УДК 343.2/.7:004(419)

С.В. Шапочка,
магістр права, начальник Управління підвищення кваліфікації державних службовців Всеукраїнського центру підвищення кваліфікації державних службовців і посадових осіб місцевого самоврядування Національного агентства України з питань державної служби

МІЖНАРОДНІ СТАНДАРТИ З КІБЕРБЕЗПЕКИ ТА ДОСВІД БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ І КІБЕРШАХРАЙСТВОМ

У статті проаналізовано міжнародні норми і стандарти з кібербезпеки, досвід боротьби з кіберзлочинністю та кібершахрайством у зарубіжних країнах, ефективність роботи спеціалізованих підрозділів та взаємодії з громадськістю, рівень та форми міжнародного співробітництва, нескоординованість дій правоохоронних органів з іншими суб'єктами протидії кіберзлочинності, основні етапи формування законодавства у сфері боротьби з кіберзлочинами, проблеми уніфікації міжнародного законодавства, а також запропоновано заходи запобігання злочинам, що вчиняються з використанням комп'ютерних мереж взагалі та кібершахрайства зокрема.

Ключові слова: *кібербезпека, кіберзлочинність, кібершахрайство, запобігання кібершахрайству.*

В статье проанализированы международные нормы и стандарты по кибербезопасности, опыт борьбы с киберпреступностью и кибермошенничество в зарубежных странах, эффективность работы специализированных подразделений и взаимодействия с общественностью, уровень и формы международного сотрудничества, нескоординированность действий правоохранительных органов с другими субъектами противодействия киберпреступности, основные этапы формирования законодательства в сфере борьбы с киберпреступностью, проблемы унификации международного законодательства, а также предложены меры предотвращения преступлений, совершаемых с использованием компьютерных сетей вообще и кибермошенничества в частности.

Ключевые слова: *кибербезопасность, киберпреступность, кибермошенничество, предупреждение кибермошенничества.*

Paper analyzes international norms and standards on cybersecurity, the experience of combating cybercrime and cyber fraud in foreign countries, the effectiveness of specialized units and interaction with the public, the level and forms of international cooperation, the uncoordinated actions of law enforcement agencies with other participants in countering cybercrime, the main stages in the formation of legislation in the sphere of struggle against cybercrime, the issues of unification of the international law as well as it suggests measures to prevent crimes committed by using computer networks in general and with cyber fraud in particular.

Keywords: *cybersecurity, cybercrime, cyber fraud, cyber fraud prevention.*

Україна визначилась і демонструє неухильне дотримання зовнішнього вектору розвитку, спрямованого на всесвітню економічну, політичну, культурну, релігійну

інтеграцію та уніфікацію, включення в процес злиття окремих національних ринків у один всесвітній ринок – економічну глобалізацію, інтеграцію в процеси забезпечення колективної, в тому числі кібернетичної безпеки держави, боротьби з кіберзлочинністю та кібертероризмом, запобігання шахрайству, що вчиняється з використанням комп'ютерних мереж – кібершахрайству.

Водночас законодавство України у сфері боротьби з кіберзлочинністю нині є ще недосконалим та потребує уніфікації з урахуванням результатів випереджувальної еволюції країн-лідерів, їх досягнень та міжнародного досвіду, а також запиту суспільства на зміни.

Разом з тим, тенденції до поширення й масштаби кіберзлочинності та її соціально-небезпечні наслідки викликають серйозне занепокоєння міжнародного співтовариства, спонукаючи до вдосконалення, трансформації норм, що регулюють суспільні відносини в кіберпросторі.

Проведенням наукових досліджень окремих аспектів щодо боротьби зі злочинами, що вчиняються з використанням мережі Інтернет взагалі та шахрайства зокрема, займаються такі вчені, як І.Г. Богатирьов, В.М. Бутузов, В.В. Василевич, В.Д. Гавловський, О.М. Джужа, Д.О. Зиков, А.А. Комаров, О.Є. Користін, В.Д. Ларичев, А.К. Лебедєв, О.В. Лисодєд, А.В. Микитчик, О.В. Смаглюк, К.В. Тітуніна, С.С. Чернявський, В.І. Шакун, О.М. Юрченко та інші.

У попередніх наукових публікаціях ми вивчали різні аспекти шахрайства, що вчиняється з використанням можливостей мережі Інтернет як у контексті охорони конституційних прав громадян, так і захисту національної безпеки України, а також були вироблені заходи протидії такій діяльності. Ця стаття є логічним продовженням нашого дослідження.

Кіберзлочинність як сукупність кіберзлочинів (комп'ютерних злочинів) – суспільно небезпечних винних діянь у кіберпросторі та(або) з його використанням, відповідальність за які передбачена законом України про кримінальну відповідальність та(або) які визнані злочинами міжнародними договорами України [1], є відносно новим явищем в Україні, яке швидко прогресує, але його характер і особливості в різних країнах практично не мають істотних відмінностей; етапи та зміст процесу становлення кримінально-правової системи боротьби з кіберзлочинами в різних країнах практично повторюється [2]. А кібербезпека – захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних й потенційних загроз національній безпеці України у кіберпросторі [1], є пріоритетом діяльності країни.

При цьому, розвиток Інтернет-технологій, глобальної, локальних мереж та систем дозволили підняти на новий інтернаціонально-континентальний рівень торговельно-економічні відносини і електронну комерцію, змінюються, зміцнюючись, і позиції транснаціональної злочинності, набуваючи нових рис, необмежених можливостей [3, с. 63].

Для запобігання кібершахрайству, що зростатиме з поширенням та подальшим розвитком сфери використання інформаційних технологій, створюючи таким чином умови для протиправної діяльності як окремими особами, так і злочинними групами, необхідне постійне міжнародне співробітництво, вивчення та врахування міжнародного досвіду, законодавства у цій сфері. Експерти зазначають, що Україна – дуже важливий центр хакерства, поряд із Росією, Бразилією, Китаєм, Індією.

Україна, з її низьким рівнем обізнаності про загрози використання комп'ютерів і низьким рівнем інформаційної безпеки, стає для злочинців справжнім

полігоном. Розкрадання коштів у системах Інтернет-банкінгу, даних кредитних карт, DDoS атаки на сайти, шахрайство в інформаційних мережах, інсайдерські витоки інформації стають повсякденним явищем. Недостатня кількість державних експертів у сфері комп'ютерно-технічної експертизи, складнощі з уведенням у правове поле досліджень фахівців комерційних організацій є питаннями, що потребують вирішення невідкладно.

Контроль та боротьба з означеним видом злочину як частини кіберзлочинності на рівні окремої держави малоефективні, адже однією з характерних ознак шахрайства з використанням комп'ютерних мереж є відсутність територіальних обмежень у реалізації злочинної діяльності. Так, Л.А. Остапенко зазначає, що: "наддержавний характер глобальних мереж об'єктивно вимагає розвитку міжнародно-правового регулювання в цій галузі. У глобальному інформаційному просторі кримінально-правова політика кожної держави безпосередньо впливає на кримінологічну ситуацію в цілому. Присутність у глобальних мережах національних сегментів, у яких не криміналізовані певні дії, призводить до активного "освоєння" злочинцями цих сегментів" [4, с. 179].

Отже, важливу роль під час запобігання шахрайству з використанням комп'ютерних мереж у правоохоронній діяльності відіграє міжнародна взаємодія. У. Зібер розглядає шість основних етапів формування законодавства про боротьбу з кіберзлочинами, прийнятого в різних країнах, починаючи з 1970-х рр.: "a) захист даних і захист недоторканності приватного життя; b) кримінальне законодавство про боротьбу з економічними злочинами, пов'язаними з використанням комп'ютерів; c) захист інтелектуальної власності; d) захист від протизаконного і шкідливого контенту; e) кримінально-процесуальне законодавство; f) правове регулювання захисних заходів, таких як криптографія і вимоги відносно аутентифікації" [5, п. 37].

У ст. 23 Конвенції про кіберзлочинність Рада Європи встановлює загальні принципи міжнародного співробітництва, за якими сторони співпрацюють у кримінальних розслідуваннях шляхом застосування відповідних міжнародних документів, угод, укладених на основі міжнародних норм, національного законодавства, з метою розслідування або переслідування кримінальних правопорушень, пов'язаних із комп'ютерними системами і даними, або з метою збирання доказів у електронній формі, які стосуються кримінальних правопорушень" [6]. Реакцію міжнародного співтовариства щодо розвитку кіберзлочинності проілюстровано в таких міждержавних угодах, як: Бангкокська декларація з попередження злочинності та кримінального правосуддя (2005 р.), Бухарестська декларація про міжнародне співробітництво в боротьбі з тероризмом, корупцією і транснаціональною організованою злочинністю (2006 р.), Всесвітній саміт з інформаційного суспільства та Конвенції Ради Європи "Про кіберзлочинність" (2001 р.) [7; 8; 9]. У цих документах йдеться про спільне протистояння кіберзлочинності шляхом прийняття відповідних законодавчих актів, які не будуть суперечити законам окремої держави та договорам, які ратифікувала ця держава [10].

У свою чергу, О. В. Манжай [11, с. 126–127] слушно зазначає, що базовими нормативно-правовими актами міжнародної взаємодії в боротьбі зі злочинністю є багатосторонні договори (конвенції), наприклад, Мінська конвенція 1993 року, з урахуванням вимог якої розроблено низку національних підзаконних нормативно-правових актів.

Аналіз національного законодавства України з питань запобігання кіберзлочинності й вчинення кібершахрайства дозволяє стверджувати про те, що законо-

давець певною мірою визначив основні поняття, запобіжні заходи з профілактики та протидії злочинності в кіберпросторі.

Водночас законодавство повинно корелювати з сучасним рівнем розвитку технологій, а пріоритетом є організація взаємодії і координація зусиль правоохоронних органів, спецслужб, судової системи, їх інформаційне та ресурсне забезпечення [10].

На нашу думку, міжнародний досвід використання засобів запобігання кібершахрайству, юрисдикції суб'єктів такої діяльності на прикладах окремих країн є достатньо важливими для дослідження.

Так, О.А. Баранов констатує, що США, гостро відчуваючи проблему кіберзлочинності, намагаються побудувати розгалужену систему боротьби з нею [2]. У ФБР створено Центр кіберзлочинів і оцінки загрози інфраструктурі (Computer Investigation and Infrastructure Threat Assessmtnt Centr), який отримав широкі повноваження з контролю за найбільш чутливими складовими інформаційної інфраструктури держави: фінансовою системою, телефонною мережею, управлінням рухом, управлінням енергосистемою тощо.

У Федеративній Республіці Німеччина (ФРН) боротьбу з кіберзлочинністю здійснює: Федеральна кримінальна поліція; Національний центр по боротьбі з кіберзлочинністю при Федеральному агентстві з інформаційних технологій, головним завданням якого є координація діяльності державних органів у боротьбі з кіберзлочинністю та використання новітніх технологій у боротьбі з кібератаками [13]. З метою координації профілактичної діяльності в багатьох країнах створені відповідні органи – національні ради, основними функціями яких є:

– збір інформації, планування, виконання та оцінка програм профілактики злочинів;

– координація діяльності поліції та інших органів, що працюють у цій сфері, забезпечення участі населення, співробітництво зі ЗМІ;

– науково-дослідна робота, навчальна підготовка тощо.

Поліція ФРН запровадила адресну роботу превентивного характеру із громадськістю, орієнтовану на самозахист, що здійснюється шляхом безкоштовних консультацій населення, як за допомогою технічних засобів уберегти від злочинців майно, не стати жертвою злочину.

У США використовуються такі моделі превентивної діяльності: громадських установ, безпеки індивідуума та впливу через навколишнє середовище.

У Канаді широко використовується участь громадян у превенції злочинів, знижуючи страх перед злочинцями, підтримуючи відчуття особистої безпеки.

Уся ця діяльність дістає моральну й матеріальну підтримку суспільства й держави [12, с. 60–61]. Слід підкреслити, що в цьому випадку частина культурно-виховних запобіжних заходів здійснюється саме правоохоронними органами, котрі активно взаємодіють з громадянами, що без сумніву позитивно впливає на зниження показників злочинності, а також на рівень довіри суспільства до результатів правоохоронної діяльності.

Директор Європейського поліцейського офісу (Європол) Роб Уайнрайт визнав, що проблема кіберзлочинності набула глобального масштабу, а збитки від діяльності кібершахраїв сягнули десятків мільярдів доларів. Незважаючи на віртуальність злочинів, збиток вони завдають цілком справжній. За деякими оцінками, через кіберзлочинців щорічно світова економіка втрачає 114 млрд дол. При цьому США оцінили свої збитки за всі роки існування глобальної мережі у 400 млрд дол., що у три рази більше щорічних витрат на освіту" [10].

У Великій Британії боротьбу з кіберзлочинністю здійснюють відділ по боротьбі з кіберзлочинами, що входить до складу Агентства по боротьбі з організованою злочинністю, який взаємодіє з відповідними підрозділами ФБР; Поліцейський національний відділ по боротьбі зі злочинами у сфері високих технологій (Police National E-Crime Unit) з координуючими функціями [13].

Проведене вище дослідження системи суб'єктів запобігання кібершахрайству дає можливість визначити такі напрями розвитку:

– створення експертно-криміналістичних установ, підрозділів у правоохоронних органах для проведення своєчасних експертиз за державний рахунок у справах про запобігання кібершахрайству та іншим злочинам у кіберпросторі;

– розвиток підготовки державних та приватних експертів з досліджень економічної сфери, комп'ютерних технологій, програмування тощо, котрі будуть проводити й моніторинг тенденцій злочинності в кіберпросторі, аналіз статистичної інформації;

– організація взаємодії і координація зусиль правоохоронних органів, спецслужб, судової системи, громадських організацій, центрів підготовки спеціалістів з боротьби з кіберзлочинністю задля зниження рівня злочинності, підвищення поваги та довіри до правоохоронців (окремими засобами при цьому мають бути активна діяльність ЗМІ, участь громадян у превентивних заходах);

– забезпечення суб'єктів запобігання вчиненню кібершахрайства необхідними ресурсами, технічними засобами для проведення запобіжних заходів різного характеру, що відповідатимуть технологічному прогресу;

– на державному рівні організація і врегулювання діяльності Міжвідомчого центру по боротьбі з кіберзлочинністю відповідального за координацію діяльності державних органів у цій сфері та використання новітніх технологій у протидії з кібератакам.

Дослідження шляхів удосконалення системи суб'єктів запобігання кібершахрайству нерозривно пов'язане з пошуком напрямів розширення системи запобіжних заходів.

Зазначимо найбільш конструктивні запобіжні профілактичні засоби, котрі ефективно використовує міжнародне співтовариство.

Так, у країнах ЄС виділяють два рівні профілактики злочинів: соціальний і ситуаційний. Соціальна профілактика спрямована на зміну несприятливих умов формування особистості людини, особливо мікросередовища й мікросоціальної ситуації. Ситуаційна виходить із того, що окремі категорії кіберзлочинів учиняються за певних обставин, у певний час і певних місцях.

У ФРН виділяють первинну, вторинну і третинну превенцію. Первинну спрямовано на подолання дефіциту соціальності й позитивної правосвідомості як головної причини злочинів. Вторинна здійснюється поліцейськими органами й пов'язана із правовими засобами втримання від учинення злочинів. Третинна превенція – це ті профілактичні заходи й засоби, що застосовуються у процесі покарання та ресоціалізації злочинців [12, с. 60, 61]. Отже, профілактика кіберзлочинів починається з використання організаційно-виховних запобіжних заходів. На наш погляд, вдалим є приклад ФРН, котрий демонструє взаємодію громадян із патрульними, що є одним із засобів ситуативної профілактики злочинів.

Також слід удосконалювати взаємодію правоохоронних органів з іншими державними органами. Наприклад, відповідно до Концепції Державної програми інформаційно-телекомунікаційного забезпечення правоохоронних органів, діяльність яких пов'язана з протидією злочинності, планується створити систему, що сприятиме істотному вдосконаленню інформаційної взаємодії правоохоронних та

інших державних органів у сфері протидії злочинності, поліпшенню координації їх діяльності, забезпеченню спільного формування та використання інформаційних ресурсів для ефективної протидії злочинності, здійсненню аналітичної, статистичної та управлінської діяльності у сфері захисту конституційних прав та свобод людини і громадянина від злочинних проявів як найбільш небезпечної загрози державній безпеці України.

А тому перспективними напрямами розвитку інформаційних технологій суб'єктів боротьби з кіберзлочинністю взагалі та кібершахрайством зокрема є :

– створення єдиного інформаційно-аналітичного комплексу як інтегрованої системи інформаційних ресурсів підтримки оперативно-службової діяльності, підвищення спроможностей з протидії кіберзлочинності;

– розробка автоматизованої системи проведення оперативно-розшукових заходів у телекомунікаційних мережах загального користування з автоматизованим проведенням окремих оперативно-технічних заходів та негласних слідчих (розшукових) дій;

– розвиток ідеї використання автоматизованих робочих місць спеціаліста (криміналіста, слідчого, детектива, дільничного тощо), що інтегрується до інформаційної системи;

– впровадження дистанційної системи підготовки та перепідготовки персоналу [14, с. 159–160].

З огляду на позитивний зарубіжний досвід, доцільно вдосконалювати заходи запобігання кібершахрайству шляхом:

– упровадження профілактичних засобів запобігання кіберзлочинності та кібершахрайству за рахунок ситуативної профілактики у вигляді організації співпраці поліції з громадянами;

– формування та врегулювання програмних документів щодо взаємодії правоохоронних органів та інших державних органів у сфері протидії кіберзлочинності шляхом створення автоматизованої інтегрованої інформаційної системи, що включатиме аналітичні, статистичні ресурси, пошукові системи, бази даних про злочинців та правопорушників;

– створення єдиного комплексу заходів на основі міжнародної взаємодопомоги в розслідуванні кіберзлочинів, виявленні, закріпленні та вилученні комп'ютерної інформації, її передачі іншій державі, а також у наданні сприяння при проведенні транскордонного обшуку в комп'ютерних мережах, з метою використання в кримінальному судочинстві як доказів після відповідного документування і копіювання комп'ютерної інформації [15, с. 289].

Дослідження ефективності та результативності міжнародного співробітництва правоохоронних та судових органів України в боротьбі з кіберзлочинністю та кібершахрайством дає право стверджувати про недостатню врегульованість законодавством цієї діяльності.

Позаяк міжнародне співробітництво – це ресурс позитивного досвіду запобігання кібершахрайству, доцільно навести думку науковців К.К. Горяінова, В.С. Овчинського, Г.К. Синилової [16] про те, що така співпраця у сфері боротьби зі злочинністю може здійснюватись в основних формах:

– надання взаємної правової допомоги з кримінальних справ;

– видача фізичних осіб, що вчинили злочини, для притягнення до кримінальної відповідальності або виконання вироку;

– передача засуджених до позбавлення волі для подальшого відбування покарання в державі їх громадянства або постійного місця проживання;

– обмін оперативною, правовою або іншою інформацією;

– виконання доручень з міжнародного розслідування;

– забезпечення прав і свобод громадян одної держави під час здійснення кримінального правосуддя в іншій;

– підготовка персоналу, обмін досвідом роботи правоохоронних органів різних держав у боротьбі із міжнародною кіберзлочинністю;

– надання експертних та консультативних послуг, спеціальних науково-технічних засобів та здійснення іншої ресурсної допомоги;

– спільне вивчення проблем злочинності та боротьби з нею, прогнозування та програмування цієї діяльності;

– участь у конгресах, нарадах, семінарах, симпозіумах, науково-технічних конференціях з проблем міжнародного співробітництва у запобіганні злочинності.

Аналіз міжнародного досвіду, норм і стандартів має супроводжуватися внесенням конструктивних змін до законодавства України, його уніфікації у взаємодії з міжнародним співтовариством. Координація реалізації заходів запобігання кібершахрайству, що здійснюється державами міжнародного співтовариства, є необхідною для забезпечення оперативного ефективного реагування на соціально-небезпечні наслідки розвитку комп'ютерних технологій. За оцінками вітчизняних і зарубіжних фахівців, розв'язання проблем попередження і розслідування кіберзлочинів – це складне завдання для правоохоронних органів через недостатній рівень обміну міжнародним досвідом та міжнародної співпраці в цій сфері [17].

З огляду на характеристики кібершахрайства – високий рівень латентності, необмежені часом і простором можливості, динамічно зростаючу кількість нових способів учинення [17, с. 334, 335] тощо, а також невідповідність законодавства викликам та потенційним й реальним загрозам, нескоординованість дій правоохоронних органів з іншими суб'єктами протидії кіберзлочинності дозволяють злочинцям уникати кримінальної відповідальності та покарання, ускладнюють їх переслідування.

Таким чином, ефективна протидія кібершахрайству можлива лише за умови узгодженої взаємодії та єдності, реалізації спільної кримінальної політики, удосконалення законодавства, налагодження міжнародного співробітництва [18, с. 73].

Позаяк жодна людина, компанія чи держава одноособово не здатні повною мірою ефективно боротися з кіберзлочинністю та кібершахрайством, а лише можуть досягати спорадичних результатів – міжнародна конструктивна взаємодія, гармонізація та уніфікація законодавства України, країн Європейського Союзу, спільне проведення розслідувань кіберзлочинів, пошук кіберзлочинців тощо може забезпечити виконання міжнародним співтовариством концепції та свого "обов'язку захищати", будучи не пасивним власником певних прав, а активним суб'єктом дії.

Отже, актуальність запобігання кібершахрайству залишається незмінною, а дослідження цього питання – доречним, на часі нині та буде перспективним у майбутньому.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про основні засади забезпечення кібербезпеки України: Закон України від 19 червня 2015 р. № 2126а. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=55657 (дата звернення 10.07.2017).

2. *Баранов О.А.* Кримінологічні проблеми комп'ютерної злочинності. URL: http://www.bezpeka.com/ru/lib/spec/crim/art71.html (дата звернення 12.07.2017).

3. *Shapochka S.* Preventing Fraud Using Computer Networks. Internal Security. 2013. № 2. P. 63–75.

4. *Осипенко Л.А.* Борьба с преступностью в глобальных компьютерных сетях: международный опыт. Москва, 2004.

5. Организация Объединенных Наций. Одиннадцатый Конгресс Организации Объединенных Наций по предупреждению преступности и уголовному правосудию. Семинар-практикум: Меры по борьбе против преступлений, связанных с использованием компьютеров: справочный документ. Док ООН. A/TONF. 203/14.

6. Конвенція про кіберзлочинність / Рада Європи; Конвенція, Міжнародний документ від 23.11.2001. Офіційний вісник України. 2007. № 65, стор. 107, стаття 2535, код акту 40846/2007.

7. Бангкокська декларація ООН "Взаємодія та заходи у відповідь: стратегічні союзи в сфері попередження злочинності і кримінального правосуддя" від 25 квіт. 2005 р. URL: http://www.un.org/russian/events/11thcongress/ bangkok_decl.pdf (дата звернення 03.07.2017).

8. Бухарестская декларация о международном сотрудничестве в борьбе с терроризмом, коррупцией и транснациональной организованной преступностью/ URL: http://www. un. org/ru/documents/decl_conv/declarations/ bucharest_decl. shtml (дата звернення 05.07.2017).

9. Всесвітній саміт з інформаційного суспільства та Конвенції Ради Європи "Про кіберзлочинність" (2001 р.). URL: http://www.itu.int/net/wsis/index.html (дата звернення 17.07.2017).

10. Кіберзлочинність в Україні. Соціальна мережа науковців. URL: http://www.science-community.org/uk/node/16132 (дата звернення 24.07.2017).

11. *Манжай О.В.* Нормативно-правова база здійснення оперативно-розшукових заходів шляхом використання кіберпростору. Право і безпека. № 2 (34). 2010. С. 122–128.

12. *Миронюк Т.В.* Превентивна та віктимологічна профілактика міжнародний аспект. Віктимологічна профілактика окремих видів злочинів: тези доповідей круглого столу. (Київ, 29 квітня 2014 року); ред. кол. О.М. Джужа, В.В. Василевич, Т.Л. Кальченко та ін. Київ: Нац. акад. внутр. справ, 2014. 215 с.

13. *Манжай О.В.* Досвід Великобританії, ФРН та КНР. Навчально-тренувальний центр боротьби з кіберзлочинністю та моніторингу кіберпростору на громадських засадах. Офіційний веб-сайт. URL: http://cybercop.in.ua/index.php/naukovi-statti/80-naukovi-statti/201-dosvid-velikobritaniji-frn-ta-knr (дата звернення 18.07.2017).

14. *Безруков Д.В.* Інформаційні технології в діяльності органів внутрішніх справ: поняття, напрямки використання, перспектива. Протидія кіберзлочинності в фінансово-банківській сфері : матеріали Всеукр. наук.-практ. конф., м. Харків, 23 квіт. 2013 р., МВС України, Харк. нац. ун-т внутр. справ; Незалеж. асоц. банків України, Харк. банк. Союз – регіон. представник НАБУ. Харків: ХНУВС, 2013. 286 с.

15. *Волеводз А.Г.* Противодействие киберпреступлениям: правовые основы международного сотрудничества. Москва: ООО "Издательство "Юрлитинформ", 2001. 496 с.

16. Теория оперативно-розыскной деятельности: учеб.; под ред. К.К. Горяинова, В С. Овчинского, Г.К. Синилова. Москва: ИНФРА-М., 2007. 832 с.

17. *Шапочка С.В.* Кримінологічна характеристика шахрайства, що вчиняється з використанням комп'ютерних мереж. Боротьба з організованою злочинністю і корупцією (теорія і практика). 2011. № 2–3. С. 329–336.

18. *Шапочка С.В.* Методологічні засади криміналістичної кібернетики. Науковий вісник Національної академії внутрішніх справ. 2012. № 3. С. 65–77.

Отримано 09.10.2017