МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХЕРСОНСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ БІЗНЕСУ І ПРАВА
КАФЕДРА ПУБЛІЧНОГО ТА МІЖНАРОДНОГО ПРАВА І ПРАВООХОРОННОЇ ДІЯЛЬНОСТІ

МІЖНАРОДНО-ПРАВОВА ОСНОВА ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

Кваліфікаційна робота (проєкт)

на здобуття ступеня вищої освіти "бакалавр"

Виконав:
студент IV курсу 12-481 групи
Спеціальності: 293 "Міжнародне право"
Освітньо-професійної програми
"Міжнародне право"

Романович Владислав Євгенович

Керівник: к.ф.н., доц. Задорожня Н.О.

Рецензент: доцентка кафедри
професійних та спеціальних дисциплін
Херсонського факультету ОДУВС,
к.ю.н., доцентка Новікова М.М.

Херсон - 2021

ЗМІСТ

ВСТУП

Актуальність теми.Рівень цивілізованості держави обумовлюється сучасністю розвитку в усіх сферах життя. Сьогодні на ряду з побутовими сферами життя у сучасному суспільстві все більше починають слідкувати за розвитком інноваційних технологій, пов'язанних з мережею Інтернет. За допомогою комп'ютерів і інших сучасних пристроїв можна зробити як і дуже корисні речі для населення і світу загалом, так можна і зробити багато шкоди суспільству. З розвитком інформаційних технологій злочинів в цій сфері з кожним роком стає все більше і більше. З розвитком інформаційної сфери більш вправними стають і злочинці, розвиваючи свої методи ведення злочинної діяльності. Для цього і створюються різні служби безпеки, які допомагають державам у боротьбі із злочинним світом інноваційних технологій.

Кібербезпека останнім часом стає все більше і більше популярною в суспільстві, розкриваються теоретичні питання міжнародної інформаційної безпеки, як складової для підтримки миру.Захист інформаційної сфери у найрозвинутіших країнах стає стратегічною потребою і потребує чималих зусиль її досягнення. Сама інформаційна безпека залежить насамперед від держави, від її діяльності на національному рівні та міжнародній арені, бо саме від неї залежить напрям і розвиток країни та її суспільства. Робити вона це може за допомогою різних політичних інститутів, за допомогою своєї законодавчої ініціативи, ратифікування різного роду міжнародних документів або імплементування міжнародних правових норм.

На сьогодні кіберзлочинність – це реальна проблема, яка загрожує багатьом державам світу, навіть найрозвинутішим. Загроза може йти з будь-якої країни і може виходити за межі розуміння традиційного

терміну «злочин» та його юрисдикції. Особливу небезпеку це може становити тому, що це дає можливість розробити, розповсюджувати та застосовувати кіберзброю.

Питанням протидії кіберзлочинам та й взагалі злочинам у інформаційній сфері займалися такі науковці як Ю.М. Батурін, С.Я. Лихова, Дворецький С.Ю, М.А. Міхейченко, В.Г. Пилипчук, В.М. Брижко, М. В. Маркарян, О.Ю. Запорожець, О.В. Орлова, А.І. Марущак, О.І. Котляревський, В.Д. Гавловський, В.В. Пивоваров та інші.

Мета кваліфікаційної роботи-аналіз організаційних і правових основ протидії кіберзлочинності у міжнародній сфері. Відповідно до поставленої мети вирішувалися наступні **завдання:**

-визначити зміст поняття кіберзлочинності;

-з’ясувати проблеми протидії злочинам в інформаційній сфері у міжнародній практиці;

-охарактеризувати співпрацю України та Європейського Союзу в Інтернет сфері;

-проаналізувати законодавчу базу, створену для боротьби з кіберзлочинами.

Об’єктом кваліфікаційної роботивиступають відносини між державами в інформаційній сфері.

Предметом кваліфікаційної роботи є аналіз національного та міжнародного законодавства щодо питання кібербезпеки та боротьби із злочинами в інформаційній сфері.

Методи дослідження. Метод системного аналізунадав змогу дослідити проблеми безпеки Інтернет сфери в міжнародному та національному праві та їх зв'язок.Застосуваннялогіко-правового методу дозволило визначитись з проблематикою протидії кіберзлочинам. Також застосовувався метод узагальнення. Метод порівняння дозволив

побачити спільні та відмінні риси національного законодавства та законодавства країн світу.

Практичне значення роботи полягає у можливості застосування її для підготовки методичних матеріалів з кримінальногота порівняльного кримінального права.

Структура кваліфікаційної роботи складається зі вступу, двох розділів, висновків та списку використаних джерел.

РОЗДІЛ 1.

ТЕОРЕТИКО-ПРАВОВІ ЗАСАДИ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

1.1.Зміст поняття кіберзлочинність у контексті міжнародного права

Швидкий розвиток суспільства призводить до інтенсивного розвитку всього, чим воно користується: від нових предметів побуту до нових наукових відкриттів, технічно-промислових проривів. Інформаційна сфера також не залишається осторонь цих події і прогресує з кожним днем, але нажаль, прогресує не тільки на благо людства, а й на задоволення злочинних намірів певного його прошарку. Чим якісніше стають інформаційні технології(новітні засоби захисту, сучасні програми для забезпечення спокійного перебування в мережі Інтернет, сучасні шифри) , тим професійніше стають злочинці(кібератаки, фішинг, спам) і це стосується не тільки кіберсфери.

Інформаційна діяльність є фундаментом суспільного життя в усіх країнах світу, а також стратегічним принципом для прогресивного розвитку. Відображення правових аспектів інформаційної діяльності лягли в основу поняття інформаційний суверенітет, який визначається як здатність держави контролювати і реагувати на потоки інформації, які поступають з-поза меж країни з метою дотримання законів країни, прав і свобод громадян, гарантування національної безпеки своєї держави.

Було визначено, що інформаційний суверніт є невід’ємним правом людини, суспільства та держави на самовизначенність і участь у формуванні, розвитку і подальшого функціонування національної інформаційної діяльності відповідно чинного законодавства.

У зв’язку з цим для створення сучасних методик організації інформаційної безпеки виникає потреба в дещо більшій універсалізації

визначення, в якому передбачалися б всі рівні суверенності над інформаційними ресурсами та можливостями їх використання. [1,с.108].

Інформаційний суверенітет тісно пов’язаний з інформаційною базою, що є основою існування і розвитку нації. Тобто,більшість суверенних масивів інформації містять ту частину загального інформаційного ресурсу, без якої неможливе існування і розвиток нації.

Варто звернути увагу на те, що загроза техніко-технологічного відставання інформаційної сфери існування суспільства зумовлює загрози інформаційному суверенітету під впливом цілої низки негативних чинників. Серед них найбільш відчутною є засновані зазвичай на нових технологічних рішеннях комп’ютерна злочинність, комп’ютерний тероризм, несанкціоноване проникнення в суверенні масиви інформації, що становлять державну та іншу передбачену законом таємницю, інтелектуальну власність соціальних структур та окремих членів суспільства. [2,с.60-62].

Із появою реальної загрози в Інтернет сфері, з’явилось і таке поняття як кіберзлочин.Єдиного визначення, що таке «кіберзлочин» немає. Використовують різні поняття: незаконний доступ, комп’ютерні злочини. Згідно з Конвенцією про кіберзлочинність, яку Україна ратифікувала у 2005 році, вказано, що кіберзлочинність - це незаконне перехоплення конфіденційних даних, шахрайство, пов’язане з комп’ютерами, втручання у данні, правопорушення пов’язані з дитячою порнографією. Отже, можна виділити для себе, що таке кіберзлочинність на міжнародній арені. Кіберзлочинність-це шахрайство, несанкціонований доступ до персональних даних користувачів Інтернету, розміщення протиправного контенту на його просторах, що має на меті пропагування різного роду злочинних дії, як-то екстремізм, тероризм, расизм.

Міжнародне співтовариство багато разів висловлювала своє невдоволення, а часом і своє занепокоєння, що новітні зміни у інформаційних технологіях, цифрових винаходах можуть змінити не тільки суспільство загалом, хоча на це і розраховано, зробити більш комфортним життя людей, а й ще те, що ці зміни можуть погано вплинути на забезпечення світового спокою та безпеки, можуть негативно вплинути на побудову та розвиток цілих держав [3].

У сфері комунікаційних технологій дуже відома Женевська декларація принципів «Побудова інформаційного суспільства: глобальна задача у новому тисячолітті», яка підкреслює важливість інформаційного збагачення, його серйозний вплив на практично всі сфери нашого життя. Ця декларація визначила за необхідне формувати та розвивати кібербезпеку, забезпечувати її на всіх рівнях життя та погоджувати свої дії з усіма компетентними та зацікавленими міжнародними органами. В процесі цього не потрібно забувати і про приватне життя людини, захист особистих даних. ООН висловила підтримку у дотриманні кібербезпеки та висловила необхідність використовувати інформаційні ресурси тільки в мирних цілях, пам’ятаючи при цьому про права людини та дотримання їх, запобігання використовуванню ресурсів у злочинних, терористичних діях. В цій декларації прямо не вказано, що таке кіберзлочин, але з її положень випливає, що боротьба з ним є першочерговим завданням глобальної культури кібербезпеки[4].

Після Женевської декларації з’явився Женевський план дій «Зміцнення довіри і безпеки при використанні ІКТ», який розвинув ідеї та положення принципів попередниці. Він зобов’язав державні органи попереджати, попереджати і реагувати на прояви кіберзлочинності і зловживання ІКТ шляхом розробки керівних принципів, які враховують постійнізусилля у цій сфері; формування законодавства, що дає змогу

ефективно розслідувати і переслідувати зловживання; сприяння ефективним зусиллям взаємодопомоги [5].

Необхідність розвитку та стимулювання культури кібербезпеки,впровадження глобальної культури кібербезпеки, а також кримінального переслідування кіберзлочинності визначила і Туніська програма для інформаційного суспільства,була прийнята у 2005 році. Вона була другим етапом у проведенні Всесвітнього саміту з питань інформаційного суспільства, де у 2003 році було прийнято чотири документи, зокрема прийнятий Женевський план[6].

Слід зазначити, що в жодному міжнародно-правовому документі немає закріпленого терміну «кіберзлочинність». Отже, за відсутністю його, та єдиного міжнародно- правового документу, що закріплював би чіткі, поетапні кроки в боротьбі з кіберзлочинністю, рішучим кроком було рішення створити та прийняти регіональні договори. Аналізуючи документи, можна зробити висновок, що в них використовується різний понятійний апарат:

1. Конвенція Ради Європи про кіберзлочинність від 21.11.2001 р. не містить термін «кіберзлочинність» (cybercrime), його характеристика відсутня. У документі перелічені окремі види діянь, які можна віднести до кіберзлочинності. Конвенція має на меті доповнення подібнихконвенцій для підвищення ефективності кримінальних розслідувань і переслідувань.Таким чином, узагальнивши наведені положення, можна стверджувати, що кіберзлочин – це кримінальне правопорушення, яке робиться в інформаційній сфері і спрямоване проти конфіденційності, цілісності і доступності комп’ютерних систем, мереж і комп’ютерних даних, а також зловживання такими системами, мережами і даними[7].

2. Конвенція про боротьбу із злочинами у сфері інформаційних технологій Ліги арабських держав від 21.12.2010 р. застосовує термін «злочини у сфері інформаційних технологій» (information technology offences), визначення якого в тексті договору також відсутнє.В той же час, виходячи із контексту ст. 2 можна стверджувати, що злочини у сфері інформаційних технологій – це злочини, пов'язані з будь-якими матеріальними чи віртуальними засобами або групами засобів, що використовуються для зберігання, сортування, організації, отримання, обробки, розробки та обміну інформацією відповідно до команд та інструкцій [8].

3. Угода про співробітництво держав-членів Співдружності Незалежних Держав у боротьбі із злочинністю в сфері комп'ютерної інформації від 01.06.2001 р. визначає «злочин в сфері комп'ютерної інформації» (преступление в сфере компьютерной информации), як кримінально каране діяння, предметом посягання якого є комп'ютерна інформація, а саме така інформація, що знаходиться в пам'яті комп'ютера, на машинних чи інших носіях у формі, доступній сприйняттю ЕОМ (електронно-обчислювальна машина) чи передається по каналах зв'язку [9].

4. Угода про співробітництво в сфері забезпечення міжнародної інформаційної безпеки Шанхайської організації співробітництва від 16.06.2009 р. (вступила в силу з 05.01.2012) містить термін «інформаційна злочинність», що тлумачиться як використання інформаційних ресурсів та (або) вплив на них в інформаційному просторі в протиправних цілях [10].

Дослідивши всі ці регіональні акти, можна дійти до висновку, що в усіх перелічених міжнародно-правових актах існують положення, направленні на забезпечення боротьби з кіберзлочинністю та іншою суспільно-небезпечною діяльності в інформаційній сфері.

1.2. Проблема протидії кіберзлочинам у міжнародній практиці

Перший відомий випадок кіберзлочину був здійсненний у СРСР. Він був зареєстрований у Вільнюсі у 1979 році. Це був перший злочин, зроблений за допомогою комп'ютера. І це викрадення інформації становило збитків на 78 584 карбованців. Цей випадок був занесений у міжнародний реєстр подібних злочинів і став перший у своєму роді, можна сказати, що він поклав початок новим правопорушенням у колишньому СРСР [11, с .271].

Сьогодні у багатьох зарубіжних країнах налагоджена система співробітництва, яка виникла на необхідності обміну досвідом на міжнародному рівні. Ці питання контролюються кожною країною відповідно до розробленої та діючої стратегії кібербезпеки: США та більшість країн-учасниць ЄС у своїх стратегіях виносять питання боротьби з кіберзлочинністю на передові позиції. Саме США стала першою країною, яка прийняла відповідний закон та створила Національну стратегію безпеки в кіберпросторі. Причиною створення даного документу стала терористична атака 11 вересня 2001 року. [12,с.55].

На державному рівні в США проводиться виважена політика щодо боротьби з кіберзлочинністю, що дозволяє залучати до співпраці урядові організації та зацікавлених осіб, таким чином об'єднуючи їх зусилля. Щодо кримінального законодавства США у сфері кіберзлочинності, то воно включає в себе Закон «Про боротьбу зі спамом» (ControllingtheAssaultofNon-solicitedPornographyandMarketing, 2003);

Закон «Про злочини, пов’язані з засобами доступу» (Fraudandrelatedactivityinconnectionwithaccessdevices); Закон «Про злочини, пов’язані з комп’ютерами»(Fraudandrelatedactivityinconnectionwithcomputers); Закон «Про злочини, пов’язані з електронною поштою» (Fraudandrelatedactivityinconnectionwithelectronicmail) [13].

Кіберзлочини можна поділити на три категорії: злочини проти інтелектуальної власності; злочини, що завдають шкоди комп’ютерному обладнанню; злочини проти користувачів комп'ютерної мережі. [14].

Наряду з США активну боротьбу з кіберзлочинністю проводять в країнах Європейського Союзу. В ЄС створений необхідний нормативно-правовий фундамент з питань захисту кіберпростору. Стратегія кібербезпеки ЄС була прийнята в 2013 році. Її особливістю є те, що стратегією були охоплені різні аспекти кіберпростору, зокрема, внутрішній ринок, правосуддя, внутрішня та зовнішня політика. Разом із Стратегією була розроблена та прийнята законодавча пропозиція про посилення безпеки інформаційних систем ЄС. Пріоритетами міжнародної політики ЄС у кіберпросторі, як їх визначає Стратегія, є:

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

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

– розвиток потенціалу кібербезпеки через співробітництво з міжнародними партнерами та організаціями, приватним сектором та громадянським суспільством [15].

На сьогоднішній день країни-учасниці ЄС намагаються зробити так, щоб інформаційні системи були здатні протистояти подіям в кіберпросторі, які можуть негативно вплинути на доступність, цілісність і конфіденційність інформації. [16].

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

В країнах ЄС активно створюються спеціальні органи боротьби з кіберзлочинністю. Ці органи можна поділити на дві групи. Першу групу складають органи, що займаються формуванням та реалізацією національної політики по боротьбі з кіберзлочинністю. Другу групу складають органи, що здійснюють запобігання та розслідування злочинів, що вчиняються в кіберпросторі. Формування національної політики щодо забезпечення кібербезпеки здійснюють органи загальної компетенції або ж спеціально створені органи. Так, органами загальної компетенції є Комітет з питань безпеки Фінляндії, Центр захисту національної інфраструктури Великобританії, Управління національної безпеки Чехії, Національне управління з питань безпеки та контртероризму, Міністерство адміністрації та впровадження цифрових технологій Польщі.

Одним із найбільш великим ризиком інформаційної безпеки Франції відносять кібертероризм, тому що бачуть в цьому пряму терористичну погрозу. Французька влада вважає,що терористи поширюють інформацію через ЗМІ, які детально висвітлюють теракти, ситуації із захопленням заручників, реагування влади на заяви терористичних угруповань і таким чином посилюють негативний інформаційний простір, який вигідний терористам, що фактично збільшує присутність терористичних груп в інформаційному середовищі країни. [18].

Наразі одним із найважливіших питань забезпечення інформаційної безпеки ФРН стала боротьба з дезінформацією та спростування недостовірних даних, що загрожують суспільству на різних рівнях: внутрішньому і зовнішньомудіяльності держави. Проблемою є пропагандистські впливи Росії у ФРН, що свідчать про наявність численних мереж проросійської пропаганди в європейських країнах.У тижневику DerSpiegel (жовтень, 2014 р.) було опубліковано матеріал про «кремлівську пропаганду». Особи, які підконтрольні Кремлю,створили у ФРН мережу промосковських експертів, щоб переконати німецьке суспільство у тому, що «Німеччина підтримує Росію» в російсько-українському конфлікті. На думку аналітиків, саме ФРН є пріоритетним об’єктом російської пропаганди в Європі, оскільки наявність понад чотирьох мільйонів російськомовних мешканців країни надає РФ можливість здійснювати потужний вплив на їхню мотивацію щодо політичних і виборчих процесів в крані.

Інструментом російської пропаганди в Німеччині вважається телеканал RussiaToday з річним бюджетом в 350 млн.дол. в той час, коли фінансування російської служби «Голос Америки» на рік становить лише 13 млн доларів. Саме за підтримки «Газпрому» і «Россотрудничества» у ФРН здійснюються деструктивні

пропагандистські кампанії, в яких для маніпуляцій використовуються суперечності між політичними партіями та різними групами, інтереси яких також беруть до уваги.Дієвим інструментом протидії російській пропаганді у ФРН і викриття дезінформації, зазначають дослідники, можуть стати якісні медіа для російськомовної меншини Німеччини. Така політика інформаційної безпеки, на думку експертів, є винятково важливою для ефективної боротьби зі шкідливим інформаційним ресурсом [19].

Варто зазначити, що Європейська Комісія ЄС підписала угоду (Agreementwithindustryoncybersecurityandstepsupeffortstotacklecyber-threats 2016) та план дій в галузі кібербезпеки для інтенсифікації зусиль, спрямованих на боротьбу з кіберзагрозами у форматі державно-приватного партнерства. Також важливо підкреслити, що першу стратегію кібербезпеки «Національний план захисту інформаційної інфраструктури» у форматі співпраці з агентством ENISA було ухвалено урядом ФРН.

У цій стратегії зазначалося, що забезпечення відкритості кіберпростору, а також цілісності, достовірності та конфіденційності інформаційних ресурсів в мережевому середовищі стало одним з важливих пріоритетів німецької держави як на національному, так і на міжнародному рівні. Стратегія інформаційної безпеки Великої Британії у рамках співпраці з агентством ENISA забезпечує розвиток кібербезпеки як механізму впровадження інновацій, залучення інвестицій та поліпшення якості сервісів у сфері інформаційно-телекомунікаційних технологій, запобігання ризикам кібератак злочинних і терористичних угруповань.

Можна зазначити, що європейські стандарти інформаційної безпеки підтримуються всіма країнами-членами ЄС, що свідчить про спільні підходи до критеріїв оцінки інформаційних загроз, однак їх

диференціація у провідних європейських країнах є відмінною залежно від пріоритетів національної безпекової політики.Так, стратегії інформаційної безпеки Великої Британії враховують як міжнародні, так і національні інтереси держави щодо формування комплексної системи захисту від сучасних інформаційних і кіберзагроз, оскільки у програмному документі «Стратегія національної безпеки» (2011 р.) зазначається, що серед низки критичних для безпеки держави викликів виокремлюються кіберзагрози та антитерористичні заходи. [20, с.88-90].

РОЗДІЛ 2

ДОСВІД УКРАЇНИ В СФЕРІПРОТИДІЇ КІБЕРЗЛОЧИНАМ

2.1.Співпраця України та Європейського Союзу в Інтернет сфері

Вектор на євроінтеграцію, який вибрала Україна, закріплений в Угоді про асоціацію між Україною та Європейським Союзом 2014 року. Цей напрям є стратегічним орієнтиром у відносинах між нашою державою та Союзом європейських держав. Він став незмінним зовнішньополітичним пріоритетом нашої держави.

Кібератаки, які завдають іноді незворотньої шкоди, є проблемою не тільки для України, а і для Європейського Союзу разом з його державами-членами. Тому було вирішено зробити розбудову державних структур, які б відповідали за безпеку в кіберпросторі, поглиблення партнерства між державами та організаціями приватного характеру, які мають розуміння і бажання допомогти у вирішенні проблеми. Найголовніше, що було вирішено зробити-це удосконалення правових основ протидії «хакерським» атакам. Прикладом цьому може слугувати дворівневе правове регулювання і відповідне управління на рівні ЄС та її держав-членів.

Політична дискусія щодо змісту спільної інформаційної політики ЄС розглядається як необхідна умова, що призведе до розбудови ефективного інформаційного суспільства. Ця дискусія характеризується різноманіттям підходів, базується на політиці неоліберального консенсусу. Втілені в документах ЄС нормативно–правові засади забезпечення інформаційної політики та дискусії з приводу їх доцільності виступають особливим предметним виміром, який дозволяє визначити проблемні аспекти в розбудові інформаційного суспільства на теренах ЄС [21, с.418].З 1990-х років, після проголошення державної

незалежності в Україні, розпочалося активне формування національного інформаційного законодавства. За цей час прийнято значну кількість законів та інших нормативно-правових актів, що дозволило врегулювати найбільш важливі норми інформаційних відносин та інформаційної діяльності.

Нині інформаційні відносини в Україні регулюються низкою нормативних актів, зокрема: Конституцією України, законами України “Про інформацію”, “Про мови”, “Про науково-технічну інформацію”, “Про телебачення і радіомовлення”,“Про інформаційніагентства”, “Про зв’язок”, “Про національну програму інформатизації”, “Про концепцію національної програми інформатизації”, “Про захист персональних даних”, “Про авторське право і суміжні права”, “Про державну таємницю” тощо. Знаковим з погляду права є Указ Президента України від 30 вересня 2010 року № 926/2010, яким проголошено 2011 рік в Україні Роком освіти та інформаційного суспільства, а також визначено потребу подальшого розвитку інформаційної сфери суспільства і держави [22,с.11].

Відносини між Україною та ЄС розпочалися одразу після проголошення нашою державою своєї незалежності. Саме в тому, доленосному для нашої країни 1991 р. 2 грудня було підписано Декларацію Європейського Союзу щодо України. В ній було позитивно відмічений Всеукраїнський референдум, його демократичний характер та було запропоновано співпрацю, ведення конструктивного діалогу з ЄС. Це було початком наших взаємовідносин, у процесі яких Україна могла стати однією з країн-учасниць. Але найголовнішим і найвагомішим документом між нашою країною та Європейським Союзом є звичайно Угода про асоціацію між Україною та ЄС, яка була підписана 27 червня 2014 року.

Згідно зі ст. 22 «Боротьба зі злочинністю та корупцією» Угоди про асоціацію сторони домовилися про співпрацю у боротьбі з кримінальною і незаконною організованою діяльністю та з метою її попередження. Серед основних видів незаконної організованої діяльності особливу увагу приділяють питанню протидії кіберзлочинності [23].

Для підвищення ефективності кримінальних розслідувань і переслідувань, що стосуються кримінальних правопорушень, пов'язаних з комп'ютерними системами і даними, і для надання можливості збирання доказів, що стосуються кримінального злочину в електронній формі,23 листопада 2001 було прийнято Конвенцію про кіберзлочинність [24]. Україна ратифікувала цей міжнародний документ 7 вересня 2005 року. Ратифікувавши Конвенцію,Україна визнала, те що формування спільної кримінальної політики, яка створена задля захисту суспільства від кіберзлочинів, є необхідною потребою для всіх країн, а також зобов'язалась привести своє законодавство в той стан, що не буде суперечити Конвенції. Це стало ще одним кроком на шляху євроінтеграції України.

Фактично всі перетворення українського законодавства були пов'язані з внесенням змін до двох кодексів – Кримінального кодексу України і Кримінального процесуального кодексу України.

У науковій праці Ю.Ю. Орлова «Реалізація вимог Міжнародної конвенції про кіберзлочинність у законодавстві України» проводиться ґрунтовне дослідження проведених змін в українському законодавстві. Провівши паралелі між положеннями Конвенції і Кримінального кодексу України, можна зробити висновок, що за більшість злочинів, зазначених у Конвенції, у нашій країні передбачено кримінальну відповідальність. Так, статтям 2–10 Конвенції про кіберзлочинність

відповідає низка відповідних статей Кримінального кодексу України[25, с.218].

У травні 2007 році Європейською Комісією представлено документ «На шляху до загальної політики в сфері боротьби з кіберзлочинністю», в якому «кіберзлочинність» визначається як кримінальні дії, скоєні з використанням електронних комунікаційних мереж та інформаційних систем або проти таких мереж та систем.

Політика Європейської Комісії в сфері боротьби з кіберзлочинністю реалізується за чотирма основними напрямами.

По-перше, це законотворчий процес. Найбільш важливим законодавчим рішенням є Рамкове рішення Ради Міністрів ЄС щодо атак на інформаційні системи від 17 січня 2005 року. Рамкове рішення покликане забезпечити мінімальний рівень зближення кримінального права для найбільш поширених форм кримінальної діяльності відносно інформаційних систем, таких як незаконний доступ, незаконне втручання у систему та дані. По-друге, Європейська Комісія заохочує транскордонне співробітництво правоохоронних органів країн-членів ЄС шляхом організації конференцій, створення цілодобових контактних пунктів у країнах-членах ЄС, розвитку платформи для навчання експертів у сфері боротьби з кіберзлочинністю. По-третє, Європейська Комісія розвиває співробітництво між державним і приватним секторами у боротьбі з кіберзлочинністю, зокрема, співпрацю між правоохоронними органами та приватними компаніями. По-четверте, Європейська Комісія заохочує підписання країнами-членами та іншими країнами Конвенції про кіберзлочинність, розробленої Радою Європи, та бере участь у міжнародних робочих групах.

В умовах сьогодення, а точніше в умовах гібридної війни, яку веде сусідня до нас держава, державні діячі зрозуміли, що є інформаційна

загроза, що може бути завдана за допомогою різноманітних кібератак. Так і сталося 23 грудня 2015 року. Хакери здійснили потужну атаку на енергетичну сферу Прикарпаття, постраждали щонайменше 6 постачальних енергокомпаній.

Рішенням Ради національної безпеки і оборони України від 28 квітня 2014 року «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України» з метою попередження та нейтралізації потенційних і реальних загроз національній безпеці в інформаційній сфері було вирішено розробити і затвердити низку нормативно-правових актів. Зокрема: Стратегію розвитку інформаційного простору України; проект нової редакції Доктрини інформаційної безпеки України; Стратегію кібернетичної безпеки України; проект Закону України про кібернетичну безпеку України; законопроекти про внесення змін до законів України «Про основи національної безпеки України», «Про інформацію», «Про захист інформації в інформаційнотелекомунікаційних системах», «Про Службу безпеки України», «Про Державну службу спеціального зв'язку та захисту інформації України» для приведення національного законодавства у відповідність із міжнародними стандартами з питань інформаційної та кібернетичної безпеки, вдосконалення системи формування та реалізації державної політики у сфері інформаційної безпеки України [26].

Також про важливість забезпечення кібербезпеки нашої держави і необхідність боротьби з кіберзлочинністю йдеться у Стратегії національної безпеки України, де серед актуальних загроз національній безпеці України – загрози кібербезпеці і безпеці інформаційних ресурсів. Дана Стратегія спрямована на реалізацію до 2020 року визначених нею пріоритетів державної політики національної безпеки, а також реформ, передбачених Угодою про асоціацію між Україною та ЄС і Стратегією

сталого розвитку «Україна–2020», схваленою Указом Президента України від 12 січня 2015 року № 5.

У Плані дій для України на 2015–2017 роки європейські партнери оцінили проведену роботу України на шляху інтеграції до Європейської спільноти, зокрема і в сфері кіберзлочинності. За підсумками проведеного аналізу ситуації встановлено, що деякі проблеми залишилися невирішеними. Насамперед це ті, що пов'язані зі співпрацею проти кіберзлочинності. Крім того, потребує завершення законодавчих реформ стосовно кіберзлочинності (процесуальне законодавство та пов'язані з цим гарантії), закінчення розробки навчальних стратегій щодо кіберзлочинності у сфері судочинства та надання підтримки реалізації проекту стратегії кібербезпеки [27,с.219].

2.2.Нормативно-правові засади боротьби з кіберзлочинами в Україні

У зв'язку з розвитком інформаційних технологій перед державою стоять завдання, що стосуються правового регулювання цих процесів.

У 2005 р. Україна ратифікувала Конвенцію про кіберзлочинність і таким чином імплементувала положення міжнародного акта у вітчизняне законодавство.

В січні 2016 року Радою національної безпеки та оборони України було прийнято за основу Стратегію кібербезпеки України з урахуванням викликів, які стоять перед нашою державою: агресивних дій Російської Федерації, посилення тенденцій використання кіберпростору розвідувальними і спеціальними військовими структурами, терористами, криміналітетом [28].

Стратегія передбачає розвиток національної системи забезпечення захисту кіберпростору, своєчасного виявлення та нейтралізації кіберзагроз, а також запобігання їм з урахуванням досвіду та практики

країн НАТО і Євросоюзу. Метою стратегії є створення умов для безпечного функціонування кіберпростору, його використання в інтересах особистості, суспільства і держави. В документі підкреслюється, що поряд з перевагами сучасного цифрового світу і розвитком інформаційних технологій, вони можуть використовуватися для вчинення терористичних актів, у тому числі шляхом порушення штатних режимів роботи автоматизованих систем управління технологічними процесами на об'єктах інфраструктури.

Більше поширення одержує політично мотивована діяльність у кіберпросторі у вигляді атак на урядові і приватні сайти в мережі Інтернет. «Економічна, науково-технічна, інформаційна сфера, сфера державного управління, оборонно-промисловий і транспортний комплекси, інфраструктура електронних комунікацій, сектор безпеки і оборони України стають все більш уразливими для розвідувально-підривної діяльності іноземних спецслужб в кіберпросторі. Цьому сприяє широке, іноді домінуюче, присутність в інформаційній інфраструктурі України організацій, груп, осіб, які прямо або побічно пов'язані з Російською Федерацією», – йдеться в концепції [29].

Стратегія передбачає комплекс заходів, пріоритетів та напрямів забезпечення кібербезпеки України. Крім цього, Стратегія передбачає залучення експертного потенціалу наукових установ, професійних і громадських об'єднань до підготовки проектів концептуальних документів у цій сфері; підвищення цифрової грамотності громадян та культури безпеки поведінки в кіберпросторі; розвиток міжнародного співробітництва і підтримку міжнародних ініціатив у сфері кібербезпеки, в тому числі поглиблення співпраці України з ЄС і НАТО.

Відповідно до документу, основу національної системи кібербезпеки складуть Міністерство оборони, Державна служба

спеціального зв’язку та захисту інформації, СБУ, Національна поліція, НБУ, розвідувальні органи.

Президент України 8 червня 2016 року, підписав Указ «Про Національний координаційний центр кібербезпеки». Діяльність Центру дозволить забезпечити координацію суб’єктів національної безпеки і оборони України під час реалізації Стратегії кібербезпеки України, підвищити ефективність системи державного управління у формування та реалізації державної політики у сфері кібербезпеки. Підставою для розроблення зазначеного Положення є Указ Президента України від 15 березня 2016 року № 96, яким введено в дію рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» і затверджена Стратегія кібербезпеки України. Національний координаційний центр кібербезпеки є робочим органом РНБО.

Стрімкий розвиток технологій Інтернету зумовлює появу та розвиток нових видів кіберзлочинів, які тягнуть за собою серйозні та незворотні наслідки. Величезний технічний потенціал та безмежні можливості у віртуальному просторі все частіше використовуються кіберзлочинцями для шахрайства, тероризму та для реалізації політичної мети. Тому так важливо на сучасному етапі встановити систему національного кіберзахисту та співпрацювати з іншими державами, міжнародними організаціями у цій сфері. Питань правового регулювання відносин у сфері кібербезпеки торкалися у своїх дослідженнях вітчизняні та закордонні автори. Водночас із 2016 року правове регулювання цих відносин зазнало змін. З огляду на це дослідження правового регулювання відносин у сфері кібербезпеки є актуальним та теоретично і практично вчасним.Збільшення оцифрування послуг та активне використання Інтернету призвело до еволюції кіберпростору, що також викликало значні проблеми для

безпеки урядів у всьому світі щодо злочинів, вчинених за допомогою комп'ютерних систем.

В Україні це було продемонстровано кібератаками на енергетичні компанії у грудні 2015 р., нападами на основні українські телеканали в день місцевих виборів у 2017 р. 27 червня 2017 року сталась масштабна хакерська атака хробаком-винищувачем NotPetya, яка вразила майже 80% підприємств в Україні, а також перекинулась на підприємства за кордоном нашої держави. Зловмисники викрадали інформацію з підприємств та відкривали доступ до їх комп'ютерних мереж.

У відповідь на масштабні кібератаки останніх років в Україні було прийнято Національну стратегію кібербезпеки. Створення Національного координаційного центру з кібербезпеки та оновлення законодавства в галузі кіберзлочинності відповідно до вимог Будапештської конвенції є двома основними кроками у підвищенні кіберстійкості країни. Ці заходи супроводжуються налагодженням співпраці з міжнародними партнерами в кіберсфері з питань кіберзлочинності та кіберзахисту [30, с.379-380].

ВИСНОВКИ

Відповідно до завданьдослідженняз'ясовано, що сьогодні на ряду з побутовими сферами життя у сучасному суспільстві все більше починають слідкувати за розвитком інноваційних технологій, пов'язаних з мережею Інтернет. Якісніше стають інформаційні технології: новітні засоби захисту, сучасні програми для забезпечення спокійного перебування в мережі Інтернет, сучасні шифри, професійніше стають і злочинці.

Єдиного поняття «кіберзлочин» в науковій літературі немає. Використовують різні поняття: незаконний доступ, комп'ютерні злочини. Згідно з Конвенцією про кіберзлочинність, яку Україна ратифікувала у 2005 році, вказано, що кіберзлочинність - це незаконне перехоплення конференційних даних, шахрайство, пов'язане з комп'ютерами, втручання у данні, правопорушення, пов'язані з дитячою порнографією.

Отже, можна зазначити, що таке кіберзлочинність на міжнародній арені. Кіберзлочинність-це шахрайство, несанкціонований доступ до персональних даних користувачів Інтернету, розміщення протиправного контенту на його просторах, що має на меті пропагування різного роду злочинних дії, як-то екстремізм, тероризм, расизм.

Міжнародне співтовариство багато разів висловлювала своє невдоволення, а часом і своє занепокоєння, що новітні зміни у інформаційних технологіях, цифрових винаходах можуть змінити не тільки суспільство загалом, зробити більш комфортним життя людей, а й ще те, що ці зміни можуть погано вплинути на забезпечення світового спокою та безпеки, можуть негативно вплинути на побудову та розвиток цілих держав.

У сфері комунікаційних технологій дуже важлива Женевська декларація принципів «Побудова інформаційного суспільства: глобальна задача у новому тисячолітті», яка підкреслює важливість інформаційного збагачення, його серйозний вплив на практично всі сфери нашого життя. В процесі цього не потрібно забувати і про приватне життя людини, захист особистих даних. ООН висловила підтримку у дотриманні кібербезпеки та висловила необхідність використовувати інформаційні ресурси тільки у мирних цілях, пам'ятаючи при цьому про права людини та дотриманню їх, запобіганню використовування ресурсів у злочинних, терористичних діях. Після Женевської декларації з'явився Женевський план дій «Зміцнення довіри і безпеки при використанні ІКТ», який розвинув ідеї та положення принципів попередниці. Він зобов'язав державні органи попереджати, виявляти і реагувати на прояви кіберзлочинності і зловживання ІКТ шляхом розробки керівних принципів, які враховують неперервні зусилля у цій сфері; розробку законодавства, що дає змогу ефективно розслідувати і переслідувати зловживання; сприяння ефективним зусиллям взаємодопомоги.

Необхідність розвитку та стимулювання культури кібербезпеки, впровадження її глобальної культури, а також кримінального переслідування кіберзлочинності визначила Туніська програма для інформаційного суспільства, була прийнята у 2005 році, яка була другим етапом у проведенні Всесвітнього саміту з питань інформаційного суспільства, де у 2003 році було прийнято чотири документи, зокрема відомий Женевський план. Також у рамках боротьби з кіберзлочинністю було прийнято ряд наступних міжнародних документів: конвенція Ради Європи про кіберзлочинність, конвенція про боротьбу із злочинами у сфері інформаційних технологій Ліги арабських держав, угода про співробітництво держав-членів Співдружності Незалежних Держав у

боротьбі із злочинністю в сфері комп'ютерної інформації, угода про співробітництво в сфері забезпечення міжнародної інформаційної безпеки Шанхайської організації співробітництва.

Відносини між Україною та ЄС розпочалися одразу після проголошення нашою державою своєї незалежності. Саме 2 грудня 1991 року було підписано Декларацію Європейського Союзу щодо України. В ній було позитивно відмічений Всеукраїнський референдум, його демократичний характер та було запропоновано співпрацю, ведення конструктивного діалогу з ЄС. Це було початком наших взаємовідносин, у процесі яких Україна могла стати однією з країн-учасниць. Але найголовнішим і найвагомішим документом між нашою країною та Європейським Союзом є Угода про асоціацію між Україною та ЄС, яка була підписана 27 червня 2014 року.

Для підвищення ефективності кримінальних розслідувань і переслідувань, що стосуються кримінальних правопорушень, пов'язаних з комп'ютерними системами і даними, і для надання можливості збирання доказів, що стосуються кримінального злочину в електронній формі, 23 листопада 2001 було прийнято Конвенцію про кіберзлочинність. Україна ратифікувала цей міжнародний документ 7 вересня 2005 року. Ратифікувавши Конвенцію, Україна визнала, те що формування спільної кримінальної політики, яка створена задля захисту суспільства від кіберзлочинів, є необхідною потребою для всіх країн, а також зобов'язалась привести своє законодавство в той стан, що не буде суперечити Конвенції. Це стало ще одним кроком на шляху євроінтеграції України.

Також про важливість забезпечення кібербезпеки нашої держави і необхідність боротьби з кіберзлочинністю йдеться у Стратегії національної безпеки України, де серед актуальних загроз національній

безпеці України – загрози кібербезпеці і безпеці інформаційних ресурсів. Дана Стратегія спрямована на реалізацію до 2020 року визначених нею пріоритетів державної політики національної безпеки, а також реформ, передбачених Угодою про асоціацію між Україною та ЄС і Стратегією сталого розвитку «Україна–2020», схваленою Указом Президента України від 12 січня 2015 року № 5. У 2005 р. Україна ратифікувала Конвенцію про кіберзлочинність і таким чином імплементувала положення міжнародного акта у вітчизняне законодавство. Зокрема, Конвенцією пропонується розмежування кіберзлочинів залежно від об'єкта правовідносин.

У Плані дій для України на 2015–2017 роки європейські партнери оцінили проведену роботу України на шляху інтеграції до Європейської спільноти, зокрема і в сфері кіберзлочинності. За підсумками проведено аналізу ситуації встановлено, що деякі проблеми залишилися невирішеними. Насамперед це ті, що пов'язані зі співпрацею проти кіберзлочинності. Крім того, потребує завершення законодавчих реформ стосовно кіберзлочинності (процесуальне законодавство та пов'язані з цим гарантії), закінчення розробки навчальних стратегій щодо кіберзлочинності у сфері судочинства та надання підтримки реалізації проекту стратегії кібербезпеки.

Президент України 8 червня 2016 року, підписав Указ «Про Національний координаційний центр кібербезпеки». Діяльність Центру дозволить забезпечити координацію суб'єктів національної безпеки і оборони України під час реалізації Стратегії кібербезпеки України, підвищити ефективність системи державного управління у формування та реалізації державної політики у сфері кібербезпеки. Підставою для розроблення зазначеного Положення є Указ Президента України від 15 березня 2016 року № 96, яким введено в дію рішення Ради національної

безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» і затверджена Стратегія кібербезпеки України.

Список використаних джерел

1.Довгань О.Д. Національний інформаційний суверенітет – об'єкт інформаційної безпеки. «*Інфомація і право»*. 2014 №3(12)/2014 С.112.

2.Горова С.М. Сучасний національний інформаційний суверенітет і особливості його забезпечення в умовах глобалізації. *Збірнк матеріалів науково-практичної конференції*. 2013. С.416.

3.Резолюция ГА ООН №66/24 «Достижения в сфере информатизации и коммуникаций в контексте международной безопастности» от 13.12.2011 р.URL:https://www.un.org/ga/search/view_doc.asp?symbol=A/RES/66/24&referer=/english/&Lang=R (дата звернення 02.12.2020).

4.Декларация принципов «Постороение информационного общества – глобальная задача в новом тысячителитии» от 12.12.2003.URL:https://zakon.rada.gov.ua/laws/show/995_c57#Text (дата звернення 02.12.2020).

5.Національна комісія, що здійснює державне регулювання у сфері зв'язку та інформації.URL:https://nkrzi.gov.ua/index.php?r=site/index&pg=6&language=uk (дата звернення 02.12.2020)

6.Підсумкові документи Всесвітнього саміту з питань інформаційного суспільства.URL::http://comin.kmu.gov.ua/control/uk/publish/printable_article?art_id=61592(дата звернення 02.12.2020).

7.Конвенція Ради Європи про кіберзлочин.URL:https://zakon.rada.gov.ua/laws/show/994_575#Text(дата звернення 02.12.2020).

8.ArabConventiononCombatingInformationTechnology Offences URL: https://www.asianlaws.org/gcld/cyberlawdb/GCC/Arab%20Convention%20on%20Combating%20Information%20Technology%20Offences.pdf(дата звернення 02.12.2020).

9.Соглашение о сотрудничестве в формировании информационных ресурсов и систем, реализации межгосударственных программ государств-участников Содружества Независимых Государств в сфере информатизации.URL:https://zakon.rada.gov.ua/laws/show/997_842#T(дата звернення 03.12.2020)

10. Соглашение между правительствами государств-членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопастности.URL:http://docs.cntd.ru/document/902289626(дата звернення 03.12.2020).

11.Батурин Ю.М. «Проблемы компьютерного права.*Юридическая литература* М. 1991 С.272

12.Петровський О.М., Лівчук С.Ю.Проблеми боротьби з кіберзлочинністю: міжнародний досвід та українські реалії. *Молодий вчений* 2019 № 12.1 (76.1) С.59

13.Європейський інформаційно-дослідницький центр Законодавство та стратегії у сфері кібербезпеки країн Європейського Союзу США, Канади та іншихURL: http://euinfocenter.rada.gov.ua/uploads/documents/28982.pdf (дата звернення 03.12.2020).

14.United States Secret Service USSS URL:https://www.secretservice.gov/(дата звернення 04.12.2020).

15.EU International Cyberspace Policy URL: https://eeas.europa.eu/topics/eu-international-cyberspace-policy_en(дата звернення 04.12.2020).

16.ANSSI URL:https://www.ssi.gouv.fr/publication (дата звернення 05.12.2020).

17. Титаренко О.М. «Стратегія захисту національного кіберпростору: досвід Франції». URL:http://www.dridu.dp.ua/konf/konf_dridu/itis%20seminar%202015/pdf/22.pdf (дата звернення 05.12.2020).

18.Élections européennes:lute contre la propaganda mensongère.URL:https://blogs.mediapart.fr/patrick-cahez/blog/110419/elections-europeennes-lutte-contre-la-propagande-mensongere (дата звернення 05.12.2020).

19.Електронний новинний журнал Tagesschau URL:https://www.tagesschau.de/inland/neurechte-russland-101.html (дата звернення 06.12.2020).

20.Копійка М. В.Стратегічні ризики інформаційної безпеки європейських країн.*Міжнародні та політичні дослідження*.2019. Вип. 32 С.102

21.Міхейченко М. А. Спільна інформаційна політика: політична дискусія у країнах–членах ЄС. *Збірник наукових праць «Гілея*: науковий вісник».Випуск 93 С.422

22.Пилипчук В.Г., Брижко В.М. Проблеми становлення і розвитку інформаційного законодавства в контексті євроінтеграції України. навч. посіб. *Інформація і право.2011* № 1(1) с.19

23.Угода про асоціаціюміж Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-
членами, з іншої сторони.URL:https://zakon.rada.gov.ua/laws/show/984_011#Text(дата звернення 07.12.2020).

24.Конвенція про кіберзлочинність.URL:https://zakon.rada.gov.ua/laws/show/994_575#Text (дата звернення 08.12.2020).

25.Маркарян М. В. Стан і перспективи адаптації законодавства України до вимог ЄС у сфері кіберзлочинності М. В. Маркарян Правове регулювання економіки : зб. наук. пр. М-во освіти і науки України, ДВНЗ «Київ. нац. екон. ун-т ім. Вадима Гетьмана». Навч.-наук. ін-т «Юридич. ін-т» ; редкол.: А. М. Колодій (голов. ред.) та ін. 2017. №16. С.222

26.Рішення РНБО від 28 квітня 2014 року «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України».URL:https://zakon.rada.gov.ua/laws/show/449/2014#Text (дата звернення 08.12.2020).

27.Маркарян М. В. Стан і перспективи адаптації законодавства України до вимог ЄС у сфері кіберзлочинності. М. В. Маркарян Правове регулювання економіки : зб. наук. пр. М-во освіти і науки України, ДВНЗ «Київ. нац. екон. ун-т ім. Вадима Гетьмана». Навч.-наук. ін-т «Юридич. ін-т» ; редкол.: А. М. Колодій (голов. ред.) та ін. 2017. №16 с.222

28.Про рішення Ради національної безпеки і оборони України «Про Стратегію кібербезпеки України».Указ Президента України № 96/2016 від 27 січня 2016 року. URL:https://zakon.rada.gov.ua/laws/show/96/2016#Text (дата звернення 08.12.2020).

29.Про Національний координаційний центр кібербезпеки.Указ Президента України № 242/2016 від 07 червня 2016 року.URL:https://zakon.rada.gov.ua/laws/show/242/2016#Text(дата зверненя 08.12.2020).

30.Дешко Л. М. та Бонарєва К. Д., «Кібербезпека в Україні: Національна стратегія та міжнародне співробітництво», Порівняльно-аналітичне право. 2018. № 2. С.405.