It is concluded that the value of the criminal procedural proving is the following: its correct realization makes possible guaranteeing the rights and legitimate interests of all participants of the criminal proceedings on the basis of equality and issues that arise during criminal proceedings may be solved only on the basis of reliably established circumstances in the course of proving; participation of interested persons in the criminal proceedings while proving is a guarantee of realizing the principles of criminal process; evidence found during the investigation make grounds for the correct and objective procedural decisions in the criminal proceedings.

Keywords: proving, rights and legal interests, participants of criminal procedure, principles of criminal procedure.

УДК 341.1:343.346.8

С. В. Демедюк,
Т. С. Демедюк

МІЖНАРОДНИЙ ДОСВІД ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

Висвітлено проблемні питання, що розглядались на міжнародній науково-практичній конференції «Протидія кіберзлочинності» в Сінгапурі. Зокрема: відкриття та можливості Глобального Інноваційного комплексу; надання для тренінгів спеціалістів сфери протидії кіберзлочинності країн-учасниць Інтерполу модельних справ, розроблених Інтерполом; характеристика найбільш вразливих класичних операційних систем; створення інформаційного порталу TURN BACK CRIME.

Ключові слова: боротьба з кіберзлочинністю, зарубіжний досвід, правоохоронні органи, підготовка фахівців.

1–3 жовтня 2014 року в Сінгапурі відбулася міжнародна науково-практична конференція «Протидія кіберзлочинності» [1], у якій брала участь делегація від Національної академії внутрішніх справ та МВС України. Конференція була присвячена відкриттю Міжнародного Глобального Інноваційного кіберкомплексу, створеного за участі Інтерполу та Європолу. У рамках роботи цієї конференції було актуалізовано основні тренди протидії кіберзлочинності у загальносвітовому контексті.

Питаннями вивчення зарубіжного досвіду боротьби з кіберзлочинністю займалися О. М. Бандурка, А. В. Вінаков, А. В. Войціховський, М. Ю. Літвінов, О. В. Манжай, В. В. Марков, В. В. Носов, Д. Й. Никифорчук, Л. А. Осипенко, М. М. Перепелиця, В. В. Тулупов, В. Г. Хахановський та багато інших авторів.

Ця стаття має на **меті** проаналізувати висвітлені на конференції проблемні питання та шляхи їх подолання, а також запропонувати особливості імплементації останніх в Україні.

Означену конференцію було відкрито Генеральним секретарем Міжнародної організації кримінальної поліції (МОКП) Інтерполу Рональдом Ноблем (рис. 1).

Рис. 1. Відкриття конференції

На початку конференції Генеральний секретар Інтерполу представив майбутнього Генерального секретаря Інтерполу Юргена Штока, якого було обрано на засіданні в Ліоні для подальшого керівництва Інтерполом на наступні 6 років (рис. 2).

Рис. 2. Рональд К. Нобль та Юрген Шток

Натомість головною подією конференції стало відкриття Міжнародного Глобального Інноваційного комплексу (далі – Комплекс) (рис. 3, 4), створеного за участі Інтерполу та Європолу.

Рис. 3. Відкриття Міжнародного Глобального Інноваційного комплексу

Рис. 4. Генеральний секретар МОКП Інтерполу Рональд К. Нобль вітає з відкриттям Глобального Інноваційного кіберкомплексу виконавчого директора цього комплексу Нобору Накатані

У рамках цього комплексу запущено глобальний інформаційний портал Інтерполу, на якому будуть розміщуватись інформаційні матеріали, спрямовані на профілактику віктимної поведінки серед громадськості (журнали, фільми, залучення знаменитостей). Під час виступу Рональд К. Нобль висловив стурбованість із приводу того, що класичні злочини все частіше стають пов'язаними з кіберзлочинністю, яка не має кордонів, відстані, часу. Він заявив про зміну пріоритетів МОКП із супроводження розслідувань на профілактику.

Слід відмітити, що комплекс готувався на протязі 10 років, відтоді, як у 2004 р. в Катарі було прийнято відповідне рішення. Можливості комплексу передбачають:

– його використання під час проведення кримінальних розслідувань;

– модельні навчальні програми підготовки та підвищення кваліфікації фахівців у протидії кіберзлочинності;

– накопичення, обмін позитивним досвідом;

– координацію зусиль правоохоронних органів країн-учасниць МОКП під час проведення міжнародних операцій.

Серед іншого у рамках презентації комплексу було позитивно оцінено проведені правоохоронними органами України, США, Великобританії, Японії, Філіппін, Індонезії, Малайзії операції:

– «секс Торшн», в результаті якої затримано 56 осіб, ліквідовано 4 транснаціональні кримінальні угруповання;

– «Зевс», завданням якої було знешкодження міжнародної організованої злочинної групи, яка з метою викрадення фінансових реквізитів та доступу до банківських рахунків розповсюджувала шкідливе програмне забезпечення «Зевс». Під час операції знешкоджено інфраструктуру мережі, що включала понад 40 тисяч інфікованих комп'ютерів та серверів, левова частка яких знаходилась на території України. Спричинені збитки понад 300 мільйонів доларів. Члени організованого злочинного угруповання – хакери з Одеси та Харкова на чолі з громадянином Російської Федерації.

Цю ж тему підтримав заступник директора із стратегічного планування і розвитку та кіберінновацій комплексу пан Улкуніємі. Він надав для ознайомлення копію навчальної справи та зазначив, що для тренінгів спеціалістів у сфері протидії кіберзлочинності країн – учасниць МОКП будуть надавати модельні справи, розроблені Інтерполом, оскільки через таємницю слідства учасники не завжди можуть розповісти свої ситуації.

Генеральний директор із технологій міжнародної організації «Трендмікро» пан Генес доповів про особливості технічних рішень

Комплексу: спеціальна інформаційно-пошукова система, яка в режимі реального часу (онлайн) збирає та узагальнює відомості як з відкритих джерел, так і з банків даних країн-учасниць про наявні та потенційні кіберзагрози. Також представив збірник інформації щодо наявних кіберзагроз (віруси, зокрема банківської сфери). Цей збірник має стати періодичним виданням [2].

Євген Касперський – засновник і керівник провідного міжнародного розробника антивірусного програмного забезпечення, яке єдине з зарубіжних компаній сертифіковано в Україні, доповів про основні тенденції розповсюдження шкідливого програмного забезпечення (вірусів) серед усіх наявних операційних систем, зокрема, які використовуються мобільними телекомунікаторами. Він представив дослідження лабораторії Касперського щодо фактичного стану і тенденції збільшення використання з корисливих мотивів вірусів. Зокрема зазначив, що найбільш вразливими серед класичних операційних систем є продукція компанії Microsoft – 95 %, особливо Microsoft Windows XP, оскільки ця операційна система офіційно припинила підтримку програмного забезпечення, але нею продовжують користуватись у державному та фінансовому секторі держав колишнього СРСР, у тому числі в Україні. Найменш вразливими є операційні системи, розроблені на базі Linux, Mac OC. Також зазначив тенденцію розповсюдження вірусів серед мобільних операційних систем. Найбільш вразлива мобільна операційна система Android – 90 %, Cymbian (Nokia) – 5 %, Microsoft Windows Phone – 3 %, Apple та інші – 2 %. Така тенденція пов'язана з поширенням зазначених операційних систем.

Євген Касперський також підтвердив інформацію Генерального секретаря Інтерполу про поєднання кіберзлочинів із класичними злочинами (крадіжки зерна, вугілля, нафти, газу шляхом використання вірусів для втручання в програмне забезпечення компаній, які забезпечують продажу продукції). Ці віруси змушують систему відвантажувати більшу кількість, ніж обліковано. Було наведено приклад Нідерландів, де вантажопотік комп'ютеризований. Тут для здійснення контрабанди було інфіковано програмне забезпечення системи, що надавало змогу злочинцям уникати прикордонний і митний контроль. Також доповідач звернув увагу на інфікування банкоматів РФ (одне організоване злочинне угруповання спричинило збитки РФ на $67 млн). Однак банки не звертаються до правоохоронних органів, щоб не зашкодити своїй репутації.

Під час конференції було також заслухано директора Глобальної інформаційної компанії Інтерполу з профілактики злочинності «Відверни злочин» [3] Рорайму Андріані (рис. 5).

Рис. 5. Директор Глобальної інформаційної компанії Інтерполу з профілактики злочинності «Відверни злочин» Рорайма Андріані

Вона зазначила, що у зв'язку зі зміною пріоритетів Інтерполу на профілактику розпочато глобальну інформаційну кампанію за основними напрямками:

1. Створення інформаційного порталу, який планують увести в експлуатацію у II кварталі 2015 року. Його основними функціями мають стати: інформування громадськості щодо можливих схем злочинного посягання; віктимологічна профілактика; пропаганда співпраці громадян із правоохоронними органами; збір і узагальнення повідомлень про злочинні посягання, що надходять від громадян на цей портал. Тобто громадяни всього світу можуть подавати звернення на сторінку порталу TURN BACK CRIME з метою профілактики штучної латентності.
2. Випуск наочної агітації та друкованої продукції.
3. Пропаганда доброчесного способу життя та співпраці з правоохоронними органами шляхом розповсюдження відеороликів зі знаменитостями (футболісти, актори, зірки).
4. Організація спільних зустрічей представників правоохоронних органів, знаменитостей та громадськості з метою активізації співпраці громадян з правоохоронними органами.

Голова відділу стратегічного планування Європолу EC3 Олівер Бургерсдійк доповів про основні можливості координаційного центру Європолу з виявлення діяльності транснаціональних злочинних угруповань за усіма напрямками. Він навів приклад операції «Дендій» – спільної операції Інтерполу, Європолу, IATA (міжнародної асоціації

авіатранспорту), під час якої було затримано офіціанта аеропорту Франкфурта-на-Майні, який здійснював придбання авіаквитків за гроші, викрадені шляхом копіювання платіжних карток відвідувачів кафе.

Також Олівер Бургерсдійк повідомив про операцію «Парселпост», під час якої затримали організовану злочинну групу, куди входили громадяни України, члени якої організували на території Євросоюзу мережу скупок краденого. До злочинної діяльності залучалися громадяни, яким передавали викрадені речі для організації збуту через інтернет-аукціони. Оплата проходила через міжнародну систему грошових переказів Western Union, потім гроші переводилися на рахунки Європейських банків.

Віце-президент корпорації McAfee (розробки в центрі інновацій Інтерполу) Радж Самані доповів про злочинні схеми відмивання коштів через організацію діяльності фіктивних інтернет-казино. Члени організованого злочинного угруповання за змовою з організаторами казино вносять необхідну суму кількома сотнями трансакцій з різних джерел, після чого певна сума надається членам організованого злочинного угруповання під виглядом виграшу з одночасним оформленням необхідних документів про походження коштів для податкових та фіскальних органів.

Віце-президент міжнародної корпорації Codenomicon (організація, що здійснює розробку програм з усунення кіберзагроз) Самі Петаджасоя презентував автоматичну систему обміну оперативною інформацією про потенційні кіберзагрози та механізм вчинення кіберзлочинів, яка буде використовуватись в Міжнародному Глобальному Інноваційному кіберкомплексі для розробки стратегій запобігання цим злочинам. Ця система аналізує і надає інформацію усім учасникам Інтерполу на стадії кіберзагрози, тобто ще до того, як кіберзлочин може бути вчинено на території інших держав.

Під час Конференції відбулася також панельна дискусія на тему «Банки та фінанси. Основні тенденції та кіберзагрози». Учасниками дискусії стали:

– експерт з протидії кіберзлочинам ING Банку Феррі Хейджен;

– голова підрозділу протидії кіберзлочинам міжнародної корпорації VBS (міжнародна фінансова компанія), Швейцарія, Брук Нікель;

– директор інформаційного центру Азійського фінансового сектора Роберт Пох.

Вони доповіли про основні тенденції кіберзлочинності у фінансовій сфері. Зокрема:

– зараження шкідливим програмним забезпеченням POS-терміналів;

– активізацію транснаціональних організованих злочинних угруповань зі створення БОТ-мереж, які в подальшому використовуються для отримання відомостей про платіжні реквізити та організацію у втручання в систему дистанційного банківського обслуговування.

Так, використовуючи методи соціальної інженерії, зловмисники розсилали на адреси працівниць банків (бухгалтерії, фінансових відділів) електронні листи, що містили в собі посилання на сайти, в яких міститься шкідливий програмний код (вірус). Листи було легендовано під сайти знайомств у вигляді фото котиків, квітів. Працівниці банків, заходячи на такі сайти, завантажували в комп'ютер шкідливе програмне забезпечення, яке здійснювало подальше інфікування усієї комп'ютерної мережі банку. Далі все це використовувалось для контролю за банкоматами (одночасна видача готівки з усіх банкоматів мережі банку; викрадення реквізитів платіжних інструментів; втручання в систему дистанційного банківського обслуговування).

Наступна панельна дискусія була на тему «Віртуальні валюти», у ній взяли участь:

– аташе Євросоюзу при службі розслідувань Департаменту захисту батьківщини, США, Ерік Барнет;

– голова відділу стратегічного планування Європолу ЕСЗ Олівер Бургерсдійк;

– заступник начальника управління «К» МВС Російської Федерації Вадим Сушнік.

Вони доповіли про основні тенденції використання віртуальних валют для легалізації коштів, здобутих злочинним шляхом, зокрема такі платіжні системи: Bitcoin, Darkcoin, Liberty Reserve, в яких не відстежують, хто і яким чином вносить гроші, їх рух, тобто це електронні гаманці.

Заступник директора з питань протидії корупції та фінансовим злочинам Глобального центру Інтерполу Джеймс Андерсон доповів про основні напрямки діяльності його підрозділу:

– протидія корупції в країнах – членах Інтерполу;

– міжнародне відстеження фінансових операцій та повернення коштів, здобутих незаконним шляхом, до країни походження;

– створення єдиної захищеної системи обміну даними про фінансові злочини:

1) фінансове (інвестиційне) шахрайство;
2) відмивання коштів та фінансовий тероризм;
3) цифрові обмінники та віртуальні валюти;
4) шахрайство з платіжними картками (підробка, незаконне зняття коштів через банкомати).

Очільник підрозділу підтримки Європолу Бенуа Годарт доповів про порядок організації та заходи активізації міжнародної співпраці між країнами – членами МОКП Інтерполу та Європолу. Доповідач наголосив на необхідності співпраці між керівництвом Інтерполу та Європолу, за результатами якого країни – члени МОКП Інтерполу можуть направляти запити в Європу через Генерального секретаря Інтерполу і отримувати інформацію, запити на встановлення інформації та встановлювати користувача IP-адреси.

Також відбулося засідання робочої групи, в якому взяли участь:

– представник управління боротьби з кіберзлочинністю поліції Макао, який доповів про основні положення кримінального розслідування щодо зараження банкоматів шкідливим програмним забезпеченням шляхом втручання в операційну систему за допомогою модифікованого електронного чіпа, що використовується в платіжних картках, вчинене громадянами України, двоє з яких затримані і засуджені в Макао;

– представник одного з провідних розробників банкоматів Малайзії, який доповів про результати досліджень банкоматів, що були інфіковані вказаним шкідливим програмним забезпеченням. Він зазначив, що зараження банкоматів відбувалося шляхом безпосереднього доступу до їх жорстких дисків. Незаконно інстальоване програмне забезпечення дозволяло злочинцям у будь-який час, за допомогою платіжної картки з модифікованим електронним чіпом, отримувати кошти з банкоматів без проведення офіційних трансакцій. Такі дії стали можливими через халатне відношення банків до забезпечення надійної безпеки управлінської частини банкоматів. Для недопущення такого в майбутньому банкам необхідно відповідно до рекомендацій розробників замінити заводські ключі доступу до блоку управління та встановити відповідну сигналізацію;

– представники України обговорили з іноземними колегами основні аспекти розслідування цих кіберзлочинів, вчинених транснаціональними ОЗГ, які діють у країнах Азії та Латинської Америки за участю громадян України. Обговорено з представниками Макао і Тайланду подальші дії у вищевказаній справі та механізм отримання інформації від засуджених українців для можливого встановлення усіх учасників ОЗГ;

– представник «Лабораторії Касперського» зазначив: шкідливе програмне забезпечення, яке використовували члени вищевказаного ОЗГ, було розроблене російськомовними програмістами для російсько-, англо- і китайськомовних версій. З метою налагодження обміну зразками виявленого шкідливого програмного забезпечення та локалізації місць його виготовлення і розповсюдження сторони домовилися про порядок обміну відповідною інформацією;

– у свою чергу представник Глобального інноваційного комплексу розповів про порядок проведення злочинцями аутентифікації та авторизації своїх незаконних операцій через банківський процесінг, який використовувався останніми під час заволодіння готівкою з банкоматів. Також доповів учасникам наради про першочергові заходи, яких мають вживати служби безпеки банків для недопущення у майбутньому несанкціонованого втручання в роботу банкоматів;

– представник Росії зазначив, що завдяки обміну інформацією з МОКП Інтерпол було здійснено успішну ліквідацію російського відділення транснаціонального ОЗГ, якому протягом 2013–2014 років вдалося заволодіти коштами з банкоматів на суму $67 млн;

– водночас керівник підрозділу боротьби з кіберзлочинністю Молдови зазначив, що завдяки інформації з Макао, України і Російської Федерації, провідні банки Молдови змогли своєчасно захистити свої банкомати та запобігти викраденню грошей. Найгірші наслідки, які були спричинені цим шкідливим програмним забезпеченням, – це безпідставна видача незаповненої чекової стрічки замість очікуваної готівки.

Методи роботи Управління боротьби з кіберзлочинністю МВС України були позитивно відзначені керівництвом Європолу. У зв'язку з цим члени української делегації були запрошені на особисту зустріч із заступником директора Європолу – керівником Центру боротьби з кіберзлочинністю Європолу (ЄС3) Трольс Ортінгом для обговорення інших питань, пов'язаних з недопущенням розповсюдження вчинення аналогічних злочинів на території європейських країн.

Підсумовуючи вищезазначене, хотілося б зауважити, що усі виступи на конференцій мали профільний професійний характер та були присвячені проблемі імплементації певних прогресивних рішень у сфері протидії кіберзлочинності до чинного законодавства країн – учасниць Інтерполу. На сьогодні існують певні труднощі із вирішенням цього питання в Україні через складну суспільно-політичну ситуацію та факти зовнішньої агресії. Тим не менш, працівниками МВС України підготовлено низку пропозицій щодо удосконалення чинного законодавства у досліджуваній сфері, які, сподіваємось, знайдуть підтримку у Верховній Раді України.

Список використаних джерел: 1. INTERPOL-Europol cybercrime conference reinforces multisector commitment to cybersecurity : 3 Oct. 2014 [Електронний ресурс] // Interpol : [сайт]. – Режим доступу: http://www.interpol.int/News-and-media/News/2014/N2014-194. **2.** Combating cybercrime through cooperation focus of INTERPOL-Europol conference : 1 Oct. 2014 [Електронний ресурс] // Interpol : [сайт]. – Режим доступу: https://www.europol.europa.eu/content/combating-cybercrime-through-cooperation-focus-interpol-europol-conference. **3.** Turnbackcrime : сайт [Електронний ресурс] / Interpol Turn Back Crime. – Режим доступу: http://www.turnbackcrime.com.

Надійшла до редколегії 28.10.2014

Демедюк С. В., Демедюк Т. С. Международный опыт противодействия киберпреступности

Отражены проблемные вопросы, которые рассматривались на международной научно-практической конференции «Противодействие киберпреступности» в Сингапуре. В частности: открытие и возможности Глобального Инновационного комплекса; предоставление для тренингов специалистов сферы противодействия киберпреступности стран – участниц Интерпола модельных дел, разработанных Интерполом; характеристика наиболее уязвимых классических операционных систем; создание информационного портала TURN BACK CRIME.

Ключевые слова: борьба с киберпреступностью, зарубежный опыт, правоохранительные органы, подготовка специалистов.

Demedyuk S. V., Demedyuk T. S. Foreign cybercrime combating experience

The article outlines the challenging issues that were discussed during the international research and training conference «Cybercrime Counteraction» in Singapore. The opening process and capabilities of the Global Innovative complex (its usage in criminal investigations; model training programs for training experts in cybercrime counteraction; gaining and sharing positive experience; effort coordination of the law enforcement agencies of ICPO member states carrying out international investigative activities) are described. The author emphasizes the necessity of providing cybercrime combating expert trainings with model tasks developed by Interpol as its participants are not always authorized to use their own cases due to secrecy of investigation. Most vulnerable classical operating systems are characterized. The main functions of the data portal TURN BACK CRIME created to prevent artificial latency are described. The article also outlines the most common types of cyber frauds and gives the examples of sums of sustained loss. Factual material as to the participation of the Cybercrime Combating Department of the MIA of Ukraine in international investigative activities aimed at organized crime counteraction are given. It is emphasized that many banking institutions are willing to conceal cybercrimes committed against their employees and clients because of the reputation hazards. It is also outlined that at present Ukraine faces certain difficulties in solving problems of innovative experience implementation in the field of cybercrime counteraction due to the shift of the primary focus of the administrative bodies to other problems, namely complex socio-political situation and the facts of external aggression.

Keywords: cybercrime combating, foreign experience, law enforcement, training experts.

УДК 343.137.9

Р. В. Новак

Поняття та значення особливих порядків кримінального провадження

Розглянуто процесуальне значення особливих порядків кримінального провадження України та визначено основні способи спрощення кримінальної процесуальної форми. Запропоновано визначення поняття особливих порядків кримінального провадження та вказано основні ознаки кожного з них. Виділено дві групи ознак – суб'єктні та нормативні, котрі характеризують усі особливі порядки кримінального провадження, які містяться в Кримінальному процесуальному кодексі України.

Ключові слова: особливі порядки кримінального провадження, кримінальне провадження на підставі угод, кримінальна процесуальна форма, Кримінальний процесуальний кодекс України.

Побудова правової держави в Україні можлива тільки за умови комплексного та системного реформування всіх сфер суспільного