МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Тернопільський національний економічний університет
Навчально-науковий інститут інноваційних освітніх технологій
Кафедра безпеки, правоохоронної діяльності та фінансових розслідувань

ЯРОШИНСЬКИЙ Роман Вікторович

Правові основи боротьби з організованою кіберзлочинністю в економічній сфері / Legal basis for the fighting against organized cybercrime in the economic sphere

спеціальність: 262 - Правоохоронна діяльність
освітньо-професійна програма - Економічна безпека та фінансові розслідування

Випускна кваліфікаційна робота

Виконав студент групи
ПДЕБзмхм-21
Р. В. Ярошинський
_____

Науковий керівник:
к.е.н., доцент Т. О. Сліпченко
_____

Випускну кваліфікаційну роботу
допущено до захисту:

"___" _____ 20___ р.

Завідувач кафедри
_____ **Н. Б. Москалюк**

ш67
02.12.19

ТЕРНОПІЛЬ - 2019

ЗМІСТ

ВСТУП……3

РОЗДІЛ І. ІСТОРИКО-ТЕОРЕТИЧНІ ЗАСАДИ БОРОТЬБИ З ОРГАНІЗОВАНОЮ КІБЕРЗЛОЧИННІСТЮ……8

1.1 Теоретичні основи дослідження сутності кіберзлочинності……8

1.2 Історія розвитку законодавства у сфері боротьби з організованою кіберзлочинністю в Україні……..13

РОЗДІЛ ІІ. МЕХАНІЗМ ПРАВОВОГО РЕГУЛЮВАННЯ БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ В ЕКОНОМІЧНІЙ СФЕРІ……19

2.1 Структура механізму боротьби з кіберзлочинністю в економіці держави……..19

2.2 Особливості боротьби з організованою кіберзлочинністю в економічній сфері……...23

РОЗДІЛ ІІІ. ОСНОВИ БОРОТЬБИ З ОРГАНІЗОВАНОЮ КІБЕРЗЛОЧИННІСТЮ В ЕКОНОМІЧНІЙ СФЕРІ У МІЖНАРОДНОМУ ЗАКОНОДАВСТВІ……29

3.1 Методи боротьби з організованою кіберзлочинністю в економічній сфері та їх ефективність: міжнародний досвід……29

3.2 Перспективи боротьби з організованою кіберзлочинністю в економічній сфері України……37

ВИСНОВКИ

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

ВСТУП

Актуальність теми. Кіберзлочинність - це не традиційний злочин, а відносно молоде явище, пов’язане із виникненням та поширенням Інтернету. Із самого моменту виникнення даний вид злочинності проявив себе зручним для зловмисників особливо часто такі злочини скоються з мотивом незаконного збагачення.

Своєрідна природа Всесвітньої павутини надала глобальним користувачам анонімність, що, безсумнівно, стало необхідною умовою виникнення цього виду злочинів. У свою чергу, розповсюдження кіберзлочинності пов'язане з необхідністю ще більш жорстко законодавчо врегулювати це питання у світі та в Україні.

Протидія будь-якому негативному впливу вимагає формування розуміння сутності проблеми та знання її генезису. Оскільки швидкість розвитку суспільства нерозривно пов’язана з досягненнями науково-технічного прогресу та злочинними проявами, важливим є також звернення до питання історичного розвитку впровадження правових механізмів для боротьби з кіберзлочинністю закордоном та в Україні.

Збільшення кількості кіберзагроз на економічну складову нашої державі все актуальнішим робить питання оптимізації правового регулювання даної сфери. В світлі євроінтеграційних процесів важливою для України є демонстрація того, що ми готові протистояти загрозам найстрімкіше зростаючому виду злочинності в економічній сфері. Окрім того, в сучасних умовах важливою є готовність приймати необхідні зміни, що відповідатимуть стандартам, встановленим на європейському та світовому рівнях.

Постійний розвиток правового регулювання боротьби з організованою кіберзлочинністю в економічній сфері України є важливим з огляду на наступні фактори.

По-перше, на сьогодні практично усі державні та недержавні економічні процеси відбуваються із застосуванням інструментів

кіберпростору. По-друге, в умовах неоголошеної війни, у якій вимушена приймати участь Україна, віртуальний простір є одним із фронтів, у якому наша держава має слабкі показники, а кіберзагрози, щодо економіки держави крадуть такі необхідні ресурси. По-третє, рівень усвідомлення загрози кіберзлочинів та їх небезпечності у суспільстві все ще є невисоким, особливо з приводу економіки держави, коли суб'єкт злочинного посягання значно складний та не зрозумілий для більшості суспільства.

За таких умов проблема перспектив правового регулювання боротьби з кіберзлочинністю в Україні є однією із першочергових для наукового дослідження з метою забезпечення належних змін на практиці.

Таким чином, економічна, соціальна і правова значущість проблеми боротьби з кіберзлочинністю в економічній сфері зумовили вибір теми дипломного дослідження: «Правові основи боротьби з організованою кіберзлочинністю в економічній сфері».

Потребують уваги також теоретичні та практичні проблеми, боротьби з кіберзлочинністю в економічній сфері, які були предметом багатьох спеціальних наукових досліджень. Зазначена проблематика відображена певним чином в аспекті вивчення та дослідження таких вчених та провідних науковців як: Дж. Арас, О.О. Баєв, Г.Р. Бєляков, Дж. Блумбекер, В.Л. Бурячок, В.М. Бутузов, Г.П. Власова, В.Я. Вовк, А.В. Войціховський, В.Д. Гавловський, Р.Є. Джансараєва, В.Б. Дзюндзюк, Д.В. Дубов, О.Є. Користін, М.О. Кравцова, М.Ю. Літвінов, Р.В. Лук'янчук, О.В. Манжай, В.В. Марков, М.А. Ожеван, Ю.М. Онищенко, О.В. Орлов, А.А. Протасевич, П.І. Пушкаренко, К.М. Рудой, Є.Д. Скулиш, В.Г. Хахановський, В.В. Чернєй та ін.

Нормативною базою дослідження є Конституція України, Кримінальний кодекс України, Кримінально процесуальний кодекс України, Цивільний кодекс України, Господарський кодекс України, міжнародні документи, а саме Конвенція про кіберзлочинність, закони та постанови Верховної Ради України, акти Президента України, акти Кабінету Міністрів

України, рішення Конституційного Суду України, рішення судів загальної юрисдикції, рішення Європейського суду з прав людини, які стосуються боротьби з організованою кіберзлочинністю, законодавство зарубіжних держав в частині захисту свого кіберпростору.

Метою роботи є дослідити правові основи боротьби з організованою кіберзлочинністю в економічній сфері держави.

Досягнення зазначеної мети обумовлено вирішенням наступних завдань дослідження:

1. Дослідити теоретичні основи дослідження сутності кіберзлочинності;

2. Розглянути історія розвитку законодавства у сфері боротьби з організованою кіберзлочинністю в Україні;

3. Визначити структуру механізму боротьби з кіберзлочинністю в економіці держави;

4. Проаналізувати особливості боротьби з організованою кіберзлочинністю в економічній сфері;

5. Встановити методи боротьби з організованою кіберзлочинністю в економічній сфері та їх ефективність, а саме міжнародний досвід з цього приводу;

6. Дослідити перспективи боротьби з організованою кіберзлочинністю в економічній сфері України.

Об’єктом дослідження є правові основи які регулюють захист кіберпростору в економічній сфері України та світу.

Предметом дослідження є теоретична база знань, щодо правового забезпечення боротьби з організованою кіберзлочинністю в економічній сфері держави.

У більшості сучасних праць з цієї проблематики переважно йдеться лише про кіберзлочинність взагалі. Проведене нами дослідження свідчить, теоретичної бази знань, щодо захисту кіберпростору в економічній сфері держави дуже мало.

Методи дослідження. Методи дослідження вивчаються в рамках методології юриспруденції, як окремої наукової дисципліни. Методи пізнання відіграють вагому роль в процесі дослідження. Правильно вибраний метод значно збільшує достовірність результатів, полегшує роботу над дослідженням.

Для забезпечення об'єктивності, всебічності і повноти нашого дослідження, а також для отримання науково обґрунтованих і достовірних результатів роботи використано сукупність філософсько-світоглядних, загальнонаукових і спеціальних методів наукового пізнання.

При написанні даної роботи та при проведенні досліджень, використовувались наступні методи: синтез, логічність, аналіз та узагальнення літературних джерел.

Крім того, основним у цій системі виступає загальнонауковий метод пізнання, на базі якого проблеми даної роботи розглядаються в єдності їх соціального змісту і юридичної форми.

Використовувались такі загальнонаукові методи, як історичний, порівняльний, і системний.

Історичний дав змогу вивчити особливості формування забезпечення правових основ боротьби з організованою кіберзлочинністю в економічній сфері.

За допомогою порівняльного методу були співставлення положення чинного законодавства України, європейських країн та міжнародних норм, щодо проблематики забезпечення боротьби з організованою кіберзлочинністю в економічній сфері.

Системний метод застосовувався при обґрунтуванні самостійності принципів побудови системи забезпечення боротьби з організованою кіберзлочинністю в економічній сфері, дозволив концептуально сформувати і обґрунтувати теоретичні підвалини і розробити категоріально-понятійний апарат дослідження.

Системно-структурний підхід застосовувався для дослідження проблем правового регулювання щодо вирішення проблематики реалізації та забезпечення боротьби з організованою кіберзлочинністю в економічній сфері.

Практична значимість роботи є безумовно великою оскільки, в умовах інтеграції України до Європейського союзу питання щодо забезпечення боротьби з організованою кіберзлочинністю в економічній сфері з урахуванням зарубіжного досвіду набули значного поширення.

Результати нашого дослідження можуть бути використані у навчальному процесі – під час викладання навчальних дисциплін з юриспруденції та інформатики.

Крім того, вони можуть бути використані для подальших наукових досліджень.

Також їх можна буде застосувати у правозастосовній сфері – у практичній діяльності правоохоронних органів.

Наше дослідження, крім вище зазначеного, також може мати успіх у виховні роботі, з метою підвищення рівня правосвідомості та правової культури суспільства, виховання поваги до держави.

Структура роботи. Магістерська робота викладена на 60-ти сторінках комп’ютерної верстки. Складається з вступу та трьох розділів, висновків, списку використаної літератури який включає в себе 71 літературне джерело, з яких 28-м електронних.

РОЗДІЛ І. ІСТОРИКО-ТЕОРЕТИЧНІ ЗАСАДИ БОРОТЬБИ З ОРГАНІЗОВАНОЮ КІБЕРЗЛОЧИННІСТЮ

1.1 Теоретичні основи дослідження сутності кіберзлочинності

В Україні проблема боротьби з кіберзлочинністю ускладнена тим, що сам термін «кіберзлочинність» в офіційних нормативно-правових документах не визначено, навіть не зважаючи на те, що поняття є звичним як для лексикону правоохоронних органів України та держав світу, так і для правової доктрини нашої держави. Застосування сучасних інформаційних технологій в практично усіх сферах суспільного життя, у тому числі в економіки держави висуває проблему боротьби з кіберзлочинністю у число основних.

Окрім безпосередньої шкоди, можливої від несанкціонованого доступу до економічної інформації, її розповсюдження, модифікації, знищення тощо, кіберзлочинність є джерелом загрози державній безпеці, економіці, правам та інтересам людини. Ступінь загрози, яку несуть комп'ютерні злочини є не до кінця усвідомленою у суспільстві з причини недостатньої наукової розробленості фундаментальних понять, пов'язаних із нею.

Разом із тим, інтернет є надійним притулком великої кількості злочинців, які завдяки своїй анонімності та безмежності мережі, використовують його для здійснення протиправної діяльності.

Будь-які терміни із частиною «кібер-» на сьогодні ще не отримали сформованого визначення ні на науковому, ні на нормативно-правовому рівнях та залишаються предметом наукової дискусії.

Не є виключенням і поняття кіберзлочинності, яке не розкрито у тому числі і нормами Конвенції «Про кіберзлочинність» від 23.11.2001 року [1]. У даному міжнародному документі містяться вказівки на:

1) правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем;

2) правопорушення, пов’язані з комп’ютерами,

3) правопорушення, пов’язані з порушенням авторських та суміжних прав [15].

Тобто, варто зробити висновок, що кіберзлочинність та міжнародному рівні розуміється як сукупність зазначених злочинів. Проаналізувавши роботи вітчизняних науковців можна резюмувати, що в Україні кіберзлочинність пов’язується передусім із віртуальним простором.

Так, з точки зору Д. П. Біленчука, кіберзлочинністю є злочинність у змодельованому за допомогою комп'ютера інформаційному просторі, в якому перебувають відомості про осіб, предмети, факти, події, явища і процеси, представлені в математичному, символьному або будь-якому іншому виді, й рухи, що перебувають у процесі, по локальних і глобальних комп'ютерних мережах, або відомості, що зберігаються в пам'яті будь-якого фізичного або віртуального устрою, а також іншого носія, спеціально призначеного для їхнього зберігання, обробки й передачі [2, с. 32].

О. Ю. Іванченко розуміє кіберзлочинність подібним чином, як сукупність злочинів, що вчиняються у віртуальному просторі за допомогою комп’ютерних систем, шляхом використання комп’ютерних мереж чи інших засобів віртуального простору, в межах комп’ютерних мереж, а також проти комп’ютерних систем, комп’ютерних мереж і комп’ютерних даних [5, с. 173].

Спільною рисою, і відповідно недоліком, концепцій тлумачення явища кіберзлочинності є нехтування авторами ознак економічної злочинності у цілому, акцентуючи увагу на специфіці кіберзлочинів та кіберпростору, як осередку їх вчинення.

Тому, пропонуємо тлумачити кіберзлочинність як сукупність окреслених кримінальним законом вчинків, скоєних на тій чи іншій території або щодо об’єктів, розташованих на ній за відповідний період часу, вчинених у віртуальному просторі шляхом деструктивного впливу на комп’ютерні системи, комп’ютерні мережі і комп’ютерні дані.

На сучасному етапі поняття «боротьба із кіберзлочинністю» є досить незвичним для вітчизняної науки, не зважаючи на те, що злочинні дії із застосуванням Всесвітньої мережі несуть високий рівень суспільної небезпеки.

Для аналізу поняття боротьби із кіберзлочинністю звернемось до законодавчих актів, які становлять нормативно-правову базу боротьби із комп'ютерними злочинами - Конституції України, Конвенції про кіберзлочинність, Кримінального кодексу України, Кримінального процесуального кодексу України тощо. В Основному Законі поняття «боротьби із кіберзлочинністю» відсутнє взагалі.

Законодавцем у статті 17 Конституції зазначено, що забезпечення інформаційної безпеки України є найважливішою функцією держави та справою всього Українського народу [6], проте мова все ж йде не про протистояння небезпекам, а про забезпечення безпеки. Норми Конвенції «Про кіберзлочинність», ратифікованої Верховною Радою України, містять поняття «боротьба із кіберзлочинністю», проте у них відсутня його дефініція.

Нормами Кримінального кодексу України здійснено розподіл окремих видів кіберзлочинів у Розділі XVI Особливої частини «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем і комп'ютерних мереж – статті 361, 362 та 363, Розділі V Особливої частини «Злочини проти виборчих, трудових та інших особистих прав і свобод людини і громадянина» зазначені окремі види злочинів, в яких комп'ютерні продукти визначені як засіб злочину - статті 163, 176, 177 та Розділі VII «Злочини у сфері господарської діяльності» - стаття 200 (Незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, електронними грошима, обладнанням для їх виготовлення), проте поняття «боротьба із кіберзлочинністю» також не закріплено.

Подібним чином дане питання врегульоване і нормами Кримінального процесуального кодексу України - стаття 263 врегульовує питання зняття

інформації з транспортних телекомунікаційних мереж, стаття 264 - зняття інформації з електронних інформаційних систем, стаття 268 установлення місцезнаходження радіоелектронного засобу тощо, проте про «боротьбу із кіберзлочинністю» мова також не йде.

Отже, відсутність належного законодавчого закріплення поняття «боротьба із кіберзлочинністю» є однією із причин наявності проблем у його теоретичному розумінні та неоднозначності наукового тлумачення. За таких умов, важливим є аналіз того, яким чином у нормативно-правових джерел розкрито споріднені до досліджуваного нами поняття.

Звертаючись до нормативно-правових актів, що здійснюють регулювання діяльності суб'єктів боротьби із кіберзлочинністю, у положенні про Департамент кіберполіції Національної поліції України вживається термін «протидія кіберзлочинності».

Тобто, боротьбою із кіберзлочинністю є активне протистояння деструктивній діяльності осіб, які здійснюють злочинні діяння із використанням всесвітньої мережі Інтернет, що вчиняється правоохоронними органами, в Україні – Службою Безпеки України, Департаментом кіберполіції Національної кіберполіції, законодавцями держав та іншими соціальними групами, зацікавленими у подоланні даної проблеми. Боротьба є активною, цілеспрямованою, науково обґрунтованою діяльністю держави, спрямованої подолати негативне суспільне явище кіберзлочинності, а термін «боротьба» позначає та підкреслює активний характер цієї діяльності, який не є притаманним іншим термінам. Тому, не зважаючи на свою недосяжність, подолання кіберзлочинності є одним із важливих завдань держави і залишатиметься таким і надалі. У противагу зробленим нами висновкам, аналізуючи тлумачення поняття «протидія», відзначаємо що нею є дія, спрямована проти іншої дії, що перешкоджає їй [11, с. 73].

Таким чином, дослідивши наукові позиції щодо визначення поняття «боротьба зі злочинністю», ми встановили, що даному питанню приділена

недостатня увага з боку науковців. На підставі проведеного дослідження сформулюємо авторську дефініцію поняття «боротьба з економічною злочинністю», що дозволить нам вдаліше встановити сутність досліджуваного явища – «боротьби із кіберзлочинністю в економічній сфері».

Боротьбою з економічною злочинністю є комплексна активна система заходів, що застосовується у якості реакції держави на протиправне поягання на її економічну складову, діяльність осіб чи їх груп та входить до компетенції правоохоронних органів та органу законодавчої влади за сприяння окремих осіб чи груп осіб, зацікавлених у подоланні даної проблеми та в економічному зростанні держави [17, с. 209].

З цією метою було створено Департамент кіберполіції Національної поліції України , а також факультету підготовки фахівців для підрозділів боротьби з кіберзлочинністю у Харківському університеті внутрішніх справ у 2013 році [18, с. 6]. Дані кроки, у сукупності із поступовим прийняттям необхідної нормативно-правової бази є свідченням того, що наша держава здійснює активну діяльність та намагається нівелювати ще на початкових етапах негативні для суспільства наслідки від кіберзлочинності.

Щодо боротьби із кіберзлочинністю в Україні, за загальним правилом вона здійснюється Департаментом кіберполіції Національної кіберполіції, вітчизняним законодавцем та іншими соціальними групами, зацікавленими у подоланні даної проблеми. За таких умов законодавець здійснює свою діяльність у законодавчому та організаційному напрямках, а Департамент кіберполіції Національної кіберполіції у профілактичному.

Основним критерієм визначення зазначеного терміну є рівень суспільної небезпеки, який характеризує вчинене діяння. Проте, поняття «кіберправопорушення в економічній сфері» не розкриває сутності злочинної дії та середовища її вчинення, виходячи із суто технічних аспектів. Кіберзлочини розглядаються як специфічний вид злочинної діяльності, що здійснюється у кібернетичних комп’ютерних системах.

Проте, увагу привертає точка зору автора щодо неприпустимості ототожнення кіберзлочинів та інформаційних злочинів. Стверджується, що «інформаційне середовище» є занадто загальним поняттям для сфери використання комп'ютерних систем, що не розкриває суті процесів автоматизованої обробки інформації [24, с. 92].

Таким чином, оскільки економічна кіберзлочинність в нашій державі все ще переважно існує як потенційна загроза, важливим на даному етапі є застосування превентивних заходів. Це все зумовлює необхідність створення ефективної системи запобігання, виявлення та припинення такої діяльності, що стане запорукою успішності боротьби із кіберзлочинністю в Україні.

1.2 Історія розвитку законодавства у сфері боротьби з організованою кіберзлочинністю в Україні

Стрімке впровадження нових технологій у галузях економіки, та цифрових технологій наприкінці XX – на початку XXI століття спричинило появу нових суспільних відносин та відповідних проблем, пов'язаних із прагненням людства до розвитку, полегшення праці та покращення умов життєдіяльності.

Разом із тим, відкриття нових горизонтів для світового співтовариства нерозривно пов'язане із появою нових форм злочинної діяльності та іншими проявами недобросовісного використання досягнень науково-технічного прогресу. Потреба вдосконалення засад правового регулювання боротьби з кіберзлочинністю є однією із першочергових, тож відповідні правові приписи мають відповідати вимогам часу і сучасних умов.

Відповідно, кожен етап становлення даного інституту як у світі, так і в Україні, значним чином позначався на правовій регламентації діяльності у мережі Інтернет та захисті інтересів громадян від кіберзагроз.

Тому зрозуміло, що кіберзлочинність є відносно новим видом злочинної діяльності, який потребує спеціальних навичок і знань та

специфіка якого полягає у тому, що технічні можливості для його вчинення з'явились порівняно нещодавно, а отже варто звернутись до історичних передумов його появи та розвитку.

Виникнення терміну «комп'ютерна злочинність» хронологічно пов'язується із початком 60-х років минулого століття, коли були виявлені перші випадки злочинів, зроблених з використанням електронних обчислювальних машин [30, с. 5].

«Батьківщиною» даного виду злочинності вважаються Сполучені Штати Америки, де у 1945 р. було створено першу електронну обчислювальну машину, одну із ранніх форм комп'ютерів, яка використовувалась для розшифровування німецьких військових кодів, а 48 згодом й з іншою метою. Те саме має місце і в наш час, коли комп'ютери та мережеві системи використовуються в першу чергу для вирішення завдань інформаційної безпеки, а вже згодом для інших локальних цілей [31, с. 133].

Тому не випадково, що вчинення першого в історії комп'ютерного злочину відбулось у Міннесоті, де у 1966 році було зафіксовано перший випадок використання електронної обчислювальної машини як інструмента при пограбуванні банку [32, с. 79].

Тобто на той момент на науковому рівні вже було сформовано чітке розуміння про появу нового виду злочинності та про необхідність її подолання. Відмітимо, що на той момент комп'ютерна злочинність остаточно сформувалась як самостійний елемент кримінальної системи, оскільки 1970-ті роки характеризуються появою перших професійних комп'ютерних злочинців – хакерів. Варто відзначити, що одними із перших хакерів були Стів Возняк та Стів Джобс, які налагодили виробництво пристроїв для злому телефонних мереж [29, с. 3].

На той момент явище кіберзлочинів вже поширилось і на територію колишнього СРСР, до складу якого входила і Україна - в 1979 році у Вільнюсі, внаслідок кіберзлочину була нанесена шкода державі у розмірі 80 тисяч карбованців [32, с. 79]. Тобто, різниця у розвитку комп'ютерної

злочинності у світових державах та у Радянському Союзі становила приблизно два десятки років, що є яскравим свідченням наскільки вагомою була і є відмінність у розробці правових інструментів боротьби із кіберзлочинами. Якщо на даному етапі на території більш розвинутих держав вже діяли певні основи законодавства про кіберзлочинність, то для СРСР комп'ютерні злочини постали у якості абсолютно нового явища. На той момент кіберзлочинність уже значно поширилась світом, а боротьба із нею набула глобальних масштабів.

У 1983 році в Сполучених Штатах Америки відбулась історична подія – перший арешт кіберзлочинця, про який стало відомо громадськості. Групою підлітків було здійснено Інтернет-злом близько 60 комп'ютерів. Після арешту один із учасників дав свідчення, тож усі інші члени організованої групи отримали умовний термін покарання [33, с. 86].

Наступна вагома подія, яка має безпосереднє відношення до генезису правового регулювання боротьби з кіберзлочинністю в світі відбулась у 1986 році у Сполучених Штатах Америки – було прийнято перший в історії комп'ютерний закон «The Computer Fraud and Abuse Act», нормами якого здійснено заборону неавторизованого доступу до комп'ютерних систем та отримання секретної військової інформації

Наступна важлива подія у історії розвитку кіберзлочинності – це так звана «справа Володимира Льовіна», учасника організованої злочинної групи, яка використовуючи Інтернет, спробувала перевести грошові кошти із рахунків банку на власні. До цього моменту вчинення жодного великого міжнародного злочину не розголошувалось громадськості, тож дана справа вважається першою, віднесеною до категорії транснаціональних мережевих комп'ютерних злочинів [36, с. 35].

Виникнення явища кібертероризму датується 1998 роком, коли 12-річним хакером було здійснено злом комп'ютерної системи, що контролювала водоспуск дамби у штаті Арізона, що у перспективі могло призвести до затоплення одразу двох міст [37, с. 175].

Наразі відбувається останній етап розвитку кіберзлочинності – етап появи нових форм комп'ютерних злочинів. Як відзначає В. Б. Дзюндзюк, серед них варто відзначити наступні: Інтернет-війна – уперше групи комп'ютерних активістів, засуджуючи військові дії Югославії та НАТО, здійснювали злом урядових комп'ютерів та поширювали антивоєнну Інтернет-пропаганду; Інтернет-страйк – групова діяльність, яка призводить до перевантаження Інтернет-сайту на неможливість його відвідування іншими користувачами тощо [29, с. 5-6].

В економічній сфері найчастіші напади хакерів на банківські мережі, на особисті кабінети платників податків, введення комп'ютерних вірусів на підприємства, через програму С1, злом платіжних пристроїв та інше.

Очевидно, що такий перелік нових форм є далеко невичерпним, проте основна мета його відзначення – продемонструвати, що питання правового регулювання боротьби з кіберзлочинністю в економічній сфері потребує постійної еволюції і вдосконалення, адже комп'ютерні злочинці постійно змінюють напрямки та методи своєї діяльності.

Таким чином, нами встановлено, що генезис розвитку кіберзлочинності та генезис правового регулювання боротьби з кіберзлочинністю в економічній сфері не можна ототожнювати. Кіберзлочинність розвивається у відповідності з еволюцією новітніх технологій, тому на сьогоднішній день є сферою, яка постійно на крок попереду її нормативно-правового регулювання. Беручи за основу розвитку кіберзлочинності, відмічаємо, що на перших двох етапах законодавче регулювання даного інституту фактично не здійснювалось взагалі.

Варта уваги так звана «вінницька справа» 1998 року, у якій зловмисник, використавши систему електронних платежів, незаконно переказав понад 80 мільйонів гривень, а на той час ця сума становила приблизно 20 мільйонів доларів, на рахунок одного з латвійських банків [45, с. 89].

Україною ратифіковано Конвенцію про кіберзлочинність і таким чином імплементовано положення міжнародного акту у вітчизняне законодавство. Норми Конвенції вже частково були розглянуті нами у межах даного підрозділу, тож доцільно відмітимо, що її прийняття послужило початком нового етапу генезису правового регулювання боротьби з кіберзлочинністю в Україні, який триває і по сьогоднішній день. Курс України до євроінтеграції свідчить про подальшу інтеграцію міжнародних правових норм у вітчизняну систему.

Стан розвитку законодавства про кіберзлочинність свідчить про те, що дана сфера однозначно потребує удосконалення, а застосування європейського досвіду є доцільним з огляду на рівень його розвитку. Відзначимо, що на сучасному етапі розвиток кіберзлочинності в нашій державі ще не досяг значних масштабів. Серед суттєвих кібератак варто виділити нещодавнє застосування невідомими зловмисниками вірусу «Petya.A» проти значної кількості стратегічних об’єктів нашої держави. Зокрема, відомо, що одним із шляхів потрапляння вірусу до комп’ютерних мереж було оновлення бухгалтерського програмного забезпечення «M.E.Doc» [15].

Щодо прикладів вітчизняної судової практики, 21 січня 2016 року Стрийським міськрайонним судом Львівської області було розглянуто справу щодо несанкціонованого втручання в роботу автоматизованих систем, зокрема банкомату. Зловмисники встановили два несанкціоновані пристрої, які мають умовну назву «накладка на банкомат» і призначені для прихованого розміщення на банкоматі з метою отримання інформації з магнітних стрічок банківських карт користувачів та здійснення відеофіксації виконання ними операцій на цифровій клавіатурі банкомату, що призвело до проникнення в автоматизовану систему вказаного банкомату та витоку інформації 45 клієнтів вказаної вище банківської установи, на яких містилась інформація з магнітних стрічок карт та пінкодів клієнтів банку [55].

Не зважаючи на те, що даний злочин було кваліфіковано за статтями 300 та 301 Кримінального кодексу України, а саме ввезення, виготовлення, збут і розповсюдження порнографічних предметів та творів, що пропагують культ насильства і жорстокості, расову, національну чи релігійну нетерпимість та дискримінацію, даний проступок все ж має чіткі ознаки кіберзлочинів, адже його вчинення пов’язується із Всесвітньою мережею.

Тому, зробимо наступний висновок: не зважаючи на те, що деякі із проступків, які містять ознаки кіберзлочинів, не кваліфікуються як останні, законодавцем все ж на належному рівні здійснюється правове регулювання тих загроз, які є актуальними на сьогодні.

Водночас, останні тенденції свідчать про те, що в подальшому існуючий механізм потребує значного вдосконалення із урахуванням нещодавніх викликів.

РОЗДІЛ ІІ. МЕХАНІЗМ ПРАВОВОГО РЕГУЛЮВАННЯ БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ В ЕКОНОМІЧНІЙ СФЕРІ

2.1 Структура механізму боротьби з кіберзлочинністю в економіці держави

Механізм правового регулювання, як юридична категорія спрямований на впорядкування явищ правової дійсності, забезпечення їх єдності, взаємозв'язку й взаємодії, що виражається у можливості перетворення правових норм у реальний вплив на поведінку суб'єктів суспільних правовідносин.

Поняття «механізм правового регулювання» можна у загальному визначити як чітко встановлену та організовану систему юридичного інструментарію, яка забезпечує правовий вплив нормативних приписів на сферу суспільних відносин, що дозволяє регламентувати межі дозволеної та забороненої поведінки учасників відповідного кола суспільних відноси, з метою забезпечення законності та правопорядку у відповідності до потреб та інтересів держави, громадянського суспільства, окремих індивідів тощо [15].

Виходячи з цієї «тези механізм правового регулювання боротьби з кіберзлочинністю в економіці держави» можна визначити як чітко визначену й організовану систему юридичного інструментарію в економічній сфері, яка забезпечує правовий вплив шляхом застосування нормативних приписів на суспільні відносини, які виникають, змінюються та припиняються у сфері протидії вчиненню економічних злочинів, що дозволяє впливати на бажану поведінку учасників таких відносин, з метою досягнення належної й ефективної боротьби з кіберзлочинністю.

Поділяючи існуючі в теорії права підходи до визначення правових засобів механізму правового регулювання, можна стверджувати, що кожний елемент такого механізму виконує специфічну роль у регулюванні поведінки людей, виникаючих на цій основі суспільних відносин.

Тому вважаємо, що до структури механізму правового регулювання боротьби з кіберзлочинністю віднесено такі елементи:

1) норми права;

2) правовідносини;

3) юридичні факти [23].

Правові норми, правовідносини та юридичні факти є взаємопов'язаними і взаємозалежними категоріями.

Правові норми як складові елементи структури механізму правового регулювання боротьби кіберзлочинністю – це закріплені у нормативно-правових актах та міжнародних нормативно-правових договорах правила поведінки, які регулюються відносини, що виникають, припиняються та змінюються у сфері діяльності з подолання інформаційної злочинності, й забезпечуються легальним примусом з боку держав або учасників міжнародних відносин.

Законодавство Європейського Союзу у сфері інформаційної безпеки розвивалося у руслі міжнародних ініціатив Ради Європи, Організації економічного співробітництва і розвитку, Міжнародного Союзу Електрозв'язку, Організації Об'єднаних Націй. Законодавчі заходи у боротьбі із кіберзлочинністю здійснювалися у рамках програм Європейського Союзу, прийнятих рішеннями Європейського Парламенту і Ради, і переважно були спрямовані на захист економічної безпеки, сприяння безпечному користуванню Інтернетом, формуванню сприятливого середовища для розвитку європейської Інтернет-індустрії [3, с. 8-9].

Щодо правовідносин як структурного елементу механізму правового регулювання боротьби кіберзлочинністю, то вони опосередковують частину суспільних відносин, які регламентуються правовими нормами законодавства та міжнародних договорів з питань боротьби з інформаційною злочинністю, й забезпечують необхідний регулюючий вплив на поведінку учасників відповідного правовідношення з метою досягнення позитивного правового результату – попередження й профілактику кіберзлочинності, припинення

вчинюваних протиправних діянь, співробітництво у сфері розшуку злочинців та інше.

Юридичні факти є важливим самостійним складовим елементом механізму правового регулювання боротьби з кіберзлочинністю, оскільки вони є як конкретною життєвою обставиною, так і юридичним явищем. Останнє з названого й викликає найбільшу увагу з огляду на здатність факту об'єктивної реальності мати юридичні ознаки та характеристики, передбачені правовою нормою.

У становленні національного правового регулювання боротьби з кіберзлочинністю найсуттєвішим фактором є виникнення механізму, який дасть можливість запровадження єдиного безперервно діючого порядку у суспільних відносинах та підпорядкувати поведінку людей загальним і однаковим умовам, що диктуються вимогами суспільного життя. Сам термін «регулювання» означає впорядкування чого-небудь, керування чимось, підпорядковуючи його відповідним правилам чи певній системі [7, с. 12].

Тобто, дане поняття можна роз'яснити як визначення та регламентування поведінки людей, закріплення її меж, та спрямування її розвитку за допомогою встановлення певних норм. Одним із різновидів регулювання є правове, тобто те, що здійснюється за допомогою норм права, які поширюються на усі випадки суспільних відносин певного виду.

Іншими словами, правовим регулювання є упорядкування поведінки осіб і керування нею, що здійснюється за допомогою встановлених та санкціонованих державою правил, які поширюються на усі випадки, передбачені відповідними суспільними відносинами, та усіх суб'єктів, що вступили у нормативно-регламентовані суспільні відносини.

Крім того, національне правове регулювання боротьби з кіберзлочинністю в Україні – це впорядкування поведінки осіб у кіберпросторі та керування нею, що здійснюється за допомогою встановлених, санкціонованих чи ратифікованих державою законних та підзаконних нормативно-правових актів, а також міжнародних договорів і

угод, укладених Україною, які поширюються на усі випадки деструктивної діяльності у кіберпросторі, та усіх суб'єктів, що вступили у нормативно-регламентовані суспільні відносини.

Враховуючи, що на сьогодні все ще несформованим є єдине розуміння того, що ж являє собою кіберзлочинність, відмітимо що регламентація даного інституту все ж здійснюється на високому рівні. Проте, нагальною проблемою є відсутність узгодження між нормативно-правовими актами та відсутність єдиного понятійного апарату, що повинно бути усунене найближчими роками.

Обраний курс до тісного співробітництва з провідними європейськими державами та участі у різноманітних міжнародних організаціях вимагає наближення рівня та змісту вітчизняного законодавства до європейських аналогів.

Сьогоднішня нормативно-правова база боротьби із кіберзлочинністю місцями не відповідає динаміці розвитку сучасних суспільних відносин, а тому важливим та актуальним питанням підвищення рівня узгодженості норм чинного законодавства. В той же час, національне правове регулювання боротьби з кіберзлочинністю характеризується високим рівнем деталізації та охопленням значного об'єму суспільних відносин.

Вирішення даної проблеми вважається одним із пріоритетних напрямків державної економічної політики, тож еволюція законодавчих інструментів відбувається постійно. Прийняття Стратегії кібербезпеки України свідчить про те, майбутнє інституту правового регулювання боротьби з кіберзлочинністю пов'язується із поліпшенням умов для безпечного функціонування кіберпростору [23, с. 19].

2.2 Особливості боротьби з організованою кіберзлочинністю в економічній сфері

Кібератаки, щодо фінансових злочинів і шахрайство. Здійснюються організованими групами осіб, що добре фінансуються і займаються викраденням коштів та інших активів за допомогою сучасних технологій.

Кіберзлочинність – це п’ятий за розмірами вид економічної злочинності в України після незаконного привласнення майна, корупції та хабарництва, недобросовісної конкуренції та маніпуляції з фінансовою звітністю.

За п'ять років кіберзлочинність в Україні виросла вдвічі. За останні п’ять років в Україні кількість інформаційних злочинів зросла щонайменше у 2,5 рази. Стрибок кількості всіх кіберзлочинів відбувся у 2017 році. Після цього кількість злочинів має тенденцію зростати. Так в 2017 було зафіксовано 1795 справ, в 2018 — 1023, за останні півроку — 1005 [70].

За результатами опитування на кіберзлочинність припадає 23% випадків шахрайства у світі, про які повідомили учасники опитування, і 17% в Україні [70].

Дані огляду в сфері інформаційної безпеки свідчать про те, що кіберзлочини стають більш складними та витонченими, що перешкоджає процесу їх виявлення та попередження. Це може призвести до ще більших збитків та втрат у майбутньому. Новий ризик чи реальні випадки шахрайства, обсяги яких неухильно зростають. Не всі із зазначених вище 5 видів кібератак є типовими для України.

Проте абсолютно точно можна стверджувати, що загроза кіберзлочинності – це реальна проблема, яка може негативно вплинути на організації в Україні. У попередньому Всесвітньому огляді економічних злочинів ми вже ставили запитання стосовно кіберзлочинів. З огляду на незначну кількість зафіксованих випадків кіберзлочинності результати не були виділені окремо в огляді за 2017-2018 роки.

Враховуючи підвищену загрозу кіберзлочинності, в огляді за 2018 рік ми акцентували свою увагу саме на цьому виді шахрайства і знову включили питання, чи стикалися організації з випадками кіберзлочинності за останні 12 місяців.

Більше третини (37%) опитаних в Україні підтверджують, що кількість випадків кіберзлочинності в їхніх організаціях зросла. Близько 4% вказали на зниження цього показника, і 59% відповіли, що ситуація не змінилася.

Збільшення ризику кіберзлочинності можна пояснити наступними факторами:

- Регулярні згадування у засобах масової інформації про випадки кібератак викликали підвищену увагу до цього виду шахрайства та змусили організації запровадити додаткові механізми контролю, які і дозволили виявити більшу кількість таких економічних злочинів;
- Неоднозначне визначення поняття кіберзлочинності: багато респондентів перекласифікували деякі традиційні види економічних злочинів як кіберзлочинність, тому що вони були скоєні з використанням комп'ютерів, електронних пристроїв чи мережі Інтернет;
- Підвищена увага з боку регулюючих органів;
- Використання новітніх технологій, які «полегшують» скоєння кіберзлочинів.

Як нами вже було зазначено існує багато видів кримінальних правопорушень в економічній сфері, пов'язаних із використанням комп'ютерів [13], у рамках яких має місце розкрадання грошових коштів:

- атаки хакерів на банки або фінансові системи;
- шахрайства, пов'язані з переказом «електронних» грошей;
- шахрайства з банківськими пластиковими картами та ін.

За інформацією НБУ України, за 2017 р. загальна кількість шахрайських операцій із платіжними картами в нашій країні виросла відразу на 47 % і з 35 до 57 збільшилася кількість банків, із рахунків яких зникали

кошти. Як і колись, за кількістю несанкціонованих списань із рахунків лідирували фізичні особи (щодня від населення надходить до 50 скарг, із рахунків за минулий рік зникло 11,4 млн грн).

У банківській системі також з'явилися «нововведення»: на зміну скіммінгу прийшов новий вид крадіжки грошей із банківських карт.

Відповідно до назви цієї технології «Шим» (shim – тонка прокладка) замість традиційних громіздких накладок на щілину приймача пластикових карт банкоматів (скіммерів) у шиммінгу використовується дуже тонка та гнучка плата, що впроваджується через цю щілину всередину банкомату і практично непомітна. За даними міністерства, у 2015 р. було виявлено 45 таких апаратів, а за перший квартал 2017 р. було виявлено вже 37 пристроїв.

Кількість виявлених в Україні скіммінгових пристроїв у 2016 р. зросла на 62 %, а в 2017 р. сліди таких пристроїв вже виявляються кілька разів на тиждень.

Фішинг – ще один механізм реалізації кіберзлочинів, заснований на використанні майстерно підроблених веб-сторінок. Зовнішній вигляд таких сторінок зазвичай ідентичний справжній, однак є ряд відмінних ознак: – як правило, у фішингових сторінах у правій частині адресного рядка браузера відсутнє зображення замка, що свідчить, що обмін даними відбувається по захищеному з'єднанню, адреса в адресному рядку починається не з https://, а з http://; – як правило, на «фішинговій» сторінці повідомлення шахраї просять ввести отриманий від банку разовий пароль, номер мобільного телефону тощо.

За даними МВС України, із січня до кінця листопада 2017 р. в Україні порушили 745 кримінальних справ із кіберзлочинів, у цей період було засуджено 113 осіб.

Один із найпоширеніших видів мережевих атак на сучасні інфраструктури – DDoS-атаки (Distributed Denial of Service) [8]. Це атака на комп'ютерну систему з метою довести її до відмови, тобто створити такі умови, при яких легітимні користувачі системи не можуть отримати доступ

до надаваних системою ресурсів (серверів або сервісів), або цей доступ ускладнений. Відмова «ворожої» системи може бути як самоціллю (наприклад, зробити недоступним популярний сайт), так і одним із кроків до оволодіння системою [22, с. 81].

Якщо атака виконується одночасно з великої кількості комп'ютерів, то говорять про DDoS-атаку, одна з різновидів якої представлена на рис. 4. У деяких випадках до DDoS-атаки призводить легітимна дія, наприклад розміщення на популярному інтернет-ресурсі посилання на сайт, розміщений на не дуже продуктивному сервері.

Для того, щоб приховати свою IP-адресу, атакуючий фальсифікує адресу відправника, тобто крім описаного вище різновиду DDoS-атаки існує різновид DRDoS (Distributed Reflector DoS).

Фінансові та комерційні втрати через DDoS (упущений дохід, відтік клієнтів, зниження продуктивності праці і погіршення репутації) набагато перевищують прямі та операційні збитки організацій. Захист від DDoS-атак полягає у відсіканні паразитного трафіку на рівні підприємства та провайдера під час доступу до інтернет, а також у нейтралізації мереж ботнетів, які здійснюють розподілені атаки.

Нині основним документом, що регулює питання міжнародного співробітництва в боротьбі з кіберзлочинністю, є «Конвенція про кіберзлочинність» [37]. Конвенція встановлює заходи, яких повинні вжити країни на національному рівні щодо правопорушень проти конфіденційності, цілісності та доступності комп'ютерних даних і систем; правопорушень, пов'язаних із комп'ютерами; правопорушень, пов'язаних із розповсюдженням дитячої порнографії, та правопорушень, пов'язаних із порушенням авторських і суміжних прав [4].

Окремий розділ Конвенції присвячено міжнародному співробітництву з питань екстрадиції у зв'язку з кримінальними правопорушеннями, передбаченими Конвенцією, добровільного надання інформації щодо проведення розслідування кримінальних злочинів, визначених Конвенцією, а

також процедур, пов’язаних із запитами про взаємну допомогу в разі відсутності міжнародних угод між країнами.

За даними Євросоюзу, щодня жертвами злочинів, скоєних в мережі, стає не менш одного мільйона чоловік. Сукупний збиток від них досягає 300 млрд євро за рік. Із кіберзлочинністю ведуть боротьбу всі країни Євросоюзу [3], але досі – окремо один від одного і з вельми змінним успіхом.

Багато національних правоохоронних органів швидко досягають меж своїх можливостей, адже місце злочину в мережі інтернет кордонів не має.

Тому для колективної протидії загрозам кіберзлочинності почав роботу Європейський центр із боротьби з кіберзлочинністю. Він є структурним підрозділом Європолу (Europol) зі штаб-квартирою в Гаазі.

Серед пріоритетів Центру, розслідування інтернет-шахрайства, зокрема в системі електронного банкінгу та протидія інтернет-педофілії. Складність проблем, які характерні для кримінальних правопорушень у мережі інтернет, робить необхідним тісне співробітництво між громадськими організаціями, експертами та правоохоронними органами країн.

У цьому напрямі багатьма компаніями здійснюється співробітництво у формі обміну інформацією, проведення розслідувань комп’ютерних інцидентів та надання сприяння в підготовці кадрів співробітників правоохоронних органів різних держав.

Таким чином, можемо сказати, що для ефективної боротьби з кіберзлочинністю в економічній сфері потрібна система заходів і реалізація відповідної державної політики в цій галузі. Одні лише нові закони не здатні протистояти зростанню ІТ-злочинності. Потрібен комплекс заходів, спрямованих не лише на розвиток правозастосовної бази, але й на підвищення рівня грамотності громадян, судових та правоохоронних органів [9].

Тому, одне з головних завдань, на сьогодні для України це організація плідної взаємодії з правоохоронними органами у сфері боротьби з економічною кіберзлочинністю, а також надання своєчасної та швидкої

допомоги компаніям, що постраждали від кібератак та консультування таких компаній щодо попередження їх відразу локально.

РОЗДІЛ ІІІ. ОСНОВИ БОРОТЬБИ З ОРГАНІЗОВАНОЮ КІБЕРЗЛОЧИННІСТЮ В ЕКОНОМІЧНІЙ СФЕРІ У МІЖНАРОДНОМУ ЗАКОНОДАВСТВІ

3.1 Методи боротьби з організованою кіберзлочинністю в економічній сфері та їх ефективність: міжнародний досвід

Масштаби мережі Інтернет свідчать про те, що окремі елементи економічної кіберзлочинності не можуть обмежуватись територією певної держави, тому в будь-якому випадку національне законодавство повинно відповідати загальноприйнятим стандартам у даній сфері для можливості здійснювати міжнародне співробітництво.

При виборі країн, чий досвід є корисним для України, варто відштовхуватись від наступних критеріїв:

1) стратегічним партнером України є Сполучені Штати Америки, які останніми роками надають значну правову та фінансову допомогу Україні, тож доцільним є встановлення їх досвіду, з огляду на рівень розвитку даної держави;

2) євроінтеграційні перспективи України безпосередньо залежать від ступеня втілення європейських стандартів у вітчизняну правову систему;

3) важливим є звернення до досвіду деяких сусідніх держав, в першу чергу колишніх учасників Союзу Радянських Соціалістичних Республік, для порівняння рівнів розвитку даного інституту та встановлення позитивних моментів, на сьогодні не втілених в Україні.

Розпочнемо із досвіду Сполучених Штатів Америки. Серед норм Національної стратегії внутрішньої безпеки США, прийнятої в 2015 році, особливий інтерес представляє розділ «Кіберзахист», у змісті якого наголошується на необхідності захисту від кібератак на теренах кіберпростору та є окремий розділ щодо захисту економічної сфери.

Не зважаючи на вищесказане, у Сполучених Штатах Америки переважає концепція саморегулювання мережі Інтернет, а отже спеціальне законодавство у даній сфері представлено лише кількома нормативно-правовими актами.

Наприклад, до них варто віднести Закон про електронний підпис, прийнятий у 2000 році. Його основне призначення – забезпечення правового режиму електронного підпису в комерційних відносинах. В Сполучених Штатах Америки прийнято надавати даному нормативному акту символу вступу людства у нову еру – еру електронної комерції. Сам же Закон є доволі стислим і закріплює незначну кількість понять та механізмів – у тому числі, компетенцію державних органів, відповідальних за функціонування усієї інфраструктури у даній сфері, взаємодію її елементів та органів державної влади тощо.

Наприклад, 1 червня 1997 року президентом США була зроблена доповідь «Політика в галузі глобальної інформаційної комерції», у якій було сформульовано основні принципи політики держави у сфері надання Інтернет-послуг, один із яких: «уряд повинен встановлювати зрозумілі, мінімальні та прості правові норми лише там, де це потрібно» [49, с. 15]. Це означає, що активна боротьба із кіберзлочинністю у вигляді регламентації відповідних відносин здійснюється лише у тих сферах, де існують негативні тенденції до вчинення протиправних діянь, а інші характеризуються саморегуляцією та врегульовуються лише по мірі виникнення загроз.

Такий досвід не є позитивним для переймання, проте як свідчить практика, Сполучені Штати Америки є однією з найзахищеніших країн світу. Тому варто зробити висновок, що боротьба із економічною кіберзлочинністю повинна мати комплексний характер, а відповідне галузеве законодавство є лише одним із елементів.

Найбільшу кількість нормативно-правових актів прийнято у сферах емісії цінних паперів, охорони інтелектуальної власності, захисту від

несанкціонованого доступу до інформації щодо економічної сфери держави, бюджети корпорацій, тощо 146, с. 25].

Загалом, до недавнього часу американські юристи підтримували точку зору, що для регулювання боротьби із кіберзлочинністю важливішими є міждержавні, а не національні нормативно-правові акти, оскільки введення певних обмежень одним суб'єктом може негативно вплинути на інтереси інших сторін [47, с. 8].

Деструктивна діяльність в кіберпросторі США санкціонується значно жорсткіше, ніж у Європі. Так, у Сполучених Штатах визначено кримінальну відповідальність за неналежне зберігання та обробку інформації, що містить фінансові чи банківські дані чи її знищення у відмінний, від встановленого законом спосіб.

Для порівняння, у країнах Європейського Союзу кримінальні справи можуть заводитися лише у випадку завдання шкоди державній безпеці та основним правам громадян [52]. Тож, дослідження сучасного стану боротьби із економічною кіберзлочинністю засвідчило, що даний напрям є одним із пріоритетних у державній політиці США [17]. Тому, можна зробити висновок, що правове регулювання боротьби із економічною кіберзлочинністю у Сполучених Штатах Америки регламентується жорсткіше, ніж у Європі.

Використовуючи досвід США, найбільш доцільним напрямом буде створення в Україні підрозділу у рамках нової служби по економічній охороні держави в рамках збройних сил України.

Окрім Сполучених Штатів Америки, належне усвідомлення економічних та фінансових загроз і небезпек, які містяться в безконтрольному використанні можливостей кіберпростору деструктивними способами, належить країнам Європейського Союзу, де вже досить давно практикується законодавче регулювання Інтернету.

У даному випадку доцільно зазначити, що навіть у межах Європейського Союзу кадрові та фінансові можливості країн відрізняються, а

отже потенціал організацій, які здійснюють боротьбу із кіберзлочинцями не є однорідним.

Згідно Конвенції про кіберзлочинність, вона визначається, як кримінальні дії, скоєні з використанням електронних комунікаційних мереж та інформаційних систем або проти таких мереж та систем.

Саме з метою боротьби з економічною кіберзлочинністю був створений економічний відділ у комп'ютерній групі швидкого реагування, яка покликана боротись із новітніми комп'ютерними вірусами та виявляти слабкі місця в системі захисту економічної інформації, здійснювати розробку інтернет-стратегії для Єврокомісії і проводити спільно із різними структурами ЄС семінари з кібербезпеки.

Тобто, спектр діяльності даного органу є досить широким і включає в себе як активну практичну діяльність. В свою чергу, Європейський центр по боротьбі з кіберзлочинністю функціонує на базі Європолу та підпорядковується відділу по боротьбі з економічними злочинами.

Таким чином, правове регулювання боротьби із економічною кіберзлочинністю у Європейському Союзі характеризується наступними ознаками:

1) наявність як національного, так і міжнародного законодавства про боротьбу із економічною кіберзлочинністю;

2) діяльність по протидії економічним кіберзлочинам здійснюється одночасно національними та міжнародними організаціями, сформованими із кращих спеціалістів країн-учасників;

3) важлива роль відводиться теоретичним питанням, таким як експертне оцінювання збитків від кіберзлочинів, розробка передових методів профілактики і розслідування тощо;

4) здійснення активного інформаційного обміну.

Фундаментальне значення у протидії економічним кіберзлочинам в європейських державах має єдність та взаємодія, що відображається у залученні кращих фахівців кожної з країн-учасників до глобальних процесів.

Розглянемо більш детально правове регулювання боротьби із економічною кіберзлочинністю у Франції, оскільки дана держава одна із перших у Європі здійснила кроки до посилення ролі держави у регулюванні кіберпростору.

Так, згідно законодавства Франції найнебезпечнішим елементом економічного кіберзлочинства суспільно небезпечні діяння, пов'язані з незаконним тиражуванням комп'ютерного програмного забезпечення, незаконним втручанням до автоматизованих систем обробки даних, вторгненням на сайти, створенням та розповсюдженням шкідливих програм тощо.

Ще одним цікавим моментом регулювання даного виду злочину є встановлення вимоги до провайдерів щодо надання відомостей про авторів сайтів будь-яким третім особам, за порушення якої передбачено кримінальну відповідальність. Також даний вид відповідальності передбачено за надання неповних чи недостовірних відомостей авторами французьких сайтів та за надання провайдерами місця на сервері не ідентифікованим користувачам. При чому, за усі сайти, авторство яких не встановлено, відповідальність несе провайдер, а можливою мірою покарання є позбавлення волі строком на півроку [46, с. 21].

У сфері активної боротьби із кіберзлочинністю 14 лютого 2008 року було прийнято французьку Стратегію з питань боротьби із кіберзлочинністю, метою якої є співпраця між приватним бізнесом (постачальниками інформаційно-телекомунікаційних послуг) та правоохоронними органами з обміну інформацією та питаннях щодо об'єднання зусиль у боротьбі з кіберзлочинністю. Цікавими моментами Стратегії є курс на встановлення співробітництва провайдерів і поліції й жандармерії, та створення національної комісії з професійної етики по зв'язках із громадськістю [61].

Для цього у Франції окрім намірів створити спеціальну комісію вчиняються й інші дії. Відмітимо відкриття сайту Хартії Інтернету (Charte

de'Internet), на якому визначено принципи добровільних обов'язків користувачів та надавачів Інтернет-послуг.

Таким чином, Франція є вдалим прикладом країни для запозичення позитивного досвіду в Україну.

По-перше, дана держава у порівнянні з іншими країнами Європейського Союзу характеризується жорсткішими підходами до встановлення контролю у кіберпросторі. Тому, у контексті нещодавніх змін до вітчизняного законодавства, є доцільним звернення до досвіду країн, у яких подібні обмеження прав і свобод громадян були успішно реалізовані.

По-друге, Франція являється взірцем щодо встановлень двосторонніх відносин на рівнях «держава - держава», «держава - громадянин», «держава – приватний сектор економіки».

Останньою групою країн, на досвід яких варто звернути увагу, є сусідні держави, у першу чергу колишні учасники Союзу Радянських Соціалістичних Республік. Двадцять шість років тому кожною із держав було обрано самостійний вектор розвитку. Тому, не зважаючи на етнічну та історичну близькість, вже сьогодні ми можемо спостерігати відмінності у правовому регулюванні різноманітних суспільних інститутів.

Розглянемо досвід Республіки Білорусь, як однієї з перших держав колишнього СРСР, якої було утворено спеціальний орган для боротьби із кіберзлочинністю - управління по розкриттю злочинів у сфері високих технологій Міністерства внутрішніх справ Республіки Білорусь. 27 лютого 2001 року у структурі кримінальної міліції МВС з'явилося управління оперативно-організаційної роботи, у складі якого до листопада 2002 року активно діяло спеціалізоване відділення по розкриттю злочинів у сфері високих технологій, а вже 28 листопада 2002 року на підставі наказу Міністра внутрішніх справ, з метою вдосконалення організації роботи названих підрозділів, в МВС було створено самостійне управління, що здійснює практичну діяльність по розкриттю злочинів у сфері високих технологій пов'язаних з економічною сферою [16].

Аналізуючи законодавчу базу боротьби із кіберзлочинності в Білорусі, вона представлена незначною кількістю норм та законів: Глава Кримінального кодексу Республіки Білорусь, Закон про електрозв'язок, Закон про інформацію, інформатизації і захист інформації, Конвенція про кіберзлочини, Додатковий протокол до Конвенції про кіберзлочини, Указ «Про заходи щодо вдосконалення використання національного сегменту мережі Інтернет», Указ «Про деякі питання розвитку інформаційного суспільства в Республіці Білорусь», Указ «Про затвердження Положення про порядок взаємодії операторів електрозв'язку з органами, які проводять оперативно-розшукову діяльність» [25].

Таким чином, дослідження боротьби з економічною кіберзлочинністю досвіду країн-колишніх учасників Союзу Радянських Соціалістичних Республік на прикладі Республіки Білорусь засвідчило, що у цілому при виборі моделей для перейняття досвіду більш доцільним є звернення уваги на концепції більш розвинених європейських держав чи Сполучених Штатів Америки.

Не зважаючи на самостійний вибір шляхів розвитку, законодавство наших держав все ще є наближеним, а численні норми є похідними від радянського законодавства. Тож, робимо висновок, що використання досвіду Республіки Білорусь не вплине значним чином на вітчизняну систему правового регулювання боротьби з економічною кіберзлочинністю, проте окремі елементи є все ж доступними для запозичення, наприклад створення спеціального відділу в МВС по боротьби виключно з кіберзлочинністю, як високотехнологічного виду злочинства, пов’язаною з фінансовою та банківською сферою.

Підсумовуючи здійснене дослідження, варто зробити висновок, що втілення зарубіжного досвіду у будь-якому разі є тривалим та важким процесом, який не завжди призводить до позитивних наслідків. Аналізуючи моделі правового регулювання боротьби із економічною кіберзлочинністю, нами встановлено тенденцію до спроб встановлення контролю за

Всесвітньою мережею, проте наявні заборони все ж не містять ознак суттєвого порушення прав та свобод людини і громадянина.

У досліджуваних державах існує двосторонній діалог влади та громадян, завдяки якому у суспільстві формується вірне розуміння необхідності встановлення обмежень, заборон чи регламентів. В той же час, ми звернули увагу на незначну кількість нормативно-правових актів, які при цьому належним чином врегульовують даний інститут, тобто в них переважає саморегулювання сфери кібербезпеки, і все ж таки саме економічна сфера кібербезпеки врегульовано досить скудно, все ж таки більше уваги державами приділяється на боротьбу з кібертероризмом, у якому нам у нашому дослідження було цікаво визначити шляхи врегулювання заборони на його фінансування.

Також, доцільно відзначити роль міжнародного законодавства та міждержавних угод і конвенцій які значним чином мають вплив на суспільні відносини всередині держав.

Очевидно, що їх роль у вітчизняному праві необхідно виводити на новий рівень. Розглядаючи досвід держав колишнього Радянського Союзу, в тому числі і України, необхідно відзначити відмінність у формах контролю за економічним кіберпростором. Контроль має більш декларативний характер і неактивнішим чином впливає на права та свободи громадян.

Проте, варто враховувати відносну молодість усіх інститутів, пов’язаних із кіберпростором, тому зробимо висновок про перебування таких держав на проміжному етапі розвитку правового регулювання боротьби із кіберзлочинністю.

3.2 Перспективи боротьби з організованою кіберзлочинністю в економічній сфері України

По мірі збільшення кількості економічних кіберзагроз в нашій державі, все актуальнішим стає питання боротьби. В світлі євроінтеграційних процесів важливою для України є демонстрація того, що ми готові протистояти загрозам найстрімкіше зростаючому виду злочинності та, що вітчизняне законодавство належним чином регламентує відповідні правовідносини у економічному, фінансовому, банківському кіберпросторі.

Окрім того, в сучасних умовах важливою є демонстрація готовності приймати необхідні зміни, що відповідатимуть стандартам, встановленим на європейському та світовому рівнях.

Тож, за умов, коли сфера віртуального простору в економіці та злочинів в ньому продовжує розвиватись, питання перспектив та тенденцій розвитку боротьби з кіберзлочинністю в Україні є одним з основних в силу своєї важливості та рівня урегульованості. Постійний розвиток правового регулювання боротьби з економічною кіберзлочинністю в Україні є важливим з огляду на наступні фактори.

По-перше, на сьогодні практично усі державні та недержавні розрахункові процеси відбуваються із застосуванням інструментів кіберспростору.

По-друге, в умовах неоголошеної війни, у якій вимушена приймати участь Україна, економічний віртуальний простір є одним із фронтів, у якому наша держава в силу відставання в сфері інформаційних технологій все ще не демонструє внутрішньо та зовнішньополітичні успіхи.

По-третє, рівень усвідомлення загрози економічних кіберзлочинів та їх небезпечності у суспільстві все ще є невисоким. За таких умов проблема перспектив та тенденцій розвитку правового регулювання боротьби з кіберзлочинністю в Україні є однією із першочергових для дослідження.

Тож, ключовими факторами розвитку правового регулювання боротьби з економічною кіберзлочинністю в Україні є збільшення активності громадян в Інтернет просторі, активізація діяльності кіберзлочинців та необхідність імплементації міжнародних правових норм у вітчизняному законодавстві для боротьби із даним негативним явищем.

В той же час, звертаючись до наукової доктрини, варто відзначити недостатню увагу до даного питання з боку саме вчених-правовиків. Переважна більшість робіт у даній тематиці охоплюють тенденції поширення кіберзлочинів, або ж є не в повній мірі актуальними на сьогодні. Це є проблемою, оскільки досліджуване питання у цілому постійно перебуває в сфері наукових інтересів вітчизняних дослідників, проте ніколи не втрачає доцільності дослідження.

Тож, постійний розвиток інформаційних технологій та нормативно-правової бази їх реалізації, а також важливість дослідження тих тенденцій, які є доцільними саме на даному етапі розвитку нашої держави, зумовлюють важливість дослідження виділеної проблеми.

Оскільки на світовому рівні боротьба із економічною кіберзлочинністю розпочалась майже на десятиліття раніше, ніж в Україні, перейняття досвіду розвинутих країн очевидно ще довгий час передуватиме в переліку основних тенденцій розвитку правового регулювання боротьби з економічною кіберзлочинністю в нашій державі.

Також відмітимо, що процес консолідації європейської спільноти для боротьби із економічною кіберзлочинністю розпочався на початку поточного століття і на сьогодні вже прийнято значний масив міжнародних нормативно-правових актів.

До виконання частини з них Україна вже приєдналась шляхом ратифікації, проте ряд угод, протоколів та рекомендацій все ще не є джерелами вітчизняного законодавства. Щодо питання співробітництва також доцільно відзначити, що необхідність координації питань

співробітництва кожною країною відповідно до розробленої та чинної у ній стратегії економічної кібербезпеки [27, с. 60].

Аналізована стаття О. О. Йона та Н. Ф. Казакова датована 2013 роком, коли в Україні така стратегія ще перебувала на стадії розробки, проте, у 2016 році її було затверджено Указом Президента України «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України».

У контексті досліджуваної теми, необхідним є аналіз її норм з метою встановлення тих напрямів розвитку інституту правового регулювання боротьби з кіберзлочинністю в Україні, які виділив законодавець. Так, частина 4 Стратегії дістала назву «Пріоритети та напрями забезпечення кібербезпеки України», таким напрямком визнано економічну сферу.

Стосовно перспектив та тенденцій розвитку правового регулювання боротьби з економічною кіберзлочинністю в Україні - це певні першочергові положення, які стосуються забезпечення фінансової та банківської кібербезпеки.

Так, Радою національної безпеки і оборони України виділено наступні пріоритетні економічні напрямки кіберзахисту державних електронних інформаційних ресурсів та інформаційної інфраструктури; критичної інфраструктури розвитку потенціалу сектору безпеки і оборони у сфері забезпечення кібербезпеки та боротьби з кіберзлочинністю мають організаційний, процесуальний та технологічний характер, тож аналіз передбачених заходів засвідчив недоцільність їх віднесення до сфери правового регулювання боротьби з кіберзлочинністю [116].

Щодо питання міжнародного співробітництва, в даному напрямі обидві тенденції вживаються комплексно. Погодимось, що за своєю сутністю вони є близькими, проте не варто здійснювати їх поєднання, оскільки для розвитку вітчизняного законодавства використання зарубіжного досвіду не є першочерговим, так як важливим є слідування власній стратегії, що ураховує ті питання, які є нагальними для сьогодення. Можливість ознайомлення із

досвідом країн, які працюють в зазначеному напрямку не перший рік дозволить зробити такі механізми більш придатними та актуальними, проте повне копіювання в силу специфіки кожної з окремих держав є неможливим.

Також доцільно відзначити, що закріплений Радою національної безпеки і оборони України напрям з-поміж іншого включає і гармонізацію нормативних документів зі стандартами ЄС та НАТО, що доцільніше віднести до тенденції розвитку вітчизняної нормативно-правової та термінологічної бази у цій сфері, оскільки міжнародні нормативно-правові акти, ратифіковані Верховною Радою України, є важливим джерелом вітчизняного права. Останніми роками звичними є дискусії щодо доповнення Кримінального кодексу України статтями про злочини в комп'ютерній сфері, а також щодо значного посилення покарань за злочини скоєні в економічній сфері.

В даному контексті варто зазначити, що за останні роки до Розділу XVI даного нормативно-правого акту вже вносились зміни декілька разів, в тому числі й щодо зміни санкцій статей Кримінального кодексу України, виключення та доповнення Розділу новими статями.

Проте, враховуючи безперервний розвиток інформаційних технологій та форм вчинення економічних кіберзлочинів, варто розуміти, що можливим є настання моменту, коли чинні санкції не відповідатимуть негативним наслідкам шкідливих діянь на фінансову сферу кіберзлочинців.

Саме тому логічним вбачаємо виділення такої тенденції розвитку правового регулювання боротьби з кіберзлочинністю в Україні, як доповнення Кримінального кодексу України статтями про кіберзлочини та посилення покарання за вчинення злочинів в економічній сфері методом використання високих технологій.

Тенденція по встановленню співпраці на міжнародному рівні розвивалась поступово і на сьогодні вже потребує переходу на якісно новий рівень. Як нами встановлено в даній роботі, серйозні зміни у законодавчому

регулюванні переважно пов’язуються із виникненням нових форм кіберзлочинності.

Наприклад, прийняття Конвенції Організації Об'єднаних Націй проти транснаціональної організованої злочинності від 15.11.2000 року можна пов’язати із виходом кіберзлочинності на новий транснаціональний рівень в середині 90-х років XX століття. Сама Конвенція не є негайною реакцією міжнародної спільноти на виникнення даної загрози, а швидше адекватною та належним чином розробленою протидією транснаціональним кіберзлочинам. Віденська декларацію про злочинність і правосуддя: відповіді на виклики XXI століття (ООН) від 17.04.2000 року вже відштовхуючись від самої назви є нормативно-правовим актом, спрямованим на об’єднання держав світу у боротьбі із злочинами, не характерними для попередніх історичних епох. У самому тексті документу йдеться про «вчинення серйозних злочинів, які мають глобальний характер», їх «транснаціональність» та на необхідність боротьби із ними.

Враховуючи, що Декларація була прийнята в той же період, що й Конвенція ООН, це є ще одним свідченням серйозного росту масштабів злочинності, у тому числі й у кіберпросторі, в той період. Тобто, на підставі цих прикладів зробимо висновок, що увага міжнародної спільноти до проблеми виникнення нових форм злочинів спричинила суттєві зміні у міжнародному правовому регулюванні боротьби із кіберзлочинністю.

Тож, побудову системи перспектив та тенденцій розвитку правового регулювання боротьби з економічною кіберзлочинністю в Україні варто здійснюватись із обов’язковим урахуванням наступних положень:

1) в нашій державі розпочато процес інтеграції міжнародних нормативно-правових актів у сфері боротьби із кіберзлочинністю у вітчизняне законодавство;

2) Україна співпрацює, проте все ще не досить активно, із зарубіжними державами у питаннях, пов’язаних із розслідуванням економічних кіберзлочинів.

3) тенденція збільшення рівня контролю за користувачами мережі Інтернет.

Тому, подальший розвиток даного інституту варто пов'язати із вдосконаленням законодавчої бази та підвищенням взаємодії відповідних підрозділів органів внутрішніх справ на міжнародному рівні – із правоохоронними органами інших держав, що полягатиме у наданні все сторонньої допомоги в питаннях подолання економічної кіберзлочинності.

Також звернемо увагу на одну із негативних тенденцій розвитку правового регулювання боротьби з кіберзлочинністю в Україні, збільшення рівня контролю за користувачами мережі Інтернет [39].

Окрім проаналізованих позицій, вважаємо за необхідне доповнити перелік основних тенденцій розвитку правового регулювання боротьби з кіберзлочинністю в Україні тенденціями, які деталізуватимуть їх зміст. Так, у рамках тенденції розвитку вітчизняної нормативно-правової та термінологічної бази у сфері боротьби з кіберзлочинністю в Україні 130 запропоновано виділити наступні тенденції:

1) розширення меж розуміння поняття кіберзлочинність;

2) посилення кримінальної відповідальності за вчинення кіберзлочинів;

3) термінологічне узгодження у нормах усіх нормативно-правових актах, що регламентують дане питання, єдиного термінологічного апарату.

В тенденції збільшення рівня контролю за користувачами мережі Інтернет виділимо наступні тенденції:

1) встановлення правил користування громадянами кіберпростором;

2) створення спеціальних органів контролю, покликаних спостерігати та виявляти порушників встановлених правил користування кіберпростором.

Для розуміння того, які заходи необхідні для розвитку правового регулювання боротьби з кіберзлочинністю в Україні, варто належним чином розкрити кожну із виділених тенденцій. Тенденція розвитку вітчизняної нормативно-правової та термінологічної бази у сфері боротьби з кіберзлочинністю в Україні полягає у прямій залежності наших успіхів та

розвитку від тієї законодавчої бази, що врегульовує питання кіберзлочинності. Будь-які суспільні відносини, як у реальному, так і у віртуальному світі мають бути належним чином регламентовані та захищені нормами законодавства.

Як нами встановлено в даній роботі, на сьогодні наша держава перебуває на третьому етапі генезису правового регулювання боротьби з економічною кіберзлочинністю, проте усі існуючі проблеми все ще не вирішено.

Проте, не зважаючи на усе, наша держава залишається вразливою до економічного кібервпливу. Причину цьому варто шукати у тому, що вітчизняні закони, які врегульовують питання кіберпростору та злочинних посягань у ньому, є недостатньо розробленими.

Очевидно, що розвиток комп'ютерних технологій дозволяє зловмисникам здійснювати кіберзлочини з метою фінансової наживи фактично безкарно, оскільки кримінальне законодавство у такому вигляді є неадаптованим до нових форм злочинів у сфері інформаційних технологій.

Наведемо актуальний приклад – в умовах гібридної війни Україна щодня отримує атаки на свою банківську сферу.

Наступною проблемою є відсутність єдиного понятійного апарату, що має вияв у вільному трактуванні ключових понять – кіберзлочинів, кібербезпеки, кіберпростору, особливо дивно це ніяк не врегульовано щодо економічної сфери тощо у нормах вітчизняного законодавства.

Наприклад, у Кримінальному кодексі України законодавець оперує такими поняттями, як «злочини у сфері використання електронно-обчислювальних машин», «комп'ютерні системи», «комп'ютерні мережі», «мережі електрозв'язку» тощо [3]. Водночас, в жодному законі не висвітлена термінологія щодо фінансових кібератак на економічну сферу нашої держави, подібна до кіберзлочинності термінологія не вживається взагалі.

Кіберзлочини роз'яснюються як складова частина технологічного тероризму, оскільки ними є у тому числі злочини, які «вчиняються з

терористичною метою із застосуванням комп'ютерних систем та комунікаційних мереж» [14], а про економічну сферу зовсім не згадано. Тобто, в даному випадку законодавцем взагалі проігноровано вживання загальноприйнятої на міжнародному рівні та у вітчизняній науці термінології.

Найбільш доцільним вбачається саме використання термінології із частиною «кібер-», яка на сьогодні ще не отримала сформованого визначення на нормативно-правовому рівні.

Наступною тенденцією, виділеною нами, є посилення міжнародного співробітництва у сфері боротьби з економічною кіберзлочинністю в Україні. Потреба міжнародного співробітництва стосовно нашої держави має трьох аспектний характер.

По-перше, в умовах формування інституту правового регулювання боротьби з економічною кіберзлочинністю в Україні важливим є звернення до досвіду тих держав, які його успішно втілили у вітчизняних правових системах, із урахуванням сильних сторін та проблем, які супроводжували даний процес.

По-друге, потреба у міжнародному співробітництві з’явилась передусім внаслідок масової появи транснаціональних комп’ютерних злочинів, скоєних з метою фінансової наживи, складність яких свідчить про те, що жодна держава не здатна їх подолати, покладаючись виключно на власні сили.

По-третє, прагнення України до євроінтеграції неможливо втілити без встановлення міцних зв’язків із європейськими державами, в тому числі і у питанні економічною кібербезпеки.

Тож, у процесі аналізу наукової літератури нами встановлено наступні проблеми, що негативним чином впливають на міжнародне співробітництво у сфері боротьби з економічною кіберзлочинністю в Україні:

1) відносна молодість даного інституту в Україні, а отже необхідність удосконалення вітчизняного законодавства до загальноприйнятих світових стандартів;

2) незначна кількість міждержавних угод у сфері боротьби із кіберзлочинністю, укладених Україною, та міжнародних нормативно-правових актів, ратифікованих нашою державою.

Тенденція збільшення рівня контролю за користувачами мережі Інтернет полягає у зміні балансу між правоохоронними інтересами та повагою до основних прав і свобод людини й громадянина в інтересах держави. Дана тенденція у цілому є вкрай негативним явищем, проте за умови досягнення кіберзлочинністю катастрофічних масштабів, подібне рішення може виступити у якості основного вирішення поставлених перед державою завдань.

Впродовж останніх десятиліть було сформовано концептуальне розуміння боротьби з економічними кіберзлочинами та захистом інтересів держави в інформаційній сфері як забезпечення належного і стійкого балансу між правоохоронними інтересами та повагою до основних прав і свобод людини й громадянина.

Загалом, питання пошуку балансу між приватними і публічними інтересами є одним із невирішених в повній мірі в Україні. Так, на сьогодні у низці законодавчих актів визнається пріоритет приватних інтересів, зокрема у Конституції України [35], у статті 32 якої встановлюється недопущення збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини.

Тому, у питаннях, пов’язаних із економічною кібербезпекою, питання балансу між правами людини та потребами й інтересами суспільства і держави є одним із основних у даній сфері в світлі прийняття останніх рішень Радою національної безпеки і оборони України. Наприклад, 15.05.2017 р. Президентом України було підписано Указ №133/2017, яким

введено в дію рішення Ради національної безпеки і оборони України від 28 квітня 2017 року «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)».

Зокрема, цим Указом в тому числі і з метою забезпечення кібербезпеки Інтернет-провайдери повинні заборонити доступ до низки російських ресурсів. Це є підтвердженням того, що контроль за користувачами мережі Інтернет це не просто перспектива, а чинний інструмент забезпечення кібербезпеки, який і в подальшому буде реалізовуватись у вітчизняному законодавстві.

Ускладнення суспільних відносин в Україні обумовлює різні форми співвідношення приватних і публічних інтересів, що істотно ускладнює їх реалізацію, внаслідок чого в правових відносинах простежується їх протистояння і навіть конфлікти [45, с. 57].

Саме такий конфлікт на сьогодні спостерігається в Україні, оскільки інтерес держави домінує над інтересами громадян, що значним чином викликає їх невдоволення. Проте, якщо навіть поверхнево звернутись до досвіду зарубіжних держав, можна зробити висновок, що подібний контроль є звичним явищем.

Наприклад, у Сполучених Штатах Америки необхідні закони приймаються по мірі появи такої необхідності [46, с. 24]. У Франції діють обмеження щодо публікації особливих категорій матеріалів, а власники веб-ресурсів підлягають реєстрації [17].

З однієї сторони, такі обмеження не є тотожними із прийнятими в Україні, проте обидві ситуації об’єднує факт встановлення контролю та обмеження можливості громадян вільно розпоряджатись благами кіберпростору.

Однією із держав із подібним до щойно встановленого в Україні контролю, є Китай. Для даної держави характерними є обмеження доступу для користувачів на окремі веб-ресурси та контрольований вхід до мережі. Проте, стрімкий розвиток науково-технічних технологій на сьогодні дозволяє

обійти ці перешкоди, на сьогодні для ефективний і повний контроль в даній державі є проблематичним [46, с. 28].

Подібна ситуація спостерігається і в Україні, оскільки не зважаючи на виконання провайдерами вимог Ради національної безпеки і оборони України, у користувачів Інтернету залишаються можливості для обходу цих заборон.

Сама ж тенденція збільшення рівня контролю за користувачами мережі Інтернет повинна втілюватись наступним чином:

1) Встановлення правил користування громадянами кіберпростором - наприклад як і у випадку з прийняттям Указу Президента України №133/2017, яким введено в дію рішення Ради національної безпеки і оборони України від 28 квітня 2017 року «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)», яким заборонено доступ до окремих Інтернет ресурсів. Схожим чином буде здійснюватись регулювання й інших питань, пов’язаних із контролем за користувачами мережі Інтернет;

2) Створення спеціальних органів контролю, покликаних спостерігати та виявляти порушників встановлених правил користування саме економічним кіберпростором – на сьогодні таким органом є Департамент кіберполіції Національної поліції України, проте збільшення обсягу контролю потребуватиме розширення такої мережі.

На відміну від тенденцій, розвитку правового регулювання боротьби з кіберзлочинністю в Україні, які є явищем, що узагальнюють напрямки розвитку відповідного інституту, визначені на сьогодні, перспективи є можливостями, що мають чи можуть бути реалізованими в майбутньому.

Ураховуючи існуючі тенденції, та виділені нами у процесі дослідження проблеми, основною перспективою ми вбачаємо ліквідацію кордонів між державами у питаннях боротьби з економічною кіберзлочинністю. Тому що кіберзлочинність – це міжнародна проблема, оскільки кіберпростір, як об’єкт її посягання, не обмежується державними кордонами. Саме тому для протидії

цим негативним явищам мають бути залучені усі без виключення країни світу, безвідносно географічного положення, рівня соціально-економічного та технічного розвитку, а також рівня прийнятого національного законодавства.

Саме тому більш розвинені у технологічному відношенні держави повинні мати можливість допомагати менш розвиненим у питаннях запобігання та розслідування економічних кіберзлочинів.

Таким чином, розвиток економічних кіберзлочинів та поява нових інструментів протиправного впливу на суспільний порядок можуть докорінно все змінити. Як ми вже відмічали, специфіка кіберзлочинів полягає у тому, що знищення будь-яких доказів чи слідів протиправної діяльності є можливим у найкоротші строки. За умови, коли дана можливість ще зменшиться, світова спільнота потребуватиме швидких дій, а ліквідація кордонів між державами у питаннях боротьби з кіберзлочинністю здатна забезпечити цю швидкість.

ВИСНОВКИ

Таким чином у ході нашого дослідження встановлено:

1. Кіберзлочинність – це сукупність окреслених кримінальним законом вчинків, скоєних на тій чи іншій території або щодо об’єктів, розташованих на ній за відповідний період часу, вчинених у віртуальному просторі шляхом деструктивного впливу на комп’ютерні системи, комп’ютерні мережі і комп’ютерні дані.

Проте термін «кіберзлочинність» в офіційних нормативно-правових документах не визначено, навіть не зважаючи на те, що поняття є звичним як для лексикону правоохоронних органів України та держав світу, так і для правової доктрини нашої держави.

2. Виокремлено 4 основних етапів процесу розвитку явища кіберзлочинності. Підготовчий етап (початок 60-років - початок 70-х років XX століття) - перші випадки злочинів, вчинених із використанням електронних обчислювальних машин,. Етап розповсюдження кіберзлочинності (початок 70-х років XX століття – 1986 рік) - поява хакерів та їх організованих груп, а завершення пов’язати із прийняттям першого в історії нормативно-правового акту, присвяченого кіберзлочинам та першого арешту хакера. Етап транснаціональних кіберзлочинів (1994 рік – початок XXI століття) – початковий момент даного етапу пов’язується із «справою Володимира Льовіна», першим великим міжнародним транснаціональним мережевим комп’ютерним злочином. Сучасний етап кіберзлочинності (XXI століття) – етап появи нових форм комп’ютерних злочинів.

3. Кіберзлочинність – це п’ятий за розмірами вид економічної злочинності в України після незаконного привласнення майна, корупції та хабарництва, недобросовісної конкуренції та маніпуляції з фінансовою звітністю

Боротьбою з такою економічною злочинністю є комплексна активна система заходів, що застосовується у якості реакції держави на протиправне

посягання на її економічну складову, діяльність осіб чи їх груп та входить до компетенції правоохоронних органів та органу законодавчої влади за сприяння окремих осіб чи груп осіб, зацікавлених у подоланні даної проблеми та в економічному зростанні держави.

4. Для ефективної боротьби з кіберзлочинністю в економічній сфері потрібна система заходів і реалізація відповідної державної політики в цій галузі. Одні лише нові закони не здатні протистояти зростанню IT-злочинності. Потрібен комплекс заходів, спрямованих не лише на розвиток правозастосовної бази, але й на підвищення рівня грамотності громадян, судових та створення спеціальних правоохоронних органів для охорони кіберпростору виключно в економічній сфері.

5. Для розгляду зарубіжного досвіду боротьби проти економічної кіберзлочиності, нами у роботі було розглянуто досвід США, ЄС, крім того окремо досвід Франції та досвід Республіки Білорусь, як приклада пострадянської держави. Основними характеристиками регулювання боротьби із економічною кіберзлочинністю у США є розгалужена система органів протидії кіберзлочинам у тому числі і в економічній сфері.

Боротьба із економічною кіберзлочинністю у ЄС характеризується тим що діяльність по протидії кіберзлочинами здійснюється одночасно національними та міжнародними організаціями, сформованими із кращих спеціалістів країн-учасників, важлива роль відводиться теоретичним питанням, таким як експертне оцінювання збитків кіберзлочинів, розробка передових методів профілактики і розслідування тощо.

Особливостями Франції у цій сфері є суттєва роль держави у регулюванні суспільних відносин в Інтернеті, контроль за користувачами шляхом встановлення вимоги до авторизації авторів веб-сайтів, співробітництва правоохоронних органів та Інтернет-провайдерів.

У Республіці Білорусь основними характеристиками боротьби із економічною кіберзлочинністю у є наявність спеціального органу із значним досвідом протистояння саме економічній кіберзлочинності.

6. Виділено перспективи боротьби з організованою кіберзлочинністю в економічній сфері України, а саме, це тенденція розвитку вітчизняної нормативно-правової та термінологічної бази у сфері боротьби з економічною кіберзлочинністю в Україні та посилення міжнародного співробітництва у сфері боротьби з фінансовою та банківською кіберзлочинністю в Україні. Крім того ми запропонували збільшення рівня контролю за користувачами мережі Інтернет та підвищити кримінальну відповідальність за даний вид злочину.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бєляков Р.Г. Взаємодія управління боротьби з кіберзлочинністю МВС України з іншими правоохоронними органами: питання сьогодення. Право і безпека : науковий журнал. Харк. нац. ун-т внутрішніх справ. Харків, 2018. № 4 (55). С. 85-88.

2. Бойченко О. В. Інформаційна безпека в органах внутрішніх справ України (організаційно-правові засади) : монографія / О. В. Бойченко ; Крим. юрид. ін-т ОДУВС. – Сімферополь : Сімфероп. міська друк., 2009. – 288 с. 2. Сідак В. С. Забезпечення інформаційної безпеки в країнах НАТО та ЄС : навч. посіб. / В. С. Сідак, В. Ю. Артемов. – Київ : КНТ, 2007. – 160 с.

3. Бойченко О. В. Угрозы информационных ресурсов государственного самоуправления / О. В. Бойченко // Материалы Международной научно-практической конференции «Проблемы и особенности влияния международной информации на экономические и общественно-политические процессы». – Симферополь : ИСВА МСУ, 2007. – С. 39–41.

4. Болгов В.М., Гадіон Н.М., Гладун О.З. Організаційно-правове забезпечення протидії кримінальним правопорушенням, що вчиняються з використанням інформаційних технологій: наук.-практ. посіб. К.: Національна академія прокуратури України, 2015. 202 с.

5. Бурячок В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник. за заг. ред. д-ра техн. наук, професора В. Б. Толубка. К.: ДУТ, 2015. 288 с.

6. Буяджи С.А. Перспективи правового регулювання боротьби з кіберзлочинністю в Україні. Право України. 2017. № 9. С. 245-251.

7. Варунц Л. Д. Досвід організації діяльності Королівської канадської кінної поліції та шляхи його використання в Україні : дис. канд. юрид. наук : 12.00.17 / Варунц Лариса Дмитрівна. – Дніпропетровськ, 2012. – 203 с.

8. Вирок Ленінського райсуда м. Кіровограда від 24 лютого 2015 року по справі № 405/1660/14-к. URL http://www.reyestr.court.gov.ua/Review/42833218

9. Вирок Першотравневого районного суда м. Чернівців від 22.05.2017 року по справі № 725/85/17. URL http://www.reyestr.court.gov.ua/Review/66614097

10. Вирок Стрийського міськрайонного суда Львівської області від 21 січня 2016 року по справі № 456/4615/15-к. URL Режим доступу: http://www.reyestr.court.gov.ua/Review/55146476 URL

11. Вирус Petya.A: киберполиция изъяла сервера M.E.Doc. URL http://news.liga.net/news/politics/14781131-virus_petya_a_kiberpolitsiya_izyala_servera_m_e_doc.htm (дата звернення: 04.02.2019)

12. Віденська декларація про злочинність та правосуддя: відповіді на виклики XXI століття. Міжнародний документ від 17.04.2000 року. URL http://zakon5.rada.gov.ua/laws/show/995_443 (дата звернення: 10.12.2019)

13. Войціховський А. В. Міжнародне співробітництво в боротьбі з кіберзлочинністю. Право і Безпека. 2018. № 4. С. 107-112

14. Голубєв В.О. Інформаційна безпека: проблеми боротьби з кіберзлочинами : Монографія. Гуманітарний ун-т "Запорізький ін-т державного та муніципального управління". Запоріжжя : ЗІДМУ, 2003. 250 с.

15. Горова С.В. Кіберпрофесіонали і кіберзлочинність // Боротьба з організованою злочинністю і корупцією (теорія і практика) : науковопрактичний журнал. Міжвідомчий науково-дослідний центр з проблем боротьби з організованою злочинністю. Київ, 2014. № 2 (33), спецвипуск. С. 170-173.

16. Гринчак І.В. Кіберзлочинність як злочин міжнародного характеру. Науково-інформаційний вісник Івано-Франківського університету права імені Короля Данила Галицького : право, економіка /

ІваноФранківський університет права імені Короля Данила Галицького. ІваноФранківськ, 2017. Вип. 12. С. 93-98.

17. Двенадцатый Конгресс Организации Объединенных Наций по предупреждению преступности и уголовному правосудию (Сальвадор, Бразилия, 12–19 апр. 2010г.) : A / CJNF.213/1 [Електронний ресурс]. – Режим доступу: http://www.un.org/ru/conf/crimecongress2010/.

18. Демедюк С.В. Міжнародний досвід протидії кіберзлочинності. Вісник Харківського національного університету внутрішніх справ : збірник наукових праць. Харківський національний університет внутрішніх справ. Харків, 2017. № 4 (67). С. 65-75.

19. Дзюндзюк В. Б. Поява і розвиток кіберзлочинності. Державне будівництво. 2013. № 1. URL http://nbuv.gov.ua/UJRN/DeBu_2013_1_3 (дата звернення: 13.11.2019)

20. Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи. Міжнародний документ від 28.01.2003. Офіційний вісник України 2010 р. № 56, / № 31. 2006. ст. 2202 /. стор. 73. стаття 1920. код акту 52082/2010

21. Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп’ютерні системи : від 28 січ. 2003 р. ; ратиф. Україною 21 серп. 2006 р. [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/994_687.

22. Европейская Конвенция по киберпреступлениям от 23 ноября 2001 года. URL: http://www.eos.ru/eos_delopr/eos_law/detail.php?ID=32003&SECTION_ID=671

23. Європіна І. В. Види протиправних діянь у сфері новітніх інформаційних технологій. Вісник Академії адвокатури України. 2010. Число 3. С. 129-136.

24. Заворуєв Р.С., Резніченко В.А. Протидія кіберзлочинності в Україні. Матеріали Всеукраїнської науково-практичної конференції 23-25 листопада 2016 р. м. Кропивницький. С. 49-50

25. Закалюк А. П. Курс сучасної української кримінології : в 3 кн. Кн. 1. Теоретичні засади та історія української кримінологічної науки. К. : Видав. дім «Ін Юре», 2017. 423 с

26. Іванченко О. Ю. Кримінологічна характеристика кіберзлочинності, запобігання кіберзлочинності на національному рівні. Актуальні проблеми вітчизняної юриспруденції. 2016. Вип. 3. С. 172-177.

27. Каланча С.Г. Кіберзлочинність: шляхи попередження та протидії. Наше право : науково-практичний журнал. Харк. нац. ун-т внутрішніх справ ;Кримінологічна асоціація України ; Київський міжнар ун-т; МАУП;Західнорегіональна асоціація клубів ЮНЕСКО. Дрогобич, 2012. № 3, ч.2. С. 213-217

28. Кархут О.Я. Механізм правового регулювання суспільних відносин у сфері освіти: теоретико-правовий аспект: автореф. дис. … канд. юрид. наук: спец. 12.00.01 «Теорія та історія держави і права; історія політичних і правових учень». К. 2014. 21 с.

29. Комп’ютерна злочинність. Навчальний посібник. Київ: Атіка, 2002. 232 с.

30. Конвенция об информационном и правовом сотрудничестве, касающемся «Информационных общественных услуг» : ETS № 180 от 4 окт. 2001 г. – [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/994_559.

31. Конвенція [ООН] проти транснаціональної організованої злочинності : прийн. резолюцією 55/25 Ген. Асамблеї від 15 листоп. 2000 р. ; ратиф. із застереженнями і заявами законом України від 4 лют. 2004 р. № 1433-15 [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/995_789.

32. Конвенція [Ради Європи] про кіберзлочинність : від 23 листоп. 2001 р. ; ратиф. Україною 7 верес. 2005 р. // Офіційний вісник України. – 2007. – № 65. – Ст. 2535.

33. Конвенція про взаємодопомогу в кримінальних справах між державамичленами Європейського Союзу. Міжнародний документ від 29.05.2000 URL http://zakon3.rada.gov.ua/laws/show/994_238?test=Up9Mf3o6frtCt4d2ZiIViVNwHI4Uks80msh8Ie6

34. Конвенція про кіберзлочинність: Міжнародний документ від 23.11.2001. Офіційний вісник України. 2007 р. № 65. стор. 107. стаття 2535. код акту 40846/2007.

35. Конституція України: Закон України від 28.06.1996 № 254к/96-ВР. Відомості Верховної Ради України. 1996. № 30. ст. 141.

36. Кримінальний кодекс України. Закон України від 05.04.2001 № 2341-III. Відомості Верховної Ради України (ВВР). 2001. № 25-26. ст.131.

37. Кримінальний процесуальний кодекс України. Закон України від 13.04.2018 № 4651-VI. Відомості Верховної Ради України (ВВР). 2013. № 9-10. № 11-12. № 13. ст.88.

38. Куракін О.М. Структура механізму правового регулювання. Науковий вісник Ужгородського національного університету. Серія: Право. 2015. Вип. 35. Ч. 2. Т. 1. С. 41-44.

39. Ліпкан В. А. Інформаційна безпека України в умовах євроінтеграції : навч. посіб. / В. А. Ліпкан, Ю. Є. Максименко, В. М. Желіховський. – Київ : КНТ, 2006. – 280 с. – (Серія: Нац. і міжнар. безпека).

40. Літвінов М.Ю. Світова та українська практика боротьби з кіберзлочинністю. Право і безпека : науковий журнал. Харк. нац. ун-т внутрішніх справ. Харків, 2014. № 1 (52). С. 85-89.

41. Лукянчук Р.В. Сучасний формат державного регулювання процесів забезпечення кібернетичної безпеки: досвід європейського союзу. Вісник Київського національного університету імені Тараса Шевченка.

Київський національний університет імені Тараса Шевченка. Київ , 2016. (Державне управління ; вип. 2 (6)). С. 34-38.

42. Люта Н.В. Кіберзлочини як сучасна загроза фінансовій безпеці банків та їх клієнтів. Наука: теорія та практика : зб. тез доп. III Всеукр. наук.-практ. заоч. конф., 16-18 жовт. 2017 р. М-во освіти і науки України, Черкас. нац. ун-т ім. Богдана Хмельницького, Навч.-наук. ін-т економіки та права, Каф. менеджменту та екон. безпеки, Всеукр. спілка вчених-економістів ; [за заг. ред. проф. Мігус І.П.]. Черкаси : Чабаненко Ю.А., 2017. С. 247-252.

43. Максименко Ю. Є. Теоретико-правові засади забезпечення інформаційної безпеки України : автореф. дис. … канд. юрид. наук : 12.00.01 / Максименко Юлія Євгеніївна. – Київ, 2007. – 20 с.

44. Манжай О. В. Проблеми нормативно-правового забезпечення боротьби з кіберзлочинністю в Україні. Форум права. 2017. № 1. С. 646-650.

45. Міщук Н. Кіберзлочинність як загроза інформаційному суспільству // Вісник Львівського університету : збірник наукових праць / Львівський національний університет ім. Івана Франка. – Львів, 2014. – (Серія економічна ; вип. 51). – С. 173-179.

46. Основні завдання Департаменту кіберполіції Національної поліції України. URL https://www.cybercrime.gov.ua/contacts (дата звернення: 02.06.2019)

47. Перелік кібератак. Вікіпедія – вільна енциклопедія. URL : https://uk.wikipedia.org/wiki/Перелік_кібератак

48. Про Державну службу спеціального зв'язку та захисту інформації України. Закон України від 23.02.2006 № 3475-IV. Відомості Верховної Ради України (ВВР). 2006. № 30. ст.258.

49. Про деякі заходи щодо захисту державних інформаційних ресурсів у мережах передачі даних. Указ Президента України від 24.09.2001 № 891/2001 // Урядовий кур’єр від 03.10.2001. № 179. URL zakon.rada.gov.ua (дата звернення: 01.02.2019)

50. Про затвердження Штату Департаменту кіберполіції Національної поліції України. Наказ Національної поліції України від 07.11.2015 № 10. URL https://www.npu.gov.ua/uk/publish/printable_article/1816252 (дата звернення: 03.06.2019)

51. Про заходи щодо зміцнення банківської системи України та підвищення її ролі у процесах економічних перетворень. Указ Президента України від 14.07.2000 № 891/2000. Урядовий кур'єр від 22.07.2000. URL zakon.rada.gov.ua (дата звернення: 17.01.2019)

52. Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні // Урядовий кур'єр від 08.08.2000. URL zakon.rada.gov.ua (дата звернення: 23.01.2019)

53. Про Національний банк України. Закон України від 20.05.1999 № 679-XIV. Відомості Верховної Ради України (ВВР). 1999. № 29. ст.238.

54. Про Національну поліцію. Закон України від 02.07.2015 № 580-VIII. Відомості Верховної Ради (ВВР). 2015. № 40-41. ст.379.

55. Про ратифікацію Конвенції Організації Об'єднаних Націй проти транснаціональної організованої злочинності та протоколів, що її доповнюють (Протоколу про попередження і припинення торгівлі людьми, особливо жінками і дітьми, і покарання за неї і Протоколу проти незаконного ввозу мігрантів по суші, морю і повітрю). Закон України від 04.02.2004 № 1433-IV. Відомості Верховної Ради України (ВВР). 2004. № 19. ст.263.

56. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України». Указ Президента України від 15.03.2016 № 96/2016. Урядовий кур'єр від 18.03.2016. № 52

57. Про рішення Ради національної безпеки і оборони України від 31 жовтня 2001 року "Про заходи щодо вдосконалення державної інформаційної політики та забезпечення інформаційної безпеки України». Указ президента України від 06.12.2001 № 1193/2001. Урядовий кур'єр від 18.12.2001. № 235

58. Про Службу безпеки України. Закон України від 25.03.1992 № 2229-XII. Відомості Верховної Ради України (ВВР). 1992. № 27. ст.382.

59. Про судову експертизу. Закон України від 25.02.1994 № 4038-XII // Відомості Верховної Ради України (ВВР). 1994. № 28. ст.232.

60. Про утворення територіального органу Національної поліції. Постанова Кабінету Міністрів України від 13.10.2015 № 831. Урядовий кур'єр від 21.10.2015. № 195

61. Протидія кіберзлочинності в Україні: правові та організаційні засади : навч. посіб. / [О. Є. Користін, В. М. Бутузов, В. В. Василевич та ін.]. – Київ : Скіф, 2017. – 728 с.

62. Пушкаренко, П. І. Кіберзлочинність як новітній феномен тіньової економіки [Текст]. Проблеми і перспективи розвитку банківської системи України : зб. наук. праць / Державний вищий навчальний заклад «Українська академія банківської справи Національного банку України». Суми, 2006. Т. 17. С. 75-82

63. Рафал Канія Розвиток правової кібернетики у Польщі в XX-му сторіччі // Інформація і право : науковий журнал / Н.-д. ін-т інформатики і права Нац. акад. правових наук України ; Нац. б-ка України ім. В.І. Вернадського Нац. акад. наук України ; Відкритий міжнар. ун-т розвитку людини "Україна" ; голов. ред. Пилипчук В.Г. Київ, 2018. № 1 (24). С. 81-88.

64. Рудой К.М. Протидія кіберзлочинності як напрям забезпечення міжнародної безпеки ОВС України. Публічне право : науково-практичний юридичний журнал. Всеукр. громадська організація "Майбутнє країни" ; Ужгород. нац. ун-т. Київ, 2015. № 3 (19). С. 144-149.

65. Сень Р. Ю. Досвід іноземних країн у сфері розслідування кіберзлочинів / Руслан Юрійович Сень // Актуальні питання діяльності правоохоронних органів у сфері протидії кіберзлочинності : матеріали міжнар. наук.-практ. конф., м. Харків, 12 листоп. 2014 р. / МВС України, Харків. нац. ун-т внутр. справ. – Харків : Права людини, 2014. – С. 192–194.

66. Сироїд Т. Л. Правова основа міжнародної співпраці у сфері боротьби з кіберзлочинністю / Сироїд Тетяна Леонідівна // Актуальні питання діяльності правоохоронних органів у сфері протидії кіберзлочинності : матеріали міжнар. наук.-практ. конф., м. Харків, 12 листоп. 2014 р. / МВС України, Харків. нац. ун-т внутр. справ. – Харків : Права людини, 2014. – С. 194–196.

67. Угода про співробітництво держав-учасниць Співдружності Незалежних Держав в боротьбі зі злочинами у сфері комп'ютерної інформації. Міжнародний документ від 01.06.2001. URL http://zakon4.rada.gov.ua/laws/show/997_353

68. Чернєй В. В. Роль відомчої освіти та науки в забезпеченні протидії кіберзлочинності в Україні. Науковий вісник Національної академії внутрішніх справ. 2014. № 3. С. 3-15.

69. A Brief History of Computer Crime: An Introduction for Students. M. E. Kabay, PhD, CISSP-ISSMP Program Director, MSIA School of Graduate Studies Norwich University. URL http://www.mekabay.com/overviews/history.pdf

70. Jarrett, H. Marshall; Bailie, Michael W. (2018). Office of Legal Education Executive Office for United States Attorneys. Retrieved June 3, 2013. 213 p. URL https://www.justice.gov/sites/default/files/criminalccips/legacy/2015/01/14/ccmanual.pdf

71. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism : USA PATRIOT ACT (Act of 2001). Public Law 107–56—OCT. 26, 2001 URL https://www.gpo.gov/fdsys/pkg/PLAW107publ56/pdf/PLAW-107publ56.pdf (дата звернення: 08.07.2019)