УДК 343.98

ПРОБЛЕМИ БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ: МІЖНАРОДНИЙ ДОСВІД ТА УКРАЇНСЬКІ РЕАЛІЇ

Петровський О.М., Лівчук С.Ю.
Національний університет водного господарства та природокористування

У статті проведено дослідження у сфері боротьби з кіберзлочинами в ЄС і США, виділено позитивні сторони, які було б доцільно запровадити в Україні. Також проаналізовано проблеми, що виникають в області боротьби з комп'ютерними злочинами в Україні і надано пропозиції шляхів їх вирішення.
Ключові слова: кіберзлочинність, інформаційний злочин, інформація, боротьба, протидія, Стратегія, NERC CIP.

Постановка проблеми у загальному вигляді. Верховною Радою України було зроблено спробу врегулювати відносини, що виникають у кіберпросторі, а саме ухвалено Закон України «Про основні засади забезпечення кібербезпеки в Україні». Незважаючи на ці кроки Україна постійно стає жертвою кібератак, в зв'язку з чим питання протидії кіберзлочинності набуває особливої актуальності.

Метою статті є аналіз та дослідження проблемних питань протидії кіберзлочинності в Україні та на цій основі надати пропозиції щодо їх вирішення.

Виклад основних положень. Сьогодні у багатьох зарубіжних країнах налагоджена система співробітництва, що обумовлюється необхідністю обміну досвідом на міжнародному рівні. Ці питання координуються кожною країною відповідно до розробленої та діючої стратегії кібербезпеки: США та більшість країн-учасниць ЄС у своїх стратегіях виносять питання боротьби з кіберзлочинністю на передові позиції. Саме США стала першою країною, яка прийняла відповідний закон та створила Національну стратегію безпеки в кіберпросторі. Причиною написання даного документу стала терористична атака 11 вересня 2001 року. Стратегія була частиною більш загальної Стратегії забезпечення національної безпеки (National Strategy for Homeland Security). Крім того, за оцінками фахівців, саме в США щорічно втрати корпорацій від злочинності перевищують 200 млрд, а від комп'ютерних злочинів – 6 млрд. дол., тому питання боротьби з кіберзлочинністю для цієї країни є надзвичайно актуальним [9].

На державному рівні в США були прийняті такі важливі програмні документи, які створюють фундамент для боротьби з кіберзлочинністю, як: Міжнародна стратегія для кіберпростору «Процвітання, безпека, відкритість у мережевому світі» (2011); Кіберстратегія Міністерства оборони від квітня 2015 року; Міжвідомчий план дій з кібербезпеки систем управління (Cross-Sector Roadmap for Cybersecurity of Control Systems); План дій з посилення кібербезпеки найважливіших об'єктів інфраструктури (Roadmap for Improving Critical Infrastructure Cybersecurity, 2014); План дій з забезпечення кібербезпеки систем енергопостачання (Roadmap to Achieve Energy Delivery Systems Cybersecurity). Загалом у США проводиться виважена політика щодо боротьби з кіберзлочинністю, що дозволяє залучати до співпраці урядові організації та зацікавлених осіб, таким чином об'єднуючи їх зусилля.

Щодо кримінального законодавства США у сфері кіберзлочинності, то воно включає в себе Закон «Про боротьбу зі спамом» (Controlling the Assault of Non-solicited Pornography and Marketing, 2003); Закон «Про злочини, пов'язані з засобами доступу» (Fraud and related activity in connection with access devices); Закон «Про злочини, пов'язані з комп'ютерами» (Fraud and related activity in connection with computers); Закон «Про злочини, пов'язані з електронною поштою» (Fraud and related activity in connection with electronic mail); Закон «Про перехоплення електронних повідомлень та прослуховування переговорів» (Wire and Electronic Communications in Terception and Interception of Oral Communications); Закон «Про зберігання повідомлень та доступ до записів транзакцій» (Stored Wire and Electronic Communications and Transactional Record Access) [6]. Усі види кіберзлочинів поділяються на три групи: злочини проти інтелектуальної власності; злочини, що завдають шкоди комп'ютерному обладнанню; злочини проти користувачів комп'ютерної мережі.

Для протидії кіберзлочинності в США були створені спеціальні підрозділи та відомства:

1. Electronic Crimes Task Forces ECTF підрозділ Секретна служба США (United States Secret Service USSS), що було створене у 1865 році для розслідування і запобігання фальшивомонетництва. Проте з роками відбулась еволюція її функцій і на сьогоднішній день Секретна служба США бореться з економічними та комп'ютерними злочинами [3].

2. Федеральне агентство США, що підпорядковане міністерству внутрішньої безпеки США (уведено в підпорядкування в 2003 р. до цього було підпорядковано міністерству фінансів США). Воно утворює взаємодію між службами, правоохоронними органами (федерального рівня, рівня штату, локальними), приватним сектором, академічним співтовариством, що в свою чергу виявляють і запобігають кіберзлочинам.

3. US Cyber Command (Військовий підрозділ, який здійснює свою діяльність у кіберпросторі).

4. United States Computer Emergency Readiness Team (Національний відділ кіберзахисту Департаменту внутрішньої безпеки США).

5. Computer Crime and Intellectual Property Section (Відділ комп'ютерної злочинності і інтелектуальної власності).

6. Internet police (Інтернет-поліція, мережева поліція).

Поряд з США активну боротьбу з кіберзлочинністю проводить в країнах Європейського Союзу. В ЄС створений необхідний нормативно-правовий фундамент з питань захисту кіберпростору. Стратегія кібербезпеки ЄС була прийнята в 2013 році. Її особливістю є те, що стратегією були охоплені різні аспекти кіберпростору, зокрема, внутрішній ринок, правосуддя, внутрішня та зовнішня політика.

Разом із Стратегією була розроблена та прийнята законодавча пропозиція про посилення безпеки інформаційних систем ЄС. Пріоритетами міжнародної політики ЄС у кіберпросторі, як їх визначає Стратегія, є:

– Свобода та відкритість: стратегія визначає принципи користування основоположними правами людини та громадянина у кіберпросторі;

– Застосування законодавства ЄС у кіберпросторі в тій самій мірі, як і у фізичному світі. Відповідальність за безпеку кіберпростору лежить на усьому суспільстві: від звичайних громадян до цілих держав;

– Розвиток потенціалу кібербезпеки через співробітництво з міжнародними партнерами та організаціями, приватним сектором та громадянським суспільством [1].

Не зважаючи, на прийняття такого важливого стратегічного документа, все ж існують численні загрози. Серед основних недоліків системи кібербезпеки ЄС можна виділити:

По-перше, відсутність єдиної європейської системи реагування на кібератаки.

По-друге, відмінність стандартів у сфері кібербезпеки в різних країнах. По-третє, відсутність чіткого уніфікованого категоріального апарату.

По-четверте, недостатній рівень координації діяльності між наднаціональними і національними цивільними та військовими органами, що призводить до дублювання їх завдань.

По-п'яте, низький рівень обміну інформацією про кіберінциденти між державами-учасницями.

По-шосте, недостатній рівень державно-приватного співробітництва, що обумовлено низькою зацікавленістю приватного сектора представляти державним структурам інформацію про кіберінциденти.

По-сьоме, значна диспропорція рівня готовності до протидії кіберзагрозам на національному рівні. На сьогодні тільки 10 з 27 країн ЄС відпрацювали національні стратегії кібербезпеки. На сьогодні найзахищенішими країнами є Данія, Великобританія, Фінляндія, Швеція, Франція і Нідерланди [5].

Франція орієнтується на те, щоб інформаційні системи були здатні протистояти подіям в кіберпросторі, які можуть негативно вплинути на доступність, цілісність і конфіденційність інформації. Франція робить ставку на технічні засоби захисту інформації, боротьбу з кіберзлочинністю і встановлення кіберзахисту. Відповідно до оприлюдненої стратегії Франції в галузі оборони і безпеки інформаційних систем [2], основними цілями є:

1. Мати кіберзахист світового рівня.

2. Гарантувати свободу рішень Франції шляхом захисту конфіденційної та секретної інформації.

3. Зміцнити кібербезпеку критичної національної інфраструктури.

4. Забезпечити безпеку в громадянському кіберпросторі.

17 липня 2014 року Прем'єр-міністр Франції оприлюднив першу глобальну політику безпеки інформаційних систем, яка фіксує правила захисту державних інформаційних систем і якою держава демонструє свою рішучість надавати приклад у сфері досягнення необхідного рівня кібербезпеки. 27 березня 2015 року Декретом № 2015-351 уряд Франції сформулював нові положення безпеки інформаційних систем операторів галузей, роль яких має критичне значення для життєдіяльності нації. Зазначене свідчить, що питання безпеки інформаційного простору у сучасному світі є особливо актуальними та потребують розв'язання на державному рівні [10].

Підхід Сполученого Королівства також спрямований на розвиток кібербезпеки. Мета: вивести Сполучене Королівство на перше місце з інновацій, інвестицій та якості сервісів у сфері інформаційно-телекомунікаційних технологій, і тим самим, в повній мірі скористатися всіма перевагами і достоїнствами кіберпростору. Необхідно виключити ризики типу кібератак злочинців, терористів та інших держав з метою зробити кіберпростір безпечним для громадян і економіки.

Зауважимо також, що в країнах ЄС активно створюються спеціальні органи боротьби з кіберзлочинністю. В загальному ці органи можна поділити на дві групи. Першу групу складають органи, що займаються формуванням та реалізацією національної політики по боротьбі з кіберзлочинністю. Другу групу складають органи, що здійснюють запобігання та розслідування злочинів, що вчиняються в кіберпросторі.

Формування національної політики щодо забезпечення кібербезпеки здійснюють органи загальної компетенції або ж спеціально створені органи. Так, органами загальної компетенції є Комітет з питань безпеки Фінляндії, Центр захисту національної інфраструктури Великобританії, Управління національної безпеки Чехії, Національне управління з питань безпеки та контр тероризму, Міністерство адміністрації та впровадження цифрових технологій Польщі. Ряд зарубіжних країн, також створили спеціальні органи, завданням яких є формування і реалізації політики у сфері кібербезпеки. Так, у Франції діє Національна служба безпеки інформаційних технологій, у Великобританії функціонує Управління кібербезпеки та інформаційного забезпечення, у Австрії – Керівна група з кібербезпеки.

Отже, зарубіжні країни використовують такі основні напрямки боротьби зі злочинністю: створення політичних програм боротьби зі злочинністю; нормативно-правове регулювання інформаційної сфери; встановлення кримінальної відповідальності за кіберзлочини; міжнародне співробітництво у сфері протидії кіберзлочинності; створення спеціальних органів для попередження та розкриття кіберзлочинів.

Враховуючи досвід розвинених країн Україна має можливість використати дієві способи та методи, щодо запобігання та кращого виявлення кіберзлочинів. Аналіз протидії кіберзлочинності у багатьох країн-членів ЄС та США дозволяє зробити висновок про те, що вітчизняна система потребує вдосконалення, зокрема приведення у відповідність до міжнародних стандартів. З цією метою варто:

1. Сформувати державну політику так, щоб можна було б забезпечити досконалу боротьбу з кіберзлочинністю та залучити до цієї проблеми громадські та урядові організації.

2. Забезпечити технічний розвиток інновацій, що буде гарантувати кібербезпеку.

3. Удосконалити діяльність та переглянути повноваження спеціальних органів, сферою праці яких є кіберпростір та боротьба з кіберзлочинами.

4. Затвердити на законодавчому рівні більш широкий перелік злочинів які відносяться до кіберзлочинів та збільшити міру покарання.

У той час, коли у світі ведеться активна боротьба з кіберзлочинністю, Україна у цьому ж напрямі робить повільні і невпевнені кроки. Нормативне регулювання сфери кібербезпеки в Україні не є чітко врегульованим. що і сприяє загостренню даної проблеми. На сьогоднішній день Україна є лідером серед країн, які найчастіше страждають від кібератак. Так, у 2011 рік було здійснено 131 злочин у сфері кіберзлочинності з роками результати ставали дедалі гіршими. У 2012 році було вчинено вже 255 злочинів у сфері електронно-обчислювальних машин, а за 2013 рік – 595 злочинів. За даними 2016-2017 рр., офіційно зафіксовано 705 таких злочинів і, за прогнозами, з роками ця кількість буде лише зростати [4].

Для ефективної боротьби з кіберзлочинністю в Україні, за прикладом зарубіжних країн варто було б: створити політичне підґрунтя (концептуальний рівень), удосконалити систему законодавства (законодавчий рівень), визначити систему органів, основними функціями яких було б забезпечення кіберзахисту України (інституціональний рівень).

Одним із перших кроків в напрямку створення політичного підґрунтя стало прийняття Указу Президента «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» [6].

Основною метою даної Стратегії є забезпечення безпечних умов користування кіберпростором, захист інтересів особистості, суспільства і держави. Враховуючи всі позитивні та негативні сторони за умовами Стратегії Україна повинна утворити велику високотехнічну систему для забезпечення надійності і безпеки зв'язку в інформаційній сфері. А враховуючи стан України в даних питаннях це здається не простим завданням. Також, Стратегією визначено мету щодо утворення «активного кіберзахисту», що спрямована на розширення правових меж сектора безпеки і оборони в кіберпросторі, створення засобів та інструментів які б могли відповідати на агресію у віртуальному просторі.

Названа Стратегія потребує чималих змін і перетворень у законодавстві, але безсумнівно, вона є хорошим поштовхом для позитивних змін у сфері кібернетичної безпеки.

Крім того, Розпорядженням Кабінету Міністрів України від 10.03.2017 № 155-р «Про затвердження плану заходів на 2017 рік з реалізації Стратегії кібербезпеки України» було затверджено заходи, спрямовані на удосконалення нормативно-правового регулювання кібербезпеки, створення технологічної складової національної системи кібербезпеки, налагодження більш тісного співробітництва з міжнародними партнерами України, налагодження процесу підготовки кадрів у сфері кібербезпеки.

Щодо законодавчої складової, то Закон України «Про основні засади забезпечення кібербезпеки України» беззаперечно став найбільш прогресивним кроком для держави у сфері боротьби з кіберзлочинністю. Суттєвими перевагами закону можна назвати: визначення основних понять, таких як: «кіберпростір», «кіберзлочин», «кіберзлочинність», «кібертероризм» та інші. Також вказано основні принципи боротьби з кіберзлочинами як такими; зазначення основних принципів забезпечення кібербезпеки України; визначення сукупності суб'єктів забезпечення кібербезпеки та взаємопов'язаних заходів політичного, науково-технічного, інформаційного, освітнього характеру, організаційних, правових, оперативно-розшукових, розвідувальних, контррозвідувальних, оборонних, інженерно-технічних заходів, а також заходів криптографічного і технічного захисту національних інформаційних ресурсів, кіберзахисту об'єктів критичної інформаційної інфраструктури.

Хоча цей закон і дав великий поштовх для розвитку національного законодавства з питань забезпечення кібербезпеки, його все ж не можна назвати ідеальним. Проаналізувавши норми Закону України «Про основні засади забезпечення кібербезпеки України» нами було визначено такі основні проблеми:

По-перше, законом не визначено єдиний орган, основною функцією якого мало б стати оперативне керування над всіма суб'єктами забезпечення кібербезпеки у мирний час. Це може стати значною проблемою, адже функції органів чітко не розмежовані, а це приводить до дублювання деяких повноважень, що, на нашу думку, є недопустимим. Наприклад, завданням РНБО стало здійснення лише координації та стратегічного управління. Генштабу – оперативне командування в «особливий період».

По-друге, відсутність трансформаційного підходу. Закон не визначає організацію, яка б управляла упровадженням кібербезпеки на загальнонаціональному рівні.

По-третє, надмірні повноваження держспецзв'язку щодо аудиту об'єктів інфраструктури, що є приватною власністю. Насамперед, це зачепить весь великий та середній бізнес. В той же час, Державний спеціальний зв'язок наділений правом визначення вимог для аудиторів та щодо порядку їх атестації. Це несе в собі загрозу тиску зі сторони держави на бізнесменів і на бізнес в цілому. Це також може стати поштовхом для розвитку корупції. Яскравим прикладом є видання ліцензій для аудиторів в першу чергу «своїм» підприємствам, якими, в свою чергу, перевірка

проводитиметься «на папері», що прямо суперечить державній політиці з дерегуляції.

По-четверте, загроза тотального шпигунства. За прийнятим законом Службі безпеки України надається надмірне право проводити таємні перевірки щодо кібербезпеки критичних об'єктів. По суті, СБУ надається повноваження щодо проведення хакерських атак на приватний бізнес.

По-п'яте, занадто широкий перелік об'єктів, яких стосується закону. Це не дозволить в повній мірі контролювати усіх їх і забезпечити нормальне регулювання питань забезпечення кібербезпеки для усіх об'єктів.

Таким чином, норми названого закону потребують суттєвого доопрацювання в окреслених нами напрямках.

Враховуючи викладене необхідно констатувати, що для формування ефективної системи протидії кіберзлочинності в Україні, необхідно вжити низку системних заходів на концептуальному, нормативно-правовому, та інституціональному напрямах.

– на концептуальному рівні: визначити основні загрози кібербезпеці та сформувати заходи спрямовані на їх відвернення та попередження, створити систему технологічних засобів складової національної системи кібербезпеки, налагодити більш тісне співробітництва з міжнародними партнерами України.

– на законодавчому рівні: по-перше, визначити єдиний органу, який би здійснював оперативне управління усіма суб'єктами, чиїм завданням є забезпечення кібербезпеки (кіберпідрозділи силових відомств) у мирний час. Ми пропонуємо визнати таким органом Генштаб Збройних Сил України, що відповідає моделі у прибалтійських країнах;

по-друге, обмежити повноваження Державного спецзв'язку та Служби безпеки України, що зменшить ризик шпигунства та розвитку корупції. Це стане можливим, якщо аудит буде проводитись незалежними аудиторами, що зменшить ризик корупціювання гілок великого та середнього бізнесу. NERC CIP в США є прикладом саморегулюючої організації, що розробила галузеві стандарти з кібербезпеки для енергетичного сектора, які можна було б запровадити в Україні;

по-третє, скасувати можливість таємних перевірок критичних об'єктів, що знаходяться у приватній власності;

по-четверте, обмежити об'єкти, які перераховані в Законі України «Про основні засади забезпечення кібербезпеки України», залишивши у ньому винятково ті об'єкти, які знаходяться у власності держави. Також важливим кроком стане перерахування решти критичних об'єктів, які знаходяться у приватній власності, в окремому законопроекті

– на інституціональному рівні: скоротити перелік тих суб'єктів, чиї повноваження стосуються забезпечення кібербезпеки України, чітко визначити компетенцію кожного з таких органів для попередження дублювання їх функцій.

Список літератури:

1. EU International Cyberspace Policy [Електронний ресурс]. – Режим доступу: http://www.eeas.europa.eu/policies/eu-cyber-security/index_en.htm
2. La stratйgie de la France en matiиre de cyberdйfense et cybersйcuritй [Електронний ресурс]. – Режим доступу: http://www.ssi.gouv.fr/publication/la- strategie-de-la-france-en-matierede-cyberdefense-et-cybersecurite-2/
3. United States Secret Service USSS [Електроний ресурс]. – Режим доступу: http://www.secretservice.gov/investigation/
4. Відповідь Генеральної Прокуратури України на запит О.О. Ткача від 11.05.17 № 19/4-681 вих. - 17/ [Електронний ресурс]. – Режим доступу: https://dostup.pravda.com.ua/request/statistika_kibierzlochinnosti_v#outgoing-23042
5. Европейский опыт создания эффективной системы кибербезопасности [Електронний ресурс]. – Режим доступу: http://cybersafetyunit.com/evro peyskiy- opyit-sozdaniya-effektivnoy-sistemyi-kiberbezopasnosti/
6. Законодавство та стратегії у сфері кібербезпеки країн Європейського Союзу США, Канади та інших [Електронний ресурс]. – Режим доступу: http://parlament.org.ua/wp-content/uploads/2016/11/INFODOVIDKA-ZAKONODAVSTVO-TA-STRATEGIYI KIBERBEZPEKA.pdf
7. Закон України «Про основні засади забезпечення кібербезпеки України» від 19.06.2015 № 2126а / [Електронний ресурс]. – Режим доступу: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_2?pf3516=2126a&skl=9
8. Словник термінів з кібербезпеки / за заг. ред. О. Копатіна, Є. Скулишина. – К.: Аванпост- Прим, 2012. – 214 с.
9. См.: Youtsen M. Research on European Juvenile Delinquency // HEUNI Publication Series. 1987. – № 7. – С. 57-62.
10. Стратегія захисту національного кіберпростору: досвід Франції [Електроний ресурс]. – Режим доступу: http://www.dridu.dp.ua/konf/konf_dridu/itis%20seminar%202015/pdf/22.pdf
11. Указ Президента України Про рішення Ради національної безпеки і оборони України «Про Стратегію кібербезпеки України» від 27.01.2016 р. № 96/2016/[Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/96/2016

Петровский А.Н., Ливчук С.Ю.
Национальный университет водного хозяйства и природопользования

ПРОБЛЕМЫ БОРЬБЫ С КИБЕРПРЕСТУПНОСТЬЮ: МЕЖДУНАРОДНЫЙ ОПЫТ И УКРАИНСКИЕ РЕАЛИИ

Аннотация
В статье проведено исследование в сфере борьбы с киберпреступностью в ЕС и США, выделено положительные стороны, которые было бы целесообразно ввести в Украине. Также проанализированы проблемы, возникающие в области борьбы с компьютерными преступлениями в Украине и предоставлено предложения путей их решения.
Ключевые слова: Киберпреступность, информационный преступление, информация, борьба, противодействие, Стратегия, NERC CIP.

Petrovsky O.M., Livshchuk S.Y.
National University of Water and Environmental Engineering

PROBLEMS OF COMBATING CYBERLOVICITY: INTERNATIONAL EXPERIENCE AND UKRAINIAN REALITY

Summary
The article is devoted to research on the fight against cybercrime in the EU and the USA, and identifies the positive aspects that would be appropriate to introduce in Ukraine. Also analyzed are the problems that arise in the field of combating computer crimes in Ukraine and provided suggestions for ways to solve them.
Keywords: Cybercrime, Information Crime, Information, Struggle, Counteraction, Strategy, NERC CIP.