4. *Латышина Д. И.* История педагогики (История образования и педагогической мысли) : учеб. пособие / Д. И. Латышина. – М. : Гардарики, 2006. – 603 с.

5. *Левківський М. В.* Історія педагогіки: навч.-метод. посібник. – Вид 3-е, доп. / М. В. Левківський. – К. : Центр учбової літератури, 2008. – 190 с.

6. *Любар О. О.* Історія української школи і педагогіки : навч. посіб. / О. О. Любар, М. Г. Стельмахович, Д. Т. Федоренко. – К. : Знання, 2006. – 447 с.

7. *Мосіяшенко В. А.* Історія педагогіки України в особах : навч. посіб. / В. А. Мосіяшенко, О. І. Курок, Л. В. Задорожна. – Суми : ВТД " Університетська книга", 2005. – 266 с.

8. *Прокопенко Л. Л.* Генеза та розвиток державної освітньої політики в Україні (IX – початок XX ст.) : монографія / Л. Л. Прокопенко. – Дніпропетр. : ДРІДУ НАДУ, 2008. – 488 с.

9. *Прокопенко Л. Л.* Становлення державного управління освітою в Україні : історико-теоретичний аспект / Л. Л. Прокопенко [Електронний ресурс]. – Режим доступу : http://www.kbuapa.kharkov.ua/e-book/db/2007-1-2/doc/1/07.pdf.

10. *Сірополко С.* Історія освіти в Україні / С. Сірополко. – К. : Наук. думка, 2001. – 912 с.

11. Українка Леся. Волинські образки. 1. Школа / Л. Українка [Електронний ресурс]. – Режим доступу : http://www.l-ukrainka.name/uk/Prose/VolynObrazky.html.

12. *Ушинский К. Д.* Три элемента школы / К. Д. Ушинский [Электронный ресурс]. – Режим доступа : http://az.lib.ru/u/ushinskij_k_d/text_0080.shtml.

Надійшла до редколегії 17.02.2014 р.

УДК 343.98

О. В. ОРЛОВ, Ю. М. ОНИЩЕНКО

ПОПЕРЕДЖЕННЯ КІБЕРЗЛОЧИННОСТІ – СКЛАДОВА ЧАСТИНА ДЕРЖАВНОЇ ПОЛІТИКИ В УКРАЇНІ

***Р**озглянуто питання попередження кіберзлочинності як складової держаної політики в галузі боротьби зі злочинами з використанням інформаційних технологій. Проаналізовано методи боротьби зі зловживаннями в кіберпросторі. Надано пропозиції щодо попередження кіберзлочинності в державі.*

Ключові слова: кіберзлочин, кібербезпека, комп'ютерна мережа, загроза, інтернет, інформаційні технології.

***T**he problem of cybercrime prevention as a part of public policy in fighting IT crimes has been studied. The author has analyzed methods of combating improper use in cyberspace. The author also has made suggestions to prevent cybercrime in the country.*

Key words: cybercryme, cybersafety, computer network, threat, Internet, information technologies.

Сучасне інформаційне суспільство охоплює всі сфери життєдіяльності людини і держави. Але людство, поставивши собі на службу телекомунікації та глобальні комп'ютерні мережі, не передбачало, які можливості для зловживання створюють ці технології. Сьогодні жертвами злочинців, що орудують у віртуальному просторі, можуть стати не лише люди, але і цілі держави. При цьому безпека тисячі користувачів може виявитися залежно від декількох злочинців. За таких умов особливе значення набуває пошук нових можливостей забезпечення безпеки держави у зв'язку з формуванням нової сфери протиборства зі злочинністю – кіберпростору. Кількість злочинів, що здійснюються в цієї галузі, зростає пропорційно кількості користувачів комп'ютерних мереж, і, за оцінками інтерполу, темпи зростання злочинності, наприклад, у глобальній мережі інтернет, є найшвидшими на планеті.

Кіберзлочинність – неминучий наслідок глобалізації інформаційних процесів. Простота, легкість, анонімність, доступність і заощадження часу – якості, що роблять інформаційні технології привабливими для людства, – не могли не притягнути до себе уваги осіб, що здійснюють протиправну діяльність. Зі зростанням використання інформаційних технологій у різних сферах діяльності людини зростає і використання їх з метою вчинення злочинів. Це зростання також є неминучим процесом, оскільки законодавче регулювання відносин у сфері інформаційних технологій не може ні випередити їх розвиток, ні навіть йти з ним у ногу.

Проблематика попередження злочинності у сфері інформаційних технологій та кіберебезпеки досить часто обговорюється фахівцями в інформаційній сфері в журналах, на конференціях, круглих столах і засобах масової інформації. Деякі аспекти попередження кіберзлочинності вивчали та обговорювали у своїх статтях С. Битко, В. Бутузов, А. Волеводз, Д. Дубов, Н. Дубова, С. Кльоцкін, В. Мілашев, М. Литвинов, В. Мохор, Т. Тропіна, В. Хахановський та інші.

Проте на даний час недостатньо ґрунтовних досліджень щодо проблем державної політики та попередження злочинів у галузі кібербезпеки.

Мета статті – дослідити та проаналізувати проблеми, які виникають при попередженні кіберзлочинності як складової держаної політики в галузі боротьби зі злочинами з використанням інформаційних технологій. Надати пропозиції щодо попередження кіберзлочинності в країні.

Сьогодні у світі дослідження проблем боротьби зі злочинами в кіберпросторі приділяється значна увага, що обумовлено об'єктивними процесами розвитку інформаційно-телекомунікаційних технологій і їх впровадженням у різні сфери громадської діяльності. С. Мельник визначає кіберпростір як простір, сформований інформаційно-комунікаційними системами, в якому проходять процеси перетворення (створення, зберігання, обміну, обробки та знищення) інформації, представленої у вигляді електронних комп'ютерних даних [1].

Нині не існує скільки-небудь узагальнених даних для формування понять основних елементів характеристики кіберзлочинів. Усе ще не існує чіткого визначення поняття кіберзлочина і дискутуються різні точки зору щодо їх

класифікації. У сучасних умовах соціально-економічного розвитку злочинність в Україні стала реальністю громадського життя.

Підтвердженням зростання комп'ютерних злочинів в Україні є статистичні дані. За даними Управління боротьби з кіберзлочинністю МВС України, найбільш поширеними видами кіберзлочинів є: несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів) та несанкціоновані дії з інформацією, яка ними оброблюється. За 10 місяців 2012 р. зафіксовано 44 таких втручання. За даними Державної служби фінансового моніторингу України, в 2012 р. було зареєстровано 179 спроб несанкціонованого доступу до рахунків клієнтів банків на загальну суму понад 150 млн грн, при цьому сума коштів, у подальшому знятих злочинним шляхом лише готівкою, становить 9,5 млн грн [2].

Кіберзлочинність – це злочинність у так званому "віртуальному просторі". Віртуальний простір можна визначити як створений за допомогою комп'ютерів інформаційний простір, в якому знаходяться відомості про осіб, предметів, фактів, подій, явищ і процесів, представлені в математичному, символьному або будь-якому іншому виді і що знаходяться в процесі руху локальними і глобальними комп'ютерними мережами або відомості, що зберігаються в пам'яті будь-якого фізичного або віртуального пристрою, а також іншого носія, спеціально призначеного для їх створення, зберігання, обробки і передачі.

Конвенція Ради Європи говорить про чотири типи комп'ютерних злочини "у чистому вигляді", визначаючи їх як злочини проти конфіденційності, цілісності і доступності комп'ютерних даних і систем:

1) незаконний доступ – ст. 2 (протиправний умисний доступ до комп'ютерної системи або її частини);

2) незаконне перехоплення – ст. 3 (протиправне умисне перехоплення не призначених для громадськості передач комп'ютерних даних на комп'ютерну систему, з неї або в її межах);

3) втручання в дані – ст. 4 (протиправне ушкодження, видалення, порушення, зміна або припинення комп'ютерних даних);

4) втручання в систему – ст. 5 (серйозна протиправна перешкода функціонуванню комп'ютерної системи шляхом введення, передачі, ушкодження, видалення, порушення, зміни або припинення комп'ютерних даних) [3].

Узагальнюючи різні точки зору, можна зробити висновок про те, що нині існують дві основні течії наукової думки.

Одна частина дослідників відносить до комп'ютерних злочинів дії, в яких комп'ютер є або об'єктом, або знаряддям посягань.

Дослідники ж другої групи відносять до комп'ютерних злочинів тільки протизаконні дії у сфері автоматизованої обробки інформації. В якості головної класифікуючої ознаки, що дозволяє віднести ці злочини у відособлену групу, виділяється спільність способів, знарядь, об'єктів посягань [4].

Іншими словами, об'єктом посягання є інформація, що обробляється в комп'ютерній системі, а комп'ютер слугує знаряддям посягання.

Зростання об'ємів інформації, комп'ютерних мереж і кількості користувачів, спрощення їх доступу до циркулюючої в мережах інформації істотно підвищує вірогідність розкрадання або руйнування цієї інформації.

Нині значущість проблеми захисту інформаційних ресурсів, у тому числі особистих, визначається такими чинниками:

– розвитком світових і національних комп'ютерних мереж і нових технологій, що забезпечують доступ до інформаційних ресурсів;

– перекладом інформаційних ресурсів на електронні носії і концентрацією їх в інформаційних системах;

– підвищенням "ціни" створюваної і накопиченої інформації, що слугує реальним ресурсом соціально-культурного і особового розвитку;

– розробкою і вдосконаленням інформаційних технологій, які можуть ефективно використовуватися кримінальними структурами.

Виділяються такі основні тенденції розвитку комп'ютерної злочинності в Україні:

– високі темпи зростання;

– корислива мотивація більшості вчинених комп'ютерних злочинів;

– ускладнення способів вчинення комп'ютерних злочинів і поява нових видів протиправної діяльності у сфері комп'ютерної інформації;

– зростання кримінального професіоналізму комп'ютерних злочинців;

– омолоджування комп'ютерних злочинців і збільшення долі осіб, що раніше не притягувалися до карної відповідальності;

– зростання матеріального збитку від комп'ютерних злочинів у загальній частці збитку від інших видів злочинів;

– перенесення центру тяжіння на скоювання комп'ютерних злочинів з використанням комп'ютерних мереж;

– переростання комп'ютерної злочинності в розряд транснаціональної злочинності;

– високий рівень латентності комп'ютерних злочинів.

Боротьба з кіберзлочинністю повинна стати пріоритетною функцією всіх правоохоронних органів і силових відомств.

Результати аналізу характеристики комп'ютерної злочинності дозволяють прогнозувати ускладнення боротьби з нею з огляду на те, що способи вчинення комп'ютерних злочинів з кожним роком набувають усе більш витонченого характеру. До вирішення цієї проблеми необхідно підходити комплексно.

Фахівці виділяють такі елементи організації діяльності правоохоронних органів у глобальних інформаційних мережах:

– вивчення і оцінка обстановки в мережах;

– здійснення оптимальної розстановки сил і засобів, забезпечення взаємодії;

– управління, планування і контроль; координація дій суб'єктів правоохоронних органів [5].

Важливим елементом системи заходів боротьби з комп'ютерною злочинністю є заходи превентивного характеру, або заходи попередження.

Сукупність потреб, задоволення яких забезпечує існування і можливість прогресивного розвитку кожного громадянина, суспільства і держави – це частина національних інтересів, без реалізації яких неможливо забезпечити стабільний стан держави і суспільства, а також нормальний розвиток країни як незалежного суб'єкта міжнародних відносин.

Усі інтереси, що захищаються, в інформаційній сфері підрозділяються на інтереси особи, держави, суспільства. Проблема кіберзлочинності нині зачіпає як цілі країни, так і окремих осіб.

Виходячи з вищевикладеного, можна зробити висновок, що протидія кіберзлочинності – це частина національних інтересів держави.

Кіберзлочинність уже стала великою проблемою для всього світу, і проблема нестримно наростає. Правоохоронні органи намагаються поспіти за нею: законодавці ухвалюють нові закони, поліцейські агентства формують спеціальні підрозділи по боротьбі з кіберзлочинністю. Кіберзлочин як і будь-який інший злочин є не лише правова, але і соціальна проблема.

Необхідно створити уніфіковану класифікацію і формальну модель кіберзлочинів, які полегшать і протидію, і розслідування кіберзлочинності.

Організація забезпечення безпеки інформації повинна носити комплексний характер і грунтуватися на глибокому аналізі можливих негативних наслідків. При цьому важливо не упустити які-небудь істотні аспекти. Аналіз негативних наслідків припускає обов'язкову ідентифікацію можливих джерел загроз, чинників, що сприяють їх прояву і, як наслідок, визначення актуальних загроз безпеки інформації.

Під час такого аналізу необхідно переконатися, що всі можливі джерела загроз ідентифіковані, ідентифіковані і зіставлені з джерелами загроз усі можливі чинники (уразливості), властиві об'єкту захисту, усім ідентифікованим джерелам і чинникам зіставлені загрози безпеки інформації.

Попередження злочинності складається зі стратегій і заходів, спрямованих на зниження ризику вчинення злочинів і нейтралізацію потенційно шкідливих наслідків для приватних осіб і суспільства в цілому. У багатьох випадках стратегії протидії кіберзлочинності є невід'ємною частиною стратегій забезпечення кібербезпеки. Обстеження, у тому числі проведені в країнах, що розвиваються, показують, що більшість індивідуальних користувачів інтернету нині вживають основні запобіжні заходи. Уряди, що представили відповіді, організації приватного сектора і наукові установи, підкреслюють значення інформаційно-просвітницьких кампаній, що зберігається, у тому числі кампаній з питань нових загроз і кампаній, орієнтованих на конкретні цільові групи, наприклад дітей. Найбільша ефективність навчання користувачів досягається в разі поєднання навчання із системами, які допомагають користувачам безпечним чином досягти своїх цілей. Якщо витрати користувачів перевищують безпосередню отримувану ними вигоду, у людей зникає стимул застосовувати заходи безпеки. Організації приватного сектора також повідомляють, що обізнаність користувачів і співробітників має бути частиною комплексного

підходу до забезпечення безпеки. Указуються такі принципи і оптимальні види практики: відповідальність за підвищення обізнаності, політика і практичні заходи у сфері управління ризиками, керівництво на рівні рад директорів і професійна підготовка співробітників. Дві третини респондентів з організацій приватного сектора провели оцінку ризику кіберзлочинності, і більшість повідомляє про використання таких технологій забезпечення кібербезпеки, як міжмережевий захист, збереження цифрових доказів, ідентифікація змісту даних, виявлення вторгнень і контроль і моніторинг системи. У той же час було зазначено, що малі і середні підприємства або не приймають достатніх заходів для захисту систем, або помилково вважають, що вони не стануть мішенню злочинців.

Важливу роль у попередженні кіберзлочинності відіграє нормативно-правова база – як відносно приватного сектора в цілому, так і відносно постачальників послуг зокрема. Майже в половині країн ухвалені закони про захист даних, які передбачають вимоги відносно захисту і використання персональних даних. Деякі з цих режимів містять конкретні вимоги до постачальників послуг інтернету і інших постачальників електронних засобів зв'язку. Хоча закони про захист даних вимагають видаляти персональні дані, якщо їх більше не потрібно, в деяких країнах зроблені виключення для цілей карних розслідувань, згідно з якими постачальники послуг інтернету зобов'язані зберігати певні види даних упродовж певного терміну. У багатьох розвинених країнах є також правила, що вимагають від організацій у разі витоку даних повідомляти приватних осіб і регулюючі органи. Постачальники послуг інтернету зазвичай несуть обмежену відповідальність як "прості канали передачі" даних. Модифікація переданого змісту даних підвищує міру відповідальності, так само як і фактичне або передбачуване знання про незаконну діяльність. З іншого боку, оперативне вжиття заходів після отримання повідомлення знижує міру відповідальності. Незважаючи на наявність технічних можливостей, що дозволяють постачальникам послуг фільтрувати зміст інтернету, при обмеженні доступу до інтернету повинні дотримуватися критерії передбачуваності і співмірності, що передбачаються міжнародним правом у сфері прав людини, яке захищає право шукати, отримувати і передавати інформацію.

Центральним елементом у справі попередження кіберзлочинності є державно-приватне партнерство. Про наявність такого партнерства повідомляють більше половини всіх країн. Це партнерство рівною мірою створюється як на підставі неофіційних домовленостей, так і на юридичній основі. Найчастіше партнерські відносини встановлюються з організаціями приватного сектора, за ними йдуть наукові установи та міжнародні і регіональні організації. Партнерські відносини в основному використовуються для полегшення обміну інформацією про загрози і тенденції, а також для діяльності із попередження кіберзлочинності і вжиття заходів у конкретних випадках. У контексті деяких державно-приватних партнерств організації приватного сектора застосовують запобіжний підхід до проведення розслідувань і звернення в судові органи для боротьби з кіберзлочинністю. Такі заходи доповнюють зусилля правоохоронних органів і можуть допомогти понизити

заподіюваний жертвам збиток. Наукові організації виконують різноманітні функції у справі попередження кіберзлочинності, у тому числі за допомогою навчання і професійної підготовки фахівців, розробки законодавчої бази і політики, а також підготовки технічних стандартів і знаходження рішень. В університетах працюють і використовують наявні можливості експерти по кіберзлочинності, різні групи реагування на комп'ютерні інциденти і спеціалізовані науково-дослідні центри.

У зв'язку зі зростаючою кількістю злочинів, пов'язаних з використанням комп'ютерів, якому сприяє створення глобальних міжнародних і публічних електронних мереж, великого значення набуває міжнародна співпраця і координація дій у цій сфері. Просвіта і підвищення обізнаності громадськості може призводити до скорочення кількості злочинів в електронному середовищі. Транснаціональний характер злочинності з використанням комп'ютерної мережі дає підстави вважати, що розробка загальної політики з основних питань має бути частиною будь-якої стратегії боротьби зі злочинністю. Для розслідування кіберзлочинів потрібен персонал, що має конкретний судовий і технічний досвід і знання, а також наявність конкретних процедур. Для ефективного розслідування таких злочинів держави можуть потребувати допомоги з боку інших держав. Така допомога охоплює як співпрацю персоналу правоохоронних органів у робочому порядку, так і офіційну взаємну правову допомогу, що робиться через центральні органи.

Необхідно, щоб реалізація на практиці викладених пропозицій сприяла підвищенню ефективності протидії державних організацій, силових структур і спецслужб злочинам, що здійснюються у сфері комп'ютерних технологій. Адже проблеми дослідження комп'ютерних інцидентів можна вирішити і вирішувати надалі тільки при тісній взаємодії всіх зацікавлених представників держави і суспільства.

Література:

1. *Мельник С.В.* До проблеми формування понятійно-термінологічного апарату кібербезпеки / С. В. Мельник, О. О. Тихомиров [Електронний ресурс]. – Режим доступу : http://www.nbuv.gov.ua/portal/natural/Znpviknu/2011_30/Zbirnik_30_28.pdf.

2. Інформація щодо проведення в Харкові Всеукраїнській науково-практичній конференції "Протидія кіберзлочинності у фінансово-банківській сфері" [Електронний ресурс]. – Режим доступу : http://hbs.kharkov.ua/news_arc1.html.

3. Конвенція про кіберзлочинність. Рада Європи; Конвенція, Міжнародний документ від 23.11.2001 [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/994_575.

4. Кіберзлочинність в Україні [Електронний ресурс]. – Режим доступу : http://www.science-community.org/ru/node/16132.

5. Модели киберпреступлений [Электронный ресурс]. – Режим доступа: http://www.masiev.com/articles/informatsionnaja-bezopasnost/modeli-kiberprestuplenij-chast-2.

Надійшла до редколегії 20.01.2014 р.