УДК 343.9+341.4
DOI https://doi.org/10.32782/2524-0374/2022-8/101

КОМП'ЮТЕРНА ЗЛОЧИННІСТЬ: КРИМІНАЛЬНО-ПРАВОВИЙ ТА КРИМІНОЛОГІЧНИЙ АСПЕКТ (ДОСВІД ДЕРЖАВ ЄВРОПЕЙСЬКОГО СОЮЗУ)

COMPUTER CRIME: CRIMINAL-LEGAL AND CRIMINOLOGY ASPECT (EXPERIENCE OF EUROPEAN UNION STATES)

Налуцишин В.В., д.ю.н., професор,
професор кафедри кримінального права та процесу
Хмельницький університет управління та права імені Леоніда Юзькова

Крушинський С.А., к.ю.н, доцент,
завідувач кафедри кримінального права та процесу
Хмельницький університет управління та права імені Леоніда Юзькова

У поданій статті досліджуються питання кримінальної відповідальності за комп'ютерні злочини у країнах Європейського Союзу, дається їхня загальна характеристика, розкриваються характерні особливості та відмінні риси. Наголошується на актуальності проблематики кіберзлочинності, її диференціація, заснована на Конвенції Ради Європи про кіберзлочинність, та про особливості кримінальної регламентації злочинів, вчинених з використанням комп'ютерів та комп'ютерних мереж у Швеції, Німеччині, Франції, Нідерландах. Відзначено, що питання протидії подібним злочинам мають особливе значення в усіх країнах Європейського Союзу. Незважаючи на відмінності в позиціях законодавців щодо криміналізації діянь, вчинених з використанням комп'ютерних засобів, у всіх країнах посягання на кіберпростір розглядаються як посягання на основи держави, а захист від таких посягань є однією з найважливіших державних функцій. Констатовано, що кримінальні кодекси більшості європейських держав включають правові норми щодо комп'ютерного шахрайства, комп'ютерного розкрадання; отримання інформації, що становить комерційну та банківську таємницю шляхом неправомірного доступу до комп'ютерної інформації (комерційне, банківське шпигунство); вимагання з використанням засобів комп'ютерної техніки. За вчинення комп'ютерних злочинів передбачені покарання у вигляді штрафу або позбавлення волі у різних розмірах (до 300000 євро) та на різний строк (до 20 років). За вчинення злочинних посягань на системи автоматизованої обробки даних до кримінальної відповідальності можуть бути притягнуті як фізичні, так і юридичні особи (Франція). За результатами дослідження зроблено висновок про необхідність детального вивчення складів злочинів у сфері комп'ютерної інформації з метою їхньої правильної кваліфікації та підвищення ефективності кримінально-правової боротьби з ними.

Ключові слова: кіберзлочинність, Європейський Союз, комп'ютерні злочини, комп'ютерний саботаж, протидія комп'ютерній злочинності.

The submitted article examines the issues of criminal responsibility for computer crimes in the countries of the European Union, gives their general characteristics, reveals characteristic features and distinguishing features. Emphasis is placed on the relevance of the issue of cybercrime, its differentiation based on the Council of Europe Convention on Cybercrime, and the specifics of the criminal regulation of crimes committed using computers and computer networks in Sweden, Germany, France, and the Netherlands. It was noted that the issue of combating such crimes is of particular importance in all countries of the European Union. Despite the differences in the positions of legislators regarding the criminalization of acts committed using computer means, in all countries encroachments on cyberspace are considered as encroachments on the foundations of the state, and protection against such encroachments is one of the most important state functions. It was established that the criminal codes of most European states include legal norms regarding computer fraud, computer theft; obtaining information constituting a commercial and banking secret through illegal access to computer information (commercial, banking espionage); extortion using computer equipment. Computer crimes are punishable by fines or imprisonment in various amounts (up to 300,000 euros) and for various terms (up to 20 years). Both individuals and legal entities may be held criminally liable for criminal encroachment on automated data processing systems (France). According to the results of the study, a conclusion was made about the need for a detailed study of the composition of crimes in the field of computer information in order to properly qualify them and increase the effectiveness of the criminal legal fight against them.

Key words: cybercrime, European Union, computer crimes, computer sabotage, combating computer crime.

В останні роки проблема злочинів, що вчинені з використанням цифрових технологій, залишається однією з найактуальніших і несе серйозну загрозу не тільки національній безпеці України, але і всьому світовому співтовариству. Це зумовлено прискореним впровадженням у повсякденне життя суспільства досягнень інформаційних технологій, що дозволяють злочинцям залишатися поза увагою правоохоронних органів.

Варто відзначити, що законодавці всіх європейських країн включили норми про відповідальність за комп'ютерні злочини до своїх кримінальних кодексів. Вважаємо, що розвиток та подальше вдосконалення вітчизняного законодавства про відповідальність за злочини у сфері комп'ютерної інформації та протидії їм, неможливі без використання досвіду застосування кримінального законодавства країн Європейського Союзу.

Резюмуємо, що на сьогодні однозначного трактування визначення поняття «комп'ютерний злочин» чи «злочин, пов'язаний з використанням комп'ютерів» немає. Зазвичай, в нормативно-правових актах, поняття «кіберзлочинність», «комп'ютерні злочини», «злочини, з використанням електронних засобів зв'язку», «злочини у сфері високих технологій», «IT-злочини» часто взаємозамінюються.

Першим міжнародним договором про злочини, вчинені через Інтернет та інші комп'ютерні мережі, для європейських держав, і не тільки, є Конвенція Ради Європи про кіберзлочинність від 23 листопада 2001 р. та Додатковий протокол до неї від 28 січня 2003 р.

Конвенція Ради Європи про кіберзлочинність спочатку підрозділяла кіберзлочини на чотири групи (потім було прийнято додатковий протокол, і тепер груп – п'ять), виділяючи в *першу групу «комп'ютерні злочини»*, називаючи їх злочинами проти конфіденційності, цілісності та доступності комп'ютерних даних та систем:

• незаконний доступ – ст. 2 (протиправний навмисний доступом до комп'ютерної системи чи її частини);

• незаконне перехоплення – ст. 3 (протиправне навмисне перехоплення не призначених для громадськості передач комп'ютерних даних на комп'ютерну систему, з неї або в її межах);

• втручання у дані – ст. 4 (протиправне ушкодження, видалення, порушення, зміна чи припинення комп'ютерних даних);

• втручання у систему – ст. 5 (серйозне протиправне перешкоджання функціонування комп'ютерної системи шляхом введення, передачі, пошкодження, видалення, порушення, зміни або припинення комп'ютерних даних).

До *другої групи* входять злочини, пов'язані з використанням комп'ютерних засобів. Підробку з використанням комп'ютерних технологій Конвенція визначає як введення, зміну, знищення або блокування комп'ютерних даних, що тягнуть за собою порушення автентичності даних з наміром, щоб вони розглядалися або використовувалися в юридичних цілях як автентичні, незалежно від того, чи ці дані піддаються безпосередньому прочитанню і чи є вони зрозумілими. Шахрайство в кіберпросторі, згідно з Конвенцією – це позбавлення іншої особи її власності шляхом будь-якого введення, зміни, видалення або блокування комп'ютерних даних або будь-якого втручання у функціонування комп'ютерної системи, з шахрайським чи безчесним наміром неправомірного отримання економічної вигоди для себе чи третіх осіб.

Третю групу становлять злочини, пов'язані з контентом (змістом даних). Йдеться про дитячу порнографію, причому в Конвенції досить докладно пояснюється, які саме дії щодо поширення дитячої порнографії мають переслідуватися.

До *четвертої групи* увійшли злочини, пов'язані з порушенням авторського права та суміжних прав. Види таких злочинів у Конвенції не вирізняються: встановлення таких правопорушень віднесено документом до компетенції національних законодавств держав.

П'ята група – злочини, які посягають на безпеку. До цієї категорії належать такі діяння, як кібертероризм та використання кіберпростору в терористичних цілях (наприклад, залучення до скоєння злочинів терористичного характеру чи інше сприяння їхньому вчиненню) [1].

Положення Конвенції є першою спробою визначення нормативного поля комп'ютерної злочинності на міждержавному рівні та мають рекомендаційний характер для країн-учасниць. Держави, які підписали цю Конвенцію (в тому числі і Україна), мають право самі визначати рівень заходів покарання щодо правопорушників. Це можуть бути як кримінально-правові чи адміністративні заходи, так наприклад, і заходи технічного характеру.

У зв'язку з цим видається виправданим розгляд деяких аспектів кримінально-правової регламентації відповідальності за злочини у сфері комп'ютерної інформації та протидії їм у країнах Європейського Союзу.

Еволюція законодавства розвинених країн Європи демонструє, що перший крок у напрямі кримінально-правової охорони комп'ютерної інформації, розвитку кримінального законодавства протидії економічної кіберзлочинності зроблено законодавцем ***Швеції*** з прийняттям Закону про комп'ютерні злочини (1973 р.) [2]. Цим нормативним правовим актом передбачено кримінальну відповідальність: за протиправне проникнення в систему комп'ютерної мережі; за введення в комп'ютерну інформацію дезінформації; за здійснення розкрадання таких об'єктів, як кошти (електронні), а також цінні папір, інші види майна та інші, включаючи послуги та цінну для певних кіл інформацію. Законом про дані (1974 р.) [3] у кримінальне законодавство запроваджено категорію «зловживання за допомогою комп'ютера».

На початку 90-х років минулого століття, у зв'язку з активізацією кіберзлочинів, Кримінальний кодекс Швеції [4] одним із перших був доповнений положеннями, що передбачають кримінальну відповідальність за злочини, вчинені із застосуванням комп'ютерної інформації та інформаційних технологій: за шахрайство, вчинене наданням або неповної, або неправдоподібної інформації, або внесенням корективів до комп'ютерної програми або до звітність.

Також, передбачена відповідальність за: діяння, що здійснюються шляхом незаконного впливу на безпосередній результат автоматичної обробки комп'ютерної інформації, іншої тотожної обробки, що спричинило вигоду для суб'єкта злочину та збитки для жертви; правопорушення, пов'язане з поштовою або комунікаційною таємницею; застосування технічних механізмів з наміром надати протиправний вплив на таємницю телекомунікаційної властивості; протиправний доступ до процесів обробки комп'ютерних даних; протизаконне коригування, усунення, додавання певного запису до реєстру даних та деякі інші.

Так, відповідно до ст. 1 Розділу 9 КК Швеції, особа, яка шляхом надання неправильної або неповної інформації, або внесення змін до програми або звітності, або будь-якими іншими способами незаконно впливає на результат автоматичної обробки інформації або будь-якої іншої подібної автоматичної обробки, яка тягне за собою вигоду для особи, яка вчинила злочин, та збитки для будь-якої іншої особи, має бути засуджена за скоєння шахрайства та піддана такому ж покаранню.

Основою політики Швеції у сфері кібербезпеки є Стратегія з покращення інтернет-безпеки 2006 року та План дій з інформаційної безпеки 2012 року.

Цікавим видається досвід ***Федерати́вної Респу́біки Німе́ччини.***

Основою політики ФРН у сфері кібербезпеки є Стратегія кібербезпеки 2011 р. та Національний план із захисту інформаційної інфраструктури [5].

У німецькій юридичній науці виділяються різноманітні склади комп'ютерних злочинів:

1) злочини, скоєні за допомогою висловлювань (включаючи поширення порнографії (§ 184 КК ФРН), зображення насильства (§ 131 КК ФРН), нанесення образ (§ 185 КК ФРН), екстремістська пропаганда (§ 86));

2) втручання в особисту сферу (включаючи порушення конфіденційності (§ 201 КК ФРН), порушення особистої сфери життя за допомогою зйомок (§ 201а КК ФРН), переслідування (§ 238 КК ФРН);

3) шахрайство та комп'ютерне шахрайство (включаючи шахрайство (§ 263 КК ФРН) та комп'ютерне шахрайство (§ 263а КК ФРН);

4) атаки програмного та апаратного забезпечення (включаючи розкрадання (комп'ютерної) інформації (§ 202а КК ФРН), перехоплення даних (§ 202Ь КК ФРН), підготовку до розкрадання (комп'ютерної) інформації та перехоплення даних (§ 202с КК ФРН), зміна даних (§ 303а КК ФРН), комп'ютерна диверсія (§ 303Ь КК ФРН);

5) підробка документів за допомогою комп'ютера (включаючи підробку документів (§ 267 КК ФРН), фальсифікацію технічних даних, записаних на електронних носіях (§ 268 КК ФРН), фальсифікацію даних, суттєвих для доказів (§ 269 КК ФРН);

6) інші комп'ютерні злочини (включаючи отримання вигоди від виконаної роботи обманним шляхом (§ 265 КК ФРН), недозволена організація азартних ігор (§ 284 КК ФРН), пошкодження пристроїв телекомунікації (§ 317 КК ФРН) [6].

У КК Німеччини [7] комп'ютерні злочини (злочини у сфері комп'ютерної інформації) структурно розміщуються в різних розділах.

Так, §202а «Шпигунство даних», включений до розділу 15 «Порушення недоторканності та таємниці приватного життя», і передбачає відповідальність особи за незаконне отримання даних, які їй не призначаються та особливо охороняються від незаконного до них доступу, або хто передає їх іншій особі. Цей злочин карається позбавленням волі терміном до трьох років чи грошовим штрафом.

Відповідно до §263а «Комп'ютерне шахрайство», той, хто діючи з наміром отримати для себе чи третьої особи майнову вигоду, завдає шкоди майну іншої особи, впливає на результат обробки даних шляхом неправильного

створення програм, використання неправильних чи неповних даних чи іншого неправомірного впливу на процес обробки даних, не маючи на це відповідних повноважень, карається позбавленням волі на строк до п'яти років або грошовим штрафом. Комп'ютерна інформація, у цьому випадку, виступає способом вчинення розкрадання. Вказаний злочин поміщений у розділ 22 «Шахрайство та зловживання довірою».

У розділі 23 «Підробка документів» § 269 «Фальсифікація даних, що мають доказове значення» встановлює відповідальність за різні способи фальсифікації документів. Зокрема, відповідальність настає за збереження або зміну за допомогою ЕОМ, шляхом обману даних, що мають доказове значення, що призводить до сприйняття документів як сфальшованих або підроблених, або використання такого роду збережених або змінених даних.

За здійснення діяння, передбаченого в § 303a «Зміна даних» передбачена відповідальність у вигляді позбавлення волі на строк до двох років або грошового штрафу, якщо особа «протиправно стирає, робить непридатною для використання або змінює дані». За діяння, зазначене в § 303b «Комп'ютерний саботаж», що виявилося в порушенні обробки даних, що мають істотне значення для чужого підприємства, організації або органу, якщо особа вчинила злочин, передбачений § 303a або зіпсувала, пошкодила, зробила непридатною для подальшого використання за призначенням або змінила пристрій для переробки даних, або носій інформації, особа карається позбавленням волі на строк до п'яти років або штрафом. В особливо тяжких випадках (завдання втрати майна у великому розмірі; діянні у вигляді промислу або у складі банди, організованої для тривалого здійснення комп'ютерного саботажу, або діяннями порушується забезпечення населення життєво важливими товарами чи послугами або обмежується безпека Федеративної Республіки Німеччина) передбачена відповідальність у вигляді позбавлення волі на строк від шести місяців до десяти років. Злочини, передбачені §§ 303a, 303b, включені до розділу 27 «Пошкодження майна».

Щодо заходів протидії комп'ютерним злочинам, варто відмітити, що в Німеччині, відповідно до Стратегії кібербезпеки, створено Національне агентство кіберзахисту, для взаємодії з поліцією, розвідкою та Федеральним управлінням з інформаційної безпеки. Основним завданням Національного агентства кіберзахисту стало створення системи для оперативного виявлення та ефективного відбиття хакерських атак, а також забезпечення безпеки критично важливих інформаційних систем» [5].

З метою запобігання вчиненню комп'ютерних злочинів Федеральному відомству кримінальної поліції, відповідно до § 20k (1) Закону про кримінальну поліцію (Bundeskriminalamtgesetz), надано право втручатися в технічні засоби інформаційних систем. Це право обмежується розслідуваннями щодо злочинів, пов'язаних із «небезпекою для життя, обмеженнями свободи та національної безпеки». Дистанційний доступ застосовується лише щодо комп'ютерних систем підозрюваних у справі чи осіб, які спілкуються з підозрюваними. Встановлено максимальний термін для перехоплення даних – три місяці. Правоохоронні органи можуть використовувати будь-які засоби, необхідні для доступу до зашифрованих даних на конфіскованих пристроях, що, природно, включає і злом такого пристрою [8].

1 вересня 2017 р. Бундестаг схвалив Закон про покращення правозастосування у соціальних мережах, відомий також під назвою Закон про Facebook. Згідно вказаного Закону онлайн-платформам тепер загрожує штраф у розмірі до 50 млн. євро, якщо вони протягом 24 годин після отримання офіційного повідомлення не видалять «заздалегідь незаконні» повідомлення (повідомлення образливого характеру), спрямовані на розпалювання ненависті та інші повідомлення. Для видалення нелегального контенту компаніям надається семиденний період [9].

В основі діяльності ***Французької Республіки*** в кіберпросторі лежить Стратегія безпеки та оборони інформаційних систем 2011 року [10].

Кримінальний кодекс Франції [11] включає значну кількість комп'ютерних злочинів. Так, у Кримінальному кодексі в Книзі другій «Про злочини та проступки, вчинені проти особи» розділі II «Про посягання на особистість людини» главі VI «Про посягання на особистість» у відділі V «Про посягання на права особи щодо використання карт та персональних даних» передбачена відповідальність за посягання, пов'язані з використанням картотек та обробкою даних на ЕОМ (ст.ст. 226-16 – 226-22). За вчинення вказаних дії законодавець передбачає відповідальність у вигляді позбавлення волі на строк п'ять років та штрафом у розмірі 300 000 євро (ст.ст. 226-16, 226-17, 226-18, 226-19, 226-21) або позбавленням волі на термін три роки та штрафом у розмірі 100 000 євро (ст. 226-22).

У Книзі третій «Про майнові злочини та проступки» у розділі II «Про інші майнові посягання» у главі III «Про посягання на системи автоматизованої обробки даних» передбачено відповідальність за злочини, які посягають на системи автоматизованої обробки даних: ст. 323-1 «Доступ або збереження шахрайським шляхом у всій автоматизованій системі обробки даних або її частині»; ст. 323-2 «Перешкоджання або спотворення роботи автоматизованої системи обробки даних»; ст. 323-3 «Шахрайське введення даних в автоматизовану систему обробки, вилучення, зберігання, відтворення, передача, видалення або шахрайське модифікування даних, що містяться в ній». Законодавець за зазначені дії передбачив максимальну відповідальність у вигляді грошового штрафів у розмірі 150 000 євро та п'яти років позбавлення волі (ст. 323-1) або штрафу 300 000 євро та позбавленням волі на строк сім років (ст.ст. 323-2, 323-3). Крім цього, за аналізовані види злочинних посягань до кримінальної відповідальності можуть бути притягнуті як фізичні, так і юридичні особи (ст. 323-6).

У Книзі четвертій «Злочини та правопорушення проти нації, держави та громадського спокою» у розділі I «Про посягання на основні інтереси нації» у главі I «Про зраду та шпигунство» у відділі III «Про передачу інформації іноземній державі» передбачено відповідальність за дії, що здійснюються з комп'ютерною інформацією на шкоду інтересам держави (ст.ст. 411-7, 411-8). За вказані посягання передбачена відповідальність у вигляді десяти років позбавлення волі та штрафом у розмірі 150 000 євро. У відділі IV «Про саботаж» та відділі V «Про надання неправдивих відомостей» передбачено відповідальність відповідно за «знищення, пошкодження або незаконне заволодіння будь-яким документом, матеріалом, конструкцією, обладнанням, установкою, приладом, технічним пристроєм чи автоматизованою системою обробки інформації або неякісне виконання робіт, якщо це може завдати шкоди основам інтересів держави» (ст. 411-9) та «надання, з метою обслуговування інтересів іноземної держави, іноземної компанії чи організації або такої, що перебуває під іноземним контролем, цивільній чи військовій владі Франції неправдивої інформації, яка може ввести їх в оману та порушити фундаментальні інтереси нація» (ст. 411-10). Покарання: за ст. 411-9 – п'ятнадцять років позбавлення волі та штраф у розмірі 225 000 євро (1) та двадцять років позбавлення волі та штраф у розмірі 300 000 євро (2), за ст. 411-10 – сім років позбавлення волі та штраф у розмірі 100 000 євро.

У главі III «Про інші посягання, які підлягають відповідальності» у відділі III «Про посягання на таємницю національної оборони» встановлено відповідальність за «знищення, розкрадання, вилучення або копіювання даних, що мають характер секретів національної оборони, що містяться в пам'яті ЕОМ або картотеках, а також ознайомлення з цими даними сторонніх» (ст.ст. 413-9, 413-10,

413-11) і передбачено покарання у вигляді трьох років позбавлення волі та штрафу у розмірі 45 000 євро або п'яти років позбавлення волі та штрафу у розмірі 75 000 євро.

Створена 2009 році Французька агенція безпеки інформаційних систем (ANSSI) є національним органом, який відповідає за кібербезпеку.

З метою протидії посяганням у сфері кіберпростору 22 грудня 2018 р. було ухвалено Закон № 2018-1202 про боротьбу з маніпулюванням інформацією, який дозволяє судді винести розпорядження про негайне видалення онлайн-статей, які, на його думку, є дезінформацією під час виборчих кампаній. Крім цього, Французьке агентство з національного мовлення має право призупиняти телевізійне мовлення каналів, що контролюються або знаходяться під впливом іноземної держави, якщо вони «навмисно поширюють неправдиву інформацію, яка може вплинути на щирість голосування». Цим же Законом також було відновлено ст. 112 законодавчої частини Виборчого кодексу, згідно з якою будь-яке порушення оператором обов'язків щодо надання відповідної інформації карається позбавленням волі на строк до одного року та штрафом у 75 000 євро [12].

Чільне місце серед європейських держав, що активно протидіють комп'ютерним злочинам з моменту їх появи в житті суспільства, займають ***Нідерланди***. В основі кіберстратегії Нідерландів лежать Національна стратегія кібербезпеки та Оборонна кіберстратегія [13].

З метою протидії комп'ютерним злочинам законодавець Нідерландів створив Консультативний комітет з комп'ютерних злочинів, який виробив конкретні рекомендації щодо внесення змін до Кримінального кодексу та Кримінально-процесуального кодексу Нідерландів. Консультативний комітет не дав визначення комп'ютерних злочинів, але розробив їх класифікацію.

В своїй діяльності поліцейське розвідувальне управління Нідерландів використовує для вивчення п'ять видів комп'ютерних злочинів: 1) скоєні звичайним способом, але з використанням технічної підтримки в комп'ютерному середовищі; 2) комп'ютерне шахрайство; 3) комп'ютерний терор (вчинення злочинів з метою пошкодження комп'ютерних систем): а) використання несанкціонованого доступу; б) використання шкідливих програм, типу комп'ютерних вірусів; в) вчинення інших дій, включаючи фізичне пошкодження комп'ютера; 4) крадіжка комп'ютерного забезпечення (піратство); 5) залишкова категорія, що включає всі інші типи злочинів, які не підпадають під перелічені категорії.

Так, відповідно до ст. 139c КК Нідерландів умисне з корисливою метою використання тією чи іншою особою технічних пристроїв для перехоплення або запису даних, що йдуть по телекомунікаційним системам або приєднаному обладнанню, карається штрафом або позбавленням волі на строк до 1 року. Крім того, особа, яка забезпечує інших суб'єктів засобами для незаконного перехоплення та запису даних, що передаються по автоматизованих або телекомунікаційних системах, підлягає покаранню у вигляді штрафу або позбавлення волі на строк до 6 місяців (ст. 139d). Зрештою, особа, яка володіє даними, про які вона знає або повинна знати, що вони отримані внаслідок незаконного прослуховування, запису або перехоплення даних автоматизованих або телекомунікаційних систем, також підлягає покаранню у вигляді штрафу або позбавлення волі на строк до 6 місяців (ст. 139e) [14].

В подальшому Кримінальний кодекс Нідерландів було доповнено новими складами: ст. 138a (1) «несанкціонований доступ до комп'ютерних мереж»; ст. 138a (2) «несанкціоноване копіювання даних»; ст. 350a (1), 350b (1) «комп'ютерний саботаж»; ст. 350a (3), 350b (2) «поширення вірусів»; ст. 273 (2) «комп'ютерне шпигунство».

Так, ст. 138a (1) «несанкціонований доступ до комп'ютерних мереж» розділу V «Злочини проти громадського порядку» КК Нідерландів передбачає відповідальність «особи, яка навмисно незаконно проникає в комп'ютерний пристрій або систему для зберігання і обробки даних, або в частину такого пристрою, або системи, винна в неправомірному вторгненні в комп'ютер». За вказане передбачене покарання у вигляді тюремного ув'язнення не більше шести місяців або штраф третьої категорії.

У ст. 138a (2) «несанкціоноване копіювання даних» розділу V «Злочини проти громадського порядку» встановлено відповідальність за «неправомірне проникнення в комп'ютер». Зокрема, копіювання даних, що зберігаються в комп'ютерному пристрої або системі, або запис таких даних для особистого використання або використання іншою особою, внаслідок незаконного проникнення, карається тюремним ув'язненням терміном не більше чотирьох років чи штрафом четвертої категорії.

Статті 350a (1), 350b (1) «комп'ютерний саботаж» включені до розділу XX VII «Знищення або заподіяння шкоди». У першому випадку, для «особи, яка навмисне та незаконно змінює, стирає, робить непридатною або недоступною інформацію, що зберігається, обробляється або передається за допомогою комп'ютерного пристрою або системи, чи вносить туди додаткові дані», передбачена відповідальність у вигляді ув'язнення не більше двох років або штраф четвертої категорії. У другому випадку для «особи, яка через недбалість чи необережність незаконно змінює, стирає, призводить до непридатного стану або робить недоступними дані, що зберігаються, обробляються або передаються за допомогою комп'ютерного пристрою чи системи, або вносить туди інші дані», і в разі спричинена цим даним серйозної шкоди, передбачена відповідальність у вигляді тюремного ув'язнення або ув'язнення на строк не більше одного місяця або штраф другої категорії.

Статтею 350a (3) передбачена відповідальність «особи, яка навмисне та незаконно робить доступними або поширює дані, які спрямовані на заподіяння шкоди шляхом копіювання в комп'ютерному пристрої або системі». За вказане посягання передбачене покарання у вигляді ув'язнення не більше чотирьох років або штраф п'ятої категорії. За ст. 350b (2) «особа, яка за недбалістю чи необережністю незаконно робить доступними або поширює дані, призначені для заподіяння шкоди шляхом копіювання у комп'ютерному пристрої або системі» карається тюремним ув'язненням або ув'язненням не більше одного місяця або штрафом другої категорії.

Таким чином, кримінальне законодавство Нідерландів надає досить широкі можливості для протидії різним видам комп'ютерних злочинів, встановлюючи крім спеціальних норм додаткові кваліфікуючі обставини вже існуючих кримінально-правових норм.

Законом про комп'ютерні злочини III (wet Computercriminaliteit III) 2019 р. надані нові повноваження поліції Нідерландів для посилення боротьби з комп'ютерними злочинами. Зокрема, правоохоронцям дозволено негласно здійснювати дистанційний доступ до персональних комп'ютерів, мобільних телефонів та серверів під час розслідування тяжких злочинів (дитяча порнографія, незаконний обіг наркотиків та ін.). Закон дозволяє поліції блокування доступу до певних даних, копіювання файлів, прослуховування каналів зв'язку та використання віртуальних особистостей (наприклад, підлітків) як «приманок» для виявлення та припинення злочинних дій [15].

Підсумовуючи аналіз кримінально-правових норм та заходів протидії комп'ютерним злочинам в країнах Європейського Союзу, слід зазначити, що, безумовно, підхід до криміналізації діянь, що посягають на інформаційну безпеку, у кримінальному законодавстві кожної держави не можна визнати ідентичним, він різний і у визначенні об'єкта злочину і видів діянь, у закріпленні способів вчинення таких посягань, та й заходів протидії їм.

Заслуговує на увагу позитивий досвід ряду держав Європейського Союзу щодо притягнення до відповідальності юридичних осіб за посягання на системи автоматизованої обробки даних.

ЛІТЕРАТУРА

1. Конвенція про кіберзлочинність, ухвалена Радою Європи 23 листопада 2001 р. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text (дата звернення: 10.08.2022).
2. Закон про комп'ютерні злочини (Швеція) від 2 квітня 1973. Сайт «Law Library of Congress» («Юридична бібліотека Конгресу США»). URL: http://www.loc.gov/law/help/guide/nations/sweden.php (дата звернення: 10.08.2022).
3. Закон про дані (Швеція) від 4 квітня 1973. Сайт «Law Library of Congress» («Юридична бібліотека Конгресу США»). URL: http://www.loc.gov/law/help/guide/nations/sweden.php (дата звернення: 10.08.2022).
4. The Swedish Criminal Code. Brottsbalk (1962:700). URL: https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/brottsbalk-1962700_sfs-1962-700. (дата звернення: 10.08.2022).
5. Cyber Security Strategy for Germany. URL: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Germancybersecuritystrategy20111.pdf. (дата звернення: 10.08.2022).
6. Hilgendorf, E., Valerius, B. (2022). Computer- und Internetstrafrecht. 3. Auflage.: Springer. Rund 250 S. Bibliographien.
7. Уголовное уложение (Уголовный кодекс) Федеративной Республики Германия: научно-практический комментарий и перевод текста закона. 2-е изд., перераб. и доп. Москва: Проспект, 2016. 312 с.
8. Закон про Федеральне управління кримінальної поліції від 1 червня 2017 р. URL: https://www.buzer.de/gesetz/4850/index.htm (дата звернення 20.07.22 р.).
9. Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (NetzDG). URL: https://www.gesetze-im-internet.de/netzdg/BJNR335210017.html (дата звернення: 10.08.2022).
10. French national digital security strategy. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/France_Cyber_Security_Strategy.pdf. (дата звернення: 10.08.2022).
11. Станіч В. С. Кримінальний кодекс Французької Республіки / під ред. В. Л. Менчинського. Переклад на українську мову – К. І. Мазуренко. К., 2017. 348 с.
12. LOI n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information. URL: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000037847559. (дата звернення: 10.08.2022).
13. The National Cyber Security Strategy 2 (NCSS2). URL: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS2Engelseversie.pdf. (дата звернення: 10.08.2022).
14. Уголовный кодекс Голландии. Пер. с англ. И.В. Мироновой. 2-е изд. СПб.: Изд-во «Юридический центр Пресс», 2001. 510 с.
15. Wet Computercriminaliteit III. URL: https://www.openrecht.nl/commentaar/a8d9faae-6c8f-400c-b156-ad17c7a67848/. (дата звернення: 10.08.2022).