УДК 343.973

Цимбалюк Віталій Степанович – головний науковий співробітник Науково-дослідного центру Академії прокуратури України, кандидат юридичних наук, старший науковий співробітник

Кримінологічний аспект стратегії формування та розвитку електронного банкінгу

У статті розглянуто окремі питання національної безпеки України у кримінологічному аспекті стратегії формування та розвитку інформаційного суспільства на прикладі такого нового сектору економіки, як електронний банкінг.

Глобалізація світової економіки під впливом транскордонних засобів електронної телекомунікації, зокрема Інтернет, надає широкі технологічні можливості для здійснення господарської діяльності. Важливою складовою цієї діяльності є оперативне (швидке) здійснення розрахунків, управління фінансовими потоками, у тому числі на міждержавному рівні із застосуванням міжнародної банківської системи електронних платежів.

В останні роки національна і міжнародна кредитно-фінансова системи, у тому числі й корпоративні банківські інформаційні системи електронних платежів, зазнали значних технологічних перетворень, пов'язаних з інтеграцією з Інтернет. Банки найбільше зацікавлені у такій інтеграції, зокрема, у реалізації ідей: "віртуальних грошей" (e-mane), "пластикової електронної валюти" "електронних гаманців" і т.ін.

Однією з постійно існуючих проблем при цьому є безпека формування та розвитку глобальних електронних інформаційних систем під впливом нових здобутків науково-технічного прогресу у сфері інформатики [1–18].

Різні проблеми розвитку інформатизації суспільства, у тому числі у сфері економіки, знайшли широке висвітлення у публікаціях вітчизняних та зарубіжних дослідників. Серед вітчизняних дослідників можна відмітити таких, як Д.С. Азаров, В.М. Брижко, В.М. Бутузов, В.Д. Гавловський, Р.А. Калюжний, В.Я. Мацюк, А.А. Музика, В.А. Некрасов, Б.В. Романюк, І.Ф. Хараберюш, О.І. Хараберюш, М.Я. Швець, В.К. Шкарупа та ін.

Мета проведення дослідження була визначена комплексно: у контексті кримінологічного аспекту суспільних відносин у інформаційній сфері стосовно кіберзлочинності та визначення кримінологічних досліджень як джерела формування міжнародного інформаційного права й інформаційного права України у аспекті міжнародної та національної безпеки.

Серед основних завдань дослідження було визначено прогнозування нових напрямків протидії кіберзлочинності, у тому числі у аспекті проблематики національної та міжнародної безпеки у сфері застосування сучасних комп'ютерних інформаційних технологій, як основи формування інформаційного суспільства.

Розкриття основних результатів дослідження пропонується, виходячи з того, що як інновація, нині серед практиків і у наукових колах виношуються нові ідеї розвитку економіки суспільства під впливом здобутків інформатики. За приклад, пропонується звернути увагу на новий різновид електронного банкінгу: інтеграцію через Інтернет банківського та бухгалтерського обслуговування приватних підприємців, особливо тих, бізнес яких здійснюється на основі індивідуальної трудової діяльності. При цьому банк традиційно не виступає в ролі податкового агента, а надає тільки інформаційні послуги, у тому числі стосовно підготовки

документів бухгалтерського обліку та податкової звітності клієнту. При цьому клієнт-підприємець має можливість не тільки здійснювати оперативний управлінський контроль своєї фінансової спроможності, але і за своїм підписом сплачувати з банківських рахунків податки, інші обов'язкові платежі та звітувати у відповідних державних органах про результати своєї господарської діяльності, у тому числі із застосуванням електронного підпису.

Для деяких вітчизняних фінансистів та правників сьогодні це може здатися фантастикою. Але, свого часу, фантастикою здавалися ідеї першопрохідців електронного світу. "У телефоні стільки слабких місць, що його не можна серйозно розглядати як засіб для спілкування", – зазначала внутрішня інструкція компанії Western Union у 1876 році. Нині телефонний е-банкінг зробив цю компанію всесвітньою. Том Ватсон, засновника IBM, колись скептично говорив, що на світовому ринку може знайтися попит на 5 комп'ютерів. Нині важко уявити солідний банк без комп'ютерної інформаційної системи. "Немає ніяких підстав думати, що хтось захоче мати комп'ютер у своєму домі", – говорив у 1977 році Кен Ослон, засновник корпорації Digital Equipment …. [11].

Подальші дослідження подібних прогнозів в історії формування інформаційного суспільства та коментарі стосовно розвитку електронних інформаційних технологій – справа часу і зацікавлених у цьому дослідників.

Як приклад, тільки в Україні кількість Інтернет – користувачів, за даними компанії MMG (Miniwatt's marketing group), з 2000 до 2005 років збільшилася у 25 разів і становить приблизно 5 млн. (11,3 % населення) [9]. Кількість магазинів в російському Інтернет за 2006 рік збільшилася приблизно на 47 %. За оцінками експертів Інтернет – корпорації Яндекс, у 2006 році російський ринок стосовно роздрібної електронної торгівлі товарами із застосуванням Інтернет зріс на 42 %. Обороти західної е-торгівлі зросли приблизно на 25 % [10].

Останнім часом для оперативного фінансового обслуговування у сфері Інтернет – торгівлі з'явилася нова послуга банківської діяльності, яка отримала на практиці умовну назву – мобільного електронного банкінгу (мобе-банкінг). Ця послуга вже практикується багатьма банками передових у технічному відношенні країн шляхом агрегації з послугами електронних (пластикових) кредиторських та дебіторських карток, а також розширення мережі банкоматів. Агрегація Інтернет та стільникової мобільної телефонії дала нові прояви і правовідносин у фінансовій сфері.

Звертає на себе увагу наступне повідомлення у засобах масової інформації. 12 лютого 2007 року Асоціація операторів мобільного зв'язку (GSMA), яка об'єднує операторів стандарту GSM, у співпраці з MasterCard (у якій приймають участь 25 тисяч банків) оголосили про розробку пілотної програми зі створення грошових переказів через стільникові телефони. Передумовами цього є те, що у 2006 році в різних країнах тільки мігранти відправили додому в загальній кількості 200 млрд. дол. Нова технологія покликана спростити відправлення грошей на транскордонному рівні і до 2012 року у чотири рази збільшити світовий обсяг грошових переказів. MasterCard і 19 операторів мобільного зв'язку з клієнтською базою 600 млн. у 100 країнах світу вже почали випробувати електронну систему міжнародних грошових переказів. За повідомленнями учасників ринку, серед них найбільші міжнародні оператори мобільного зв'язку Vodafone, індійський Bharti Airtel, єгипетський Orascom Telecom, Cingular (США), Telecom Italia, міжнародний MTN і Turkcell.

Розробники проекту виходять з того, що з 6,5 млрд. людей на Землі лише менше 1 млрд. мають банківський рахунок, але у світі широко розповсюджені мобільні телефони (біля 2,5 млрд.). Нова система платежів дозволить пересилати гроші за невеликий відсоток "швидко і безпечно". В рамках проекту GSMA і MasterCard планується створити центр, який об'єднає роботу національних операторів і платіжних систем. Так, абоненти зможуть перераховувати гроші зі своїх

мобільних рахунків, просто відіславши у сервісному SMS на сервер MasterCard номер телефону і банківського рахунку одержувача. Зняти переказану суму можна буде і у банку чи банкоматі із застосуванням пластикової картки MasterCard.

За допомогою нового проекту мобільні оператори і банки планують заробити на стрімкому зростанні світового ринку грошових переказів, який за даними Всесвітнього банку, з 2000 по 2006 роки збільшився удвічі: з 132 млрд. до 268 млрд. За прогнозами GSMA, проект дозволить до 2012 року вчетверо збільшити об'єм грошових переказів (до 1 трлн.) і збільшити приблизно удвічі кількість їх користувачів (мінімум – до 1,5 млрд. людей). Учасники проекту не виключають, що до нього приєднається й Україна.

В той же час, підтримуючи зазначений проект, його автори відмічають, що при його реалізації оператори можуть мати проблему підтримки безпеки мобе-банкінгу [13]. Останнє можна розглядати як посилку до прогнозу нової загрози національним і міжнародній безпеці у сфері економіки в умовах інформатизації, зокрема і у кримінологічному аспекті, як новий прояв кіберзлочинності.

За прогнозами експертів ООН, у недалекому майбутньому світова економіка зіткнеться, перш за все, з ростом економічної злочинності, пов'язаної із застосуванням прогресуючих у своєму розвитку фінансових схем і механізмів та сучасних технологій [6]. Стосовно конкретних прикладів такого прогнозу: FBI-2005 Computer Crime Survey повідомило, що тільки у 2005 році у США фірми зазнали збитків від кіберзлочинів на суму понад 67 млрд. дол. Протиправного впливу зазнали дев'ять з десяти організацій. За звітом британської дослідної компанії Get Safe Online у 2006 році, приблизно кожен десятий європеєць, який користується Інтернет, став жертвою кіберзлочинців.

Керівники британської галузі телекомунікації доповнюють, що від Інтернет-шахрайств у 2006 році стали потерпілими 3,5 млн. жителів Великобританії. Британські кримінологи зазначають, що свого часу резонансним і сенсаційним у світі було пограбуванні 2,5 млн. фунтів стерлінгів з поштового вагону потягу Глазго – Лондон. Нині вже "злочинами століття" не вважають такі як: привласнення 500 млн. дол. (Роберт Максвел, керівник групи державних компаній); 450 млн. дол. (Ейзіл Нейдір, глава компаній Polly Peck); 10 млн. фунтів стерлінгів (за повідомленням директора Bank Commerse International) [10].

У контексті економічної безпеки стосовно інформаційного впливу на масову свідомість учасників електронної економіки пропонується звернути увагу на те, що дослідники компанії Gartner підрахували, що тільки вже традиційна онлайн-комерція в Америці у 2006 році втратила 2 млрд. дол. через стурбованість користувачів стосовно безпеки здійснення електронних платежів. Ця стурбованість суспільства має підстави і зумовлює економічний інтерес держави до проблеми, хоча б з тієї позиції, що державний бюджет країн втрачає оперативність надходження податків із зазначеної сфери економічних правовідносин.

Як свідчать дослідження, з точки зору кримінологічного аспекту латентності кіберзлочинності у сфері економіки, технологія електронних міжбанківських фінансових трансфертних операцій може вважатися зі одну з найбільш тонких і частково "закритих" галузей для дослідження у контексті фінансових інтересів держави. І це природно, адже пов'язане, перш за все, з проблемами економічної державної політики щодо негативного ставлення державних правоохоронних органів до податкового і валютно-фінансового планування компаній (господарюючих суб'єктів). Конфлікт інтересів потребує юридичного вирішення.

В той же час у окремих випадках у контексті співвідношення корпоративних інтересів та інтересів держави банківські установи зацікавлені у дослідженні кримінологічних аспектів своєї діяльності, зокрема і у сфері розвитку електронного банкінгу. До них можна віднести такі, що пов'язані з антисоціальним, зокрема, криміногенним застосуванням електронних послуг злочинними організаціями. Особливе співвідношення інтересів людини, суспільства і держави виникає стосовно

причетності до фінансування тероризму чи завдають шкоди економічним інтересам банків, у тому числі їх іміджу "порядності". Це зумовлено тим, що світова корпорація банкірів зробила правильні висновки із терористичних актів, особливо тих, що були направлені на фінансово-економічні установи. Синдром стосовно міжнародного тероризму, під умовною назвою "Манхетен", створив певний імунітет у світових фінансових структурах до повної закритості міжнародної та національних банківських систем, особливо у тих, в яких присутній приватний капітал.

Перехід кіберзлочинцями "електронного державного кордону" на сьогодні не проблема. Основна парадигма глобального інформаційного суспільства, яке невпинно розвивається полягає саме в тому, що у світовому кіберпросторі просто не можливо визначити кордонів держав у радиційному змісті. При вчиненні міжнародних фінансових трансакцій переважно застосовується низка, так званих, проксі-серверів, "анонімайзерів" чи інші аналогічні системи в різних країнах. Застосовувати звичайні технології "паперового" контролю в умовах інформаційного суспільства однаково, що намагатися вичерпати річку за допомогою шаблі.

У світі особлива увага правоохоронців вже звертається на, так звані, нелегальні міжнародні віртуальні банки, що функціонують в системі Інтернет та мобільного телефонного зв'язку. Прикладом таких банків можна назвати "Havala" в Індії, "Fei chi'en" у Китаї та "Hundi" у Пакистані. Прототипами віртуального банку можна назвати такі як: Security First Bank або Mark Twain Bank у США.

Як приклад, в Росії були розкриті механізми розкрадання коштів із системи електронної торгівлі, а також попереджено створення шахрайських віртуальних підприємств в системі е-банкінгу. Суми збитку склали більше 800 тис. та 1200 тис. дол. США. збитки від "фрікерства", тільки у Москві за першу половину 1999 року завищили 100 млн. російських рублів.

До найбільш поширених типів злочину, що відомі як "інструменти першокласних банків", можна віднести торгові операції з нібито випущеними резервними акредитивами банків (Standbay Letters of Credit), гарантіями (Prime Bank Guarantees) та борговими зобов'язаннями (Prime Bank Notes).

Зловмисники, застосовуючи схему "інструментів першокласних банків", в більшості випадків, знаходять свої жертви серед категорій осіб, які через Інтернет шукають зручної можливості розмістити свої кошти як інвестиції та таких, яким необхідно отримати "гарячі" (швидкі, короткострокові, але і не відмовляються від середньострокових та довгострокових) інвестиції у формі кредитів. Останнім часом замість не завжди зрозумілих "гарантій та зобов'язань першокласних банків" та "резервних акредитивів" злочинці застосовують такі банківські інструменти, які дійсно існують на фінансових ринках. До них можна віднести "казначейські векселя"(Treasury Bills), "облігації" (Bonds), "депозитні сертифікати" (Certificates of Deposits), "акредитиви"(Letters of Credit), "переказні векселі"(Bills of Exchange) і т.ін.

Завдяки сучасним комп'ютерним інформаційним технологіям шахрайські оборудки отримали поширення на всіх континентах. Ця проблема стала транснаціональною. За підрахунками міжнародних експертів фінансових та правоохоронних органів, номінальна вартість "інструментів першокласних банків", що знаходяться в обороті, складає близько 5 трлн. дол. США. Фінансові та господарські суб'єкти, які емітували зазначені інструменти, виконувати зобовязання за ними ніколи не будуть і не збираються це роботи. При цьому "інструменти першокласних банків" мають і свій замаскований, "таємний" вторинний ринок обігу, до якого має доступ обмежене коло людей.

Співробітники правоохоронних органів мають справи, за якими криміналітетом застосовуються нібито фінансово-господарські операцій, які ускладнені, на перший погляд, неадекватними схемами: бартерні та вексельні, давальницькі та толінгові схеми, схеми взаємозаліків; застосування фінансових технологій фондового ринку; офшорних інструментів, у тому числі для незаконного отримання грошей з податку на додану вартість тощо.

Основною і центральною ланкою фінансових махінацій, шахрайств, відмивання “брудних” грошей у світовій економіці є можливості офшорних фінансових центрів та країн з перехідною економікою, особливо ті, де триває процес приватизації. У світі існує приблизно 48 регіонів, які можна вважати “податковим раєм”, але не всі вони є привабливими для криміналітету. Деякі країни знаходяться у важкодоступних регіонах, не мають систем інтернаціонального електронного зв’язку, в деяких діють обмеження на обсяг обміну валюти. В інших юрисдикціях прийнято суворе законодавство відносно декларації податків на доходи іноземних компаній.

Про масштаби офшорної діяльності свідчать дані про реєстрацію компаній у країнах і зонах, що надають сприятливі режими оподатковування доходів і майна. За числом офшорних компаній світовими лідерами вважаються: Антильські острови, Бермудські острови, Британські Віргінські острови, Кайманові острови, Кіпр, Ліхтенштейн. Так, до 1995 року на Британських Віргінських островах було зареєстровано понад 15 тис. офшорних компаній, приблизно, по одній на кожного жителя острова (примітно, що населення адміністративного центру Віргінських островів Рід Тауна складає 4 тис. чоловік). На Каймановых островах створено близько 25 тис. компаній. На островах Терксі і Кайкос зареєстровано понад 7 тис. офшорних компаній. У чому ж економічні переваги офшорної економіки?

Декілька прикладів таких переваг говорять самі про себе. На Бермудських островах щорічний дохід від більш ніж 6,5 тис. зареєстрованих компаній до середини 90-х років складав близько 25 % валового національного доходу (250 млн. дол.), а всі доходи від міжнародної фінансової діяльності складали близько 40 % валового внутрішнього продукту країни. У Ліхтенштейну дохід від зареєстрованих 40 тис. офшорних компаній складає близько 30 % бюджетних надходжень (реєстраційні та щорічні платежі). На Кіпрі до середини 90-х років від зареєстрованих 20 тис. офшорних компаній дохід щорічно складав приблизно 200 млн. дол. (до кінця 90-х років на Кіпрі вже було зареєстровано 28 тис. офшорних компаній). Приблизно такий же дохід Антильські острови одержують за рахунок 30 тис. зареєстрованих офшорних компаній.

Дослідниками у різних країнах відзначається бурхливий ріст банків та банківських відділень, страхових та перестрахувальних компаній, які створюються саме на офшорних територіях. Для прикладу, на Каймановых островах зареєстровано понад 500 офшорних банків, у тому числі відділення або дочірні банки мають 43 з 50 найбільших банків світу. За даними МВС України, тільки на острові Науру зафіксовано 36 ”українських” банків та 265 рахунків різних банків України.

Пропонується звернути увагу на інформаційну складову офшорного бізнесу. Розширення схем із застосуванням офшорних юрисдикцій в бізнесі дало можливість для збільшення переліку послуг. Якщо раніше власники офшорних компаній обмежувалися юридичною адресою для документів та номером факсу для підтримки зв’язку зі своїм центральним офісом, то тепер клієнти готові платити за “серйозність” статусу компанії. Досить популярним став, так званий, віртуальний офіс (номер телефону з автоматичним переадресуванням повідомлення в будь-яку країну або персональну телефонну лінію з електронним секретарем, автовідповідачем).

За таких обставин досвідченні махінатори, застосовуючи досягнення інформатики, уникають схем роботи через офшорні зони, які “засвітилися” перед світовою спільнотою з негативної сторони і які знаходяться під пильним контролем урядових органів країн. Для прикладу, свого часу активно застосовувалися офшорні зони прибалтійських країн. З 1999 року Латвія, Естонія та Литва, після входження до міжнародної організації Egmont Group, яка вже об’єднує контрольні служби 53 держав, змінили свою політику стосовно правил офшорного бізнесу. Традиційна схема типу “компанія в штаті Делавар з рахунком у прибалтійському банку” вже не підходить для тіньового бізнесу.

Як свідчать дослідження, основою фінансових зловживань із застосуванням можливостей офшорних зон, є міжнародні економіко-правові взаємовідносини закордонних і вітчизняних структур. Як правило, за кордоном створюється дочірня фірма чи умовно самостійна компанія. При цьому, наприклад, у статутних документах ряду холдингів вноситься застереження, що материнська структура не контролює фінансові потоки у дочірніх фірмах. Таким чином створюється "правова завіса" – що контроль за фінансовою діяльністю дочірніх фірм немовби відсутня. Крім того, за кордоном фінансові стосунки будуються на різного роду боргових операціях, у тому числі за міжнародними торгівельними контрактами, правовий інструментарій яких дуже широкий. Виявити дійсний зміст взаємовідносин та обсяги коштів які переказуються за угодами дуже важко. Різні форми забезпечення боргових зобов'язань, гарантії, депонування цінних паперів також роблять майже неможливим виявлення дійсних господарів вкладених коштів і реальних керівників таких оборудок.

Останнім часом дослідниками звертається увага на інтеграцію фінансових ринків із застосуванням глобальних інформаційних технологій, телекомунікації. При цьому зазначається про засоби застосування криміналітетом світової фінансової системи для відмивання "брудних" грошей на фоні створення спекулятивної економіки в глобальних масштабах, що дозволяють досягти швидкого переміщення валюти. Такий оборотний капітал з "брудних" грошей у вигляді венчурних інвестицій, бартеру тощо створює фінансову суміш різного походження, яка знаходиться в постійному, невпинному русі.

У порядку узагальнення, висновків та формування пропозицій стосовно удосконалення організації протидії кіберзлочинності, зокрема у сфері електронного банкінгу пропонується звернути увагу на наступне.

Стрімкий розвиток сучасних засобів електронної телекомунікації, створення нових можливостей здійснення міжбанківських і внутрішньобанківських операцій вимагають від державних контролюючих органів розробки нових правових заходів протидії, боротьби і запобігання фінансовим правопорушенням, у тому числі – "відмиванню" злочинно здобутих грошей, податкових порушень, шахрайства з фінансовими ресурсами та "втечі" національних капіталів за кордон.

Все більше кримінологів приходять до висновку: "Апелювати стосовно позбавлення від злочинності до поліцейських заходів і пенітенціарної політики – це все рівно, що за допомогою парасольки зупиняти дощ" [12]. Найкращий засіб протидії правопорушенням – це розробка на основі глибокої наукової підтримки удосконаленого інтегрованого адміністративного, цивільного, інформаційного та іншого галузевого законодавства, яке повинно бути зрозумілим для всіх учасників суспільних відносин за принципом: "законів повинно бути мало, але вони повинні бути якісними, змістовними". При цьому не повинно бути крайнощів: не "впихувати" нові сфери суспільних відносин у "старі" міхи традиційних провідних галузей законодавства.

Найкращим засобом протидії злочинності є її профілактика, яка ґрунтується на поглиблених постійних наукових дослідженнях з відповідною фінансовою підтримкою держави. У цьому контексті пригадується стародавня китайська мудрість: "Чому загинули дракони? Тому що у них голова не відповідала розміру тіла і вони не могли пристосуватися до змін природи їх існування".

Існує необхідність реалізації нових, креативних підходів. З числа багатьох існуючих, які були сформовані за результатами проведеного дослідження, пропонуються як першочергове наступне.

В Україні назріла необхідність створення спеціальної організаційної структури, яка б проводила ґрунтовний науковий моніторинг та прогноз нових загроз міжнародній та національній безпеці в умовах формування глобалізації інформаційного суспільства та економіки. Виходячи із обсягу функцій та організаційно-правових можливостей органів державної влади нашої країни

вбачається, що така структура повинна бути складовою у структурі Ради національної безпеки та оборони України.

Враховуючи міжгалузеву та міжвідомчу сутність протидії кіберзлочинності, особливо такої, що має ознаки організованої, пропонується, що у такій структурі повинні працювати фахівці з різних державних правоохоронних органів із різною освітою, у сфері інформатики, права, економіки тощо. При цьому такі фахівці повинні обов'язково мати аналітичні здібності і бути схильні до наукової роботи, а також мати навички її здійснення, а отже – й розуміння професійної мови фахівців різних сфер суспільної діяльності.

Основними функціями запропонованої структури повинні бути: здійснення моніторингу суспільних відносин пов'язаних із застосуванням сучасних комп'ютерних технологій; підготовка аналітичних матеріалів з прогнозами реальних та можливих загроз міжнародній та національній безпеці; методичних розробок протидії їм та пропозицій для органів державної влади стосовно проблем розвитку інформаційного суспільства.

Список використаних джерел

1. *Інформаційна* безпека: проблеми боротьби зі злочинами у сфері використання комп'ютерних технологій. – Запоріжжя: Просвіта, 2001

2. *Вступ* до інформаційної культури та інформаційного права. – Ужгород, 2003.

3. *Організована* злочинність в Україні: Наук. посіб. – К.: НАВСУ,1999.

4. *Ушаков Д.Л.* Оффшорные зоны в практике российских налогоплательщиков. – М.: Юрист, 1999.

5. *Сегодня*. – 2000. – 11 жовт.

6. *Комп'ютерна* злочинність. – К.: Атіка, 2002.

7. *Tokyo* Stock Exchange. 1991 Fact Book. – Tokyo, 1991. – P.80

8. *Intersec*. – 1999. – July/August/ – P. 236–238.

9. *Сандул І. В* мережі // Кореспондент. – 2006. – № 30. – С. 45.

10. *Интернет-новости* киберсекюрити <http://www.cyber security.ru>. (станом на 26.03.2007).

11. *Е-майбутнє* та інформаційне право. – К.: НДЦПІ АПрНУ, 2006. – С. 7.

12. Див.: Bottomley A. Criminology in focus. – N.Y., 1979. – P.158.

13. *Плахов А., Кутик М., Губарь Е.* Мобильные операторы метят в банкиры // Коммерсант. – 2007. – 13 февр. – № 22. – С.8; <www.komersant.ua>.

14. *Бутузов В., Гуцалюк М., Цимбалюк В.С.* Протидія злочинності у сфері високих технологій // Міліція України. – 2002. – № 9. – С. 20–21.

15. *Виявлення* та розслідування злочинів, що вчинюються з використанням комп'ютерних технологій. – К.: НАВСУ, 2000.

16. *Проблеми* боротьби зі злочинами у сфері використання комп'ютерних технологій. – Запоріжжя: ГУ "ЗІДМУ", 2002.

17. *Е-боротьба* в інформаційних війнах та інформаційне право – К.: НДЦПІ АПрН України, 2007.

18. *Психологічні* особливості організованих злочинних об'єднань (використання психологічних знань у протидії організованій злочинності) – К.: НАВСУ, 2002.

The article is examined some questions of the national security of Ukraine in criminological aspect of the strategy of creation and development of the information society on an example of such new sector of economy, as electronic banking.