УДК 343.9.024:004.056.5(100)
DOI https://doi.org/10.24144/2788-6018.2024.04.83

БОРОТЬБА З КІБЕРЗЛОЧИНАМИ: ДОСВІД ОКРЕМИХ ЗАРУБІЖНИХ КРАЇН

Голін І.В.,
аспірант Європейського університету

Голін І.В. Боротьба з кіберзлочинами: досвід окремих зарубіжних країн.

Сьогодні питання, пов'язані з законодавчим закріпленням боротьби з кіберзлочинами, є дуже актуальними. Цей напрямок є перспективним і, на нашу думку, одним з основних для державних органів. Своєчасне прийняття чинного законодавства є поштовхом для формування системи та механізмів боротьби з віртуальними незаконними діями. У цих умовах актуальність і своєчасність нормативно-правових актів визначає напрямки, механізми та методи захисту суспільства і держави.

На основі аналізу досвіду зарубіжних країн автор проаналізував сучасні зміни у сфері кіберзлочинів. Встановлено, що процес законодавчої боротьби з кіберзлочинами в зарубіжних країнах розпочався ще у 20 столітті. Основні, фундаментальні правові акти, що формують систему протидії, також були прийняті в той час, і більшість з них досі діють. Однак це зовсім не означає, що сучасна система боротьби з кіберзлочинністю базується виключно на актах, прийнятих у минулому столітті.

В умовах агресивної війни такий злочинець стає бойовою одиницею, а його основним інструментом є кібератаки. Крім того, під час воєнного стану можливі атаки не лише з боку ворога, який використовує інформаційний простір для завдання шкоди обороноздатності України, а й з боку тих, хто вирішив скористатися ситуацією, коли правоохоронні органи перевантажені, і нажитися на коштах наших громадян.

Зазначається, що сучасний світ швидко змінюється через такі фактори, як комп'ютеризація, глобалізація та інформатизація, постійна війна. У цих умовах постійно оновлюються технології та методики, що призводить до швидких змін у кримінальній сфері, особливо у галузі кіберзлочинів. Нові шкідливі програми, шахрайські схеми та види комп'ютерних атак ставлять перед державою нові виклики у сфері протидії. Тому законодавець приймає нові зміни до чинної правової бази та вводить абсолютно нові акти. Отже, характерною рисою глобальної відповіді на нові загрози в інформаційному світі є прийняття змін до чинного законодавства України.

Ключові слова: боротьба зі злочинністю, кіберзлочини, IT, міжнародний досвід, інформаційна безпека громадян.

Golin I.V. Fighting cyber crimes: the experience of certain foreign countries.

Today, issues related to the legislative consolidation of combating cybercrimes are very relevant. This direction is promising and, in our opinion, one of the main ones for state authorities. The timely adoption of current legislation is an impetus for the formation of a system and mechanisms for combating virtual illegal actions. In these conditions, the relevance and timeliness of normative legal acts determines the directions, mechanisms and methods of protection of society and the state.

Based on the analysis of the experience of foreign countries, the author analyzed modern changes in the field of cybercrimes. It has been established that the process of legislative fight against cybercrimes in foreign countries began as early as the 20th century. The main, fundamental legal acts forming the countermeasure system were also adopted at that time, and most of them are still in effect. However, this does not mean at all that the modern system of combating cybercrime is based exclusively on acts adopted in the last century.

In the conditions of an aggressive war, such a thief becomes a combat unit, and his main tool is cyber attacks and hacking. In addition, during the martial law, attacks are possible not only from the enemy, who uses the information space to harm Ukraine's defense capabilities, but also from those who have decided to take advantage of the situation when law enforcement agencies are overburdened, and to profit from the funds of our citizens

It is noted that the modern world is changing rapidly due to such factors as computerization, globalization and informatization, permanent war. In these conditions, technologies and techniques are constantly updated, which leads to rapid changes in the criminal sphere, especially in the field of cybercrimes. New malicious programs, fraudulent schemes and types of computer attacks pose new challenges to the state in the field of countermeasures. Therefore, the legislator adopts new changes to the current legal framework and introduces completely new acts. Therefore, a characteristic feature of the global response to new threats in the information world is the adoption of changes to the current legislation of Ukraine.

Key words: fight against crime, cybercrime, IT, international experience, information security of citizens.

Постановка питання. Кожна сучасна соціально активна людина в Україні використовує мобільні пристрої та користується інтернетом, державні органи переходять на електронний документообіг, стабільна діяльність банківського сектору, залізниці й авіатранспорту, великих підприємств залежить від стабільності кіберпростору, з яким вони працюють, та базується на комунікації за допомогою електронних засобів зв'язку. В умовах агресивної війни такий злодій стає бойовою одиницею, а його основний інструмент – кібератаки і злами. Крім того, під час воєнного стану атаки можливі не лише з боку ворога, який використовує інфопростір для завдання шкоди обороноздатності України, а й з боку тих, хто вирішив скористатися ситуацією, коли правоохоронні органи перевантажені, та поживитися коштами наших громадян [1].

У цих умовах дуже актуальні питання, пов'язані з законодавчим закріпленням протидії кіберзлочинам. Даний напрямок є перспективним і, на наш погляд, одним із основних для органів державної влади. Своєчасне прийняття актуального законодавства являється поштовхом для формування системи та механізмів протидії віртуальним протиправним діям. У даних умовах актуальність і своєчасність нормативно-правових актів визначає напрями, механізми та способи захисту суспільства та держави.

Законодавство, безсумнівно, є ключовим елементом у боротьбі зі злочинами в сфері ІТ. Важливо вивчити, як ця проблема вирішується в інших країнах. Декілька факторів, таких як вища правова культура, ефективніший та відпрацьований механізм законодавчого процесу, а також висока «правова мобільність» представників та органів законодавчої влади (порівняно з Україною), роблять необхідним звернення до міжнародного досвіду у протидії кіберзлочинам.

Аналіз наукових джерел. Сучасні аспекти розвитку та становлення інформаційних відносин, а також питання протидії кіберзлочинності та кібершахрайству, були розглянуті провідними вітчизняними науковцями, такими як М. Будаков, В. Бутузов, М. Галамба, Р. Калюжний, В. Коваленко, Я. Кондратьєв, Б. Кормич, Ю. Максименко, А. Марущак, Г. Новицький, та іноземними фахівцями, зокрема А. Робертом, К. Осакве, Т. Блентаном, Д. Банісаром та ін.

Метою статті є дослідження міжнародного досвіду протидії кіберзлочинності та кібершахрайству для можливості його подальшого застосування у роботі правоохоронних органів України.

Методологічною основою дослідження є низка загальнонаукових і спеціальних методів наукового пізнання, вибір яких обумовлено особливостями його об'єкта, предмета, поставлених мети та завдань. Так, зокрема, при дослідженні питань правових засобів запобігання кіберзлочинності застосовувався діалектичний метод наукового пізнання правових процесів та явищ, що проявилося, зокрема, у широкому використанні окремих категорій діалектики (причина й наслідок, форма й зміст, сутність та явище). Використання порівняльно-правового методу наукових досліджень дозволило дослідити відповідність інституту боротьби з кіберзлочинами в Україні міжнародним стандартам, а також проаналізувати позитивний досвід зарубіжних країн щодо ефективної боротьби з кіберзлочинами. За допомогою формально-логічного методу було проведено морфологічний, граматичний, а також логічний аналіз норм кримінального законодавства. Шляхом застосування методу моделювання в дослідженні було сформульовані конкретні пропозиції щодо вдосконалення чинного законодавства України у сфері боротьби з кіберзлочинами.

Виклад матеріалу дослідження. Першою країною, що зіткнулася з цим новітнім викликом злочинного світу, стали Сполучені Штати Америки. США, як держава, що зазнає значного негативного впливу від кіберзлочинців, та є однією із перших в історії, що зайнялась розробкою відповідних нормативно-правових актів є надзвичайно цікавою та вагомою для дослідження. Як доречно відзначає Н. Савчук, американська політика у сфері кіберпростору має значний вплив на країни європейського співтовариства [2, с. 25].

Саме тому, не дивно, що саме США першими законодавчо закріпили статус кіберзлочинів та систему протидії їм. Адже саме тут у 1969 році стався перший злочин із використанням комп'ютерної мережі, і саме тут на Конференції Американської асоціації адвокатів[1] у 1974 році вперше було сформульовано поняття кіберзлочину та виявлено й перераховано його особливості.

Перші ознаки законодавчої роботи у цій сфері в США з'явилися ще у 1977 році. На основі концепції, що встановлює кримінальну відповідальність за злочини у сфері інформаційних технологій, у жовтні 1984 року було прийнято Закон про шахрайство та зловживання з використанням комп'ютерів (Computer Fraud and Abuse Act). Цей документ запровадив нові склади протиправних діянь, які підлягають кримінальній відповідальності (такі як шпигунство з використанням комп'ютера, шахрайство з вико-

[1] Американська асоціація адвокатів (англ. American Bar Association) — національне об'єднання юристів США. Незважаючи на назву, приймає в свої члени не тільки американських юристів, а й юристів інших країн світу, є однією з найбільших асоціацій у світі. Серед своїх основних цілей, організація декларує вироблення нормативів юридичної освіти для профільних вишів та розробку етичних стандартів для юристів різних спеціалізацій (зокрема, правила реклами юридичних послуг) [4, с. 232].

ристанням комп'ютера), а також відповідні покарання (зокрема штрафи та позбавлення волі). Закон про шахрайство неодноразово доповнювався та змінювався, що дозволило багатьом санкціям, встановленим цим актом, залишатися актуальними й досі бути невід'ємною частиною системи протидії віртуальним злочинам [3].

Наразі питання протидії злочинам у сфері ІТ закріплене й у найважливіших координаційних документах США, таких як Концепція національної безпеки США та Стратегія кібербезпеки США, прийнята у 2003 році [5, с. 315].

Серед норм Національної стратегії внутрішньої безпеки США, прийнятої в 2015 році, особливий інтерес, на наш погляд, представляє розділ «Кіберзахист», в якому наголошується на необхідності захисту від кібератак у кіберпросторі. США, проголошуючи себе батьківщиною Інтернету, взяли на себе відповідальність перед усім мережевим світом за забезпечення безпеки в кіберпросторі. Окрім того, цією державою проголошено курс на посилення законодавчої бази та підвищення стандартів захисту прав та інтересів громадян [6, с. 12].

Крім того, в США активно ведеться боротьба з цим видом злочинності, приділяючи значну увагу безпеці громадян загалом. США – країна що є однією з головних мішеней для кіберзлочинців з усього світу, тому їхній досвід є цінним для розробки правових інструментів, спрямованих на протидію цьому негативному явищу. Однак, незважаючи на це, в США переважає концепція саморегулювання Інтернету, що призвело до наявності лише кількох спеціальних нормативно-правових актів у цій сфері. Одним із таких актів є Закон про електронний підпис, прийнятий у 2000 році, метою якого є забезпечення правового режиму електронного підпису в комерційних відносинах. У США цей закон вважається символом переходу до нової ери – ери електронної комерції. Закон є досить стислим і визначає лише незначну кількість понять та механізмів, включаючи компетенцію державних органів, відповідальних за функціонування всієї інфраструктури у цій сфері, взаємодію її елементів та органів державної влади [7, с. 131].

Розглядаючи міжнародний досвід боротьби з кіберзлочинами в різних регіонах, можна розглянути й Японію, яка є лідером в інноваційних технологіях, робототехніці та комп'ютерних тенденціях. Відзначимо, для цієї країни питання кібербезпеки є одним з перспективних напрямків діяльності. Так, зокрема, з 2013 року головна роль у боротьбі з кіберзлочинами зосереджена в Раді з питань інформаційної безпеки Японії. Цей державний орган є також одним з основних законодавчих суб'єктів: самостійно видає нормативно-правові акти з протидії кіберзлочинності, а також аналізує, редагує і проводить експертизу подібних документів інших суб'єктів законодавчого процесу [8, с. 124].

Основним документом, що передбачає санкції, є Кримінальний кодекс Японії. Варто відмітити досить суворі покарання за суспільно небезпечні протиправні дії. Наприклад, за «фальсифікацію комп'ютерних даних» передбачено кримінальну відповідальність у вигляді позбавлення волі строком на 10 років [9, с. 214].

Слід акцентувати увагу й на Законі про заборону незаконного доступу (офіційна назва «Закон про заборону незаконного доступу та інше») був прийнятий у лютому 2012 року. Цей закон, що складається з 14 статей, має на меті запобігти кіберзлочинам та підтримувати порядок у сфері електронних комунікацій. Згідно статті 1, метою цього закону є «запобігання злочинам, пов'язаним з комп'ютерами, через телекомунікаційні лінії, а також підтримка порядку в телекомунікаціях, які здійснюються за допомогою функцій контролю доступу, шляхом заборони незаконного доступу, встановлення кримінальних покарань за це та заходів допомоги від комісії з громадської безпеки префектур для запобігання повторенню таких дій, та тим самим сприяти здоровому розвитку високоінформаційного суспільства». При цьому, Закон про заборону незаконного доступу не лише визначає незаконні дії доступу та покарання за них, але й накладає обов'язки на адміністраторів для запобігання незаконному доступу до серверів та інших систем [10].

Незважаючи на це, слід відмітити, з 2018 року в Японії практично удвічі зросла кількість що вірогідною причиною зростання кількості атак є збільшення числа можливих цілей, таких як під'єднана до Інтернету домашня техніка.

7 липня 2022 року набула чинності поправка до Кримінального кодексу Японії, відповідно до якої за образу людини в інтернеті можна потрапити до в'язниці. Віднині за кіберзалякування можна отримати тюремний термін до одного року або штраф до 300 000 єн (2200 доларів). Раніше цей злочин карався тюремним терміном до 30 днів або штрафом до 10 000 єн (менше за 74 долари). Також збільшено термін давності за образи з одного року до трьох років[1] [11].

[1] Японські урядовці почали обговорювати зміну до законодавства після самогубства зірки популярного реалітішоу Netflix "Будинок з терасою" Хани Кімури у травні 2020 року, яка зазнала знущань в інтернеті. Двох чоловіків, яких визнали винними у кібербулінгу, оштрафували на 9 000 єн (66 доларів) кожного. Суспільство висловило занепокоєння, що покарання було занадто легким і згодом це призвело до законодавчих змін. Зміну до Кримінального кодексу ухвалили лише після того, як керівна Ліберально-демократична партія Японії додала положення, яке закликає уряд переглянути закон через три роки, щоб перевірити його вплив на свободу вираження поглядів. Якщо будуть доведені факти впливу на свободу слова, закон переглянуть [11].

Що стосується практики застосування законодавства про кіберзлочини в Японії, відзначимо, якщо особа стає жертвою кіберзлочину та повідомляє про це в поліцію, зазвичай очікується, що поліція проведе розслідування, встановить винуватця та приступить до арештів та притягнення до відповідальності. Це «звичайне уявлення громадянина». Однак, на жаль, в Японії, коли мова йде, зокрема, про економічні злочини, які не пов'язані з загрозами життю або фізичному здоров'ю, особливо у випадку кіберзлочинів, практичні ресурси поліції для розслідування є обмеженими. Без ретельного розслідування та створення обширної документації з боку жертви, такої як «звіти про інциденти», важко ефективно стимулювати поліцейські розслідування навіть для високотехнологічної Японії [12].

Також, на наш погляд, вартим уваги є факт, що за даними Офісу національної безпеки президента Південної Кореї, високопоставлені чиновники національної безпеки трьох країн (США, Японія, Південна Корея) досягли угоди під час зустрічі у Вашингтоні домовилися створити робочу групу для посилення заходів проти кібератак Північної Кореї. Вважається, що Пхеньян здійснив атаки для фінансування своєї ядерної та ракетної програм. Так, ще у жовтні 2023 року Рада безпеки ООН заявила, що минулого року північнокорейські хакери вкрали криптовалюту на загальну суму в 1,7 мільярда доларів.

Офіс національної безпеки президента Південної Кореї вважає, що потенційні кіберзагрози з боку міжнародних хакерських груп будуть зменшені завдяки постійній та різноманітній роботі з країнами, які поділяють демократичні цінності. Новий консультаційний орган буде займатися розробкою заходів блокування кіберзлочинів Північної Кореї і посиленням можливостей спільного реагування трьох країн на глобальні кіберзагрози [13].

І, насамкінець, на наш погляд, вартий уваги й досвід Нідердандів. У Нідерландах, як і в багатьох інших європейських країнах, важливе місце займає Кримінальний кодекс. Варто зазначити, що ця країна почала розглядати питання законодавчого врегулювання кіберзлочинів ще з моменту їх появи, тобто з 70-х років XX століття. Однак, спочатку спроби регулювати сферу комп'ютерної злочинності були невдалими. Лише наприкінці 80-х років було створено спеціальний державний орган – Консультативний комітет із комп'ютерних злочинів. Основні функції цього органу включали створення, просування та курування державної політики щодо протидії кіберзлочинам.

Комітет також мав статус суб'єкта законотворчості, що дозволяло йому пропонувати та вносити зміни до законопроектів у сфері ІТ. У 1993 році, завдяки активній діяльності Консультативного комітету з комп'ютерних злочинів, було створено та прийнято «Закон про комп'ютерні злочини», який доповнив чинні Кримінальний кодекс і Кримінально-процесуальний кодекс Нідерландів новими статтями щодо протиправних діянь у віртуальній сфері. Ці зміни коригували традиційне чинне законодавство, зокрема, до кваліфікуючих ознак статей, пов'язаних із здирством, шахрайством і крадіжкою, були внесені відповідні доповнення [8, с. 124].

20 грудня 2016 року Палата представників Нідерландів ухвалила законопроект про конфіденційність «Computercriminaliteit III» («Кіберзлочинність III»). Закон Computercriminaliteit III чинний з 2019 року, покликаний дати слідчим (поліції, королівській поліції і навіть спеціальним слідчим органам, таким як FIOD) можливість досліджувати (тобто копіювати, спостерігати та перехоплювати) «автоматизовані операції» або «комп'ютеризовані пристрої» (для непрофесіонала: пристрої, такі як комп'ютери та мобільні телефони) для виявлення серйозних злочинів. На думку уряду, необхідно надати слідчим можливість – шпигувати за громадянами, оскільки сучасні часи призвели до того, що злочинність стала ледь простежуваною через цифрову анонімність, що зростає, і шифрування даних. У пояснювальному меморандумі, опублікованому у зв'язку із законопроектом, який є дуже важким для читання документом на 114 сторінках, описано п'ять цілей, на підставі яких можуть використовуватись слідчі повноваження:

– встановлення та захоплення певних деталей комп'ютеризованого пристрою або користувача, наприклад ідентифікація або місцезнаходження: більш конкретно це означає, що співробітники, які займаються розслідуванням, можуть таємно звертатися до комп'ютерів, маршрутизаторів та мобільних телефонів, щоб отримати інформацію, таку як IP-адреса або IMEI;

– реєстрація даних, що зберігаються на комп'ютеризованому пристрої: співробітники слідчих органів можуть записувати дані, необхідні для встановлення істини і вирішення серйозних злочинів. Наприклад, записи зображень дитячої порнографії та реєстраційні дані для закритих спільнот;

– зробити дані недоступними: стане можливим зробити дані, за якими злочин скоєно недоступними з метою припинення злочину або запобігання майбутнім злочинам. Згідно з пояснювальним меморандумом, таким чином стає можливим боротися з ботнетами;

– виконання ордера на перехоплення та запис (конфіденційних) повідомлень: за певних умов буде можливим перехоплювати та записувати (конфіденційну) інформацію з або без до-

помоги постачальника послуг зв'язку;

– виконання ордера на систематичне спостереження: слідчі отримають можливість встановити місце розташування та відстежувати рухи підозрюваного, можливо, шляхом дистанційної установки спеціального програмного забезпечення на комп'ютерний пристрій [15].

Висновки. Як можна помітити, процес законодавчої боротьби з кіберзлочинами в зарубіжних країнах розпочався ще у XX столітті. Основні, фундаментальні нормативно-правові акти, що формують систему протидії, також були прийняті в той час, і більшість з них діють досі. Однак це зовсім не означає, що сучасна система протидії кіберзлочинам базується виключно на актах, прийнятих у минулому столітті.

Сучасний світ змінюється швидко через такі фактори, як комп'ютеризація, глобалізація та інформатизація, перманентна війна. В цих умовах технології та техніка постійно оновлюються, що призводить до швидких змін і у злочинній сфері, особливо в галузі кіберзлочинів. Нові шкідливі програми, шахрайські схеми та види комп'ютерних атак ставлять перед державою нові виклики у сфері протидії. Тому законодавець ухвалює нові зміни до чинної нормативно-правової бази та впроваджує абсолютно нові акти. Отже, характерною ознакою для світової відповіді на нові загрози в інформаційному світі є прийняття змін й до чинного законодавства України.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Єрема М. Боротьба з кіберзлочинністю в умовах дії воєнного стану: Закон 2149-IX. URL: https://jurliga.ligazakon.net/analitycs/210562_borotba-z-kberzlochinnstyu-v-umovakh-d-vonnogo-stanu-zakon-2149-ix.
2. Савчук Н.В. Світовий досвід державного регулювання ринку інтернет-послуг. *Формування ринкових відносин в Україні*. 2012. № 4. С. 24–28.
3. Computer Fraud and Abuse Act. URL: https://www.techtarget.com/searchsecurity/definition/Computer-Fraud-and-Abuse-Act-CFAA#:~:text=The%20Computer%20Fraud%20and%20Abuse%20Act%20(CFAA)%20of%201986% 20is,whose%20access%20exceeds%20their%20authorization.
4. Шемшученко Ю.С. Американська асоціація юристів [Архівовано 13 квітня 2017 у Wayback Machine.] Юридична енциклопедія : [у 6 т.] / ред. кол.: Ю.С. Шемшученко (відп. ред.) [та ін.]. К. : Українська енциклопедія ім. М.П. Бажана, 1998. Т. 1 : А–Г. 672 с.
5. Грицун О.О. Питання міжнародно-правового регулювання інформаційного тероризму. *Часопис Київського університету права*. 2014. № 4. С. 312–317.
6. National Security Strategy. The White House, February 2015. Washington D.C., 2015. 29 p. URL: http://nssarchive.us/wp-content/uploads/2015/02/ 2015.pdf.
7. Буяджи С.А. Особливості правового регулювання боротьби із кіберзлочинністю у США. LEX PORTUS № 2 (4)'2017. С. 130–141.
8. Кравчук М.М. Міжнародний досвід правового регулювання захисту персональних даних в мережі Інтернет. Наукові записки Інституту законодавства Верховної Ради України. 2013. № 3. С. 123–126.
9. Орлов О.В., Онищенко Ю.М. Узагальнення міжнародного досвіду ство- рення державної системи попередження та запобігання злочинам у ме- режі інтернет. *Теорія та практика державного управління*. 2014. Вип. 2. С. 212–219.
10. Дії, заборонені Законом Японії про заборону незаконного доступу. URL: https://monolith.law/uk/it/unauthorized-computer-access.
11. В Японії посилили відповідальність за кібербулінг, відтепер за образу в інтернеті можна потрапити за ґрати. URL: https://zmina.info/news/v-yaponiyi-posyly-vidpovidalnist-za-kiberbuling-vidteper-za-obrazu-v-interneti-mozhna-potrapyty-za-graty/.
12. Кіберзлочинність. URL: https://monolith.law/uk/cybercrime.
13. Кацімон О. США, Південна Корея та Японія створили консультативну групу щодо кіберзагроз КНДР. URL: https://suspilne.media/611289-ssa-pivdenna-korea-ta-aponia-stvorili-konsultativnu-grupu-sodo-kiberzagroz-kndr/.
14. Бєлова М.В., Бєлов Д.М. Імплементація штучного інтелекту в досудове розслідування кримінальних справ: міжнародний досвід. *Аналітично-порівняльне правознавство*. № 2. 2023. С. 448–454.
15. New law to help fight computer crime. 2019. URL: https://www.government.nl/topics/cybercrime/news/2019/02/28/new-law-to-help-fight- computer-crime.