УДК 351.86:007

ОСОБЛИВОСТІ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ У СУЧАСНОМУ СВІТІ: ОГЛЯД СУБ'ЄКТІВ ЗАПОБІГАННЯ КІБЕРЗЛОЧИННОСТІ

Таволжанський Олексій Володимирович,
кандидат юридичних наук, доцент кафедри кримінології та кримінально-виконавчого права Національного юридичного університету імені Ярослава Мудрого, вул. Пушкінська, 77, м. Харків, 61000, Україна, e-mail: qwerc@ukr.net

Мета. *Метою дослідження є здійснення аналізу інституцій, що займаються запобіганням кіберзлочинності у світі, визначено основні сфери забезпечення інформаційної безпеки провідних держав з урахуванням зростання кіберзагроз. Запропоновані форми покращення кібербезпеки України з метою врахування позитивного досвіду інших держав, за для забезпечення суверенітету держави в умовах активізації процесу геополітичного тиску, інформаційних війн та мілітаризації кіберпростору.* ***Методика.*** *Методика включає комплексний аналіз та узагальнення наявного теоретичного матеріалу із піднятої проблематики на основі якого зроблені висновки та рекомендації щодо розкриття сутності досліджуваних понять.* ***Результати.*** *На основі проаналізованого матеріалу та з урахуванням досвіду провідних суб'єктів запобігання кіберзлочинності, маємо на меті привернути увагу цієї проблеми теоретиками та сучасними законодавцями.* ***Наукова новизна.*** *У роботі проаналізовано дослідження і погляди теоретиків щодо поняття кіберзлочинності та суб'єктів її запобігання та охарактеризовано позитивні. Вперше згуртовано сукупність органів та інституцій, що займаються інформаційною безпекою на державному та міждержавному рівні.* ***Практична значимість.*** *Результати дослідження сприятимуть розумінню системи заходів і суб'єктів запобігання кіберзлочинності, які впливають на сучасне позитивне право України та імплементовані міжнородно-правові норми.*

Ключові слова: *інформаційна безпека, кіберзлочин, кіберзлочинність, кібербезпека, кіберпростір, інформаційне законодавство.*

A. V. Tavolzhansky
Candidate of Sciences (Law), associate professor of the Department of Criminology and Criminal-Executive Law of the National Law University named after Yaroslav the Wise, vul. Pushkinskaya, 77, Kharkov, 61000, Ukraine, e-mail: qwerc@ukr.net

FEATURES OF PROVIDING CYBER SECURITY IN THE MODERN WORLD: REVIEW OF SUBSTANCES OF CYBER-FRAUD PROTECTION

Purpos. *The purpose of the study is to carry out an analysis of the institutions involved in the prevention of cybercrime in the world, identified the main areas of information security of the leading powers, taking into account the growth of cyber threats. The proposed forms of improvement of cybersecurity of Ukraine in order to take into account the positive experience of other states, in order to ensure the state's sovereignty in the conditions of intensification of the process of geopolitical pressure, information wars and militarization of cyberspace.* ***Methodology.*** *The method involves a comprehensive analysis and synthesis of the available theoretical material from the raised issues on the basis of which the conclusions and recommendations for the disclosure of the essence of the concepts under study are made.* ***Results.*** *On the basis of the analyzed material and taking into account the experience of the leading actors in the prevention of cybercrime, we aim to draw the attention of this problem to the theorists and modern legislators. Scientific novelty. The paper analyzes the researches and views of theorists on the concept of cybercrime and its prevention agents and is characterized positively. For the first time, a body of institutions and institutions dealing with information security at the state and interstate level has been united.* ***Practical significance.*** *The results of the study will help to understand the system of measures and actors of the prevention of cybercrime, which affect the modern positive law of Ukraine and implemented humanitarian law.*

Key words: *information security, cybercrime, cybercrime, cyber security, cyberspace, information legislation.*

Постановка завдання. Сучасне суспільство інформаційних технологій засноване на повсякденному використанні кібернетики: комп'ютерів, телекомунікаційних мереж, інших гаджетів та засобів комунікації. Процеси глобалізації та впровадження інноваційних технологій, в

тому числі з використанням засобів комунікацій та автоматизації процесів у всіх без винятку сферах життєдіяльності, призвели разом з цим до нівелювання кордонів і переплетення національних економік і національних інфраструктур країн світу.

В Україні за останні декілька років прийнято ряд нормативних актів щодо боротьби з кіберзлочинністю, зокрема: Указ Президента України Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України" [14], Розпорядження Кабінету Міністрів України від 11 липня 2018 р. № 481-р Про затвердження плану заходів на 2018 рік з реалізації Стратегії кібербезпеки України [11] тощо. Така тенденція заслуговує позитивної оцінки, але напрацювання потребують значних організаційних, матеріальних, політичних зусиль і часу. Тому надзвичайно важливим є необхідність ознайомлення з досвідом країн, які працюють в зазначеному напрямку не перший рік. Зрозуміло, форми, засоби, принципи діяльності суб'єктів протидії кіберзлочинності можуть мати інше забарвлення але загальні риси можуть бути використані в сучасному державотворенні.

Аналіз останніх досліджень і публікацій. Однією з ключових ознак проблеми кіберзлочинності є її глобальність. Кібератаки зупиняють діяльність не тільки приватних структур, а й державних органів, жодна країна повністю не захищена від кіберзлочинів. Все частіше в якості ймовірних джерел кіберзагроз розглядаються не тільки хакерів або їх групи, але й окремі держави, терористичні, злочинні угруповання, тощо. Актуальність дослідження зумовлена й тим, що останнім часом, не лише в Україні, а й у світі за «попитом» змінюється структура злочинності: на думку деяких авторів «традиційну» транснаціональну злочинність (і як її під вид економічна комп'ютерна злочинність) поступово заміщує більш складна та інтелектуальна за своїм змістом кіберзлочинність.

Певне коло проблем, пов'язаних з дослідженням кіберзлочинності як явища, а також проблематики її запобігання знайшли відбиток у наукових працях зарубіжних і вітчизняних фахівців, зокрема Ю. Батуріна, П. Біленчука, В. Бутузов, А. Волеводз, М. Вертузаєва, В. Вехова, В. Голубева, В. Пивоварова, О. Снегірьова, Б. Романюка, В. Розовський, О. Ткачової, Т. Тропина, В. Цимбалюка та інших фахівців, які надають можливість сформувати основу наукового розуміння координації та співпраці суб'єктів запобігання кіберзлочинності, притаманних їй найбільш суттєвих і характерних ознак, визначити пріоритетні шляхи і напрями боротьби з цим негативним явищем.

Постановка завдання. За останні десятиліття питання боротьби з кіберзлочинністю стає не тільки відомим пересічному громадянину, а й нагально потребує обговорення в рамках не лише науковими та практичними ресурсами окремої держави, а і міжнародного співтовариства. Експерти відносять кіберзлочинність до відносно нового специфічного виду злочинності, хоча остання, безумовно пов'язана та має схожі, родові властивості з транснаціональною злочинністю. Визначення єдиної політики, принципів і методів запобігання кіберзлочинності, а також окреслення системи інституцій діяльність яких спрямована на боротьбу з кіберзлочинністю на національному і міждержавному рівні, – нагальна потреба сучасного суспільства за для досягнення цілей запобігання кіберзлочинності.

Виклад основного матеріалу дослідження. З прийняттям у 2017 році Закону України «Про основні засади забезпечення кібербезпеки України» [5] (далі - Закон). було вкрай необхідним, вироблення єдиного понятійного апарату, як першого кроку на шляху до правової боротьби з кіберзлочинністю. Але до визначення поняття кіберпростір, кіберзлочин, кіберзлочинності і кібербезпеки потрібно підходити ретельно не тільки тому, що в результаті неправильної законодавчого формулювання можна знівелювати всю раніше проведену роботу, у зв'язку з неможливістю застосувати норму на практиці. Враховуючи відмінні ознаки цього виду злочинності, законодавство про протидію та запобігання таких порушень норм права повинно прийматися в з врахуванням міжнародних норм та напрацювань. Заходи запобігання кіберзлочинності що закінчуються по лінії кордону країни будуть безрезультатними, без врахування досвіду інших держав, а також без міжнародного співробітництва, в сучасних умовах не представляється можливим досягнення кібербезпеки жодної навіть найрозвинутішої країни.

При розгляді питання про боротьбу з кіберзлочинами на міжнародному рівні слід виділити Конвенцію Ради Європи щодо кіберзлочинності [7] (далі - Конвенція), підписану в Будапешті в 2001 г. Вона стала серйозним кроком міжнародного співтовариства до запобігання кіберзлочинів. Хоча ряд не державних інституцій (зокрема: «Фонд Електронних Меж» (Electronic Frontier Foundation, США), міжнародна організація «Суспільство Інтернет» (Internet Society), «Організація кіберправа і кіберсвободи» (Cyber - Rights & CyberLiberties, Великобританія), «Кріптополіс» (Kriptopolis, Іспанія) виражали протест щодо підписання Конвенції, при цьому така вимога обґрунтовувалась наступним: Конвенція несе, на думку авторів протесту, собі загрозу для норм захисту особи, що встановилися, невиправдано розширює поліцейські функції уряду, а також знижує відповідальність держави в правоохоронній діяльності, окремі того може призвести до порушення принципів приватності.

Зробити дієвими чи навіть удосконалити реалізацію національних стратегічних підходів можливо лише спираючись на досвід продуктивної діяльності урядових і поза державних організацій інших країн, а також міждержавних інституцій та враховуючи їх зрушення у боротьбі з загрозами інформаційній безпеці. В сучасних умовах складно уявити захищену державу яка б не займалась власним секторами зовнішньої безпеки модифікуючи їх відповідно до викликів сучасності. Жодна війна, відкрита чи прихована, не відбувається без використання кіберзброї, потенціал використання мережі Інтернет, як кіберресурсу у військових цілях поза конкуренцією. Повсякденно в політиці провідних держав розроблюються новітні заходи протидії загрозам в кіберпросторі, здійснюється коригування внутрішньої інформаційної політики, а також вдосконалюються методи кібербезпеки.

Тлумачення понять «кібербезпека» в закордонних профільних документах стратегічного рівня (проаналізовані стратегії з кібернетичної безпеки Франції, Німеччини, Канади, Туреччини, Нідерландів, Австралії) дозволяє зробити висновок, що на рівні національних та міжнародних стратегічних документів визначення кібербезпеки значно різняться. А значить, розрізняються і підходи не тільки до змісту відповідних стратегій, а й до змісту планів дій із забезпечення кібербезпеки» [17, с. 67].

Вивчення проблем, пов’язаних з питаннями взаємодії спеціальних органів держав щодо запобігання кіберзлочинності та розробка сучасних механізмів протидії кіберзлочинності є одним з пріоритетних напрямків діяльності кожної держави. Безспірно, що кіберзлочинність пов'язана безпосереднім причинно-наслідковим зв'язком з процесами глобалізації інформаційних процесів і появи глобальних телекомунікаційних мереж. Ефективна боротьба з кіберзлочинністю вимагає не лише гармонізації кримінального законодавства на міжнародному рівні, а й систематизації і адаптації комплексу процедурних заходів для співпраці щодо запобігання кіберзлочинів. На сьогодні відсутні єдині міжнародні інструменти, щодо боротьби з кіберзлочинністю, які б застосовувались більшістю держав світу. Все частіше проводяться різного роду дослідження, що до рівня захищеності країн від посягань кіберзлочинності. Так зокрема, за результатами роботи групи експертів та після обробки результатів опитування, Security & Defence Agenda провела ранжування та встановила рейтинг по 5-бальній системі. При цьому була досліджена поточна готовність до кібератак інформаційних систем 23 країн. Стан готовності для окремих країн був продемонстрований на прикладі рейтингу McAfee, який там використовується у якості основного засобу боротьби з кіберзлочинами Найвищий результат, тобто 4,5 бали, було поставлено всього 3 країнам, які мають досить невелику площу: Швеції, Ізраїлю та Фінляндії. Ще 8 країн, включаючи США, Великобританію, Францію та Німеччину, отримали друге місце з 4 балами. Росія та Польща зайняли 4 місце з 3-бальним результатом. З тих даних звіту Security & Defence Agenda, неясно, чи були виставлені якісь бали для України [6, с. 60]. Вважаємо за необхідне звернути увагу на міжнародних суб’єктів запобігання кіберзлочинності та суб’єктів другої групу країн, з наведеного вище дослідження що мають досить велику за площею територію та відповідну кількість населення.

Визначити об'єкт нашого дослідження не можна не окресливши визначення центральних понять – кіберзлочину і кіберзлочинності. Цікавою думкою, щодо ознак кіберзлочину видається підхід обраний Н. Міщук зокрема автор зазначає, що кіберзлочину, характерні наступні

особливості: − підвищена скритність вчинення злочину, що забезпечується специфікою мережевого інформаційного простору (розвинені механізми анонімності, складність інфраструктури тощо); - транскордонний характер мережевих злочинів, при якому злочинець, об'єкт злочинного посягання, потерпілий можуть перебувати на територіях різних держав; - особлива підготовленість злочинців, інтелектуальний характер злочинної діяльності; нестандартність, складність, різноманіття і часте оновлення способів скоєння злочинів і застосовуваних спеціальних засобів; - можливість вчинення злочину в автоматизованому режимі в декількох місцях одночасно, можливість об'єднувати відносно слабкі ресурси багатьох окремих комп'ютерів в потужне знаряддя вчинення злочину; - багатоепізодним характер злочинних дій при множинності потерпілих; - необізнаність потерпілих про те, що вони піддалися злочинному впливу; - дистанційний характер злочинних дій в умовах відсутності фізичного контакту злочинця і потерпілого; - неможливість запобігання та припинення злочинів даного виду традиційними засобами [10, с. 176].

Так, деякі науковці під кіберзлочином розуміють досконале суспільно небезпечне втручання в роботу комп'ютерів, комп'ютерних програм, комп'ютерних мереж, несанкціонована модифікація комп'ютерних даних, а також інші протиправні суспільно небезпечні діяння, які здійснюються за допомогою комп'ютерів, комп'ютерних мереж і програм, а також інших пристроїв доступу до модему за допомогою комп'ютера інформаційного простору, за скоєння чого передбачається кримінальна відповідальність згідно з чинним законодавством [8, 58]. За словником термінів з кібербезпеки кіберзлочин – протиправне втручання в роботу кібернетичних систем, основною управляючою ланкою яких є комп'ютер (наприклад, спотворення інформації про стан об'єкта в каналі зворотного зв'язку, спотворення керуючого сигналу й каналу зв'язку, використання шкідливого програмного забезпечення тощо), створення та використання в злочинних цілях певної кібернетичної (комп'ютерної) системи, використання в злочинних цілях існуючих кібернетичних (комп'ютерних) систем (наприклад комп'ютерних чи телекомунікаційних мереж у шахрайстві, вимаганні тощо) [13, с. 85]. Ще один розповсюджений підхід до визначення кіберзлочину передбачає що це передбачене кримінальним законом суспільно небезпечне винне діяння, що полягає в протиправному використанні інформаційних та комунікаційних технологій, відповідальність за яке встановлена законодавством про кримінальну відповідальність [2, с. 416]. М. Погорецький та В. Шеломенцев висловлюють іншу думку, розглядають кіберзлочини як злочини, вчинені в інформаційному середовищі, проти інформаційних ресурсів, тобто у сфері комп'ютерної інформації, або за допомогою інформаційних засобів. На думку останніх, терміни «інформаційне середовище», «інформаційні ресурси», «інформаційні засоби» є занадто загальними для сфери використання комп'ютерних систем і не розкривають суті процесів автоматизованої обробки інформації. Крім того, вчені вбачають загальною ознакою протиправних діянь, передбачених Конвенцією та Додатковим протоколом до неї, те, що їх вчинення на різних стадіях безпосередньо пов'язане з використанням ресурсів комп'ютерних систем (вчинення за допомогою комп'ютерних систем або через комп'ютерні системи), які, у свою чергу, є середовищем вчинення кіберзлочинів. Комп'ютерні дані при цьому, на їхню думку, слід розглядати як інформаційний ресурс комп'ютерних систем, а комп'ютерні мережі – як різновид комп'ютерних систем. Ґрунтуючись на цій позиції, кіберзлочини слід вважати такими, що вчиняються за допомогою або через комп'ютерні системи чи пов'язані саме з комп'ютерними системами, тобто із сукупністю пристроїв, із яких один чи більше відповідно до певної програми виконують автоматичну обробку даних [12, с. 90–91]. Під поняттям кіберзлочин Закон визначає, як суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України.

В свою чергу Законом наведено легальне поняття кіберзлочинності, як сукупності кіберзлочинів. Кіберзлочинністю прийнято вважати кримінально карані дії, що передбачають несанкціоноване проникнення в роботу комп'ютерних мереж, комп'ютерних систем та програм, з метою видозміни комп'ютерних даних. Досить цікавим є підхід щодо визначення ознак кіберзлочинності, за такими ознаками кіберзлочинності через: 1) кіберзлочини вчиняються у

віртуальному просторі або в межах комп'ютерних мереж. Віртуальний простір – це модульований за допомогою комп'ютера інформаційний простір, в якому містяться дані про осіб, факти, явища, процеси, представлені в математичному, символьному чи іншому вигляді. Ці відомості знаходяться в процесі руху локальними і глобальними комп'ютерними мережами, зберігаються в пам'яті будь-якого фізичного або віртуального пристроїв, спеціально призначених для їх зберігання, переробки та передачі. Крім того, кіберзлочини можуть вчинятися за допомогою комп'ютерних систем або шляхом використання комп'ютерних мереж та інших засобів доступу до віртуального простору, а також проти комп'ютерних систем, комп'ютерних мереж і комп'ютерних даних [12, с. 75]. Таким чином, електронно-обчислювана техніка може бути як засобом вчинення, так і предметом злочину [4, с. 332]; 2) кіберзлочинність має інтелектуальний характер – здійснення кіберзлочину вимагає певного набору знань, крім того інтелектуальність серед кіберзлочинців пропагується субкультурою хакерів, що дає їм стимул до розумового саморозвитку; 3) кіберзлочини, на відміну від інтелектуальних злочинів, доступні людям невисоких соціальних і вікових можливостей [12, с. 27].

Поняття суб'єктів запобігання кіберзлочинності є похідним від поняття суб'єктів запобігання злочинності. Найбільш обґрунтованим є наступне визначення суб'єктів запобігання злочинності – це державні органи, громадські організації, соціальні групи, службові особи чи громадяни, які спрямовують свою діяльність на розроблення і реалізацію заходів, пов'язаних з випередженням, обмеженням, усуненням криміногенних явищ та процесів, що породжують злочинність і злочини, а також на їх недопущення на різних злочинних стадіях, у зв'язку з чим мають права, обов'язки і несуть відповідальність [8, с. 47].

Інформаційної безпека складається з наступних елементів: діяльність іноземних політичних, військових, економічних та розвідувальних структур в інформаційній сфері; політика домінування деяких країн в інформаційній сфері; діяльність міжнародних терористичних груп; розробка концепцій інформаційних війн будь-якими структурами; культурна експансія у відношенні до конкретної країни [9, с. 24].

Суб'єкти протидії кіберзлочинності мають утворювати цілісну у функціональному і організаційному відношенні систему. В той же час зміст та глибина кіберсуперництва, включення в коло зацікавлених практично всіх ключових суб'єктів міжнародної політики обумовлює складнощі пошуку науково-методологічної форми для пояснення цього процесу та прогнозування його подальшого перебігу з напрацюванням практично корисних рекомендацій. Автор не ставить завданням визначення найдієвіших інституцій та систем протидії вчиненню кіберзлочинів, а лише окреслити сукупність існуючих суб'єктів запобігання кіберзлочинності.

Кібербезпека і шляхи досягнення кіберзахисту інформації входять до повноважень низки міжнародних інституцій, передусім спеціалізованих організацій ООН, зокрема ЮНЕСКО, МСЕ, Інтерпол та Європол, а також таких міждержавних організацій, зокрема:

1. Азійсько-Тихоокеанське економічне співробітництво (The Asia-Pacific Economic Cooperation),
2. Велика сімка (G7),
3. Організація економічного співробітництва та розвитку, (Organisation for Economic Cooperation and Developmet, OECD),
4. Шанхайська організація співробітництва, тощо.

Спроби врегулювання кібервідносин здійснює Міжнародний союз електрозв'язку (International Telecommunication Union, ITU). Зокрема на тепер затверджено ряд актів нормативного характеру врегульованих кіберпростір, та окреслення основних термінів, зокрема таких як: кібербезпека, загрози кібербезпеці та уразливості, систематизовані основні способи вчинення кіберзлочинів. Визначено заходи запобігання кіберзлочинності, приміром: з технічного захисту, втручання в роботу мереж і т.д.

В 2008 році був створений Спільний центр передового досвіду в галузі кібербезпеки НАТО (NATO Cooperative Cyber Defence Centre of Excellence, CCD CoE). Це акредитована НАТО міжнародна військова організація з метою розширення спільних можливостей кіберзахисту країн НАТО, що покращує взаємодію Альянсу в області спільного кіберзахисту. Центр був створений

сім країнами: Естонією, Німеччиною, Італією, Литвою, Латвією, Словацькою Республікою та Іспанією, що підписали Меморандум про взаєморозуміння 14 травня 2008 року.

У 2004 році європейським парламентом створено спеціальний підрозділ, що мав займатись інформаційною безпекою — Європейське агентство по мережевій і інформаційній безпеці (ENISA). Основне завдання – налагодження інформаційної безпеки на внутрішньому ринку. ENISA надавало консультативні послуги для країн Євросоюзу. Додатково ENISA займається налагодженням зв'язків між державним і не державним сектором у сфері інформаційної безпеки.

Окремо необхідно зупинитись на діяльності Європолу у боротьбі з кіберзлочинністю. 11 січня 2013 року у штаб-квартирі Європейського поліцейського офісу (м. Гаага, Нідерланди) офіційно відкрито Європейський Центр по боротьбі з кіберзлочинністю. Основними напрямками та завданнями Центру є: забезпечення координації та обміну інформацією між підрозділами правоохоронних органів Європейського Союзу та Третіми країнами; боротьба з розповсюдженням у мережі Інтернет дитячої порнографії; підготовка кваліфікованих експертів в галузі боротьби з кіберзлочинністю; розробка та застосування методів припинення злочинів у сфері інформаційних технологій. Також, Центр покликаний здійснювати захист стратегічно значущих Інтернет-ресурсів, комунікаційних систем та фінансових установ Європейського Союзу. В подальшому Європейський Центр по боротьбі з кіберзлочинністю буде співробітничати з Глобальним інноваційним комплексом Інтерполу в Сінгапурі [1, с. 37].

У 2016 року Європейським парламентом була прийнята Директиви з безпеки мережевих та інформаційних систем (Директива NIS – DIRECTIVE (EU) 2016/1148). Дослідження закріплене в Директиві NIS передбачає, що для підвищення загального рівня кібербезпеки в ЄС необхідно забезпечити: відповідний рівень готовності держав-членів, вимагаючи від них створення команди інцидентів Computer Security Response (CSIRT) і компетентного національного органу NIS; співпрацю між усіма державами-членами шляхом створення групи співпраці з метою надання підтримки і сприяння стратегічній співпраці та обміну інформацією між державами-членами; високий рівень безпеки в усіх секторах, які мають життєво важливе значення для економіки і суспільства та, до того ж, значною мірою залежать від інформаційно-комунікаційних технологій.

Що до окремих держав, то ще в 1978 році в США в штатах Флорида і Аризона був прийнятий закон «Computer crime act of 1978» [15]. Це був не просто перший закон, що встановлює кримінальну відповідальність за комп'ютерні злочини, це був перший сигнал про початок нової ери злочинів – кіберзлочинів. Ця ера знаменувала створення відповідних державних органів, що мали протидіяти кіберзлочинності.

У США створено систему органів щодо забезпечення кібербезпеки. Зокрема, до основних можна віднести Управління національної безпеки (Department of Homeland Security) при якому здійснює свою діяльність спеціальний кібербезпекововий департамент, – займається виключно безпекою високотехнологічних систем США.

Кіберкомандування (U.S. Cyber Command), що очолює підрозділи спеціального призначення, які мають на меті: ведення розвідувальної роботи в мережах, захисту власних мереж, блокування і "обвалу" структур супротивника із використанням можливостей кіберпростору

У Франції створено ряд державних інституцій та не урядових установ, що займаються запобіганням кіберзлочинності. Відомою є така структура як Національна комісія з обчислювальної техніки та свобод (CNIL). Ціль діяльності CNIL – захисті персональних даних. У цифровому світі CNIL є регулятором персональних даних. Підтримує фахівців в кіберпросторі в їх діяльності і допомагає людям контролювати свої особисті дані та здійснювати свої права. З 2004 року, має право накладення санкцій на підприємства, що порушують Закон про інформатику, картотеках і свободах 1978 року [19].

Окремим напрямком запобігання кіберзлочинності є діяльність так званого Верховного органу поширення творів і охорони прав в Інтернеті (HADOPI). Здійснена спроба визначити, що таке незаконне скачування інформації та регламентувати таку діяльність. Вищий конституційний суд країни схвалив другий варіант Закону про так звану триступеневу заборону доступу до мережі Інтернет [19].

У правоохоронній системі Франції також діють відповідні суб'єкт по боротьбі з кіберзлочинністю. Починаючи з 1998 року Національна жандармерія визначила пріоритетною діяльність щодо вирішення проблем, пов'язану з інноваційними технологіями, шляхом створення відповідних структур і навчальних закладів, зокрема:

1. Відділ кіберзлочинів технічного обслуговування судових досліджень та документації (STRJD). Він здійснює моніторинг Інтернет мережі шляхом пошуку злочинів проти людей та майна, пов'язаних із передачею нелегальних даних в Інтернеті (сайти, інтернет-ресурси, групи новин, мережі обміну, соціальні мережі тощо).
2. Комп'ютерний і електронний відділ Інституту кримінального розслідування Національної жандармерії (IRCGN). Він розробляє методи, засоби та програмне забезпечення для автоматичного виявлення педофілів тощо.
3. Відомчі бригади інформації та судових розслідувань (BDRIJ) тощо .

Наступним суб'єктом запобігання кіберзлочинності у Франції є Національне агентство безпеки інформаційних систем (ANSII), французьке агентство з кібербезпеки, яке працює з державними спецслужбами. Діяльність органу спрямована на реалізацію Французької національної стратегія цифрової безпеки, оголошеної 16 жовтня 2015 року. Ця стратегія, що впроваджується ANSSI, є результатом скоординованих міжвідомчих зусиль, спрямованих щодо реагування на виникаючі проблеми цифрового століття. Було задекларовано, що цифровий перехід сприяє не лише інноваціям та економічному зростанню, однак він одночасно несе ризики для держави, господарюючих суб'єктів та громадян. Кіберзлочинність, шпіонаж, пропаганда, саботаж та надмірне використання персональних даних загрожують цифровій довірі та безпеці. Визначено основні пріоритети в діяльності ANSSI: захист та безпека державних інформаційних систем та критично важливих інфраструктур, важливих операторів економіки та суспільства; цифрова довіра, конфіденційність, особисті дані, кібернасильство; підвищення обізнаності, початкове навчання, безперервна освіта; навколишнє середовище бізнесу цифрових технологій, промислова політика, експорт та інтернаціоналізація; цифрова стратегічна автономія, стійкість кіберпростору.

Існує Організація з регулювання мережевих ігор, Tracfin — служба Міністерства фінансів по боротьбі з відмиванням грошей, яка також сприяє, так як виявляє випадки відмивання грошей, число яких виросло в результаті використання мережі Інтернет для їх здійснення. Національна рада з цифровим технологіям, що складається з учасників приватного сектора, яким є що сказати для розробки права Інтернету. Це незалежні організації.

Доволі розповсюдженими сучасними заходами запобігання кіберзлочинності є проведення спільних навчань. В ході навчань виявляють недоліки, інфраструктури, формуються варіанти атак, інцидентів і пропонуються найбільш ефективні варіанти реагування та координації.

Cyber Europe Навчання передбачає симуляцію великих інцидентів з кібербезпеки, які загострюються, щоб стати кібернетичними кризами. Вправи пропонують можливості для аналізу передових технічних інцидентів кібербезпеки, а також для вирішення складних ситуацій безперервності бізнесу і кризових ситуацій. Навчання Cyber Europe показують сценарії, з урахуванням реальних подій, розробленими європейськими експертами з кібербезпеки [18].

Зокрема Cyber Storm (США) [2]. Учасники Cyber Storm виконують такі дії: вивчити можливості організацій з підготовки, захисту та реагування на потенційні ефекти кібер-атак; мають здійснювати стратегічне прийняття рішень і міжвідомчу координацію реагування на інциденти відповідно до політики та процедур національного рівня; підтвердження відносин обміну інформацією та шляхів комунікації для збору і поширення інформації про кіберситуації, відповідях і відновленні інформації про кібер-інциденти; а також вивчити засоби і процеси, за допомогою яких можна ділитися конфіденційною інформацією через кордони і сектора без шкоди для власних інтересів або інтересів національної безпеки.

У роботі проаналізовано дослідження і погляди теоретиків щодо поняття кіберзлочинності та суб'єктів її запобігання та охарактеризовано позитивні. Вперше згуртовано сукупність органів та інституцій, що займаються інформаційною безпекою на державному та міждержавному рівні.

Результати дослідження сприятимуть розумінню системи заходів і суб'єктів запобігання кіберзлочинності, які впливають на сучасне позитивне право України та імплементовані міжнородно-правові норми.

Висновки. Таким чином, жодна з класичних теорій та схем функціонування державних інституцій не дає повноцінної відповіді на питання як саме слід концептуалізувати наявні знання про кібербезпеку та про функціонал основних суб'єктів міжнародних відносин щодо неї. Кіберзлочинність є новим виміром людської діяльності, яка характеризується глобальністю та не обмеженістю кордонами держави.

У кіберзлочинність впливає на різноманітні верстви населення, для неї властива специфічна система внутрішнього контролю та протидії правоохоронним інституціям. Поширенню кіберзлочинності сприяють наступні чинники: процеси глобалізації світової економіки; гіперпопит на різні види інформаційних послуг у розвинутих країнах світу; розвиток сучасних інформаційних технологій, особливо Інтернет-ресурсів, що забезпечують майже неконтрольований процес формування спокус тощо.

Порівняльний аналіз досліджень передового зарубіжного досвіду боротьби з кіберзлочинністю свідчить, що вона має тенденцію до росту. Однією з умов її росту є ускладнення сучасних телекомунікаційних та технічних систем глобального зв'язку і спрощення доступу до використання комп'ютерних технологій широкого круга користувачів через персональні комп'ютери.

Виходячи з викладеного актуальним є питання узгодження дій між правоохоронними і іншими органами різних держав покликаних забезпечити стабільність кібер простору і кібербезпеку. Безспірною є потреба в діяльності спільних міжнародних підрозділів по розслідуванню кіберзлочиннів і вжиття заходів щодо кібербезпеки як окремих держав так і всього людства. Таким чином, удосконалення чинного законодавства через врахування зарубіжного досвіду дозволить не лише визначити межі кіберзлочинності в Україні та правильно кваліфікувати дії осіб, які причетні до скоєння кіберзлочинів, а й запобігти їх вчиненню у майбутньому.

Список використаних джерел

1. Алієв М.М., Куньо А.М. «Проблема кіберзлочинності та шляхи її подолання у сучасному інформаційному суспільстві». XI Міжнародна науково-технічна конференція «АВІА-2013» 21-23 травня 2013 р. К.: НАУ, 2013. Т.6. С. 35-38.
2. Бельський Ю. Щодо визначення поняття кіберзлочину. Юридичний вісник. 2014. № 6. С. 414–418.
3. Бойченко О. В. Міжнародне співробітництво правоохоронних органів держав у галузі забезпечення інформаційної безпеки. *Форум права*. 2009.- № 2. С 56-62.
4. Голіна В. В., Головкін Б. М. Кримінологія: Загальна та Особлива частини: навч. посіб. Харків: Право, 2014. 513 с.
5. Закон України "Про основні засади забезпечення кібербезпеки України" URL: http://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення 11.09.2018)
6. Казакова Н. Ф., Йона О. О. Світові тенденції боротьби з кіберзлочинністю. *Вісник Східноукраїнського національного університету імені Володимира Даля*. Луганськ: СНУ ім. В. Даля, 2013. №15 (204). Ч.1. С. 59-62.
7. Конвенція про кіберзлочинність від 23 листопада 2001 року URL: http://zakon.rada.gov.ua/laws/show/994_575 (дата звернення 11.09.2018)
8. Кримінологія: Загальна та Особлива частини: підручник/ В.В. Голіна, Б.М. Головкін, М.Ю. Валуйська, О.В. Лисодєд та ін..; за ред. В.В. Голіни і Б.М. Головкіна. Х.: Право, 2014. 512 с.
9. Малик Я. Й. Забезпечення інформаційної безпеки України у контексті світового досвіду / Я. Й. Малик, О. І. Береза. Ефективність державного управління. 2012. Вип. 32. С. 20-27.
10. Міщук Н.В. Кіберзлочинність як загроза інформаційному суспільству. *Вісник Львівського університету*. Серія економічна. Випуск 51. Львів, 2014. С.173-179.
11. Розпорядження Кабінету Міністрів України від 11 липня 2018 р. № 481-р Про затвердження плану заходів на 2018 рік з реалізації Стратегії кібербезпеки України URL:

http://zakon.rada.gov.ua/laws/show/96/2016 (дата звернення 11.09.2018)
12. Русецький А. А., Куцолабський Д. А. Теоретико-правовий аналіз понять "кіберзлочин" і "кіберзлочинність". *Право і Безпека*. 2017. № 1. С. 74-78.
13. Словник термінів з кібербезпеки / за заг. ред. О. В. Копана, Є. Д. Скулиша. К. : ВБ «Аванпост-Прим», 2012. 214 с.
14. Указ Президента України Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України" URL: http://zakon.rada.gov.ua/laws/show/96/2016 (дата звернення 11.08.2018)
15. Computer Crimes Act URL: http://www.clas.ufl.edu/docs/flcrimes/section2_1_1.html#SECTION00110000000000000000 (дата звернення 12.09.2018)
16. Cyber Storm: Securing Cyber Space URL: https://www.dhs.gov/cyber-storm. (дата звернення 13.09.2018).
17. Cybersecurity is a fascinating and highly scientific field spanning a range of disciplines and involving a wealth of organisations and actors, from both the public sector and the business world, within France and internationally. URL: http://www.ssi.gouv.fr/en/mission/word-from-director-general/ (дата звернення 11.09.2018)
18. Loi 78-17 du 6 janvier 1978 modifiée URL: https://www.cnil.fr/fr/loi-78-17-du-6-janvier-1978-modifiee (дата звернення 13.09.2018)
19. Loi favorisant la diffusion et la protection de la création sur Internet URL: http://www.senat.fr/dossier-legislatif/pjl07-405.html (дата звернення 13.09.2018)

References

1. Aliyev MM, Kunyo AM "The problem of cybercrime and ways to overcome it in the modern information society" // XI International scientific and technical conference "AVIA-2013" May 21-23, 2013. K .: NAU, 2013. T.6. P. 35-38.

2. Bel'skiy Yu. On definition of the notion of cybercrime. *Legal Bulletin*. 2014. No. 6. P. 414-418.

3. Boychenko, O. V. International cooperation of law enforcement authorities in the field of information security provision. *Forum of law*. 2009. No. 2. From 56-62.

4. Golina V.V., Golovin B.M. Criminology: General and Specialty: Teaching. manual Kharkiv: Right, 2014. 513 c.

5. The Law of Ukraine "On the Basic Principles of Cybersecurity of Ukraine" URL: http://zakon.rada.gov.ua/laws/show/2163-19 (reference date 11.09.2018)

6. Kazakova N.F., Jonah O.O. World trends in the fight against cybercrime. *Bulletin of East-Ukrainian National University named after Volodymyr Dahl*. Lugansk: SNU them. V. Dal, 2013. No. 15 (204). Ch.1. P. 59-62.

7. The Convention on Cybercrime of November 23, 2001 URL: http://zakon.rada.gov.ua/laws/show/994_575 (reference date 11.09.2018)

8. Criminology: General and Special Parts: Textbook / V.V Golina, B.M. Golovkin, M.Yu. Valuyska, O.V. Lisoded and others.; for ed. V.V Golina and B.M Golovkin. X.: Right, 2014. 512

9. Malik, Ya.I., Bereza O. I. Providing Ukraine's Information Security in the Context of Worldwide Experience. *Efficiency of Public Administration*. Aug. 32. P. 20-27.

10. Mishuk N.V. Cybercrime as a threat to the information society. *Visnyk of Lviv University. The series is economical*. Issue 51. Lviv, 2014. P.173-179.

11. Order of the Cabinet of Ministers of Ukraine dated July 11, 2018, No. 481-p On Approval of the 2018 Action Plan for the Implementation of the Cybersecurity Strategy of Ukraine URL: http://zakon.rada.gov.ua/laws/show/96/2016 (reference date 11.09.2018)

12. Rusetskii A.A., Kutsolabsky D. A. Theoretical and legal analysis of the concepts of "cybercrime" and "cybercrime". *Law and Safety*. 2017. No. 1. P. 74-78.

13. Glossary of terms on cyber security / per cons. Ed. O. V. Kopan, E. D. Skulisha-K .: WB "Avanpost-Prim", 2012. - with. 214

14. Decree of the President of Ukraine On the decision of the National Security and Defense Council of Ukraine dated January 27, 2016, "On the Strategy of Cybersecurity of Ukraine" URL: http://zakon.rada.gov.ua/laws/show/96/2016 (application date 11.08. 2018)

15. Computer Crimes Act URL: http://www.clas.ufl.edu/docs/flcrimes/section2_1_1.html#SECTION00110000000000000000 (Application Date 09.12.2018)

16. Cyber Storm: Securing Cyber Space URL: https://www.dhs.gov/cyber-storm. (application date 13.09.2018).

17. Cybersecurity is a fascinating and highly scientific field covering a wide range of disciplines and involving a wealth of organizations and actors both from the public sector and business world in France and internationally. URL: http://www.ssi.gouv.fr/en/mission/word-from-director-general/ (Appointment Date 11.09.2018)

18. Loi 78-17 du 6 janvier 1978 modifiée URL: https://www.cnil.fr/fr/loi-78-17-du-6-janvier-1978-modifiee (application date 13.09.2018)

19. For the benefit of the diffusion and protection of the création sur Internet URL: http://www.senat.fr/dossier-legislatif/pjl07-405.html (reference date 13.09.2018)

Надійшла до редакції 29 жовтня 2018 р.