БОСАК Е. С. ПОНЯТИЕ И ВИДЫ ТРАДИЦИЙ И ОБЫЧАЕВ В СИСТЕМЕ МЕР ПРЕДУПРЕЖДЕНИЯ ПРЕСТУПНОСТИ

Определены понятия традиций и обычаев в системе мер предупреждения преступности. Выделены виды традиций и обычаев, имеющих положительное профилактическое воздействие на поведение лиц.

Ключевые слова: *традиции, обычаи, предупреждение преступности, профилактическая роль, религиозные традиции, духовно-семейные традиции, профессиональные традиции, морально-этические традиции, народные традиции.*

BOSAK K. S. NOTIONS AND TYPES OF CUSTOMS AND TRADITIONS IN THE SYSTEM OF CRIME PREVENTION

The problem of crime prevention is a key issue of the national jurisprudence and practice. Scientists distinguish preventive measures along with the traditional penal ones that have no less effectiveness among precautions than punishment for a committed crime. Predominantly, the crime prevention system is based on religious, cultural, moral and ethical standards. Considering this fact traditions and customs that form the outlook of individuals and affect their behavior are distinguished in the system of crime prevention.

Considerable attention of scientists of different branches is paid to the study of traditions and customs. The author of the article analyzes the notions of traditions and customs offered not only by criminologists but by theorists of law and philosophers, etc. Based on the generalization of scientific papers in the field of customs and traditions the author concluded that the preventive role of the latter in criminology is not highlighted enough. Taking into account this fact, criminological definition of customs and traditions in the system of crime prevention is offered.

Classification criteria of traditions and customs proposed by scientists are also researched in the article. Attention is focused on their core types that play a preventive role in crime prevention. Among them are: religious traditions and customs in the system of crime prevention, which have significant meaning for preventing crimes against the person; spiritual and family traditions and customs, which play a significant role in the process of a person's education; national traditions and customs that form the national character and are the basis of patriotic education of youth and guarantee prevention of crimes against the state; professional, moral and ethical traditions and customs in the system of crime prevention.

Stated traditions and customs in any way have the preventive impact on crime in the sphere of property relations, production safety, public order, etc.

Keywords: *traditions, customs, crime prevention, preventive role, religious traditions and customs, spiritual and family traditions and customs, professional, moral and ethical traditions and customs, national traditions and customs, traditions and customs in the system of crime prevention.*

УДК 343.1(477):65.012.8+004

М. Ю. ЛІТВІНОВ,
кандидат юридичних наук,
доцент кафедри захисту інформації
факультету підготовки фахівців для підрозділів боротьби с кіберзлочинністю та торгівлею людьми
Харківського національного університету внутрішніх справ,
начальник Управління боротьби з кіберзлочинністю Міністерства внутрішніх справ України

СВІТОВА ТА УКРАЇНСЬКА ПРАКТИКА БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ

Проаналізовано світові підходи в організації боротьби з кіберзлочинністю. Визначено роль підрозділів боротьби з кіберзлочинністю в Україні та світі. Розкрито проблеми, які існують у підготовці кадрів для підрозділів боротьби з кіберзлочинністю. Визначено механізм їх вирішення. Визначено актуальні питання у світі у сфері боротьби з кіберзлочинністю, які потребують вирішення.

Ключові слова: *кіберзлочинність, боротьба з кіберзлочинністю, підрозділи боротьби з кіберзлочинністю, підготовка кадрів, Департамент боротьби з кіберзлочинністю, МВС України.*

© Літвінов М. Ю., 2014

Світові економічні процеси на сучасному етапі все більше зміщуються у бік кіберпростору. Адже його застосування як інструменту ведення бізнесу дає змогу значно підвищити прибутки. Водночас можна спостерігати і зрушення кримінального елементу у бік цього віртуального середовища, значну частину якого складає всесвітня мережа. Такому просуванню нерідко сприяє певна анонімність, якої можна домогтися у мережі. Тож сьогодні в Інтернеті з'являється велика кількість даних, що містять ознаки правопорушень.

Практично будь-який злочин, передбачений Кримінальним кодексом України, можна здійснити з використанням кіберпростору. Непоодинокими є випадки продажу наркотичних засобів, вогнепальної та холодної зброї, розповсюдження порнографічних предметів через Інтернет. Крім перелічених загальнокримінальних злочинів особливої шкоди завдають високотехнологічні правопорушення, серед яких зламування систем дистанційного банківського обслуговування, замовні DDOS-атаки на електронні ресурси, зламування та шахрайство з телекомунікаційними системами операторів зв'язку.

Оцінка криміногенної обстановки в кіберсфері дає підстави до вжиття рішучих заходів із боку правоохоронців усього світу з метою її покращення, зменшення ризику для пересічних громадян потрапити у пастку кіберзлочинців.

Питання протидії кіберзлочинності на світовому рівні є об'єктом уваги значної частини науковців та практиків, серед яких можна виділити вітчизняних фахівців В. М. Бутузова, І. О. Воронова, В. О. Голубєва, М. В. Гуцалюка, В. П. Захарова, О. В. Манжая, Ю. Ю. Орлова, Е. В. Рижкова, Ю. В. Степанова, В. П. Шеломенцева та ін.

Слід констатувати, що найбільш значущі досягнення у сфері боротьби з кіберзлочинністю на сьогодні мають Великобританія (Serious and Organised Crime Agency), Китай (People's Police), Німеччина (Bundeskriminalamt), Російська Федерація (Управление К), США (Federal Bureau of Investigation), Франція (Office central de lutte contre la criminalite liee aux technologies de l'information et de la communication), Японія (National Police Agency).

В Україні функції боротьби з кіберзлочинністю зосереджено в руках однойменного Управління (далі – УБК), яке підпорядковано Міністерству внутрішніх справ України. На теперішній час в УБК налагоджено конструктивну взаємодію щодо боротьби з кіберзлочинністю практично з усіма з перелічених вище відомств та правоохоронними органами багатьох інших країн.

Останнім часом в УБК було накопичено багато інформації про контингент осіб, причетних до організації та здійснення кіберзлочинів. У відповідному банку даних є не тільки громадяни України, останніми роками кількість іноземних громадян також істотно зросла. Це підкреслює необхідність широкої міжнародної співпраці [1].

У багатьох країнах розроблена та активно застосовується нормативно-правова база, присвячена питанням боротьби з кіберзлочинністю. Як правило, відповідні норми викладено у декількох законодавчих, а також підзаконних актах, що мають відомчий або міжвідомчий характер. Прикладом останніх є Online Investigative Principles for Federal Law Enforcement Agents 1999 p., FBI Domestic Investigations and Operations Guide від 15.10.2011 (США), Постанова Державної Ради КНР від 20.09.2000 № 292 «Заходи щодо управління сферою Інтернет-послуг» тощо.

У Німеччині питанням боротьби з кіберзлочинністю присвячено § 20k Закону «Про федеральне управління кримінальної поліції та співробітництво федерації і земель за кримінальними справами» від 07.07.1997, згідно з яким в окремих випадках дозволяється проводити санкціонований негласний онлайн-обшук.

У Китаї ст. 11 Закону КНР «Про органи державної безпеки» від 22.02.1993 [2] та ст. 6 Закону КНР «Про народну поліцію» від 28.02.1995 [3] також опосередковано зачіпають проблеми кібербезпеки. Теж саме стосується Regulation of Investigatory Powers Act (Великобританія), Copyright Act, Act on Punishment of Activities Relating to Child Prostitution and Child Pornography (Японія).

В Україні основну нормативно-правову базу боротьби з кіберзлочинністю складають Конституція України [4], у ст. 17 якої відзначається, що забезпечення інформаційної безпеки України є найважливішою функцією держави, справою всього Українського народу.

Окрім Конституції положення щодо боротьби з кіберзлочинністю містяться у Конвенції «Про кіберзлочинність» від 23.11.2001, ратифікованої Верховною Радою України 07.09.2005, Кримінальному кодексі України, Кримінальному процесуальному кодексі України, зокрема ст. 263 (зняття інформації з

транспортних телекомунікаційних мереж), ст. 264 (зняття інформації з електронних інформаційних систем), ст. 268 (установлення місцезнаходження радіоелектронного засобу), ст. 274 (негласне отримання зразків, необхідних для порівняльного дослідження). Велику роль у боротьбі з кіберзлочинністю грають Закон України «Про оперативно-розшукову діяльність» (ст. 8) та низка інших законодавчих актів, серед яких можна виділити Закони України «Про телекомунікації», «Про захист інформації в інформаційно-телекомунікаційних системах» тощо [5, с. 647, 649].

Саме УБК діє на підставі наказу МВС України «Про організацію діяльності Управління боротьби з кіберзлочинністю МВС України та підрозділів боротьби з кіберзлочинністю ГУМВС, УМВС» від 30.10.2012 № 988 [6].

Підрозділи боротьби з кіберзлочинністю беруть участь у формуванні та забезпеченні реалізації державної політики щодо попередження та протидії кримінальним правопорушенням, механізм підготовки, вчинення або приховування яких передбачає використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, а також іншим кримінальним правопорушенням, учиненим із їх використанням (сфера боротьби з кіберзлочинністю). У тому числі:

– кримінальним правопорушенням у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку;

– кримінальним правопорушенням, механізм підготовки, вчинення або приховування яких передбачає використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку (у сферах платіжних систем; обігу інформації протиправного характеру із використанням електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку (протиправного контенту); економіки, яка включає в себе фінансові та торгові транзакції, що здійснюються за допомогою мереж електрозв'язку чи комп'ютерних мереж, а також протидія забороненим видам господарської діяльності у цій сфері (електронної комерції); надання телекомунікаційних послуг; а також шахрайствам і легалізації (відмиванню) доходів, одержаних від зазначених вище кримінальних правопорушень).

Також до основних завдань УБК відноситься сприяння у порядку, передбаченому чинним законодавством, іншим підрозділам МВС України у попереджені, виявлені та припиненні кримінальних правопорушень, а також у проведенні досудового розслідування.

Міжнародна співпраця є одним із пріоритетів у діяльності УБК.

Так, за останній рік експертами ОБСЄ було проведено двотижневий тренінг для працівників УБК. У лютому–березні 2013 року фахівці УБК ділилися досвідом із колегами з інших служб. Для працівників кримінальної міліції у справах дітей було проведено тренінг, присвячений пошуку зниклих дітей із використанням соціальних мереж та інших ресурсів Інтернет. Для слідчих із усіх регіонів України було проведено 3 тренінги по основах розкриття злочинів, пов'язаних із зламом систем ДБО, збиток від яких склав минулого року більше 116 млн грн.

У березні цього року за підтримки посольства Великобританії в Україні на базі НАВС проведено тренінг з питань боротьби з дитячою порнографією в Інтернеті.

У лютому–березні 2013 року за підтримки посольства Великобританії в Україні представник УБК пройшов 5-тижневе стажування в підрозділі по боротьбі з організованою злочинністю Великобританії. Результати були предметом доповіді на щорічному конгресі з питань кіберзлочинності, що проходив у Лондоні.

У квітні цього року на базі УБК 10 співробітників пройшли спеціалізований курс навчання з питань боротьби зі шкідливим програмним забезпеченням, 7 співробітників, зокрема 1 курсант НАВС, який в цей час стажувався в УБК, успішно склали іспит і отримали міжнародні сертифікати.

За підтримки Посольства США в Україні 1 співробітник УБК пройшов 10-тижневий курс навчання в Академії ФБР, планується ще один.

Як і раніше у 2013 році було направлено 2 співробітники УБК для роботи в міжнародному центрі протидії кіберзлочинності (з 20 країн по 6 тижнів кожен). Цього року 2 співробітники кримінальної поліції Німеччини пройшли двотижневе стажування на базі УБК.

Основні завдання / рекомендації УБК на сьогодні – це обмін передовим досвідом; забезпечення роботи НКП в кожній країні; постійне навчання і підвищення кваліфікації; використання досвіду міжнародних експертів; розвиток віртуальних співтовариств, які на

неформальному рівні сприяють протидії кіберзлочинності. Ще один важливий напрям роботи УБК – це підготовка кадрів.

У зв'язку з набуттям нових повноважень слідчими, а за їх дорученням – оперативними працівниками, необхідно було переглянути підходи підготовки відповідних фахівців. Значна частина нових повноважень, зокрема у сфері проведення окремих слідчих та негласних слідчих (розшукових) дій, пов'язана із застосуванням технічних засобів. Тому працівники ОВС, задіяні у боротьбі з кіберзлочинністю, окрім володіння відповідними юридичними знаннями, повинні мати навички роботи з комп'ютерною технікою та досконало розбиратися у механізмі вчинення кіберзлочинів. На особливу увагу заслуговує комплексна підготовка таких працівників, яка базується на принципі поєднання юридичних та технічних знань. Можливість зазначеної підготовки існує у Харківському національному університеті внутрішніх справ. Тому саме на базі цього вишу було створено факультет підготовки фахівців для підрозділів боротьби з кіберзлочинністю та торгівлею людьми, фахівці якого зуміли налагодити конструктивну співпрацю з УБК.

На факультеті здійснюється підготовка фахівців за напрямами підготовки «Системи технічного захисту інформації» та «Правознавство» спеціалізації «боротьба з кіберзлочинністю» та «боротьба з торгівлею людьми». Концепція діяльності факультету полягає у підготовці кваліфікованих кадрів, здатних ефективно протидіяти високотехнологічним злочинам, що завдають значних збитків фізичним та юридичним особам, а також злочинам, пов'язаним із торгівлею людьми.

Проблема якісної підготовки кадрів для підрозділів боротьби з кіберзлочинністю є характерною не лише для України. Наприклад, у Німеччині відповідних фахівців добирають із числа випускників технічних вишів, у Російській Федерації їх готує Московський університет МВС Росії за спеціальністю «Інформаційна безпека», у США для підготовки таких фахівців існують спеціалізовані курси в Академії ФБР.

Проаналізувавши діяльність державних органів різних країн у сфері боротьби з кіберзлочинністю, хотілося б позначити низку найбільш актуальних питань у цій сфері, які потребують вирішення. По перше, це міжнародне унормування відносин у кіберпросторі та особливого порядку взаємодії правоохоронних органів різних країн у сфері кібербезпеки між собою та з представниками приватних структур, діяльність яких пов'язана з наданням послуг через мережу Інтернет або у сфері комунікацій. По друге, формування підрозділами боротьби з кіберзлочинністю якісного особового складу найвищої кваліфікації, здатного ефективно протидіяти кіберзлочинності. І, потретє, це розробка спеціалізованого програмного забезпечення.

Список використаних джерел

1. Литвинов М. Деятельность управления по борьбе с киберпреступностью МВД Украины на современном этапе [Електронний ресурс] / Максим Литвинов. – Режим доступу: http://cybersafetyunit.com/deyatelnost-upravleniya-po-borbe-s-kiberprestupnostyu-mvd-ukrainyi-na-sovremennom-etape/. – 01.07.2013.

2. State Security Law of the People's Republic of China : of 22.02.1993 No. 6 [Електронний ресурс]. – Режим доступу: http://en.pkulaw.cn/display.aspx?id=530&lib=law&SearchKeyword=state%20security&SearchCKeyword=

3. People's Police Law of the People's Republic of China : of 28.02.1995 No. 40 [Електронний ресурс]. – Режим доступу: http://en.pkulaw.cn/display.aspx?id=123&lib=law&SearchKeyword=&SearchCKeyword=.

4. Конституція України : від 28.06.1996 // Відомості Верховної Ради України. – 1996. – № 30. – Ст. 141.

5. Манжай О. В. Проблеми нормативно-правового забезпечення боротьби з кіберзлочинністю в Україні / О. В. Манжай // Форум права. – 2013. – № 1. – С. 646–650 [Електронний ресурс]. – Режим доступу: http://nbuv.gov.ua/j-pdf/FP_index.htm_2013_1_109.pdf.

6. Про організацію діяльності Управління боротьби з кіберзлочинністю МВС України та підрозділів боротьби з кіберзлочинністю ГУМВС, УМВС : наказ МВС України від 30.10.2012 № 988 [Електронний ресурс]. – Режим доступу: http://document.ua/pro-organizaciyu-dijalnosti-upravlinnja-borotbi-z-kiberzloch-doc130740.html.

Надійшла до редколегії 02.04.2014

ЛИТВИНОВ М. Ю. МИРОВАЯ И УКРАИНСКАЯ ПРАКТИКА БОРЬБЫ С КИБЕРПРЕСТУПНОСТЬЮ

Проанализированы мировые подходы в организации борьбы с киберпреступностью. Определена роль подразделений по борьбе с киберпреступностью в Украине и мире. Раскрыты проблемы, которые существуют в подготовке кадров для подразделений по борьбе с киберпреступностью. Определен механизм их решения. Определены актуальные вопросы в мире в сфере борьбы с киберпреступностью, требующие решения.

Ключевые слова: *киберпреступность, борьба с киберпреступностью, подразделения по борьбе с киберпреступностью, подготовка кадров, Департамент по борьбе с киберпреступностью, МВД Украины.*

LITVINOV M. Y. THE WORLD AND UKRAINIAN PRACTICE OF COMBATING CYBERCRIME

The world economic processes at the present stage are increasingly shifting in the direction of cyberspace because of its use as a tool of doing business allows you to significantly increase profits. However, you can also observe the criminal elements shift in the direction of this virtual environment. So, today in almost any crime mentioned in Criminal Code of Ukraine, can be committed out with the use of cyberspace.

Assessment of the crime situation in the Cyber sphere gives ground to take decisive action on the part of law enforcement officers for the purpose of its improvement, reduction of risk for ordinary citizens to fall into the trap of cybercriminals.

The main peculiarity of the fight against cybercrime is that the state alone is not in a position to confront the phenomenon itself. Only international community in permanent close cooperation can deal with such issue as a security threat of cybercrime.

The real threat for as ordinary people security as well of security for government structures made many countries of the world to adopt a number of regulations aimed at prevention and punishment of cybercrime.

In this article the world approaches in organizing of cybercrime prevention have been analyzed.

In Ministry of Internal Affairs of Ukraine the function of combating cybercrime is performed by Department of Cybercrime Combating. Currently, the Department established constructive cooperation with other countries' law enforcement agencies in combating cybercrime.

In the article the examples of legal documents in cybercrime combating are provided and relative Ukraine legislation are presented.

The main task for the Department today is the exchange of achievements; continuous learning and professional development; use the experience of international experts; the development of virtual communities, which at the informal level contribute to combating cybercrime.

Another important direction of Department activity is the personnel training. The article deals with problems that exist in the training of personnel for units to combat cybercrime.

Based on the analysis of public authorities activity of different countries in the field of combating cybercrime, the article outlines a number of the most topical issues in this area that need solution.

Keywords: *cybercrime, combating cybercrime, cybercrime units, training of personnels, Department of Cybercrime Combating, MIA Ukraine.*

УДК 343.985

В. В. МАРКОВ,
кандидат юридичних наук, старший науковий співробітник,
начальник факультету підготовки фахівців для підрозділів боротьби
з кіберзлочинністю та торгівлею людьми
Харківського національного університету внутрішніх справ;

Р. Р. САВЧЕНКО,
курсант
Харківського національного університету внутрішніх справ

ПРИНЦИПИ НАЛЕЖНОСТІ ЕЛЕКТРОННИХ ДОКАЗІВ, ОТРИМАНИХ З МОБІЛЬНИХ ПРИСТРОЇВ

Актуальність цього дослідження обумовлена відсутністю будь-яких досліджень в Україні щодо мобільної форензики, зокрема відносно відповідних електронних доказів, з урахуванням положень вітчизняного законодавства. Проаналізовано сутність мобільної форензики та електронних доказів, визначено джерела електронних доказів та дано характеристику принципів належності електронних доказів, отриманих з мобільних пристроїв.

Ключові слова: *комп'ютерна форензика, мобільна форензика, кіберзлочин, електронні (цифрові) докази, джерела електронних доказів, принципи належності електронних доказів.*

© Марков В. В., Савченко Р. Р., 2014