ISSN 2225-5036 (Print), ISSN 2411-071X (Online)
http://infosecurity.nau.edu.ua; http://jrnl.nau.edu.ua/index.php/Infosecurity

DOI: 10.18372/2225-5036.25.13665

ЄВРОПЕЙСЬКИЙ ДОСВІД З ПИТАНЬ БОРОТЬБИ З ПРАВОПОРУШЕННЯМИ В ІНФОРМАЦІЙНІЙ СФЕРІ

Анатолій Марущак

Національна академія СБ України

МАРУЩАК Анатолій Іванович

Науковий ступінь та звання: доктор юридичних наук, професор
Рік та місце народження: 1977 рік, с.м.т. Ставище, Київська область, Україна.
Освіта: Національна академія СБ України, 1999 рік.
Посада: директор Інституту НА СБ України.
Наукові інтереси: інформаційне право та інформаційна безпека.
Публікації: понад 160 наукових публікацій, серед яких монографії, підручники, навчальні посібники, наукові статті, матеріали і тезиси доповідей на наукових конференціях і інше.
E-mail: martol_law@ukr.net.
Orcid ID: 0000-0003-0069-3727.

Анотація. *Правопорушення в інформаційній сфері стають усе більш поширеними з розвитком інформаційних технологій. Дискусії ведуться навколо поєднання і співвідношення корпоративних норм обробки інформації, закріплених переважно у політиках конфіденційності або безпеки, з вимогами національного законодавства щодо цивільно-правової, адміністративно-правової, кримінально-правової охорони різних категорій інформації. У статті здійснено аналіз найбільш поширених правопорушень в інформаційній сфері: кіберправопорушень і дезінформування, проаналізовано європейський досвід з питань боротьби із такими правопорушеннями. Запропоновано рекомендації для правоохоронних органів України, а також зроблено припущення про перспективне законодавче закріплення юридичної відповідальності за дезінформування як окремий склад інформаційного правопорушення.*

Ключові слова: *інформація, кіберзлочини, дезінформування, правоохоронні органи, інформаційне право.*

Постановка проблеми

Проблематика правопорушень в інформаційній сфері стає усе більш актуальною з розвитком інформаційних технологій. Дискусії ведуться навколо поєднання і співвідношення корпоративних норм обробки інформації, закріплених переважно у політиках конфіденційності або безпеки, з вимогами національного законодавства щодо цивільно-правової, адміністративно-правової, кримінально-правової охорони різних категорій інформації. Численні кібератаки та кіберінциденти як в Україні, так і у всьому світі зумовлюють підвищення уваги державних органів і, відповідно, науковців до проблематики боротьби з правопорушеннями в інформаційній сфері.

Правопорушення в інформаційній сфері умовно поділяємо на два види: кіберправопорушення і дезінформування.

Європейські країни активно використовують міжнародно-правові інструменти для удосконалення ефективності діяльності правоохоронних органів щодо боротьби з правопорушеннями в інформаційній сфері. Так, групи реагування на інциденти (CERT) різних рівнів своїх держав взаємодіють між собою у частині оперативного обміну інформацією про технології, ознаки і методики кіберінцидентів, зокрема і транснаціональних кіберзлочинів та кібертероризму. Наприклад, на створення сприятливих умов задля оперативного обміну інформацією та досвідом між командами екстреного реагування НАТО «Computer Incident Response Capability» (NCIRC) та ЄС «Computer Emergency Response Team of the European Union» (CERT-EU) у сфері протидії кібератакам, комплексного протистояння сучасним викликам у кіберпросторі у лютому 2016 року ЄС та НАТО підписали технічну угоду щодо посилення співпраці у сфері кібербезпеки.

Одним із елементів інформаційно-аналітичного забезпечення діяльності правоохоронних органів є використання ресурсів репозиторію «Cybercrime», створеного у 2015 році в межах Комісії з попередження злочинності і кримінального правосуддя, який містить бази даних законодавства, прецедентного права (понад 180 країн) про кіберзлочинність та електронні докази, судову практику, а також записи успішних правоохоронних операцій щодо кіберзлочинів та збирання електронних доказів [1].

Корисними є також 10 найкращих стратегій з забезпечення збереження інформації від Агенції національної безпеки (NSA) та Департаменту внутрішніх справ США (IAD).

Мета статті – аналіз теоретичних положень і практики держав-членів ЄС щодо боротьби з правопорушеннями в інформаційній сфері. Об'єкт дослідження – суспільні відносини та закономірності, які виникають у процесі правоохоронної діяльності в

інформаційній сфері. Предмет дослідження – європейський досвід з питань боротьби з правопорушеннями в інформаційній сфері.

Аналіз останніх досліджень

Науковці розглядали проблематику боротьби з правопорушеннями в інформаційній сфері лише дотично (О. Корченко, Д. Горніцька, А. Гололобов [2]). У попередніх працях автор розпочав наукову дискусію щодо означеної проблематики [3, 4].

Викладення основного матеріалу

Стосовно найбільш суспільно небезпечних кіберправопорушень – кіберзлочинів – реально діючим міжнародним документом є Конвенція Ради Європи з кіберзлочинності від 21.11.2001 р. (далі – Конвенція), яка спрямована на підвищення ефективності кримінальних розслідувань і переслідувань, що стосуються кримінальних правопорушень, пов'язаних з комп'ютерними системами і даними, на надання можливості збирання доказів, що стосуються кримінального злочину в електронній формі [5]. До Конвенції приєдналося 56 країн: як члени Євросоюзу, так і США, Японія, Австралія, Аргентина, Чилі, Сенегал, Україна та інші. У 2016 році представника СБ України обрано до керівного органу Комітету – Бюро Комітету Конвенції.

Інструментом забезпечення ефективності взаємодії правоохоронних органів у сфері боротьби із загрозами в інформаційній сфері та організованою кіберзлочинністю є передбачена статтею 35 Конвенції цілодобова інформаційна мережа національних контактних пунктів «24/7».

Основними завданнями мережі є:

– забезпечення збирання і вилучення електронних доказів у провадженнях щодо вчинення транснаціональних кіберзлочинів та кібертероризму;

– забезпечення термінового збереження комп'ютерних даних, які використовуються, обробляються чи пересилаються за допомогою комп'ютерних систем і мереж та щодо яких існує загроза їх знищення або модифікації;

– отримання інформації щодо обставин вчинення транснаціональних кіберзлочинів та кібертероризму;

– встановлення місцезнаходження осіб, підозрюваних у вчиненні транснаціональних кіберзлочинів та кібертероризму;

– забезпечення оперативного інформаційного обміну щодо збережених та отриманих даних, а також щодо транснаціональних кіберзлочинів та кібертероризму.

Рада Європи останніми роками шляхом залучення якомога більшої кількості країн з різних частин світу до ратифікації Конвенції вживає зусиль щодо її перетворення на єдиний міжнародний механізм, на противагу позиції Російської Федерації, Китаю, Ірану, Південно-Африканської Республіки, які пропонують ухвалити Конвенцію щодо протидії інформаційним загрозам рішенням Ради Безпеки ООН.

Для протидії транснаціональній кіберзлочинності в ЄС застосовуються також Директива ЄС стосовно боротьби з сексуальною експлуатацією дітей он-лайн та дитячою порнографією (2011), Директива ЄС щодо протидії кібератакам на інформаційні системи (2013), Директива щодо посилення рівня кіберзахисту в інформаційно-телекомунікаційних мережах на території держав-членів ЄС (2016), Директива Єврокомісії щодо боротьби з шахрайством та іншими фінансовими злочинами в мережі Інтернет (2017), а також Стратегія кібербезпеки ЄС (2013). Остання передбачає здійснення кіберзахисту зокрема і за напрямом виявлення і розслідування кіберзлочинів.

Директива 2016/1148/ЕС від 6 липня 2016 року передбачає створення команди інцидентів Computer Security Response (CSIRT) і компетентних відповідальних національних органів NIS; співпрацю між усіма державами-членами ЄС шляхом створення уповноважених підрозділів, з метою надання підтримки та сприяння обміну інформацією між державами-членами про кіберзагрози, кіберзлочини та кіберінциденти.

До речі, угоду про співпрацю у сфері безпеки інформаційних технологій з Департаментом інформаційної безпеки Агентства внутрішньої безпеки Польщі має команда реагування на комп'ютерні інциденти Польщі (CERT Polska), яка опікується питаннями захисту та безпеки інформаційної інфраструктури і є підрозділом найбільшого приватного оператора телекомунікацій Польщі – NASK.

Крім того, Агентство внутрішньої безпеки Польщі має урядову команду реагування на комп'ютерні інциденти – CERT GOV PL, метою якої окрім іншого є забезпечення і розвиток спроможності органів державного управління захищатись від кіберзлочинів, зокрема, від атак на інфраструктуру, що складається з IT-систем і мереж, порушення або руйнування яких може загрожувати життю і здоров'ю людей, національним багатствам та навколишньому середовищу, або привести до значних фінансових втрат і до порушень у функціонуванні органів державного управління. CERT Polska (NASK) у співпраці з Департаментом інформаційної безпеки Агентства внутрішньої безпеки Польщі розробила та здійснює підтримку розподіленої інтернет-системи раннього оповіщення - ARAKIS-Gov [6].

У 2013 році, з метою оперативних та інформаційно-аналітичних можливостей взаємодії країнчленів ЄС у боротьбі з кіберзлочинністю, проведення спільних розслідувань проявів кіберзлочинності в Європейському Союзі, було прийнято рішення про заснування у м.Гаага, Нідерланди, Європейського центру по боротьбі з кіберзлочинністю (European Cybercrime Centre (EC3).

Основними завданнями Центру є :

– забезпечення координації та обміну інформацією між підрозділами правоохоронних органів ЄС та третіми країнами;

– боротьба з розповсюдженням у мережі Інтернет дитячої порнографії;

– підготовка кваліфікованих експертів у галузі боротьби з кіберзлочинністю;

– розробка та застосування методів припинення злочинів у сфері інформаційних технологій.

ЕС3 співпрацює з Глобальним інноваційним комплексом Інтерполу в Сінгапурі. Центр створений з метою координації міжнародних заходів з протидії наступним проявам кіберзлочинності:

– злочини, які скоєні міжнародними злочинними угрупованнями з метою отримання значних прибутків, або у результаті діяльності яких була нанесена значна шкода;

– злочини, які завдають значної шкоди потерпілим, зокрема, сексуальна експлуатація дітей онлайн, розповсюдження порнографії, кібернасильство тощо;

– злочини, які завдають шкоди життєво важливій критичній інфраструктурі країн-членів ЄС.

Важливу увагу правоохоронні органи ЄС приділяють взаємодії з Європейською агенцією мережевої та інформаційної безпеки (European Network and Information Security Agency, ENISA) та CERT-EU, який виявляє кібератаки за допомогою спеціалізованої технологічної системи датчиків, встановлених на абонентських лініях доступу до серверів.

CERT-EU надає інформацію про виявлені кібератаки з ознаками злочинних дій до ЕС3, який може поінформувати про них Європейську агенцію оборони (European Defence Agency) для організації кібероперацій або Європейську службу зовнішніх справ (European External Action Service) для реагування дипломатичними каналами [7].

Європол 23 травня 2018 року підписав Меморандум про взаєморозуміння, яким встановлено основи співпраці з ENISA, Європейським оборонним агентством (EDA) та CERT-EU [8].

Однією з найбільших проблем боротьби з кіберзлочинністю є ефективність процедур правової допомоги країн-підписантів Конвенції. У цьому напрямку Комітетом Конвенції з 2017 року здійснюється робота щодо укладання додаткового протоколу до Конвенції стосовно поглибленої взаємодії із світовими провайдерами Інтернет-послуг, створення спільних робочих груп з розслідування кіберзлочинів тощо.

Заслуговує на увагу досвід боротьби з кіберзлочинністю Великої Британії, у якій запроваджено Модель обміну інформацією (Information Exchange Model) між урядовими установами і приватним сектором на принципах «Chatham House» (можна поширювати і використовувати інформацію, почуту на зустрічах про виявлені атаки, втрату інформації тощо, але заборонено вказувати, хто її оприлюднив і де відбувся кіберінцидент). Координацію діяльності спільноти, організацію зустрічей, управлінську функцію забезпечує Центр із захисту національної інфраструктури (Centre for the Protection of National Infrastructure, CPNI – спеціально уповноважений орган з питань захисту критичної інфраструктури). CPNI створює канали, якими дані щодо обміну інформацією передаються в інші країни, зокрема, з цією метою створено мережу обміну інформацією з безпеки між Великою Британією і США [9].

У Великій Британії правоохоронні органи у сфері боротьби із кіберзлочинністю також використовують спеціалізовані служби, які надають послуги інформаційної безпеки, співпрацюючи як з державними, так і з комерційними організаціями, наприклад, WARP (Warning, Advice and Reporting Point) сервісною службою, завдяки якій зокрема розкриваються тенденції кіберзлочинності [10].

Аналіз зазначених та інших прикладів європейської практики з питань боротьби з кіберправопорушеннями дає можливість сформулювати наступні пропозиції для вітчизняних правоохоронних органів.

Насамперед, значно підвищить ефективність боротьби з кіберзлочинністю отримання доступу до баз даних та аналітичних матеріалів Центру ЕС3 за допомогою мобільного офісу через бездротові канали доступу до мережі Інтернет. Необхідно також продовжити роботу щодо забезпечення можливості проведення на базі ЕС3 судових експертиз для правоохоронних органів України із використанням технічних можливостей та персоналу правоохоронних органів країн-членів ЄС. Загалом, постійний обмін досвідом, зокрема на базі Європейського поліцейського коледжу (CEPOL) у Гемпширі та Об'єднаному центрі передових технологій з кібероборони НАТО (NATO CCDCOE) у Таллінні сприятиме підвищенню рівня обізнаності співробітників правоохоронних органів з новітніми технологіями боротьби з кіберзлочинністю.

Безумовно, варто забезпечити проведення навчань (тренінгів) для співробітників органів прокуратури та суддів з метою їх фахової готовності до представництва інтересів держави та розгляду справ у провадженнях щодо кіберзлочинів зокрема у частині порядку збирання цифрових доказів, їх передачі та зберігання. Це сприятиме розумінню співробітників органів прокуратури та суддів технікоюридичних особливостей проваджень щодо кіберзлочинів.

Європейська практика також засвідчує, що складовою діяльності правоохоронних органів у сфері боротьби із кіберзлочинністю є державно-приватне партнерство. У цьому контексті необхідно створити основу для співпраці шляхом підписання Меморандуму про взаєморозуміння між Інтернет-провайдерами та правоохоронними органами України.

Ефективності та оперативності виконання запитів щодо збереження електронних доказів, надання інформації національними Інтернет-провайдерами, відповіді на запити про правову допомогу тощо сприятиме імплементація положень Конвенції у національне законодавство України зокрема у частині відповідності системи збору доказової бази європейським принципам.

Зважаючи на розширення компетенції СБ України відповідно до Закону України «Про основні засади забезпечення кібербезпеки України», цілком обґрунтованим вбачається створення у державному органі спеціального призначення з правоохоронними функціями, що забезпечує державну безпеку, механізму санкціонованого обміну оперативною інформацією в режимі реального часу з іноземними партнерами подібно до платформи співробітництва України з Інтерполом і Європолом, яка функціонує

на базі Департаменту міжнародного поліцейського співробітництва Національної поліції України.

Розглянемо інший вид правопорушень в інформаційній сфері, який на противагу терміну «фейк-новини» доцільно називати дезінформування. Останніми роками особливої уваги державичлени ЄС приділяють дезінформуванням суспільства, визначаючи його як «будь-які форми неправдивої, неточної або такої, що вводить в оману інформації, розробленої, презентованої і поширюваної умисно для нанесення шкоди суспільству або для отримання прибутку» [11].

Європейська комісія у січні 2018 року створила робочу групу експертів («the HLEG») з виробленя пропозицій щодо протидії цьому протиправному явищу. Робоча група у своєму звіті рекомендує Європейській комісії не застосовувати обмежувальних заходів, які б впливали на свободу слова і право на інформацію. Разом з тим вказує на необхідності дотримання наступних заходів протидії дезінформації у мережі Інтернет:

1) підвищувати прозорість новин онлайн, впроваджуючи адекватні системи поширення інформації із забезпечення захисту персональних даних;

2) впроваджувати медійну та інформаційну грамотність для протидії дезінформації і допомоги грмадянам користуватися цифровим медійним середовищем;

3) впроваджувати технічні засоби для користувачів і журналістів з метою виявлення дезінформації і сприяння позитивній взаємодії з інформаційними технологіями, які швидко розвиваються;

4) забезпечувати різноманітність і стійкість європейської медійної екосистеми;

5) продовжувати дослідження впливу дезінформації в Європі для напрацювання заходів для різних суб'єктів з постійного удосконалення належної протидії [11].

Зазначимо, що означений вид діяльності на сьогодні остаточно не закріплений як вид правопорушення в інформаційній сфері. Це зумовлено побудовою правових систем на принципах свободи слова і права на вільний доступ до інформації. Однак, прогнозуємо, що зважаючи на суспільно негативні наслідки, яке спричиняє дезінформування, найближчим часом юридична відповідальність за цей вид інформаційного правопорушення може бути закріплена законодавчо у вигляді окремого складу правопорушення за системне умисне поширення неправдивої, неточної або такої, що вводить в оману інформації.

Такому закріпленню передуватимуть усебічні дослідження техніко-юридичних, соціологічних і навіть психологічних умов та наслідків поширення неправдивої інформації. Україна у цьому контексті має достатній досвід у межах протидії інформаційній агресії РФ.

Висновок

Аналіз європейського досвіду з питань боротьби з правопорушеннями в інформаційній сфері засвідчив, що значна увага приділяється проблемі кіберзлочинності. Питання протидії дезінформуванню стали об'єктом уваги науковців і практиків лише останніми роками.

За результатами здійсненого аналізу запропоновано низку рекомендацій для правоохоронних органів України. Зокрема, щодо необхідності доступу до баз даних та аналітичних матеріалів Центру ЕС3, підписання Меморандуму про взаєморозуміння між Інтернет-провайдерами та правоохоронними органами у межах державно-приватного партнерства.

Зроблено припущення про перспективне законодавче закріплення юридичної відповідальності за дезінформування як вид інформаційного правопорушення.

Література

[1]. Ресурси репозиторію «Cybercrime». [Електронний ресурс]. Режим доступу: https://www.unodc.org/unodc/en/cybercrime/cybercrime-repository.html.

[2]. О. Корченко, Д. Горніцька, А. Гололобов, "Розширена класифікація методів соціального інжинірингу", *Безпека інформації*, Т. 20, № 2, С. 197-205, 2014.

[3]. А. Марущак, "Проблеми розслідування кіберзлочинів в Україні". *Економіка. Фінанси. Право.* № 1, С. 23-27, 2018.

[4]. А. Марущак, "Міжнародне співробітництво у боротьбі з транснаціональною кіберзлочинністю. *Інформація і право*, № 3, С. 104-110, 2018.

[5]. Конвенція Ради Європи про кіберзлочинність від 21.11.2001 р. [Електронний ресурс]. Режим доступу: http:// zakon4. rada. gov. ua/ laws/ show/994_575.

[6]. [Електронний ресурс]. Режим доступу: https://www.arakis.pl.

[7]. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace / European Comission. High representative of the European Union for foreign affairs and security policy. – Brussels, 7.2.2013. – Join (2013) 1 final. An evaluation Framework for National Cyber Security Strategies. [Електронний ресурс]. Режим доступу: http://www.enisa. europa.eu.

[8]. [Електронний ресурс]. Режим доступу: https://www.europol.europa.eu/newsroom/news/four-eu-cybersecurity-organisations-enhance-cooperation.

[9]. Centre for the Protection of National Infrastructure. [Електронний ресурс]. Режим доступу: https://www.cpni.gov.uk.

[10]. Warning, Advice and Reporting Point (WARP). [Електронний ресурс]. Режим доступу: https://www.warpnetwork.org/services.html.

[11]. European Commission, "A multidimensional approach to disinformation: Report of the independent High level Group on fake news and online disinformation"; European Commission (2018). "Tackling Online Disinformation: A European Approach". [Electronic resource]. Online: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=51804.

УДК. 004.056.53

Марущак А.И. Европейский опыт по борьбе с правонарушениями в информационной сфере

Аннотация. *Правонарушения в информационной сфере становятся все более распространенными с развитием информационных технологий. Дискуссии ведутся вокруг сочетания и соотношения корпоративных норм обработки информации, закрепленных в основном в политиках конфиденциальности или безопасности, с требованиями национального законодательства по гражданско-правовой, административно-правовой, уголовно-правовой охране различных категорий информации. В статье осуществлен анализ наиболее распространенных правонарушений в информационной сфере: киберправонарушения и дезинформации, проанализирован европейский опыт по борьбе с такими правонарушениями. Предложены рекомендации для правоохранительных органов Украины, а также сделано предположение о перспективном законодательном закреплении юридической ответственности за дезинформацию как отдельный состав информационного правонарушения.*

Ключевые слова: *информация, киберпреступления, дезинформирование, правоохранительные органы, информационное право.*

Marushchak A. European experience of offense prevention in the information sphere

Abstract. *Offenses in the information sphere are becoming more widespread with the development of information technology. Serious considerations are given to the combination and correlation of corporate regulations of information processing, which are mainly enshrined in confidentiality or security policies, with the requirements of national legislation on civil law, administrative law, and criminal law protection of various categories of information. The article analyzes the most common violations in the information sphere: cybercrime and disinformation, the European experience in combating such violations. Recommendations for law enforcement agencies of Ukraine are proposed, as well as assumption of adoption of legal responsibility for disinformation as a separate kind of information offense is made. The conclusion for the impotence of trainings for staff of the prosecutors and judges in order to enhance their skills in cybercrime proceedings regarding digital evidence collection, transmission and storage is made. This will facilitate the understanding of technical and legal peculiarities of cybercrime proceedings by the staff of the prosecutors and judges. The implementation of the provisions of the Cybercrime Convention in the national legislation of Ukraine will facilitate the efficiency of requests for the preservation of electronic evidence, the provision of information by national Internet service providers, the response to legal aid requests etc., in particular in connection with European evidence-base collection system. Taking into account negative consequences caused by disinformation, in the near future legal liability for this type of information offense can be enshrined by law in the form of a separate offense for systematic intentional distribution of the false, inaccurate or misleading information. Such consolidation will be preceded by comprehensive consideration of technical, legal, sociological and even psychological conditions and the consequences of the dissemination of false information.*

Key words: *Information, Cybercrime, Disinformation, Law Enforcement Agencies, Information Law.*

Отримано 5 *лютого 2019 року*, затверджено редколегією *1 березня 2019 року*