УДК 343.13:002.6

В.М. БУТУЗОВ, *кандидат юридичних наук,*
головний науковий співробітник Міжвідомчого
науково-дослідного центру з проблем боротьби
з організованою злочинністю при РНБО України

ОСОБЛИВОСТІ РЕФОРМУВАННЯ ОРГАНІЗАЦІЙНО-ФУНКЦІОНАЛЬНОЇ СТРУКТУРИ ПРОТИДІЇ КОМП’ЮТЕРНІЙ ЗЛОЧИННОСТІ

Анотація. *До питань протидії комп’ютерній злочинності у стратегічній перспективі, проблематики формування організаційної та функціональної структури існуючих у правоохоронних органах підрозділів по боротьбі з комп’ютерними злочинами.*

Характерною рисою останнього десятиліття став прискорений розвиток засобів для обробки інформаційних потоків та зростання ролі інформації в забезпеченні національної безпеки. Роль інформації зросла не тільки в процесі підготовки та прийняття рішень державного рівня, вона значно збільшилася в духовній, соціальній, політичній та економічній сферах діяльності. З розвитком людського суспільства, появою приватної власності, боротьбою за владу та подальшим розвитком людської діяльності інформація набула всі якості товару, тобто стала мати ціну. Цінність інформації збільшується від можливості отримати матеріальні, політичні або військові дивіденди.

Інформатизація у сферах життєдіяльності, інтенсивність інформаційних процесів та зміна контенту призводять до якісних змін самих цих сфер. Сучасні інформаційні технології приводять до нових форм культурної експансії, військових і терористичних дій, збору та моніторингу інформації, появі нових можливостей по нагляду за громадянами. Враховуючи залежність держави від функціонування різноманітних комунікаційних та інформаційних систем, суспільство, в свою чергу, стає все більш уразливим від порушення працездатності цих систем. Однією з основних загроз інформаційній безпеці є феномен комп’ютерної злочинності який у більшості розвинених країн світу зводиться в ранг загрози не тільки інформаційній безпеці, але й національній безпеці в цілому.

Сьогодні для людей, які відповідальні за безпеку інформації, важливо, як ніколи, визначати, розробляти та управляти політикою безпеки, тим самим запобігаючи новітнім загрозам, що викликані бурхливим розвитком інформаційних технологій. Важливо також навчитися уникати цих загроз у майбутньому. Для кожної держави життєво важливим інтересом стало формування державної політики у сфері забезпечення інформаційної безпеки; розробки першочергових заходів щодо вдосконалення правового, методичного, науково-технічного та організаційного забезпечення безпеки особи та суспільства в сфері комп’ютерної інформації.

Багато країн світу розглядають комп’ютерні мережі як життєво важливий компонент їх економічної, соціальної та політичної інфраструктури. В свою чергу, порушення обміну даними може паралізувати роботу цілих корпорацій, банків і державних структур, що призведе до суттєвих матеріальних втрат у цілих галузях. Поряд із цим, прослідковуються серйозні тенденції до використання комп’ютерної техніки організованими злочинними групами, терористичними організаціями, а наслідки від комп’ютерних злочинів поширюються на міждержавний рівень.

Характер і масштаби комп’ютерних злочинів за останнє десятиліття значно змінилися. Небезпека, яку вони несуть для держави, значно збільшилася. На сьогодні такі

злочинні дії характеризуються розширенням масштабів загрози та посиленням їх економічної та політичної складових. Середовищем учинення комп’ютерних злочинів стають глобальні інформаційні мережі, які все частіше використовуються в якості агітаційного та комунікаційного засобу терористичними угрупованнями, для підбурювання вчинення злочинів на ґрунті расизму, екстремізму та ксенофобії, розповсюдження дитячої порнографії, переслідування з метою шантажу, здійснення незаконного бізнесу в галузі розваг, порушення авторських прав на програмне забезпечення, незаконного збирання відомостей про особу. Все більшого обсягу набирає використання в Інтернеті електронних платіжних систем при шахрайствах та у процесі “відмивання” коштів.

У багатьох країнах світу, у тому числі й в Україні, найбільш поширеними видами злочинів із використанням комп’ютерної техніки є несанкціоноване втручання в роботу комп’ютерних та телекомунікаційних мереж; виготовлення та розповсюдження шкідливих програм чи технічних засобів; порушення правил експлуатації комп’ютерних та телекомунікаційних мереж; несанкціонована зміна маршрутизації міжнародного телефонного трафіку; шахрайство як операторів зв’язку, так і абонентів телекомунікаційних компаній; шахрайство з використанням комп’ютерної техніки, шахрайство в мережі Інтернет; викрадення ідентифікаційних даних осіб; інші традиційні злочини (привласнення, підробка, вимагання, службові злочини), що вчиняються з використанням комп’ютерних технологій.

Поряд із такими засобами ураження комп’ютерних інформаційних систем як комп’ютерні віруси, програмні закладні пристрої слід відмітити засоби пригнічення інформаційного обміну в телекомунікаційних мережах, його фальсифікації, передачі по каналах державного і недержавного управління інформації та засоби, що дозволяють впроваджувати програмні закладки у державні та корпоративні інформаційні системи та керувати ними на відстані [1].

В свою чергу, програмні та технічні засоби, створені для подолання систем захисту інформаційних і телекомунікаційних систем, що призводить до витоку, втрати, підробки, блокування інформації або до порушення встановленого порядку її маршрутизації, є інформаційною зброєю в арсеналі злочинців. Такі засоби (інформаційна зброя) можуть бути застосовані для деструктивних впливів на державні організації при виконанні ними управлінських функцій, кредитно-фінансові установи, транспортні та промислові підприємства, інформаційно-телекомунікаційні організації та ін.

Інформаційна зброя, створена для впливу на комп’ютерні мережі супротивника, містить у собі різні види сучасних засобів та методів і може бути ефективно використана злочинними і терористичними угрупованнями. Тим часом, сам факт ведення інформаційної війни може бути з легкістю замаскований під міжнародні комп’ютерні злочини, вчинені як приватними особами так і організованими злочинними угрупованнями. Сьогодні проблема протидії транснаціональній комп’ютерній злочинності набула особливої актуальності. Комп’ютерна злочинність та її наслідки – нова форма антигромадської поведінки, що представляє собою загальну загрозу безпеці та нормальному функціонуванню світового співтовариства. Крім того, у суб’єктах комп’ютерної злочинності вже простежуються стійкі соціальні групи.

Після закінчення холодної війни з об’єктивних причин почалося “переформатування” як світового співтовариства взагалі, так і регіональних зокрема. Тобто змінилася геополітична модель світу, коли з одного боку, держави практикують винятково прагматичну політику, максимально концентруючи владу [2], а з іншого – влада від держав переходить до інших суб’єктів (транснаціональних утворень). У цьому

аспекті можна відмітити початок протистоянь держав і великих власників, а саме – фінансово-промислових та транснаціональних груп, а також, безпосередньо, й подальший розвиток корпоративних війн різних рівнів і масштабів.

Комп’ютерну злочинність, як і комп’ютерний тероризм, уявляється можливим розглядати як один із аспектів інформаційного протиборства інтересів конкуруючих компаній, політичних сил, держав, що, в свою чергу, слід розуміти як дії, спрямовані на досягнення інформаційної переваги в інформаційному протиборстві шляхом впливу на інформацію та інформаційні системи супротивника з одночасним забезпеченням безпеки власних інформаційних систем та інформації [3]. Інформаційне протиборство може охоплювати всі види інформації та інформаційні системи; поширюватись на весь інформаційний простір чи територію супротивника (конкурента); створювати кризові ситуації у різноманітних сферах життєдіяльності людини; здійснюватись як фахівцями громадських структур, так і спецпідрозділів силових структур [4].

Безпосередньо, комп’ютерний тероризм передбачає інформаційні атаки на обчислювальні центри, центри керування воєнними мережами й медичними закладами, банківські та інші фінансові мережі, засоби передачі даних за допомогою комп'ютерних мереж. Він може здійснюватись з метою саботажу (урядових установ), заподіяння економічного збитку (великим виробничим корпораціям), дезорганізації праці з потенційною можливістю смертей. Інформаційна атака на комп’ютерну інформацію, обчислювальні системи, апаратуру передачі даних, інші складові інформаційної інфраструктури, що здійснюється терористичними угрупованнями або окремими особами, є основною формою комп’ютерного тероризму. Така атака дозволяє проникати в систему, перехоплювати управління або пригнічувати засоби мережного інформаційного обміну, проводити інші деструктивні впливи.

З ростом впливу на політичній арені фінансово-промислових груп і транснаціональних корпорацій, які мають певне лобі у владних структурах, з’явилася потреба використовувати можливості силових відомств у своїх власних, як правило, комерційних цілях. У багатьох країнах з’явилася можливість, а в деяких випадках навіть необхідність, створення так званих “фінансово-силових утворень”. Таким чином, відбулося злиття фінансово-промислового капіталу та силових можливостей.

Правоохоронним органам відомі випадки залучення на платній основі приватними компаніями фахівців силових і кримінальних структур як для “тестування” систем безпеки компаній – конкурентів, так і при вирішенні питань по захисту корпоративних інтересів. Напади на комп’ютерні мережі шляхом несанкціонованого доступу здійснюються з метою порушення роботи відповідних установ. Логічно, що такі фахівці задіють весь арсенал спеціальних прийомів і методів для досягнення поставленої перед ними мети.

З огляду на гостроту та актуальність питання боротьби з комп’ютерною злочинністю у стратегічній перспективі сьогодні особливої ваги набуває проблематика формування організаційної та функціональної структури існуючих у правоохоронних органах підрозділів по боротьбі з комп’ютерними злочинами, яка на сьогодні не відповідає поставленим перед ними завданням. Тому настала необхідність у новому концептуальному підході щодо питання протидії комп’ютерної злочинності національними правоохоронними органами. Так, у новому підході, що пропонується до уваги, формуванню відносин та об'єднанню зусиль різних силових відомств у процесі створення ефективної системи протидії комп’ютерній злочинності відведено провідну роль. У питанні створення ефективної структури повинні бути зацікавлені правоохоронні органи та органи сектору безпеки, тобто всі суб'єкти оперативно-

розшукової діяльності, які мають функції по захисту національних інтересів в інформаційній сфері, що, врешті-решт, повинно дати оптимальний результат.

У багатьох державах світу простежується тенденція до створення та подальшої реорганізації у складі правоохоронних органів (поліції, органів сектору безпеки) спеціалізованих підрозділів з протидії комп’ютерній злочинності. Все частіше держави виходять з ініціативами щодо протидії комп’ютерній злочинності. Так, у 2008 році Міністром внутрішніх справ Франції було оприлюднене французьку Стратегію з питань боротьби з кіберзлочинністю.

Для реалізації зазначеної Стратегії були поставлені наступні задачі:

- поліпшити співробітництво з операторами електронних комунікацій, що дозволить прискорити передачу інформації поліції та жандармерії;
- створити умови для адекватної протидії кіберзлочинності з боку поліції та жандармерії, для чого слід використовувати всі відомі національні та міжнародні нормативно-правові акти, розробляти новітні й модернізувати існуючі технічні засоби, що знаходяться в розпорядженні поліції та жандармерії, розробляти методи щодо упередження такого виду злочинності.

У Стратегії визначено наступні основні напрями:

- модернізація методів розслідування за рахунок удосконалення технічних та нормативно-правових актів для ідентифікації користувачів мережі Інтернет;
- розробка та встановлення правил співробітництва суб’єктів, що надають послуги з Інтернету, зі службами, зацікавленими в боротьбі з кіберзлочинністю;
- зміцнення міжнародного співробітництва;
- приведення у відповідність до сучасних вимог та зміцнення взаємодії представників поліції та жандармерії за рахунок створення групи, що буде займатися шахрайствами в мережі Інтернет;
- підвищення кваліфікаційного рівня (підготовка фахівців), залучення поліції та жандармерії до дослідницьких програм, до тематики досліджень і розвитку французької промисловості;
- створення Міжвідомчого комітету з розслідування справ, пов’язаних з інформаційними технологіями та комунікаціями [5].

У США було прийнято антитерористичний закон, що має назву “Акт Патріота США 2001 року”, в якому пропонується створити нові форми взаємодії та обміну оперативною інформацією. Відповідно до Закону створюються координаційні структури, зміцнюються існуючі форми взаємодії та обміну даними. Закон прямо дозволив передачу інформації розвідувального характеру, що стала оперативним надбанням одного правоохоронного відомства або розвідувального органу, іншим правоохоронним органам чи розвідки [6]. У лютому 2003 року у США розроблено та опубліковано “Національну стратегію захисту кіберпростору”, в якій розроблено послідовний та комплексний підхід до захисту життєво важливих комунікаційних технологій американської нації. Згідно із задекларованою інформацією стратегію розроблено після кількох років консультацій із великої кількістю осіб, у т. ч. працівників органів управління та організацій приватного сектору.

Очевидно, що сьогодні необхідно гостро ставити питання про створення “структури-підрозділу” принципово нового типу, яка повинна стати системоутворювальним підґрунтям для вирішення такого державного завдання, як захист інформаційного простору. Слід враховувати, що на формування та практичну діяльність такого підрозділу однозначно будуть впливати внутрішні та зовнішні

фактори, а саме: геополітичні чинники, фінансово-економічні проблеми, внутрішня політика, стан інформаційних, технологічних, наукових сфер і зростання злочинності.

Основні завдання в процесі функціонування “структури-підрозділу” повинні формулюватися як організація ефективної роботи за допомогою спеціальних сил та засобів усіх суб’єктів оперативно-розшукової діяльності, що мають функції захисту національних інтересів в інформаційній сфері, а саме і одержання упереджувальної інформації, її кваліфікована обробка та аналіз, проведення адекватних заходів щодо попередження, виявлення та нейтралізації загроз в інформаційній сфері, прогнозування розвитку цього виду злочинності.

Пропонується розглядати створення принципово нової “структури-підрозділу” як інструменту розбудови та розвитку системи протидії потужним трансрегіональним, регіональним або локальним “недружнім” утворенням (інституціональним груповим суб’єктам), а не тільки реструктуризації підрозділів існуючої системи. Діяльність “структури-підрозділу” має зосередитися на проведенні багаторівневих оперативних комбінацій, які повинні мати ініціативно-випереджувальний і навіть провокаційний характер, на засадах експерименту. Очевидно, що сили та засоби діяльності такої “структури-підрозділу” стануть поліпроцесуальними та поліфункціональними, багатопредметними, а тому різними за професійними ознаками. Пропонована “структура-підрозділ” повинна ефективно функціонувати в різних ситуаціях, де необхідно буде задіяти різні спеціальні знання, включаючи не тільки традиційні правоохоронні.

Мова йде про дуже важливу функцію, а саме: виявлення та визначення мотивів і цілей злочинного впливу різних інституціональних і соціальних групових суб’єктів – складових комп’ютерної злочинності, наприклад: організовані злочинні групи (транснаціональні, міжрегіональні, регіональні), терористичні організації, розвідки як закордонних держав, так і приватних компаній, груп протесту, кібернетиків-професіоналів і т. ін. З цією метою корисним кроком стала б розробка класифікації інституціональних і соціальних групових суб’єктів.

Тому, використовуючи особливі знання, маючи можливість моделювати розумово, використовуючи попередній досвід діяльності суб’єктів оперативно-розшукової діяльності, при контакті з представниками противної сторони легше визначити, хто в результаті є твоїм супротивником. І залежно від ступеня загрози та спрямованості (чи то втручання в роботу телекомунікаційної або кредитно-фінансової системи; саботаж виробництва та наукових розробок; порушення конституційних і виборчих прав; вплив на масову свідомість, у тому числі заклики до розв’язання міжнаціональної ворожнечі, расизму та екстремізму; різні види шпигунства) доводити до відома зацікавлених органів (залежно від їх компетенції) про факт вчинення злочину та технологічний спосіб впливу. У свою чергу, статистика цих даних за рахунок високої кореляції дій даних соціальних груп дозволить відслідковувати процеси, що відбуваються в злочинному середовищі, а також передбачати активізацію та напрям наступних комп’ютерних злочинів.

Можна стверджувати, що на сьогоднішній день основна проблема підрозділів у силових відомствах – невідповідність існуючих форм і методів прямому призначенню та новим завданням на сучасному етапі розвитку інформаційного суспільства, а також ігнорування нових підходів до організації такого специфічного виду діяльності. Тому, на наш погляд, стратегічним напрямом сьогодні є використання різноманітного передового досвіду та існуючих практик різних відомств – суб’єктів оперативно-розшукової діяльності.

Безсумнівно, при створенні “структури-підрозділу” основна увага має бути приділена інтелекту, можливості отримувати перевагу над супротивником по різних напрямах. Тому необхідна змішана – різноспеціалізована та різнорівнева підготовка фахівців і керівників. Вони в перспективі зможуть відпрацьовувати неоднорідні інформаційні потоки, відтворювати реальну і повну картину подій, які вже відбулися, і прогнозованих ситуацій, а також виступати механізмом еволюційного впливу перетворення та реформування існуючих структур.

Винятково важливим є вибір напряму формування ланок усіх рівнів “структурипідрозділу” та наступного кадрового наповнення фахівцями, які потенційно вирішуватимуть поставлені завдання. Такий підхід дозволить у сучасних умовах успішно протидіяти супротивникові по захисту національних інтересів, активно нейтралізувати ворожі акції та реалізовувати превентивні заходи.

Виходячи з національних інтересів і потенціалу України, для створення цілісної системи протидії комп’ютерній злочинності, з урахуванням проблемних питань організації та управління на всіх рівнях, необхідний пошук, формування та реалізація шляхів рішень на основі передових наукових методів системного і структурного підходу. Основними напрямами даної діяльності пропонується вважати наступні:

- посилення міждержавної взаємодії та координації зусиль в області боротьби з комп'ютерною злочинністю;
- створення національного законодавства, що забезпечить захист інформації у комп'ютерних мережах;
- вироблення та реалізація єдиної науково-технічної політики захисту державних інформаційних ресурсів та інформаційно-телекомунікаційної інфраструктури з метою протидії комп'ютерній злочинності;
- розробка і впровадження в практику комплексу виховних заходів у групах, схильних до вчинення комп’ютерних злочинів;
- організація міжвідомчої взаємодії та координації державних органів при оцінці реальних і потенційних загроз у сфері комп’ютерної інформації, а також виробленні та реалізації заходів щодо їх усунення;
- забезпечення реалізації державного контролю за розробкою, виробництвом, застосуванням, експортом та імпортом засобів захисту інформації;
- створення системи уніфікованих нормативно-методичних і технічних документів у сфері захисту комп’ютерної інформації;
- посилення діяльності з професійної підготовки та перепідготовки кадрів, зайнятих у сфері інформаційної безпеки;
- створення правової бази, що забезпечує боротьбу з комп’ютерними злочинами;
- визначення або створення державного органу з функцією координації боротьби з комп’ютерною злочинністю.

З метою виявлення та усунення або нейтралізації негативних соціальних процесів і явищ, що породжують комп’ютерну злочинність, необхідно утворити організаційні структури у межах певного державного органу з функцією координації боротьби з комп’ютерною злочинністю, а саме:

1. Створити спеціалізований підрозділ по боротьбі з комп’ютерними злочинами. Серед його завдань, з урахуванням положень Конвенції Ради Європи про кіберзлочинність, необхідно визначити наступні:

• організація та координація боротьби зі злочинами у зазначеній сфері (весь спектр злочинів, віднесених міжнародними та національними нормативними актами до комп’ютерних, а також злочини у сфері телекомунікацій);

• здійснення оперативно-розшукової діяльності в інформаційно-телекомунікаційних системах, у тому числі проведення оперативно-технічних заходів по збиранню та перехопленню комп’ютерної інформації у масштабі реального часу;

• проведення аналізу оперативної обстановки у сфері інформаційно-телекомунікаційних технологій. Подання аналітичних матеріалів та прогнозу щодо тенденцій та наслідків від проявів комп’ютерної злочинності на розгляд визначеному державному органу та органам державної влади;

• розроблення та впровадження в практичну діяльність органів внутрішніх справ ефективних методик документування комп’ютерних злочинів, а також традиційних злочинів, учинених із використанням сучасних інформаційних та телекомунікаційних технологій;

• надання допомоги галузевим службам з питань розкриття злочинів, учинених із використанням інформаційних технологій;

• забезпечення засобами швидкої комунікації взаємодії з компетентними підрозділами інших країн при документуванні та розкритті злочинів даного виду.

2. Створити єдиний орган (Контактний національний пункт), який у відповідності з внутрішньодержавним законодавством і практикою, з урахуванням міжнародних норм права повинен забезпечувати надання технічних порад, збереження даних, збирання доказів, надання юридичної інформації і встановлення місцезнаходження підозрюваних. Визначений орган для здійснення контактів у цілодобовій мережі повинен мати можливість термінового встановлення контакту з органом іншої країни.

Використана література

1. Мунтіян В.І. Основи теорії інформаціогенної моделі економіки / В.І. Мунтіян. – К.: Видавництво “КВІЦ”. – 368 с.

2. Згуровський М.З. Сталий розвиток: короткий термінологічний словник / М.З.Згуровський, Г.О. Статюха, І.М. Джигерей. – К.: НТУУ “КПІ”. – 2008. – 50 с.

3. Циганков В.Д. Психотропное оружие и безопасность России / В.Д. Циганков, В.М. Лопатин. – М.: СИНТЕГ, 1999. – 113 с. – (Серия “Информатизация России на пороге XXI века”).

4. Бутузов В.М., Тітуніна К.В. Сучасні загрози: комп’ютерний тероризм // Боротьба з організованою злочинністю і корупцією (теорія і практика). – 2008. – № 17. – С. 316–324.

5. Бутузов В.М. Міжнародний досвід: ініціатива правоохоронних органів Франції з протидії комп’ютерній злочинності // Боротьба з організованою злочинністю і корупцією (теорія і практика). – 2008. – № 19. – С. 240-246.

6. Anti-terrorism bill’s expiration date may not mean mach. – Режим доступу: http://www.politechbot.com/p-02714.html

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~