remote banking systems (RBS). In many cases these traces allow us to establish the organizational scheme of crime.

The law enforcement agencies are building the international system of combating this type of crimes, they are creating methods of investigation of crimes of this category, they are strengthening cooperation with international institutions and law enforcement agencies of different countries (including via telecommunication means and systems). This makes topical further research on the development of innovative methods of detection and research of traces of crimes in the sphere of using of information technologies.

Key words: *special knowledge, computer crime, traces of the crime, information technology.*

УДК 343.1:351.746.3:004

О.В. Бочковий

СПІВВІДНОШЕННЯ БЕЗПЕКИ ГРОМАДЯН З ВРАЗЛИВІСТЮ ЗЛОЧИНЦІВ В УМОВАХ ІНФОРМАЦІЙНОГО ВІДКРИТОГО СУСПІЛЬСТВА

У статті висвітлено вплив сучасних інформаційно-технічних досягнень на безпеку суспільства та можливість злочинців уникнути відповідальності за протиправні діяння. Охарактеризовано основні переваги застосування інформаційно-аналітичних систем та можливості їх застосування правоохоронними органами, зокрема у мережі Інтернет, для виявлення та прогнозування злочинної діяльності. Доведено безпосередню залежність рівня безпеки суспільства від рівня його відкритості.

Ключові слова: *інформація, безпека, відкрите суспільство, інформаційна система, аналітична система, Інтернет, протидія, злочинність, права і свободи, оперативно-розшукова діяльність, прогноз.*

Постановка проблеми. Сучасний світ інформаційних технологій та всеохоплювальна інформатизація суспільства інтегрують кожного громадянина в мережу, хоче він того чи ні. База даних будь-якого підприємства чи організації міститься на електронних носіях, що передаються в державні органи та установи для обліку чи контролю. Від самого народження інформація про нового громадянина вноситься до бази даних і буде там знаходитися навіть після його смерті.

Звісно, що інформація про людину й раніше підлягала обліку в різноманітних органах чи установах. З кам'яних дощок у стародавні часи до карток табулятора в XX столітті змінювався лише носій інформації.

Автоматизація процесу обліку розпочалася з того, що 1804 року француз Жозеф Марія Жаккард винайшов прилад, який використовує перфоровані картки для контролю роботи ткацького верстата [1]. У 1889 р. Герман Голлеріт, син німецьких емігрантів, доопрацював перфокартковий механічний пристрій Ж.М. Жаккарда для обробки великого обсягу даних. Робота машини виявилася

настільки вдалою, що бюро перепису США використовувало її при обробці результатів перепису населення у 1890 році. Таку машину й для тих же цілей у 1897 році купила Росія. А 1902 року Г. Голлеріт створив табулятор, у якому картки подавалися автоматично.

Пізніше вже комп'ютерні технології дозволили звести воєдино величезний обсяг інформації. Проте початкова комп'ютеризація не змінила принцип процесу, адже інформація в сталому вигляді була перенесена з паперових носіїв на електронні. Спосіб обробки електронних носіїв інформації значно полегшив роботу, але сутність процесу не змінив.

Починаючи з кінця XX століття й до сьогодні нові розробки у сфері комп'ютерних технологій дозволяють вивести на якісно новий рівень роботу з обробки даних, що містяться у комп'ютерній мережі. Сучасні системи на підставі аналізу отриманих даних здатні прогнозувати дії чи події. Адже сучасні інформаційні системи можуть сформувати щодо запитуваного об'єкта інформаційне досьє з даними, які не тільки вносилися суб'єктом звернення (державним органом чи організацією), але й іншими суб'єктами свідомо чи навіть випадково. Є можливість отримувати інформацію про особу з таких джерел, як соціальні мережі Інтернет, включаючи фінансову історію та засоби відеоконтролю.

Сьогодні аналіз соціальних мереж рекомендується банками при вирішенні питання про видачу позики. У РФ Духовною академією аналізується інформація в мережі щодо абітурієнтів і, залежно від результату, вирішується питання про зарахування на навчання. Поширюється практика відділів кадрів багатьох приватних організацій щодо перевірки кандидата на посаду шляхом аналізу його профілю у соціальних мережах. Адже при зустрічі кандидат буде показувати себе з якнайкращого боку, часто приховуючи негативні сторони своєї особистості. Тоді як у соціальних мережах міститься інформація за тривалий проміжок часу і може показати різні сторони особистості, починаючи з друзів у мережі й закінчуючи відмітками (лайками) конкретних новин, фото чи перегляду відео тощо.

На жаль, в Україні не практикуються такі дослідження при розгляді кандидатури на зарахування в державні службовці чи співробітники МВС. Більше того, теорія оперативно-розшукової діяльності, утім як і практика, ігнорують сучасні інформаційно-технічні здобутки, залишаючи суспільство сам на сам зі злочинністю.

Не можна ігнорувати той факт, що сукупність даних, які можуть бути отримані за допомогою комп'ютерної мережі, робить особу абсолютно відкритою перед відповідними органами чи службовими особами, які матимуть повноваження для збору таких даних. Тобто, суспільство, у якому є довіра до відповідних служб, що здійснюють моніторинг мережі, може вважатися відкритим. Адже добропорядний громадянин, котрий є

членом відкритого суспільства, відкритий для компетентних органів так само як і особа, яка готує чи скоює злочин.

Таким чином, рівень безпеки суспільства прямо залежний від рівня його відкритості. Водночас, чим більше відкрите суспільство, тим більше вразливий злочинець, адже теж стає відкритий для правоохоронних органів.

Аналіз останніх досліджень і публікацій. Сучасний інформаційно-технічний прогрес зумовлює постійні дискусії серед науковців різних сфер, від технічних до соціально-гуманітарних наук. Не є винятком і юридична наука, адже правові відносини в інформаційній сфері потребують відповідного нормативного регулювання, а неправомірне використання інформаційних ресурсів потребує відповідної реакції правоохоронних органів. Саме тому для формування висновків та конкретних пропозицій не потрібно ігнорувати попередні наукові здобутки як теоретиків кримінального процесу, так і суміжних галузей знань. У кримінальному процесі та теорії ОРД окремі аспекти або суміжні питання цієї проблеми розглядали І.О. Воронов, Е.О. Дідоренко, О.Ф. Долженков, С.В. Єськов, В.П. Захаров, О.І. Козаченко, В.П. Крошко, Д.Й. Никифорчук, В.С. Овчинський, С.С. Овчинський, Ю.Ю. Орлов, В.Л. Ортинський, М.А. Погорецький, Б.Г. Розовський, Е.В. Рижков, В.Г. Самойлов, В.П. Столбовий, І.Ф. Хараберюш, О.М. Чистолінов, Г.О. Юхновець, В.І. Янушко й інші вчені.

Утім, злочинний світ швидко адаптується до рівня розвитку інформаційних технологій та пристосовує їх на свою користь, що потребує постійної роботи науковців та практиків для пошуку й розробки адекватних засобів та заходів протидії.

Формування цілей. Мета статті: висвітити вплив сучасних інформаційно-технічних досягнень на безпеку суспільства та можливість злочинців уникнути відповідальності за протиправні діяння. Довести пряму залежність рівня безпеки суспільства від рівня його відкритості.

Виклад основного матеріалу. Увесь світ поступово йде шляхом запровадження новітніх інформаційних технологій у правоохоронній сфері, основою яких є інформаційно-аналітичні системи. Так, в англійському журналі «Police» опублікована стаття про використання сучасних інформаційних технологій у роботі фінансових слідчих. На початку XXI століття практично кожна особа залишає за собою електронний слід інформації (наприклад, у Великій Британії загальна кількість баз даних, де громадяни можуть залишити електронний слід, становить близько трьохсот). Перед слідчими постає завдання зібрати дані з цих баз стосовно конкретної особи, потім відфільтрувати з цих відомостей такі, що відповідають параметрам розслідування, тобто, інакше кажучи, перевірити отриману інформацію стосовно більш широкого контексту розслідування для того, щоб звести воєдино всі відомості й провести аналіз, згідно з яким необхідно діяти надалі [2].

Англійські фахівці розробили новий комп'ютерний метод, який дозволяє ідентифікувати невідомі й таємні зв'язки між різними членами терористичних та кримінальних угруповань. Головною проблемою успішної реалізації великомасштабного кримінального розслідування є встановлення заплутаної системи відносин між тими, хто ймовірно може бути учасником кримінальної діяльності. Асоціативна модель даних AMD (Associative Model of Data), котра характеризується як перший великий прорив в архітектурі бази даних після появи Інтернету, дає можливість перекинути місток між розрізненими базами даних, забезпечуючи більші можливості для розслідування. Ця модель формує дані подібно до того, як ми мислимо, тим самим значно знижуючи потребу у великому обсязі програмування, дозволяючи користувачам звертатися за допомогою до комп'ютерів і одержувати відповідь на запит не протягом місяців, а протягом декількох годин.

На відміну від більшості баз даних, спроектованих так, щоб збирати вузькоспеціалізовану, суворо регламентовану інформацію (так звані структуровані бази даних), ця база даних побудована за принципом архівів даних. В архіви даних збирають усе, що вони можуть увібрати в себе, нічого не відкидаючи, тобто практично в одну базу даних збираються всі можливі інформаційні бази різних пошукових систем і банків даних, причому різних відомств і установ [3].

Досить сказати, що органи Національної поліції України щорічно реєструють більше 3 млн. подій, що мають ознаки злочину, і вже на первинному етапі обробляється інформація приблизно про 3,8 млн осіб, у тій чи іншій мірі причетних до вказаних у заявах фактів. Розслідується близько півмільйона кримінальних проваджень. Адміністративні протоколи складаються стосовно майже 6 млн. осіб. Декілька мільйонів громадян, які перебувають на обліку в оперативно-довідковій картотеці МВС, підлягають безперервному моніторингу. Тільки нормативними документами МВС регламентується функціонування 17 інформаційних баз даних [4, с. 219–228].

Правоохоронні органи зарубіжних країн широко використовують автоматизовані інформаційно-пошукові системи, які дозволяють значно оптимізувати розкриття та розслідування злочинів, учинених членами організованих угруповань [5, с. 57]. Але сучасні темпи обміну інформацією та загальний ритм життя, зокрема й злочинний, змушує постійно вдосконалювати методи та способи роботи з масивами даних, що безперервно зростають. У цьому процесі незамінними помічниками є інформаційно-аналітичні системи, основною перевагою яких є аналіз та прогнозування.

До 2014 року така інформаційно-аналітична система діяла в ГУМВС України в Луганській області. Сам збір необхідної інформації в системі та її аналіз здійснюються в межах типових моделей, розроблених загальною теорією пізнання, криміналістикою і наукою ОРД. Але будь-яка типова модель формується з урахуванням минулого досвіду і являє собою в

узагальненому вигляді те, що десь колись було. А життя не стоїть на місці, злочинці виносять уроки з поразок, програючи правоохоронним органам, та освоюють нові прийоми й форми протиправної діяльності. Тому під час збирання й аналізу оперативно-розшукової інформації робиться постійна поправка на динамічність досліджуваних процесів, можливість появи нових організаційних форм злочинних об'єднань, удосконалення старих і розробку нових прийомів протидії проведенню ОРЗ і розслідування в цілому.

Завдяки відпрацьованим технологіям за 9 місяців 2010 року тільки три співробітники одного з підрозділів УІТ УМВС в Луганській області (відділу «ОРІОН») розкрили 297 тяжких і особливо тяжких злочинів, розслідування яких традиційними методами виявилося невдалим (розслідування було припинено у зв'язку з невстановленням винного). Серед них – вбивства (зокрема подвійні), розбійні напади, грабежі, торгівля зброєю, тяжкі наркозлочини тощо. При цьому нерідко первинна інформація про злочинців спочатку взагалі відсутня в інформаційних масивах – сама система була безпосереднім джерелом нової інформації про осіб [6, с. 10–12].

Для реалізації вказаних завдань програмісти УІТ розробили та впровадили в практику такі спеціалізовані системи, як «СОВА», принциповою відмінністю якої є здійснення на практиці можливості інтеграції в єдиний інформаційний масив усіх наявних в УІТ УМВС відомчих інформаційних ресурсів (зокрема, масиви даних оперативно-розшукової діяльності) і бази даних інших відомств.

Крім того, потрібно розуміти, що можливості сучасних інформаційно-аналітичних систем у державному інформаційному просторі є неповними. Адже залучення до процесу обробки даних інформаційного простору глобальної мережі Інтернет дозволяє значно розширити потенціал автоматизованих систем з більшими можливостями виявлення, а основне – прогнозування злочинної діяльності.

Більше того, новітні технології дають змогу активно та продуктивно протидіяти транснаціональній злочинності за рахунок відсутності кордонів у глобальній мережі. Значно полегшується взаємодія та обмін даними між правоохоронними органами різних країн. Приміром, розшукуваний злочинець може бути встановлений шляхом застосування однієї з програм ідентифікації особи за фото чи відео зображенням. Такий досвід уже практикується окремими зарубіжними державними та приватними відомствами [10, 11, 12].

Для підтвердження значущості та необхідності застосування інформаційно-аналітичних систем для забезпечення відкритості суспільства та забезпечення його безпеки підкреслимо декілька їх специфічних якостей. Перше: немає необхідності доводити, що, крім усіх інших переваг, ІІАС має ще й могутній потенціал додаткових гарантій захисту прав і свобод законослухняних громадян. Система дозволяє ще на попередньому етапі відсіяти зайве, уникнути необґрунтованих підозр у скоєнні злочину значної частини осіб, на яких

через випадковий збіг обставин падає така тінь. Скорочується необхідність у допиті як свідків громадян, що не володіють, як потім з'ясовується, необхідною інформацією. Скорочуються, нарешті, витрати часу оперативних працівників, слідчих і, відповідно, терміни розслідування.

Друга важлива якість – інтегровані інформаційно-аналітичні системи дозволяють поставити на достовірно наукову основу методологію розслідування злочинів, перетворити в реальність основоположний принцип усебічності розслідування, що повсюдно не реалізується. Наприклад, у кожному підручнику проголошується вимога перевірки всіх версій, що висуваються в справі. І за загальним правилом версії, повністю або не дуже, перевіряються. Але перевіряються версії, що висуваються. А сам процес висунення версій неминуче обмежений первинною інформацією. Здебільшого вона вельми мізерна, дозволяє робити лише типові гіпотетичні прогнози.

Використання сучасних технологій створює можливість підтвердити не тільки відсутність у момент події осіб, на яких падає тінь, але й присутність тих, хто з будь-якої причини не потрапив у поле зору свідків чи не закарбувався в їх пам'яті, проте викликає оперативний інтерес. Накопичений у системі масив інформації про криміногенні установки, зв'язки, пересуваннях певних осіб створює можливість висунути версію про причетність до злочину, якщо навіть за допомогою свідків і технічних засобів не була зафіксована їх присутність у момент його здійснення.

Нарешті, у банку даних системи накопичується інформація, що працює як на користь висунутої версії, так і на її спростування. Суперечність виявляється на першій стадії аналізу. Програма обмежує суб'єктивізм слідчого. Одночасно в системі чітко фіксується час надходження інформації, що дозволяє відокремити суб'єктивні нашарування в тлумаченні події свідком.

Третя перевага – з використанням ІІАС криміналістика і наука оперативно-розшукової діяльності одержують новий напрям розвитку. Якщо раніше процес розслідування йшов від злочину до злочинця, то нині з'являється можливість будувати стратегію інакше – від злочинця до злочину.

Традиційно латентними вважалися довершені злочини, коли в процесі розслідування особу, винну в їх вчиненні, встановити було неможливо. Як свідчать і теорія, і практика, чималий відсоток довершених злочинів, зокрема тяжких, взагалі не виявляється. Причини різні – від ретельного маскування діяння до залякування або знищення осіб, від яких повинно було надійти повідомлення про довершений злочин. До цього треба також додати злочини, за якими через різні, здебільшого не зовсім об'єктивні причини, кримінальні справи, навіть за наявності заяви, не порушуються.

Накопичувані бази даних і відповідне програмне забезпечення дозволяють прогнозувати можливість скоєння злочину конкретною особою, вживати заходи для його попередження і припинення, а якщо

такі зусилля даремні – виявляти та розслідувати його по гарячих слідах. Розробки таких програм ведуться в США і деяких країнах Європи, відповідний науковий потенціал є і в Україні.

Четверта перевага – інтегровані інформаційно-аналітичні системи створюють можливість більш плідно реалізувати суворівський принцип: «Здивувати, приголомшити, перемогти».

П'ята – впровадження принципово відмінних від існуючих методик безконтактного проведення розслідування з реальними особами до завершального його етапу. За цілою низкою категорій злочинів, що розслідуються, використання інформаційно-аналітичних технологій не вимагає наявності заяви потерпілого, проведення ревізій у традиційному їх розумінні, допиту свідків для відображення, наприклад, процедури проходження бухгалтерських документів. Звідси неминуче повинен відбутися перегляд деяких на нині існуючих постулатів теорії та практики доказування. Скажімо, процесуальне закріплення використання як доказ відповідним чином оформлених результатів інформаційно-аналітичної (комп'ютерної) розвідки дозволить спростувати необхідність вилучення і залучення до кримінальної справи значного обсягу бухгалтерських документів, що разом з відмовою від проведення бухгалтерської ревізії не тільки скоротить терміни слідства, але й не створюватиме перешкод у діяльності суб'єкта господарювання, що перевіряється [7, с. 313–324].

Але важливо враховувати й зворотний бік відкритості суспільства. По-перше, очевидно, що чим більше можливостей отримати інформацію про особу, яка цікавить правоохоронні органи, чим більше джерел таких відомостей, тим краще. З іншого боку, громадяни зацікавлені в реалізації права на особисте життя. Сьогодні у світі спостерігається спотворення уявлень про права і свободи людини та громадянина. Навіть в умовах підвищеної небезпеки тероризму відбувалися виступи проти посилення правил догляду пасажирів і багажу при авіаперевезеннях, хоча всім очевидно, що йшлося про захист життя людей [8, с. 20].

Правомірність отримання, зберігання і обробки інформації, яка являє собою оперативний інтерес, у цих умовах у багатьох країнах світу, зокрема й Україні, викликало активне неприйняття з боку правозахисників. Тому регламентація правоохоронної діяльності на законодавчому і нормативному рівнях постійно вдосконалювалась. За роки незалежності в нашій країні сформовано практично нове законодавство у сфері інформації та інформатизації. Держава вдосконалює існуючу та розробляє нову нормативно-правову базу інформаційних відносин.

Основу загального правового регулювання інформаційного забезпечення ОВС становлять законодавчі акти вищої юридичної чинності загальнодержавного значення, у яких закладено фундаментальні поняття

цього виду діяльності. До таких основ насамперед належить Конституція України [9, ст. 141].

Варто зауважити, що відомості про об'єкти обліку, які зберігаються в інформаційних масивах оперативних підрозділів ОВС, є захищеною законом таємницею, що підтверджено рішенням Конституційного Суду України у справі щодо офіційного трактування статей 3, 23, 31, 47, 48 Закону України «Про інформацію» і статті 12 Закону України «Про прокуратуру» від 30 жовтня 1997 року. Пункт 2 цього рішення говорить: «частину п'яту статті 23 Закону України «Про інформацію» розуміти таким чином, що кожна особа вправі знайомитися із зібраною у відношенні неї інформацією в органах державної влади, органах місцевого самоврядування, установах і організаціях, якщо ці відомості не є державною або іншою захищеною законом таємницею».

Водночас інформація, що міститься в мережі Інтернет, є у публічному доступі й користувачі самостійно її туди поміщають, усвідомлюючи, що вона може бути переглянута сторонніми особами. Тобто, знову ж немає підстав твердити про порушення чиїхось прав чи особистих інтересів.

Таким чином, за наявності достатніх підстав поліція має право збирати, зберігати й поширювати інформацію, включаючи конфіденційну і таку, яка підпадає під спеціальні режими регулювання, що стосується всіх об'єктів кримінальної реєстрації. Неодмінними умовами для залучення таких відомостей в інформаційні процеси повинні бути, по-перше, гарантоване дотримання режиму таємності, а по-друге, відповідність правовим підставам.

Особливого значення досліджувані питання набувають сьогодні, коли криміногенна ситуація в Україні віддзеркалює тенденцію до збільшення кількості звернень громадян про кримінальні події. Отже, маємо значне зростання навантаження на працівників оперативних підрозділів ОВС, що разом з проблемами кадрового забезпечення, накопиченими протягом останніх років, тільки ускладнює кризу правоохоронної системи [8, с. 9].

Висновки. Таким чином, можна стверджувати, що перелік нових видів та напрямів застосування інформаційних технологій у правоохоронній діяльності постійно зростає, множаться способи і засоби боротьби з новими проявами злочинної діяльності, крім того, набувають специфічного розвитку форми, що вже існували. Серед них – оперативна розвідка, що традиційно розглядалася як один із видів негласної роботи. Вона, по суті, має позачасовий характер і продовжує застосовуватися, незважаючи на присутність певних негативних морально-етичних її оцінок не тільки в широких верствах населення, але й серед співробітників правоохоронних органів. Проте в сучасних умовах набуває все більшої актуальності, має високу результативність порівняно новий напрям оперативної розвідки – розвідка інформаційно-

аналітична, у подальшій локалізації іменована розвідкою комп'ютерною. Її потенціал максимально повно використовується в боротьбі зі злочинними діяннями, що реалізовуються за допомогою Інтернету.

Підсумовуючи, зазначимо, що масиви інформації, які постійно зростають щодо конкретної особи та суспільства в цілому разом з розвитком інформаційних технологій та способів обробки такої інформації неминуче призводить до прозорості соціальних зв'язків, навіть якщо такі зв'язки та відносини суспільно небезпечні. Генеральна мета – прогнозування можливості скоєння злочину в певний час у визначеному місці, виявлення латентних злочинів. Завдання цілком реальне, адже практичні підходи до його вирішення вже розробляються.

Використані джерела:

1. История компьютера. [Електронний ресурс]. – Режим доступу: http://chernykh.net/content/view/14/38/. – Назва з екрана.

2. Police. – 2001. – September. – P. 24–27. Выявление преступников с помощью информационных технологий // Борьба с преступностью за рубежом. Информбюллетень. – М : ВИНИТИ, 2003. – № 6. – С. 25.

3. Police. – 2002. – October. - P. 11–12. Раскрытие преступных связей с помощью компьютерной программы // Борьба с преступностью за рубежом. Информбюллетень – М. : ВИНИТИ, 2004. – № 6. – С. 11.

4. Задорожний Ю. А. Информационные технологии в ОРД: опыт и проблемы или проблемы и опыт? / Ю. А. Задорожний, Б. Г. Розовский // Вісник Луганського державного університету внутрішніх справ імені Е.О. Дідоренка. – 2011. – № 4. – С. 219–228.

5. Хірсін А. В. Удосконалення автоматизованих інформаційно-пошукових систем, які використовуються у боротьбі з організованою злочинністю / А. В. Хірсін // Право України. – 2004. –№ 6. – С.55–60.

6. Інформаційно-аналітичне забезпечення оперативно-розшукової діяльності: монографія / [В. А. Буржинський, М. Г. Вербенський, В. С. Гуславський та ін.]. – Луганськ : РВВ ЛДУВС ім. Е.О. Дідоренка, 2009. – 110 с.

7. Бочковий О. В. Роль і місце автоматизованих систем в інформаційно-аналітичному забезпеченні прийняття рішень про проведення оперативно-розшукових заходів, що тимчасово обмежують конституційні права громадян / О. В. Бочковий // Вісник Луганського державного університету внутрішніх справ імені Е.О. Дідоренка. Спеціальний випуск. - 2011. – № 4. – С. 313–324.

8. Гуславский В. С. Информационно-аналитическое обеспечение раскрытия и расследования преступлений : монография / В. С. Гуславский, Ю. А. Задорожный, Б. Г. Розовский. – Луганск : Элтон-2, 2008. – 287 с.

9. Конституція України [Електронний ресурс] // Відомості Верховної Ради. – 1996. – №30. – Ст.141. – Режим доступу : zakon.rada.gov.ua/go/254к/96-вр. – Назва з екрана.

10. Поиск человека по фотографи – это реальность [Електронний ресурс]. – Режим доступу : http://softopirat.com/main/399-poisk-cheloveka-po-fotografii-yeto-realnost.html. – Назва з екрана.

11. По фото в соцсети можно узнать о человеке все! [Електронний ресурс]. – Режим доступу : http://3rm.info/publications/13829-po-foto-v-socseti-mozhno-uznat-o-cheloveke-vse.html. – Назва з екрана.

12. Создана программа для поиска человека в Интернете по фото [Електронний ресурс]. – Режим доступу : http://zhzh.info/blog/2011-11-13-3096. – Назва з екрана.

Бочковой А.В. Соотношение безопасности граждан с уязвимостью преступников в условиях информационного открытого общества

В статье освещается влияние современных информационно-технических достижений на безопасность общества и возможность преступников избежать ответственности за противоправные деяния. Характеризуются основные преимущества применения информационно-аналитических систем и возможности их применения правоохранительными органами, в том числе и в сети Интернет, для выявления и прогнозирования преступной деятельности. Доказывается прямая зависимость уровня безопасности общества от уровня его открытости.

Ключевые слова: *информация, безопасность, открытое общество, информационная система, аналитическая система, Интернет, противодействие, преступность, права и свободы, оперативно-розыскная деятельность, прогноз.*

Bochkovyi O.V. Relationship to public safety criminals vulnerability in an information society open

The article highlights the impact of modern information and technological advances on the security of society and criminals evade responsibility for wrongful acts. After all, the modern world of information technology and integrate comprehensive informatization of society every citizen in the network, he wants to or not. The database of any company or organization contained in electronic media that are transferred to public authorities and institutions to account or control. From the birth of a new citizen information entered into a database and will be in there even after his death.

Since the end of the twentieth century to the present new developments in computer technology enable to bring a new level to work with data contained in a computer network. Modern systems, based on an analysis of the data are able to predict the actions or events. Indeed, modern information systems can form requested object information on file with data that not only were made the subject of an appeal (state authority or organization) but also other subjects intentionally or even accidentally. It is possible to obtain information about a person from social sources such as the Internet, including financial history and video surveillance equipment.

We can not ignore the fact that the set of data that can be obtained through a computer network makes the person completely open to the relevant authorities or officials who have the authority to collect such data. That is, a society in which there is trust in the relevant services that monitor network may reckon open. For

good citizen who is a member of an open society, open to the competent authorities as well as the person who prepares or commits a crime.

Characterized main benefits of information-analytical systems and their possible use by law enforcement agencies, including the Internet, for the detection and prediction of criminal activity.

Thus, the security level of society directly depends on its level of openness. At the same time, the more open society, the more vulnerable a criminal, too, is open to law enforcement.

Key words: *information security, open society, information system, analytical system, Internet access, opposition, crime, law and freedom of operational-search activity, prognosis.*

УДК 343.233

І.М. Калабашкін

ПРОТИДІЯ ОРГАНІЗОВАНІЙ ЗЛОЧИННОСТІ ЗАСОБАМИ КРИМІНАЛЬНОГО ПРАВА

Статтю присвячено передбаченим у Кримінальному кодексі України засобам протидії організованій злочинності, серед яких особливу роль відіграє норма, що заохочує до дій з попередження чи розкриття злочинної діяльності організованої групи чи злочинної організації, зокрема, виконання спеціального завдання з попередження чи розкриття злочинної діяльності організованої групи чи злочинної організації. Досліджено генезу норми Кримінального кодексу України про виконання спеціального завдання. Проаналізовано порядок, підстави та характер виконання спеціального завдання з попередження чи розкриття злочинної діяльності організованої групи чи злочинної організації у зв'язку із прийняттям Кримінального процесуального кодексу України. Вивчено суб'єкти, уповноважені вводити до організованих злочинних угруповань співробітників під легендою прикриття.

Ключові слова: *засоби кримінального права, оперативно-розшукова діяльність, виконання спеціального завдання, організована група, злочинна організація, організоване злочинне угруповання.*

Постановка проблеми. Із загостренням кризових явищ у суспільному та економічному житті нашої держави, збільшенням навантаження на правоохоронну систему внаслідок залучення особового складу до забезпечення проведення Антитерористичної операції, потраплянням значної кількості зброї та засобів ураження в нелегальний обіг посилилися детермінанти організованої злочинності. Вказане зумовлює необхідність вивчення наявних правових засобів протидії цьому явищу для визначення їх ефективності та особливостей застосування.

Аналіз останніх досліджень і публікацій. Проблеми правового забезпечення протидії організованій злочинності досліджено в роботах широкого кола вітчизняних учених, серед яких О.М. Литвак, Ю.В. Абакумова, Ю.В. Мантуляк, Н.Є. Міняйло, О.М. Бандурка та інші, проте не всі правові засоби про-