Соціально-правові студії. 2018. Випуск 2. С. 40-47
Social Legal Studios. 2018. Issue 2. P. 40-47

UDC (УДК) 004.056.53:351.746.2

Живко Зінаїда Богданівна,
доктор економічних наук, професор,
завідувач кафедри менеджменту
Львівського державного університету внутрішніх справ
e-mail: professor2007@ukr.net
ORCID ID: 0000-0002-4045-669X
Scopus Author ID: 36070249600
Researcher ID: E-9344-2016

Рудий Тарас Володимирович,
кандидат технічних наук, доцент,
професор кафедри інформатики
Львівського державного університету внутрішніх справ
e-mail: tarasrudyy@gmail.com
ORCID ID: 0000-0002-4106-4313

Сеник Володимир Васильович,
кандидат технічних наук, доцент,
завідувач кафедри інформатики
Львівського державного університету внутрішніх справ
e-mail: v.v.senyk@gmail.com
ORCID ID: 0000-0002-0428-6443

ТЕХНОЛОГІЇ КРИМІНАЛЬНОГО АНАЛІЗУ У ПРАКТИЦІ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

Анотація. Розглянуто нормативно-правові чинники, які становлять правову основу засад протидії кіберзлочинності, ідентифіковано проблему протидії кіберзлочинності.

Виокремлено базові елементи реалізації інформаційно-аналітичної діяльності, якими є інформаційно-аналітичні системи – системи зв'язку та трансмісії даних, інформаційна інфраструктура, бази даних правової інформації, технічні, програмні, лінгвістичні, організаційні засоби.

Здійснено аналіз стратегії застосування сучасних систем кримінального аналізу підрозділами Національної поліції України та реалізація моделі поліцейської діяльності керованої аналітикою «Intelligence Led Policing».

Ключові слова: кіберзлочин, правова інформація, кримінальний аналіз, інформаційно-аналітична діяльність.

Zhyvko Zinaida,
Doctor of Science in Economics, Professor,
Head of Department
Lviv State University of Internal Affairs
e-mail: professor2007@ukr.net
ORCID ID: 0000-0002-4045-669X
Scopus Author ID: 36070249600
Researcher ID: E-9344-2016

Rudyy Taras,
Candidate of technical sciences, Associate Professor
Professor of the Department of Informatics
Lviv State University of Internal Affairs
e-mail: tarasrudyy@gmail.com
ORCID ID: 0000-0002-4106-4313

Senyk Volodymyr,
Candidate of technical sciences, Associate Professor
Head of Department of Informatics
Lviv State University of Internal Affairs
e-mail: v.v.senyk@gmail.com
ORCID ID: 0000-0002-0428-6443

TECHNOLOGIES OF CRIMINAL ANALYSIS IN THE PRACTICE OF COUNTERING CYBERCRIME

Abstract. The normative-legal factors that form the legal basis of the principles of combating cybercrime are considered, the problem of cybercrime counteraction was identified.

There are a number of problems related to state policy in the sphere of cyber security, organization, interaction and coordination of the work of law enforcement agencies, development of modern systems of information and analytical support, automated tools of criminal analysis that work in real time.

The information-analytical activity as a special direction of information activity, connected with the detection, processing, preservation and dissemination of information in the field of management is outlined. The instrumental content of information and analytical activity in the management system is clarified by defining the content of informational and analytical support for the activities of the units of the National Police of Ukraine.

The application of technologies of information-analytical activity and corresponding informational-analytical systems in the constant regime of functioning of the units of the National Police of Ukraine on combating cybercrime will allow to structure existing information resources and use them as models of consolidated information.

The urgent need for reorganization and improvement of methods of counteracting cybercrime is substantiated. One of the fundamental approaches regarding the use of modern technologies in the field of combating cybercrime on a qualitatively new level and making optimal decisions at the same time is a criminal analysis.

The basic elements and means of realization of information-analytical activity are information and analytical systems – data communication and data transmission systems, information and telecommunication infrastructure, databases of legal information, technical, software, linguistic, legal, organizational means are singled out. In spite of this, the technological platform of information-analytical systems allows to integrate and coordinate actions between different departments of the National Police of Ukraine.

The analysis of the strategy of using modern criminal analysis systems by the units of the National Police of Ukraine in the fight against cybercrime and the implementation of the model of police activity conducted by the analytics «Intelligence Led Policing».

Keywords: cebercrime, legal information, criminal analysis, informational and analytical activity.

DOI 10.32518/2617-4162-2018-2-40-47

Вступ

Сучасні загрози, обумовлені впливом комплексу політичних, соціально-демографічних, економічних, правових, соціоінженерних, технологічних чинників, вимагають системного реагування, адекватної трансформації як усього сектора безпеки, так і інформаційної та кібербезпеки зокрема, а також включення цієї системи у сферу політичних пріоритетів держави [1].

Під впливом сучасних глобалізаційних процесів, розвитку інформаційних технологій (ІТ), телекомунікаційних сервісів, цифрової економіки інформаційна та кібербезпека набувають самостійного, трансдержавного характеру.

Розвиток та безпека інформаційного і кіберпростору, запровадження цифровізації процесів управління, гарантування безпеки й сталого функціонування інформаційно-комунікаційних систем, державних інформаційних ресурсів мають бути складовими державної політики у сфері розвитку інформаційного простору та становлення інформаційного суспільства в Україні.

Досягнення у сфері ІТ створюють нові суспільні відносини, які стають предметом кіберзлочинів, що, своєю чергою, стимулює динаміку поширення кіберзлочинності та інцидентів у сфері захисту інформаційного та кібернетичного простору і щораз виходить за межі хоча б контролю з боку правоохоронних структур держави.

Аналізуючи кіберзлочинність, треба визнати, що більшість виявлених кіберзлочинів розпорошені у звітності різних підрозділів Національної поліції України і це не дає можливості провести комплексний аналіз та характеристику кіберзлочинності. Нещодавно

створено Управління кримінального аналізу Національної поліції для консолідації усіх розрізнених джерел оперативної інформації з подальшим глибоким аналізом, що повинно стати вагомим чинником у протидії кіберзлочинності.

Проблема протидії кіберзлочинності є предметом досліджень багатьох фахівців. Спершу потрібно зазначити низку військових науковців, зокрема: В. Бурячка, В. Хорошка, В. Толубка, С. Толюпу, фахівців Державної служби спеціального зв'язку та захисту інформації України – К. Пестова, В. Кравчука та інших.

Особливості організації протидії кіберзлочинності є предметом досліджень В. Хахановського, В. Цимбалюка, С. Демедюка І. Красницького. Вагомий внесок у розвиток теорії захисту інформації та інформаційної безпеки зробили В. Дудикевич, В. Максимович, О. Петров.

Питанням викликів та кіберзагроз, пов'язаних з розвитком цифрового світу присвячено праці Д. Фарбаніца [9] (2017), Дж. Луттгенса [10] (2017), М. Карпінського [11] (2016), А. Валика [9] (2016).

Аналіз останніх досліджень дав можливість виявити низку прогалин, які стосуються державної політики у сфері кібербезпеки, зокрема: низьку обізнаність державних діячів у сфері ІТ та їх небажання визнавати проблему; слабкість телекомунікаційного та інформаційного забезпечення держави; недостатність взаємодії і координування роботи правоохоронних органів; відсутність новітніх систем інформаційно-аналітичного забезпечення, автоматизованих інструментальних засобів кримінального аналізу, які працюють у режимі реального часу. Виокремлені недоліки ще потребують глибокого вивчення.

Актуальною залишається проблема недосконалості національного законодавства і відсутності єдиної правової бази правоохоронних органів у протидії кіберзлочинності.

З огляду на згадані обставини виникає необхідність у реорганізації та вдосконаленні методів протидії кіберзлочинності. Одним із таких методів щодо застосування сучасних технологій у сфері розкриття, розслідування злочинів та прийняття водночас найоптимальніших рішень став кримінальний аналіз.

Метою дослідження є аналіз стратегії застосування сучасних систем кримінального аналізу підрозділами Національної поліції України у протидії кіберзлочинності та реалізація моделі поліцейської діяльності керованої аналітикою «Intelligence Led Policing».

1. Аналіз нормативно-правових чинників, які становлять правову основу протидії кіберзлочинності

Інформаційні відносини є об'єктом правового регулювання, але розвиток ІТ, систем телекомунікацій відбувається швидше, ніж приймаються нормативно-правові акти, якими вони регулюються, що є причиною відповідної правової колізії [2, 3].

Законодавство України у безпековій сфері не визначає загальні фреймові (рамкові) підходи та визначення, а деталізує часткові, покрокові рішення. Це твердження цілком обґрунтоване і пояснюється низьким рівнем підготовки у галузі ІТ, теорії інформаційної та кібернетичної безпеки, і керівництва держави, політичних діячів, і конкретних виконавців, які займаються розробленням нормативно-правової бази, а найголовніше – відсутність загальнодержавного підходу до протидії кіберзлочинності [4].

Однак недавнім часом відбувся певний вимушений (зовнішній політичний вплив) поступ у сфері забезпечення інформаційної та кібербезпеки, зокрема, на інституційно-організаційному рівнях: у червні 2016 р. Президент України підписав Указ про створення Національного координаційного центру кібербезпеки (першим етапом його роботи є здійснення аналізу та розроблення галузевих індикаторів стану кібербезпеки); Указ Президента України № 47/2017 про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»; 5 жовтня 2017 р. Верховна Рада України приймає Закон України «Про основні засади забезпечення кібербезпеки України»; 17 січня 2018 року Кабінет Міністрів України затвердив урядову концепцію розвитку цифрової економіки в державі на 2018–2020 роки.

Такий стан справ зумовлює вагомі зміни у ставленні нашої держави до безпеки власного інформаційного та кіберпростору, а отже, і до посиленого захисту інформації, засобів її оброблення та кіберсередовища, в якому ця інформація циркулює, визначення об'єктів впливу, тобто до вжиття заходів зі забезпечення інформаційної та кібербезпеки [5].

Невизначеними у нормативно-правовому забезпеченні залишаються питання стосовно методології підходів до проблематики забезпечення інформаційної безпеки, що є технічною основою протидії кіберзлочинності. На перше місце слід поставити співвідношення понять «інформаційна безпека» та «кібербезпека». Українська наука чітко обґрунтувала необхідність розгляду національного сегменту кіберпростору як складової інформаційного простору

держави [4]. З цього випливає і логічність розгляду питань протидії кіберзагрозам у контексті забезпечення інформаційної безпеки [5].

2. Базові елементи реалізації інформаційно-аналітичної діяльності

Сталі режими функціонування підрозділів Національної поліції України (НПУ) з протидії кіберзлочинності не тільки зумовили збільшення обсягів інформації, які доводиться збирати, накопичувати, обробляти за визначеними алгоритмами, аналізувати і зберігати, а й необхідність забезпечення віддаленого доступу до масивів структурованої інформації та стратегічних інформаційних ресурсів. Застосування технологій інформаційно-аналітичної діяльності (ІАД) та відповідних інформаційно-аналітичних систем (ІАС) дозволить структурувати наявні інформаційні ресурси і використовувати їх як моделі консолідованої інформації.

Головним аспектом функціонування ІАС є переорієнтація з версій різних систем управління базами даних на вищий якісний рівень, який дає змогу виконувати аналітичні експертні дії. Робота ІАС ґрунтується на застосуванні методів, які забезпечать практичним працівникам НПУ можливість приймати об'єктивні рішення у проблемних ситуаціях і успішно застосовувати їх на практиці. У цю сукупність методів можна включити такі складові, як діагностика стану, інтерпретація даних, прогнозування, моніторинг.

У цьому зв'язку кожна ІАС створюється і розробляється з урахуванням таких обставин:

– одержання розрізнених даних з багатьох джерел одночасно (інформація накопичується у різних форматах і згодом підлягає приведенню до єдиної форми і об'єднання у певну структуру);

– акумулювання даних і створення масивів баз даних, використання технологій пошуку та індексації;

– для кожного з користувачів у режимі реального часу організовано надання необхідної інформації для прийняття рішень, виконання конкретних заходів, здійснення певних дій;

– інструменти інтелектуального і оперативного аналізу, підготовка регулярної та планової оцінки різних станів об'єктів управління;

– вся інформація і результати її аналізу подаються у строго впорядкованій формі для ефективного сприйняття даних користувачами усіх рівнів.

Вважаємо доцільним чітко окреслити інформаційно-аналітичну діяльність як особливий напрям інформаційної діяльності, пов'язаний з виявленням, опрацюванням, збереженням та поширенням інформації у сфері управління. Інструментальний зміст інформаційно-аналітичної діяльності у системі управління уточнюється через визначення змісту інформаційно-аналітичного забезпечення діяльності підрозділів НПУ.

Технології ІАД у відповідних структурах НПУ можна визначити як взаємозалежну та сформовану сукупність організаційних, правових, інформаційних, методичних, програмно-технічних компонент, які насамперед повинні забезпечити і супроводжувати прийняття управлінських рішень за рахунок раціонального використання інформаційних ресурсів та ІТ.

З поєднанням принципів проблемної орієнтації та програмно-цільової установки щодо тематики ІАД забезпечується вибірковість підготовки інформації та доведення її до керівників підрозділів НПУ відповідно до їх місця в системі управління. Управлінські структури як суб'єкти системи ІАД постійно взаємодіють із інформаційним середовищем, регулюють процес трансмісії даних, аналізують тенденції і на цій основі здійснюють супровід прийняття управлінських рішень, оптимального управлінського впливу.

ІАД повинна враховувати неоднорідність процесу прийняття управлінських рішень і специфіку діяльності керівників підрозділів НПУ всіх категорій на різних етапах процесу прийняття рішень.

Аналітична інформація повинна відповідати таким якісним характеристикам: цінність (корисність) – ступінь сприяння досягненню мети ініціатором запиту; точність – допустимий рівень модифікування інформації; достовірність – властивість інформації відтворювати реально існуючі об'єкти з заданою точністю; повнота – необхідний обсяг відомостей для прийняття виваженого та ефективного рішення; оперативність – актуальність, відповідність інформації поточному моменту; коректність – однозначність сприйняття інформації.

3. Сучасні системи кримінального аналізу та реалізація моделі поліцейської діяльності керованої аналітикою «Intelligence Led Policing»

За даними [6] ІАД ототожнюють з поняттям аналізу, визначаючи його як дослідницьку функцію в управлінні підрозділами, без якої науково організувати їхню діяльність неможливо. Проте це твердження є не зовсім правильним. Аналітична робота є діяльністю з дослідження інформації, у той час як аналізом є метод теорії пізнання, коли шляхом розумової діяльності ціле ділиться на частини. Відтак аналіз є одним з методів аналітичної роботи, тобто способом дослідження інформації, зокрема, у

сфері організаційно-аналітичної роботи у підрозділах НПУ.

Аналітик, спираючись на інформаційні моделі (відбитки в інформаційному просторі подій, фактів, дій, ідей, думок, почуттів людей, природних, політичних, соціальних, соціоінженерних, фінансових, економічних процесів тощо), виявляє об'єктивні закономірності і тенденції, визначає рушійні механізми та, що найголовніше, причинно-наслідкові зв'язки. У цьому змісті аналітик створює нове знання про той фрагмент реальності, який стосується його професійного інтересу, будучи дослідником своєї предметної області.

Управління кримінального аналізу Національної поліції України, властиво, створене з метою консолідації усіх розрізнених джерел оперативної інформації з подальшим глибоким аналізом для прийняття обґрунтованих, оптимальних стосовно критичних ситуацій управлінських рішень на усіх керівних рівнях, що повинно активувати оперативно-розшукову діяльність.

Отже, за визначенням керівника Управління кримінального аналізу НПУ, кримінальний аналіз – це мисленнєво-аналітична діяльність працівників правоохоронних органів, що полягає у перевірці та оцінці інформації, її інтерпретації, встановленні зв'язків між даними, що отримуються у процесі розслідування та мають значення для кримінального провадження, з метою їх використання правоохоронними органами та судом, подальшого проведення оперативного і стратегічного аналізу (на думку авторів ця дефініція кримінального аналізу притаманна особисто В. Єрофеєву).

На основі [7] подамо своє розуміння терміна кримінальний аналіз. Кримінальний аналіз є специфічним видом ІАД, яка полягає в ідентифікуванні та точному визначенні внутрішніх зв'язків між інформаціями (відомостями, даними), що стосуються злочину, і довільними іншими даними, отриманими з різних джерел, їх використанням в інтересах ведення оперативно-розшукової та слідчої діяльності, прийняття адекватних управлінських рішень на основі їх аналітичної підтримки.

З огляду на викладене виникла нагальна необхідність у реорганізації та вдосконаленні методів протидії кіберзлочинності. Одним із засадничих підходів стосовно застосування сучасних технологій у сфері протидії кіберзлочинності на якісно новому рівні та водночас прийняття оптимальних рішень є кримінальний аналіз.

Отже, від того, якою мірою підрозділи кримінального аналізу НПУ спроможні якісно аналізувати наявну інформацію і як результат надавати аналітичні продукти, які є підтримкою для прийняття адекватних кіберзагрозам управлінських рішень, залежить успіх виконання поставлених завдань.

Технології кримінального аналізу передбачають впровадження моделі поліцейської діяльності, керованої аналітикою «Intelligence Led Policing» (ILP) [7], як моделі, яка спрямована на підтримку, супровід інституційного управління та рішень посадових осіб на основі процесу аналізу інформації і даних.

Основні складові розвитку моделі ILP є такими: нормативно-правова база для врегулювання; інформаційні ресурси; система наповнення інформаційних ресурсів; система оцінювання джерел та достовірності інформації; спеціальне програмне забезпечення; інтегрування спеціалізованого програмного забезпечення з інформаційними ресурсами МВС та інших джерел інформації; тренінги для аналітиків практичних підрозділів НПУ; стандартизовані форми аналітичних продуктів.

Поліцейська діяльність, керована аналітикою, спрямована на ідентифікування і точне визначення взаємозв'язків між відомостями, які стосуються кіберзлочинів, осіб, пов'язаних з ними, та даними, що походять з різних джерел і їх використання кримінальними підрозділами НПУ

Розглянемо функції підрозділів кримінального аналізу НПУ [7] відповідно до моделі ILP:

Підрозділ кримінального аналізу ДІПКП «102»:

1. Координування діяльності.
2. Адміністрування доступу до інформаційних ресурсів.
3. Підготовка аналітичних продуктів.
4. Надання інформації за запитами ініціаторів.
5. Супроводження банків даних.
6. Організаційна, кадрова та методична робота.

Підрозділи кримінального аналізу ІПКП «102» регіональних органів:

1. Координування діяльності.
2. Адміністрування доступу до інформаційних ресурсів за територіальним принципом.
3. Підготовка аналітичних продуктів.
4. Надання інформації за запитами ініціаторів.
5. Організаційна робота.

Аналітики підрозділів оперативного та превентивного блоків:

1. Підготовка аналітичних продуктів.
2. Взаємодія з підрозділами кримінального аналізу ІПКП «102».
3. Організаційна робота.

Кримінальний аналіз передбачає, що результат ІАД повинен гарантувати достатній і сталий рівень забезпеченості аналітичними продуктами ініціаторів, що стосується кожного аспекту діяльності підрозділів кримінальної поліції у режимі реального часу. Також враховуються межі всіх значущих напрямів і весь реалізований комплекс заходів, здійснюваних у сфері протидії кіберзлочинності.

Основними елементами та засобами реалізації ІАД є ІАС – системи зв'язку та трансмісії даних, інформаційно-телекомунікаційна інфраструктура, бази даних правової інформації, технічні, програмні, лінгвістичні, правові, організаційні засоби. Згадані аспекти відтворені у статтях 25, 26, 27 Закону України «Про Національну поліцію» [8]. Своєю чергою, технологічна платформа ІАС дає змогу здійснювати інтегрування та координування дій між різними підрозділами НПУ.

За даними Д. Узлова, та В. Струкова інструментарій системи кримінального аналізу ґрунтується на математичних моделях і методах інтелектуального семантичного аналізу, візуального темпорального аналізу, аналізу поведінкового профілю, аналізу прихованих закономірностей.

Візуальний темпоральний аналіз базується на відтворенні та візуалізуванні хронології подій, які відбулися і тимчасове розмежування, що дає змогу оперативно виявляти приховані просторово-тимчасові закономірності між різними подіями.

Аналіз поведінкового профілю. Найпостійнішим і найточнішим з погляду психології злочинця є його поведінковий профіль. Він відображає багато параметрів діяльності злочинця – звичний спосіб вчинення злочину, місця скоєння та інші залежності, які сукупно відповідають одному профілю. Наявність різних поведінкових ознак з певною часткою ймовірності може свідчити про те, що цей суб'єкт може бути причетний до події. З цього принципу формується так званий груповий поведінковий аналіз. Безумовно, поведінковий профіль злочинця ніяк не може існувати без впливу на інших суб'єктів. Аналіз групового поведінкового профілю дає змогу визначати спільників без явних зв'язків між собою.

Аналіз прихованих закономірностей. Між особами, довільним чином причетними до правопорушення, об'єктивно існують зв'язки (родинні, за родом професійної діяльності, географічні – стосовно до місця проживання, місця відбування покарання тощо). Подібні зв'язки існують також між особами і подіями, а також між різними подіями. Такі зв'язки можуть бути явними, опосередкованими і прихованими. Крім того, група злочинів, скоєних однією і тією ж особою, обов'язково має певні характерні загальні риси, які явно не зафіксовані. Виявлення таких прихованих закономірностей з високою часткою вірогідності може встановити ідентифікаційні зв'язки між злочинцем і всіма скоєними ним злочинами.

У практиці кримінального аналізу розрізняють такі типи аналітичних продуктів:

1. Аналітичний звіт:

– сепарована інформація з внутрішніх і зовнішніх джерел;

– висновки;

– рекомендації, прогнози, настанови;

– додаткові матеріали (графіки, схеми, дані геолокації).

2. Профіль (досьє) особи, об'єкта ОЗГ:

– максимальний обсяг інформації на об'єкт аналізу у відповідності до запиту ініціатора.

3. Інформаційне зведення:

– оброблені табличні дані шляхом вибірки з баз даних за критеріями ініціатора.

4. Витяг інформації:

– вибірка інформації з баз даних за критеріями ініціатора.

Висновки

1. На думку авторів успішне реалізування та впровадження технологій кримінального аналізу дасть можливість активно використовувати ІАД, що сприятиме підвищенню ефективності протидії кіберзлочинності.

2. Від того, якою мірою підрозділи кримінального аналізу НПУ спроможні якісно аналізувати наявну інформацію і, як результат, надавати аналітичні продукти, які є підтримкою для прийняття адекватних кіберзагрозам управлінських рішень, залежить успіх виконання поставлених завдань.

Список використаних джерел

1. Стратегія розвитку системи Міністерства внутрішніх справ України до 2020 року. URL: https://www.cyberpolice.gov.ua/strategy-2020/.
2. Рудий Т. В., Сеник В. В., Рудий А. Т., Сеник С. В. Організаційно-правові, криміналістичні та технічні аспекти протидії кіберзлочинності в Україні. *Науковий вісник Львівського державного університету внутрішніх справ.* Серія юридична. Львів: ЛьвДУВС, 2018. Вип. 1. С. 283–301.
3. Рудий Т. В., Захарова О. В., Сеник В. В., Сеник С. В., Ізьо М. І. Організаційно-правовий супровід захисту інформаційних систем підрозділів національної поліції України на основі міжнародних стандартів.

Науковий вісник Львівського державного університету внутрішніх справ. Серія юридична. Львів: ЛьвДУВС, 2017. Вип. 2. С. 213–225.
4. Бурячок В. Л., Толубко В. Б., Хорошко В. О., Толюпа С. В. Інформаційна та кібербезпека: соціотехнічний аспект. К.: ДУТ, 2015. 288 с.
5. Проблеми чинної вітчизняної нормативно-правової бази у сфері боротьби з кіберзлочинністю: основні напрями реформування. Аналітична записка / Національний інститут стратегічних досліджень. URL: http://www.niss.gov.ua/articles/454/.
6. Єсімов С. С. Юридична природа інформаційно-аналітичної діяльності Національної поліції. URL: http://aphd.ua/publication-151/.
7. Кримінальний аналіз у діяльності НПУ. Концепції впровадження в Національній поліції України моделі поліцейської діяльності, керованої аналітикою «Intelligence Led Policing». URL: www.slideshare.net/NationalPolice/ss-75925350.
8. Про Національну поліцію: Закон України. *Відомості Верховної Ради України*. 2015. № 40–41. Ст. 379. URL: http://zakon3.rada.gov.ua/laws/show/580-19.
9. Farbaniec D. (2017). Cyberwojna. Metody działania hakerów. *E-book*. URL: https://helion.pl/ksiazki/cyberwojna-metody-dzialania-hakerow-dawid-farbaniec,cyberw.htm#format/d
10. Luttgens J., Pepe M., Mandia K. (2016). Incydenty bezpieczeństwa. Metody reagowania w informatyce śledczej. *E-book.* URL: https://helion.pl/ksiazki/incydenty-bezpieczenstwa-metody-reagowania-w-informatyce-sledczej- jason-luttgens-matthew-pepe-kevin-mandia,incbez.htm#format/d
11. Karpiński M., Raif P., Rajba S., Rajba T., Martsenyuk V. Wireless Sensor Networks with randomized parameters. ICCAS 2016: 16th International Conference on Control, Automation and Systems [publication Co-Chairs: Wonpil Yu, Shinsuk Park, Luis Gomes]: il. bibliogr., Institute of Control, Robotics and Systems (ICROS): HICO, Gyeongju, Korea, 2016. P. 1470–1475.
12. Balyk A., Karpinski M. (supervisor). Using Riverbed Modeler for DDoS attack simulation. *Inżynier XXI wieku* («Engineer of XXI Century» – the VI Inter University Conference of Students, PhD Students and Young Scientists: University of Bielsko-Biala, Poland, December 02, 2016). Bielsko-Biała: Wydawnictwo Naukowe Akademii Techniczno-Humanistycznej w Bielsku-Białej, 2016. P. 53–58.

References

1. Stratehiia rozvytku systemy Ministerstva vnutrishnikh sprav Ukrainy do 2020 roku [Strategy of development of the system of the Ministry of Internal Affairs of Ukraine till 2020]. URL: https://www.cyberpolice.gov.ua/strategy-2020 [in Ukr.]
2. Rudyy T. V., Senyk V. V., Rudyi A. T., & Senyk S. V. (2018). Orhanizatsiino-pravovi, kryminalistychni ta tekhnichni aspekty protydii kiberzlochynnosti v Ukraini [Organizational-legal, forensic and technical aspects of combating cybercrime in Ukraine]. *Naukovyi visnyk Lvivskoho derzhavnoho universytetu vnutrishnikh sprav.* Seriia yurydychna [*Scientific herald of Lviv State University of Internal Affairs. Legal Series*]. Lviv: LvDUVS, 1, 283–301 [In Ukr.]
3. Rudyy T. V., Zakharova O. V., Senyk V. V., Senyk S. V., Izo M. I. (2017). Orhanizatsiino-pravovyi suprovid zakhystu informatsiinykh system pidrozdiliv natsionalnoi politsii Ukrainy na osnovi mizhnarodnykh standartiv [Organizational and legal support for the protection of information systems of the units of the National Police of Ukraine on the basis of international standards]. In R. I. Blahuta (Ed.) *Naukovyi visnyk Lvivskoho derzhavnoho universytetu vnutrishnikh sprav (Scientific herald of Lviv State University of Internal Affairs)*. Seriia yurydychna. Lviv: LvDUVS, 2, 213–225 [In Ukr.].
4. Buriachok V. L., Tolubko V. B., Khoroshko V. O., & Toliupa S. V. (2015). Informatsiina ta kiberbezpeka: sotsiotekhnichnyi aspekt [Informational and cybersecurity: sociotechnical aspect]. V. B. Tolubka (Ed.). Kyiv: DUT, 288 [In Ukr.].
5. Problemy chynnoi vitchyznianoi normatyvno-pravovoi bazy u sferi borotby z kiberzlochynnistiu: osnovni napriamy reformuvannia [Problems of the current domestic normative-legal base in the field of combating cybercrime: the main directions of reform]. *Analitychna zapyska. Natsionalnyi instytut stratehichnykh doslidzhen (Analytical note. National Institute for Strategic Studies)*. URL: http://www.niss.gov.ua/articles/454/ [In Ukr.].
6. Iesimov S. S. (n. d.). Yurydychna pryroda informatsiino-analitychnoi diialnosti Natsionalnoi politsii [The legal nature of the information and analytical activities of the National Police]. URL: http://aphd.ua/publication-151/ [In Ukr.].
7. Kryminalnyi analiz u diialnosti NPU. *Kontseptsii vprovadzhennia v Natsionalnii politsii Ukrainy modeli politseiskoi diialnosti, kerovanoi analitykoiu «Intelligence Led Policing»* [*Concepts of the implementation of the Police Model in the National Police of Ukraine, managed by the analyst «Intelligence Led Policing»*]. URL: www.slideshare.net/NationalPolice/ss-75925350 [In Ukr.].

8. Pro Natsionalnu politsiiu: Zakon Ukrainy (2015). *Vidomosti Verkhovnoi Rady Ukrainy [Information from the Verkhovna Rada of Ukraine]*, 40–41. URL: http://zakon3.rada.gov.ua/laws/show/580-19 [In Ukr.].
9. Farbaniec D. (2017). Cyberwojna. Metody działania hakerów. E-book. URL: https://helion.pl/ksiazki/cyberwojna-metody-dzialania-hakerow-dawid-farbaniec,cyberw.htm#format/d [In Eng.].
10. Luttgens J., Pepe M., Mandia K. (2016). Incydenty bezpieczeństwa. Metody reagowania w informatyce śledczej. *E-book.* URL: informatyce-sledczej-jason-luttgens-matthew-pepe-kevin-mandia,incbez.htm# format/d [In Eng.].
11. Karpinski M., Raif P., Rajba S., Rajba T., Martsenyuk V. (2016). Wireless Sensor Networks with randomized parameters / ICCAS 2016: 16th International Conference on Control, Automation and Systems [publication Co-Chairs: Wonpil Yu, Shinsuk Park, Luis Gomes]: il. bibliogr., Institute of Control, Robotics and Systems (ICROS): HICO, Gyeongju, Korea, 2016, 1470–1475 [In Eng.].
12. Balyk A., Karpinski M. (supervisor) (2016) Using Riverbed Modeler for DDoS attack simulation. *Inżynier XXI wieku («Engineer of XXI Century» – the VI Inter University Conference of Students, PhD Students and Young Scientists*: *University of Bielsko-Biala, Poland, December 02, 2016*). Bielsko-Biała: Wydawnictwo Naukowe Akademii Techniczno-Humanistycznej w Bielsku-Białej, 2016, 53–58 [In Eng.].

Стаття надійшла 26 липня 2018 року
The article was received on July 26, 2018