УДК 343.98

О. Ф. Мельников,
д.держ.упр., проф.,
професор кафедри інформаційних технологій і систем управління ХарРІ НАДУ,
м. Харків

Ю. М. Онищенко,
викладач кафедри захисту інформації ХНУВС,
м. Харків

РЕФОРМУВАННЯ ДЕРЖАВНИХ МЕХАНІЗМІВ БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ

***Р**озглянуто та досліджено проблеми реформування державних механізмів боротьби з кіберзлочинністю як складової частини державної політики щодо боротьби зі злочинами у сфері інформаційних, телекомунікаційних технологій і засобів державного регулювання та контролю над нею.*

Ключові слова: нормативна база, конвенція, кіберзлочин, кібербезпека, злочин, телекомунікаційні технології, державна стратегія.

Боротьба з кіберзлочинністю неможлива без глибокого розуміння правових проблем регулювання інформаційних мереж. Саме аналіз взаємозв'язку між технічними характеристиками мережі та зумовленими цими характеристиками правовими і соціальними складнощами, з якими стикаються правоохоронні органи та законодавці, є першим кроком до можливого розроблення механізмів адекватного реагування на розвиток і зростання кіберзлочинності.

Проведений аналіз свідчить, що науковцями опрацьований значний комплекс проблем стосовно механізмів запобігання та протидії кіберзлочинності, зокрема і як важливої складової державної політики. Проблематику реформування державних механізмів у сфері запобігання і протидії кіберзлочинності в Україні в умовах світової глобалізації не систематизовано, щобільше, подекуди не визначено й найбільш суттєвих загроз. На таке вказують більшість дослідників у своїх публікаціях як у друкованих виданнях, так і в мережі Інтернет, а саме: П. Андрушко, С. Бабанін, В. Бутузов, А. Волеводз, В. Голубєв, М. Дашян, В. Дзюндзюк, Д. Дубова, В. Марков, М. Литвинов, А. Семенченко, Ю. Сиротюк, О. Стеблинська, Т. Тропіна, В. Хахановський, В. Цимбалюк, Б. Цюпін та ін.

Різноманітні питання теорії та практики запобігання кіберзлочинності, боротьби з її проявами та протидії злочинам у сфері високих технологій розглянуто в роботах Н. Ахтирської, П. Біленчука, В. Гавловського, В. Іщенка, М. Карчевського, О. Манжая, В. Номоконова, О. Орлова, О. Осипенко, Н. Савчука, І. Хараберюша та ін.

Аналіз наукової літератури засвідчив, що, за всієї значущості, проблему реформування державних механізмів Україні опрацьовано ще не в повному обсязі. Це пояснюється тим, що державне управління в цій сфері як складова науки державного управління перетинається з проблемами національної безпеки, інформаційних технологій, соціології тощо.

Мета статті – дослідити та проаналізувати проблеми сучасної нормативної бази з боротьби з кіберзлочинністю як складової частини державної політики щодо

боротьби зі злочинами у сфері інформаційних, телекомунікаційних технологій і засобів держаного регулювання та контролю над нею, надати пропозиції щодо покращення ситуації з регулюванням та запобіганням кіберзлочинності в країні.

В останні два десятиліття Інтернет, у більш широкому розумінні – кібернетичний простір, справив величезний вплив на всі верстви суспільства, наше повсякденне життя, основні права, адже соціальна та економічна взаємодія залежить від безперебійної роботи інформаційних і комунікаційних технологій. Відкритий та вільний кіберпростір сприяв політичній та соціальній інтеграції в усьому світі. Він знищив бар'єри між країнами, громадами та громадянами, дозволяючи взаємодіяти та обмінюватись інформацією та ідеями по всьому світі. Це забезпечує свободу виразу думки та здійснення основних прав, надаючи сили людям в їхньому прагненні створити більш демократичне суспільство.

Для забезпечення прозорості та свободи використання кіберпростору необхідно, щоб норми права, якими ЄС користується повсякденно, також було застосовано і до кібернетичного простору. Основні права, демократія і верховенство закону повинно бути максимально захищено в кіберпросторі.

Наші свобода та успіх усе більше залежать від надійності та розвитку кіберпростору, який надалі процвітатиме, якщо розвиватимуться приватний сектор і громадянське суспільство. Проте свобода онлайн також вимагає охорони та безпеки. Кіберпростір повинно бути захищено від випадків зловмисних дій та від зловживань, і уряди держав відіграють значну роль у забезпеченні вільного та безпечного кіберпростору. Уряди повинні здійснювати захист доступу та відкритості, поважати і захищати основні права в Інтернеті та підтримувати надійність і безпечність Інтернету.

Нині приватний сектор володіє та оперує значною частиною кіберпростору, і тому будь-яка ініціатива в цій сфері може бути успішною тільки при визнанні приватного сектора головним її учасником. Незважаючи на те, що в останні роки цифровий світ надає значну користь, він не став безпечнішим. Випадки вразливості Інтернету, будь то від навмисних чи випадкових дій, зростають тривожними темпами і можуть порушити постачання основних послуг, які ми сприймаємо як належне, наприклад, постачання води, електрики, послуг охорони здоров'я або мобільного зв'язку. Загрози можуть мати різне походження, у тому числі кримінальне, політично вмотивоване, терористичне, у вигляді проплачених певною державою атак, а також природних лих і ненавмисних помилок. Отже, ефективний контроль негативних явищ (інцидентів) у кібепросторі, таких як злочинність, вимагає набагато інтенсивнішої міжнародної співпраці, ніж заходи боротьби з будь-якими іншими формами транснаціональної злочинності. Проте світова спільнота поки не має в розпорядженні ані міжнародного органу, що спеціально займається інтернет-злочинністю, ані загальносвітового правового інструменту, що визначає масштаби відповідальності за відповідні злочини, та, що більш важливо, принципи співпраці у розслідуванні протиправних діянь.

Деякі кроки у справі захисту від кіберзагроз робить і наша країна. Затверджено закони України "Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки" та "Про захист персональних даних", розглянуто в другому читанні та прийнято в цілому Закон України "Про документи, що посвідчують особу та підтверджують громадянство України", який, однак, був заветований Президентом України через значні невідповідності до Конституції України та певних міжнародних стандартів. Також ініційовано і прийнято низку державних програм, що закріплюють як пріоритетний напрям державної політики упровадження інформаційних технологій

у сферу державного управління та побудову інформаційного суспільства. Держава планує збільшити кількість бюджетних місць для ІТ-спеціалістів у ВНЗ, тому що ІТ-галузь зростає щорічно на 40 % і забезпечує майже 3 % ВВП, і при цьому держзамовлення у вишах скорочується на 20 % [9].

Незважаючи на все, що було зроблено, Україна залишається дуже вразливою до кібервпливу. Така ситуація вимагає створення системи забезпечення інформаційної безпеки. За даними заступника Міністра оборони України В. Можаровського, така робота вже проводиться за напрямами створення нормативно-правової бази, вертикалі управління, системи підготовки кадрів, єдиного понятійного апарату [5].

Стратегічно важливо, щоб державне управління в Україні також було адаптовано під вирішення завдань кібервійни. За даними аналітиків, Україна наближається до світового лідерства за кількістю кіберзагроз, тільки 5 % комп'ютерних злочинів стають відомими (більшість потерпілих або не знають, що їх атакували, або приховують це). Одна з головних проблем ІТ-безпеки в Україні – відсутність незаангажованого та скоординованого підрахунку й оцінювання хакерських атак. У результаті країна не знає, як зламують її ресурси, хто це робить і звідки, хоча в Україні працює структура реагування на надзвичайні комп'ютерні пригоди (CERT-UA) та існують структури забезпечення інформаційної безпеки держави в правоохоронних відомствах [12].

Те, що Україна вразлива до хакерських атак, підтвердив український інформаційний ресурс "Сгіро", опублікувавши статтю, у якій зазначається, що Україна поступово посідає місце лідера за кількістю кіберзагроз. Видання оприлюднило ціну на хакерську атаку: розсилка спаму на 2 млн користувачів – від 1 000 грн; "DDOS-атака" – від 50 дол. на добу; зламування акаунту в соціальній мережі – 250 грн. Отже, невелика вартість хакерських послуг в Україні та висока вразливість українських користувачів мережі Інтернет свідчить про слабку захищеність населення держави в інформаційному просторі, що спрощує діяльність країн – потенційних супротивників при здійсненні деструктивних дій за допомогою мережі Інтернет [2].

За словами британського дослідника організованої кіберзлочинності Міші Гленні, Україна стала одним із центрів міжнародної інтернет-злочинності через поєднання таких чинників, як високий рівень безробіття поміж молодих освічених людей, неефективність правоохоронної системи та судочинства. У 2009 р. при Міністерстві внутрішніх справ України було створено відділ із боротьби з кіберзлочинністю, але хтось, незважаючи на те, що кількість інтернет-користувачів у країні вже сягає половини населення, порахував, що у працівників цього відділу роботи буде надто мало, тому додали йому до обов'язків ще й боротьбу з торгівлею людьми [13].

Довести вину тієї чи іншої держави, а особливо її уряду, у кібернападі вкрай важко, і тому цим прийомом широко користуються. Боротьба з кіберзагрозою, як і війна з тероризмом, схожі між собою розпливчастістю форм, можливостями сформувати образ ворога з будь-кого і де завгодно.

Маємо ситуацію вічного переслідування супротивника, який постійно вислизає. Необхідно пам'ятати, що сьогодні в Україні відроджується рекет, але він тепер – інформаційний. Мета інформаційного рекету – отримання комерційної інформації, шантаж керівництва комерційних структур, заволодіння підприємством. При цьому використовується заборонена законом закордонна спецтехніка, призначена для таємного отримання інформації. Наявність інформаційного рекету – серйозна загроза національній безпеці України. Зокрема, наслідком подій із файлообмінником EX.ua,

що мали місце в Україні в лютому 2012 р., стали масовані DDoS-атаки на сайти органів державної влади. Держава виявилась неготовою забезпечити свою інформаційну безпеку.

Директор юридичної компанії "IPStyle" Марія Ортинська з приводу намірів української влади розробити відповідне законодавство для контролю Інтернету заявила про неможливість встановлення в Україні контролю українського сегмента всесвітньої мережі. За її словами, перепис інтернет-населення зробити практично неможливо, поняття блогу і блогера відсутні в законодавстві та вхід в інтернет-кафе за паспортом – це обмеження прав людини. Із набранням чинності Законом України "Про захист персональних даних", який не забезпечує захист авторських прав користувачів, реєстратори доменних імен, такі як ТОВ "Хостмайстер", мусять закривати публічний доступ до інформації про фізичних осіб [14].

Опрацьовуючи державну управлінську політику, необхідно враховувати те, що в липні 2013 р. українська аудиторія користувачів Facebook становила 2 млн 800 тис. користувачів, збільшившися всього протягом року на 70 %. Експерти відзначають високий рівень проникнення соціальних мереж у життя українців – вищий, ніж у багатьох країнах світу. За даними дослідження Universal McCann, 81 % українських інтернет-користувачів сьогодні зареєстровані щонайменше в одній соціальній мережі. Для порівняння: у США – 65 %. За даними Державної служби статистики України, у 2013 р. в Україні налічувалося 61,722 млн абонентів мобільного зв'язку [7].

Порівняно з 2010 р. їхня кількість зросла на 7 %. Отже, залежність вітчизняної аудиторії від соціальних мереж швидко зростає, а держава не робить відповідних управлінських кроків щодо правового унормування, впорядкування та захисту від ризиків посилення глибокого інформаційно-психологічного впливу.

Імовірність проведення проти України кібернетичних атак і операцій у майбутньому залишається досить високою. Потенційними протиборчими сторонами України в таких війнах можуть бути країни, що мають необхідний промисловий та інтелектуальний потенціал. Застосування ними проти України низки подібних деструктивних дій може призвести до серйозних проблем, пов'язаних із забезпеченням безперебійного функціонування головних елементів інфраструктури нашої держави, цілісності інформації та її збереження – усього того, з чим уже зіштовхнулася більшість розвинених країн Заходу. Цьому не в останню чергу сприятиме: відсутність єдиної державної політики в галузі підтримання кібербезпеки України й недостатнє фінансування відповідних заходів; збільшення технологічного відриву України від провідних держав світу й активна протидія останніх створенню конкурентоспроможних українських інформаційних технологій; монополізація інформаційного ринку України, його окремих секторів вітчизняними й закордонними інформаційними структурами; використання несертифікованих вітчизняних і закордонних інформаційних технологій, засобів захисту інформації, засобів інформатизації, телекомунікації та зв'язку у процесі створення й розвитку власної кібер- та інформаційної інфраструктури тощо [1].

Враховуючи стан та можливості України, Володимир Мурашев, український науковець, кандидат технічних наук, доцент, пропонує вирішувати проблему національної кібербезпеки таким шляхом: створення національної операційної системи та необхідних пакетів прикладних програм, у тому числі й вітчизняного антивірусу, створення та відновлення вітчизняних потужностей із виробництва матеріально-технічної телекомунікаційної бази; автоматизовані робочі місця, інформаційно-телекомунікаційні системи повинні бути суто внутрішніми та не мати прямого виходу

до світової мережі Інтернет; матеріально-технічну базу інформаційно-аналітичних систем, окремих автоматизованих робочих місць формувати виключно через вітчизняних постачальників, які мають необхідні сертифікати відповідних державних уповноважених у системі захисту інформації; повністю виключити функцію сервісу віддаленого оцінювання стану роботоспроможності, виникнення позаштатних ситуацій окремих елементів матеріально-технічної та програмно-операційної складових інформаційно-телекомунікаційної системи та окремих автоматизованих робочих місць; під час придбання відповідних операційних систем, пакетів прикладних програм необхідно обумовлювати питання постачання вихідних текстів модулів; суттєво підвищити рівень свідомості дій та операцій усіх, без винятку, безпосередніх учасників роботи з критичною інформацією в умовах автоматизованого робочого місця, інформаційно-аналітичної пошукової системи, а також усіх учасників програмно-технічного забезпечення цієї роботи; обов'язкове ознайомлення працівників з можливими засобами забезпечення несанкціонованого витоку інформації та шляхами запобігання цьому [6].

Кібербезпека є тим самим випадком, про який записано в Конституції України, що це є "справою всього Українського народу". Кабінет Міністрів України вже спланував низку кроків щодо сприяння розвитку ІТ-галузі в Україні. Прийнято рішення підвищити якість підготовки фахівців у сфері інформаційних технологій, розширити базу їхньої підготовки, розглядаються пропозиції щодо спрощення митних процедур при ввезенні з-за кордону програмного забезпечення та комп'ютерної техніки для ВНЗ. Корпорація "Microsoft" готова запропонувати проект створення ІТ-академії [10].

Завідувач відділу Національного інституту стратегічних досліджень Д. Дубов справедливо вважає, що від кібернетичних злочинів Українська держава не може захиститися самотужки, але повинна самостійно реалізувати цілу низку узгоджених кроків: сформувати чітку політику в сфері кібербезпеки; змінити ставлення громадян до сфери інформаційної безпеки держави; налагодити тісну співпрацю з приватним сектором, громадянським суспільством та звичайними громадянами [3].

Конгрес США направив на підпис президентові США Бараку Обамі закон про права розвідки на 2015 фіскальний рік, у якому містяться положення про Україну, зокрема про українсько-американську співпрацю у сфері кібербезпеки.

Розділ 312 закону HR4681 присвячено співробітництву з Україною. Текст закону було представлено Обамі 12 грудня 2014 р. та опубліковано на сайті Конгресу [15].

Як повідомляється в тексті закону, розділ 312 "висловлює думку Конгресу, що співпрацю між розвідувальними та правоохоронними органами США і України має бути розширено для вдосконалення політики кібербезпеки". Крім того, США "повинні удосконалити процедуру видачі інформації між урядами Сполучених Штатів, України та інших країн, у яких зловмисники скоюють злочини проти громадян США і американських юридичних осіб".

На думку Конгресу, президент США повинен "ініціювати американо-українські двосторонні переговори щодо загроз кібербезпеці і співробітництва в боротьбі з кіберзлочинністю, з додатковими багатосторонніми переговорами, що включають інших правоохоронних партнерів, таких як Європол та Інтерпол".

Також він повинен "працювати над отриманням зобов'язання від України покінчити з кіберзлочинністю, що спрямована проти осіб поза межами України, і працювати зі Сполученими Штатами та іншими союзниками щодо стримування й засудження відомих кіберзлочинців" [4].

Статистика свідчить, що лише протягом 2010–2014 рр. кібернетичні командування та системи безпеки, як органи державного управління, було створено в багатьох країнах світу. До їхньої типової структури входять підрозділи:

– мережевих операцій;

– інформаційних операцій та інформаційної безпеки;

– підтримки і забезпечення операцій у кіберпросторі;

– радіоелектронної боротьби;

– операційні (командні) центри (центри управління у кризових ситуаціях) тощо.

Для забезпечення кібербезпеки, перш за все, необхідно забезпечити захист від деструктивних впливів у цій сфері та протидію їм. Отже, основними складовими кібербезпеки повинні бути кібернетична розвідка, кібернетичний захист та відповідні кібернетичні впливи.

Природа кіберзлочинності, зумовлена технологічними можливостями кіберпростору, значною мірою розмиває державні адміністративно-територіальні кордони та індивідуальні ідентифікаційні характеристики суб'єктів. Така суть кіберзлочинності висуває особливі вимоги до стратегії й тактики формування державної політики забезпечення інформаційної безпеки, що повинна передбачати систему заходів міжнародного і державного характеру.

Традиційним є структурний підхід до забезпечення інформаційної безпеки шляхом виділення окремих її напрямів, об'єднаних у групи за політичними, економічними, соціальними, військовими, науковими ознаками. Доктриною інформаційної безпеки України безпосередньо окремою загрозою визначені лише прояви комп'ютерної злочинності й тероризму, що загрожують безпечному функціонуванню національних інформаційно-телекомунікаційних систем. Проте широке розуміння комп'ютерного злочину дозволяє розгалужити його на складові всіх загроз, пов'язаних із негативною інформаційною дією, несанкціонованим доступом до інформації та інформаційних ресурсів, розголошуванням і приховуванням інформації, поширенням неякісної інформації, оскільки всі вони можуть реалізовуватися з використанням технологічних можливостей телекомунікаційних систем.

Література:

1. *Бурячок В. Л.* Завдання, форми та способи ведення війн у кібернетичному просторі / В. Л. Бурячок, Г. М. Гулак, В. О. Хорошко // Наука і оборона. – 2011. – № 3. – С. 40.

2. Воровать мы умеем. Украина становится эпицентром киберпреступности / Cripo. – Режим доступу : http://cripo.com.ua/?sect_id=6&aid=128098.

3. *Дубов Д.* Від кібернетичних злочинів українська держава не може захиститися самотужки / Д. Дубов // Уряд. кур'єр. – 2012. – № 24. – С. 5. – (8 лют.).

4. Конгрес США вимагає від Обами активно залучити Україну до сфери боротьби з кіберзлочинністю // ZAXID-NET. – Режим доступу : http://strichka.com/item/18747863.

5. Можаровський В. Збройні Сили України повинні відповідати сучасним вимогам / Володимир Можаровський // Військо України. – 2012. – № 1/2. – С. 6–11.

6. *Мурашев В.* Інформаційний простір та безпека / В. Мурашев // Камуфляж. – 2011. – № 10. – С. 14–15.

7. Найзаможніша людина світу візьметься за захист України // Online Експрес. – Режим доступу : http://expres.ua/news/2014/12/26/122574-nayzamozhnisha-lyudyna-svitu-vizmetsya-zahyst-ukrayiny.

8. *Прядко И.* Новая вера. Социальные сети накрывают мир и Украину, ломая привычные схемы общения между людьми. Бесследно эта болезнь не пройдет, убеждены специалисты / И. Прядко // Корреспондент. – 2012. – № 10 (498). – С. 32–34. – (16 марта).

9. Семиноженко назначили управляющим нацпрограммы нформатизации / The Telecom Blog // ProIt. – Режим доступу : tp://www.proit.com.ua/news/telecom/2011/08/01/163453.html.

10. Україні потрібна ІТ-академія // Уряд. кур'єр. – 2012.– № 30. – С. 3. – (16 лют.).
11. Українська аудиторія Facebook з початку року зросла на 500 тис. користувачів // iPress.ua. – Режим доступу : http://ipress.ua/news/ukrainska_audytoriya_facebook_z_pochatku_roku_zrosla_na_500_tys_korystuvachiv_23946.html.
12. *Устенко А.* Из Украины со взломом / А. Устенко // Фокус. – 2011. – 9 груд. – С. 38–39.
13. *Цюпин Б.* Кому страшні українські хакери? / Б. Цюпин // Український тиждень. – 2011. – № 38. – С. 32–33. – (16–22 верес.).
14. *Яблонский С.* Эксперт: Государство не станет "пересчитывать" блогеров : [Украинское государство не будет фиксировать всех блогеров и пользователей Интернета] / Станислав Яблонский // delo.ua. – Режим доступу: http://delo.ua/tech/ekspert-gosudarstvo-ne-stanet-pereschityvat-blogerov-162029.
15. H.R.4681 – Intelligence Authorization Act for Fiscal Year 2015. – https://www.congress.gov/bill/113th-congress/house-bill/4681/text.

Melnykov O. F., Onishchenko Y. M. **Reform of State Mechanisms to Fight Cybercrime.**
And consider the problems of reforming state mechanisms to combat cybercrime and as part of state policy in the fight against crimes in the field of information, telecommunication technology and state regulation and control over it.
Key words: normative base, convention, cybercrime, cyber security, crime, telecommunication technology, the government strategy.

Надійшла до редколегії 02.09.2015 р.

УДК 321:630

О. А. Мельниченко,
д.держ.упр., проф.,
професор кафедри економічної політики та менеджменту ХарРІ НАДУ,
м. Харків

ЛІСОВЕ ГОСПОДАРСТВО ЯК ОБ'ЄКТ ДЕРЖАВНОГО УПРАВЛІННЯ

***В**иокремлено характерні ознаки вітчизняного лісового господарства. Забезпечено подальший розвиток тлумачення поняття "державне управління лісовим господарством". Удосконалено класифікацію механізмів впливу на його розвиток. Конкретизовано перелік специфічних засобів (у межах традиційних методів) державного управління лісовим господарством. Узагальнено рекомендації щодо забезпечення розвитку цієї галузі національної економіки.*
Ключові слова: державне управління, механізми, методи, засоби, розвиток, лісове господарство.

Загальновідомо, що ліси є "легенями Планети". До того ж більшість людей полюбляють проводити дозвілля в лісі, який є чудовим місцем для відпочинку, збирання грибів, ягід і лікарських рослин та ін. Ліси також є джерелом сировини для деревообробної, целюлозо-паперової, хімічної, харчової й фармацевтичної промисловості, меблевого виробництва й майстрів народних промислів тощо. Крім того, ліси є територією для здійснення господарської діяльності, яка передбачає створення робочих місць і виготовлення продукції, а з тим – формування ВВП. Саме тому цілком виправданим є твердження: "добробут місцевих громад у багатолісних районах безпосередньо залежить від сталого розвитку лісового господарства" [18, с. 52],