стосуються питань методів, що використовуються в боротьбі з транснаціональними організованими злочинами, які вчиняються з використанням комп'ютерів, телекомунікаційних мереж та інших видів сучасних технологій.

З метою попередження транснаціональної організованої злочинності рекомендується:

– розробляти та оцінювати ефективність національних проектів, впроваджувати оптимальні види практики і політики, спрямовані на попередження транснаціональної організованої злочинності;

– відповідно до основних принципів свого внутрішнього законодавства, скорочувати існуючі чи майбутні можливості організованих злочинних груп діяти на законних ринках при використанні отриманих від злочинів доходів;

– періодично проводити оцінку існуючих правових документів і видів адміністративної практики з відповідних питань з метою виявлення їхньої уразливості з погляду зловживань з боку організованих злочинних груп;

– сприяти поглибленню розуміння суспільством факту існування, причин і небезпечного характеру транснаціональної організованої злочинності, а також загроз, створюваних нею. Відповідна інформація включає відомості про заходи для сприяння участі населення у попередженні такої злочинності та боротьбі з нею і може поширюватися у відповідних випадках через засоби масової інформації.

В свою чергу, Законом України № 2824 – 15 від 07.09.2005 р. було ратифіковано Європейську Конвенцію про кіберзлочинність, якою визначено основні завдання та напрями боротьби з комп'ютерною злочинністю: перелік протиправний діянь, що віднесено до комп'ютерних злочинів; повноваження, які повинні застосовуватися відповідними підрозділами при розкритті та розслідуванні комп'ютерних злочинів; процедури збору доказів в електронній формі по комп'ютерних злочинах; заходи по забезпеченню міжнародного співробітництва та взаємної допомоги у боротьбі з комп'ютерною злочинністю.

Конвенцією до комп'ютерних злочинів віднесено наступні протиправні діяння:

1. Злочини проти конфіденційності, цілісності та доступності комп'ютерних даних і систем (злочини, родовим об'єктом яких є відносини автоматизованої обробки інформації в комп'ютерних системах).

2. Злочини, пов'язані з комп'ютерами (використання процедур автоматизованої обробки інформації в комп'ютерних системах при вчиненні традиційних злочинів).

3. Злочини, пов'язані зі змістом комп'ютерної інформації (використання процедур автоматизованої обробки інформації в комп'ютерних системах при виготовленні та розповсюдженні дитячої порнографії).

4. Злочини, пов'язані з порушенням авторських та суміжних прав (випадки коли злочини, пов'язані з порушенням авторських та суміжних прав, учинені за допомогою комп'ютерних систем).

Згідно Конвенції, при розкритті та розслідуванні комп'ютерних злочинів передбачено наступні повноваження, якими повинні наділятися відповідні підрозділи:

– термінове вилучення та збереження комп'ютерних даних, включаючи дані про рух інформації, в обсязі достатньому для ідентифікації постачальників послуг і шлях, яким була передана інформація;

– обшук комп'ютерної системи або її частини і комп'ютерних даних, що зберігаються в ній; комп'ютерного носія інформації, на якому можуть зберігатися комп'ютерні дані;

– вилучення комп'ютерної системи або її частини або комп'ютерного носія інформації; копіювання і збереження копії таких комп'ютерних даних; заборону доступу або вилучення комп'ютерних даних з комп'ютерної системи;

– витребування необхідної інформації щодо функціонування комп'ютерних систем;

– зобов'язання постачальника послуг, у межах його існуючих технічних повноважень: збирати або записувати технічними засобами або співробітничати і допомагати компетентним органам у зборі або запису даних про рух інформації та даних змісту інформації у реальному масштабі часу, які пов'язані з визначеною передачею інформації, що передається за допомогою комп'ютерних систем.

Корисним вважається розглянути процедури збору доказів у електронній формі по комп'ютерних злочинах. Відповідно до Конвенції національними підрозділами повинні забезпечуватися наступні процедури: збирання комп'ютерних даних у

реальному масштабі часу; збирання даних про рух інформації у реальному масштабі часу; збирання або запис, шляхом застосування технічних засобів, даних про рух інформації у реальному масштабі часу, що пов'язані з визначеною передачею інформації, яка передається за допомогою комп'ютерних систем; перехоплення даних змісту інформації; збирання або запис, шляхом застосування технічних засобів, даних змісту інформації у реальному масштабі часу, які належать до визначеної передачі інформації.

До основних заходів по забезпеченню міжнародного співробітництва та взаємної допомоги у боротьбі з комп'ютерною злочинністю віднесено: термінове виконання запитів про взаємну допомогу, що здійснюються терміновими засобами комунікації; термінове збереження по запиту правоохоронних органів інших країн, відповідно внутрішньодержавному законодавству, комп'ютерних даних, які мають причетність до комп'ютерного злочину (не менше, ніж 60 днів); термінове розкриття по запиту правоохоронних органів інших країн, відповідно до внутрішньодержавного законодавства, збережених даних про рух інформації, достатніх для ідентифікації постачальника послуг і шляху передачі такої інформації; збирання по запиту правоохоронних органів інших країн, відповідно до внутрішньодержавного законодавства, даних про рух інформації у реальному масштабі часу, пов'язаних із зазначеною передачею інформації, яка передається за допомогою комп'ютерної системи; перехоплення по запиту правоохоронних органів інших країн, відповідно до внутрішньодержавного законодавства, даних змісту інформації у визначених передачах інформації, що здійснюються за допомогою комп'ютерної системи; забезпечення здійснення контактів цілодобово впродовж тижня з метою надання негайної допомоги при розслідуванні або переслідуванні стосовно кримінальних правопорушень, пов'язаних з комп'ютерними системами і даними, або з метою збирання доказів у електронній формі, що стосуються кримінального правопорушення та інше.

Враховуючи, що зазначені Конвенції в Україні ратифіковано, ще невирішеними залишаються питання організації попередження і протидії правопорушенням у сфері інформаційних технологій, розширення можливостей національних правоохоронних органів з урахуванням транснаціонального характеру комп'ютерної злочинності, розроблення ефективного механізму взаємодії національних правоохоронних органів з компетентними органами інших країн. Існує необхідність удосконалення механізму оперативного обміну інформацією про громадян, які затримувалися на території інших держав за злочини, пов'язані з використанням підроблених або викрадених платіжних пластикових карток банківських установ, шахрайством у мережі Інтернет, незаконним втручанням до автоматизованих систем, комп'ютерних баз даних міністерств та відомств, а також для перевірки на причетність до вчинення злочинів у сфері банківської діяльності та інформаційних технологій.

Формування та реалізація державної політики у сфері боротьби з організованою злочинністю вимагає прийняття цілеспрямованих, системних та комплексних правових заходів. Особливо коли це стосується транснаціональних організованих угруповань, які вчиняють злочини з використанням комп'ютерів, телекомунікаційних мереж та різних видів сучасних інформаційних технологій. Слід зазначити, що крім розробки та прийняття законів щодо протидії злочинності необхідно створювати умови для їх виконання.

З огляду на зазначене, з метою підвищення якості протидії комп'ютерній злочинності необхідно також провести наступні організаційні заходи:

– створити міжвідомчу робочу групу для розроблення та координації спільних заходів протидії комп'ютерній злочинності між правоохоронними органами та операторами зв'язку, Інтернет-провайдерами, контент-провайдерами, банківськими, фінансовими установами, державними та громадськими організаціями;

– розробити нормативно-правове забезпечення доступу правоохоронних органів до інформації про протиправні дії при використанні інформаційно-телекомунікаційних технологій;

– створити міжвідомчу систему моніторингу оперативної обстановки у сфері інформаційно-телекомунікаційних технологій та розробити ефективні механізми реагування на комп'ютерні інциденти;

– розвивати експертні знання про комп'ютерну злочинність, ефективно розподіляти інформацію між відповідними відомствами, створювати спеціальні підрозділи на національно рівні, національному контактні пункти, міжвідомчі та міжнародні цільові групи;

– розслідувати кримінальні справи зазначеної категорії слідчими органів внутрішніх справ, які спеціалізуються на розслідуванні справ про комп'ютерні злочини.

При розробці та впровадженні організаційних заходів, слід врахувати, що інформаційні мережі, в більшості випадків, знаходяться у приватній власності, що ускладнює функцію контролю за ними з боку держави. У сучасних умовах, коли в силу об'єктивних причин, переважно політичного та економічного характеру, наша держава не в змозі мати на всіх напрямах достатньо потужні важелі, питання організації співробітництва держави та приватного сектору є одним з пріоритетних. Тому, діяльність запропонованої робочої групи, повинна бути направлена на відпрацювання моделі необхідного обміркованого балансу між захистом національної безпеки та ефективним захистом фінансових ринків і громадян від впливу транснаціональної комп'ютерної злочинності, у вигляді концептуальних засад публічно-приватних партнерств (співробітництва державного та приватного секторів).

Список використаних джерел

1. *Кочуров А.М.,* Лобашев А.К., Вепрев С.Б. Совершенствование подготовки специалистов по информационной безопасности в учебных центрах на основе E-learning технологий // Защита информации. Инсайд. – М. – 2007. – № 1. – С. 52 – 55.

2. *Доля А.А.* Внутренние ИТ-угрозы в России – 2006 // Защита информации. Инсайд. – М., 2007. – № 2. – С. 60 – 69.

3. *Зегжда П.Д.* Обеспечение безопасности информации в условиях создания единого информационного пространства // Защита информации. Инсайд. – М., 2007. – № 4. – С. 28 – 33.

4. *Расторгуев С.П.* Информационная война. Проблемы и модели. – М.: Гелиос АРВ, 2006. – 240 с.

5. *"НГ-сценарии"* – 1998. – № 10. – С. 7.

В статье освещена связь между организованой и компютерной преступностю. Представлены основные тенденции, проблемы и пути решения вопроса противодействия этим явлениям.

The article is dedicated to the examination of the connection between the organized and computer crime. The main tendencies, problems and ways of decision of the question of counteraction these phenomena are represented.

Стаття надійшла до редакції журналу 27 травня 2009 року.