

УДК 351.745.7:343.9:343.352

DOI <https://doi.org/10.32782/ln.2025.25.37>**РЕГУЛЮВАННЯ ВІДПОВІДАЛЬНОСТІ ЗА ПРАВОПОРУШЕННЯ,
ВЧИНЕНІ ЕЛЕКТРОННИМИ ПЛАТІЖНИМИ ЗАСОБАМИ,
В ЗАКОНОДАВСТВІ РОМАНО-ГЕРМАНСЬКІЙ ПРАВОВІЙ СІМ'І****Кулик А.В.***аспірантка кафедри кримінального права**Національного університету «Одеська юридична академія»*

Популярною є ідея Р. Давида щодо класифікації правових сімей (систем) та їх місця на правовій карті світу, згідно якої пропонується виділяти дві правові сім'ї: романо-германську (систему континентального права), до якої належать багато європейських країн, зокрема України, Німеччина, Франція, Нідерланди, Іспанія, Швейцарія, Австрія та англо-американську (англосаксонське право) сім'ю (систему загального права), до якої належать США, Велика Британія та Канада [1, с. 163].

Історичні джерела вказують на те, що романо-германська правова сім'я включає державні системи, що походять з держав континентальної Європи. Ця правова сім'я має специфіку, пов'язану з існуванням кодифікованих актів провідних галузей матеріального і процесуального права (кримінального, цивільного); з диференціацією матеріального права на приватне і публічне, з викладенням принципу примату матеріального права над процесуальним. Основним джерелом закону, що діє в романо-германській правовій сім'ї, визнається закон, який не прирівнюється до закону, а як порядок, заснований на суворому і послідовному дотриманні вимог, що містяться в законі, ніколи не вважався синонімом правоохоронної діяльності.

Основні принципи побудови романо-германської правової сім'ї базуються на кримінальному законодавстві, яке також включає кіберзлочинність. У доповіді Ради Європи з актуальних питань у сфері кіберзлочинності загалом та її диференціації, сформованій згідно з Конвенцією про злочини у сфері

комп'ютерної інформації (ETS 185) [2], цей вид кримінального правопорушення позначено як «СІА-правопорушення», тобто діяння, вчинені проти конфіденційності (Confidentiality), цілісності (Integrity) і доступності (Availability) комп'ютерних даних, інноваційних систем. Перераховано види кримінальних правопорушень, що входять до категорії кіберзлочинності: хакерство, перехоплення повідомлень, обман користувачів інтернету (тобто через спуфінг, фішинг), комп'ютерне шпигунство (наприклад, з використанням троянських коней та інших подібних технологій), комп'ютерний саботаж і вимагання (тобто використання вірусів і хробаків, DOSattacks, спам і поштові бомбардування).

Питання протидії таким кримінальним правопорушенням мають особливе значення в усіх країнах романо-германської правової сім'ї. Незважаючи на розбіжності в позиції законодавців щодо криміналізації діянь, вчинених з використанням інформаційно-комунікаційних технологій, у всіх цивілізованих країнах посягання на власність розглядаються як такі, що підривають основи держави, а захист від таких посягань є одним з найважливіших суспільних обов'язків. У зв'язку з цим кримінальні кодекси більшості держав романо-германської правової сім'ї містять заборони: комп'ютерного шахрайства; крадіжки комп'ютера; отримання інформації, що становить комерційну та банківську таємницю, шляхом незаконного доступу до комп'ютерної інформації (комерційна справа, банківське шпигунство); комп'ютерне вимагання.

На сучасному етапі такі протиправні посягання спрямовані проти відносин власності, завдаючи значної шкоди соціально-економічній сфері різних країн та окремих громадян. Еволюція законодавства в зарубіжних країнах показує, що перший крок до кримінально-правового захисту комп'ютерної інформації, розвиток кримінального права для протидії економічній кіберзлочинності зроблено законодавцем Швеції з прийняттям Закону про комп'ютерні злочини (1973) [3]. Цим нормативно-правовим актом передбачена кримінальна відповідальність: за незаконне проникнення в систему комп'ютерної мережі; за введення в комп'ютерну інформаційну дезінформацію; за вчинення крадіжок таких об'єктів, як гроші (електронні), та цінні папери, інші активи та інші, включаючи послуги та інформацію, цінні для певних кіл. Закон про дані (1974) [4] ввів у кримінальне право категорію «computer abus». На початку 1990-х років у зв'язку з посиленням кіберзлочинності Кримінальний кодекс Швеції [5] був одним із перших, який був доповнений положеннями, що передбачають кримінальну відповідальність за кримінальні правопорушення, вчинені з використанням комп'ютерної інформації та інформаційних технологій: за шахрайство, вчинене шляхом надання неповної або неправдивої інформації, або внесення коригувань до комп'ютерної програми чи звіту. Також необхідно вказати діяння, здійснене протиправним впливом, на прямий результат автоматичної обробки комп'ютерної інформації, інше ідентичне поводження, яке призвело до вигоди для суб'єкта кримінального правопорушення та збитку для потерпілого. Ця сукупність доповнюється: правопорушеннями, пов'язаними з поштовою або комунікаційною таємницею; використання технічних механізмів з наміром неправомірного впливу на телекомунікаційну таємницю; незаконний доступ до процесів обробки комп'ютерних даних; незаконне виправлення, видалення, додавання певного запису до реєстру даних; деякі інші.

Кримінальний кодекс Швеції в п. 4 гл. 8 «Про крадіжку, розбій та інші злочини, пов'язані з крадіжкою майна», регулює умови, згідно з якими крадіжка визнається великим, тобто більш тяжким кримінальним правопорушенням. Цей факт має особливе значення у зв'язку з розвитком інформаційних технологій: з 2012 року в Швеції активно використовується мобільний додаток Swish для Android, інші операційні системи, які встановлюються на мобільний телефон і використовуються як термінал, відповідний рахунок в банку з мобільним телефоном, що дозволяє здійснити миттєвий платіж, вказавши будь-яку зареєстровану ID-систему або номер телефону [5]. Відповідно, крадіжка мобільного телефону може сприяти крадіжці з банківського рахунку, а також електронних коштів і кваліфікуватися як крадіжка на підставі п. 4 гл. 8 «Про крадіжку, пограбування та інші злочини, пов'язані з крадіжкою майна».

У Кримінальному кодексі Нідерландів [6] законодавець групує кримінальні правопорушення де обман як спосіб вчинення злочину, присвячуючи цим діям окремий розділ XXV Кримінального кодексу «Desertion», що складається з 18 статей. Відповідно до вказаних норм за таке діяння кримінальну відповідальність несуть суб'єкти, які з метою незаконного отримання доходу для себе або для інших осіб шляхом присвоєння неправдивого імені, або шляхом неправдивих відомостей, спонукають потерпілого відмовитися від об'єкта права власності, подати відомості про гроші, прийняти боргові зобов'язання або відмовитися від поданих вимог. Це положення Кримінального кодексу поширюється на шахрайство, вчинене з використанням платіжної картки. В окремих правилах Кодексу, які передбачають відповідальність за діяння традиційного характеру на кшталт вимагання та крадіжки, вчинені шляхом обману, у зв'язку з розвитком високих технологій, до відповідальності за діяння, проникнення комп'ютерної інформації, що міститься в електронних системах, у тому числі електронних платіжних засо-

бах, внесено доповнення, тобто це стосується і платіжних карток.

Кримінальний кодекс Іспанії [7], структурно складається з трьох окремих книг, у книзі II містить розділ XIII «Злочини проти власності та соціально-економічної діяльності». Кримінальний кодекс позначає просте шахрайство, шахрайство в сфері електропостачання, в сфері кредиту, арешт майна шляхом обману комп'ютерними програмами, кредитними картками, чеками. Відповідно до ст. 253 КК Іспанія, кримінальну відповідальність несе особа, яка з метою отримання прибутку привласнює втрачений об'єкт або об'єкт, власник якого невідомий на момент вчинення кримінального правопорушення – відповідно, крадіжка платіжної картки підлягає кваліфікації за цією нормою кримінального права.

У Німеччині кримінально-правова система визнана досить складною та різноманітною через численні та різноманітні джерела цієї галузі правової системи. Кримінальний кодекс Німеччини, незважаючи на відсутність визначення «кримінальне покарання», визначеного в доктрині як справедлива компенсація за вину (Debt Compensation), як особливий державний засіб для запобігання кримінального правопорушення та компенсації потерпілому [8], приділяє особливу увагу кримінальним правопорушенням, вчиненим у сфері інформаційно-комунікаційних технологій, тобто економічної кіберзлочинності. Цей кодифікований акт у розділі 22 Спеціальної частини CC Germany «Шахрайство та зловживання довірою» містить окремі правила, що передбачають відповідальність за різні види шахрайства та зловживання довірою (§ 263а «Комп'ютерне шахрайство», § 264а «Інвестиційне шахрайство», § 265 «Страхове зловживання», § 265а «Отримання послуг шляхом шахрайства», § 266 «Порушення довіри», § 266а «Втрата та крадіжка заробітної плати», § 266b «Зловживання чеками та кредитними картками»), фундаментальні основи яких містяться в положеннях § 263 Кримінального кодексу Німеччини «Шахрайство». Відповідно до § 263 CC Німеччини, «Будь-хто, хто, маючи

намір отримати для себе або третьої особи незаконну майнову вигоду, завдає шкоди майну іншої особи, ввівши в оману або підтвердивши це непорозуміння, свідомо виклавши неправдиві факти або спотворивши чи приховавши правдиві факти, карається...». Точкою припинення правопорушення є точка, в якій завдано шкоди майну потерпілого, а не точка, в якій збагачується винний або інша третя особа. Шкода виникає лише тоді, коли або частина майна потерпілого вилучена, або шкода обтяжена зобов'язаннями і таким чином знижує вартість такого майна в цілому [8].

Як засіб вчинення діяння це положення Кримінального кодексу Німеччини передбачає обман. Базуючись на законодавчому плані шахрайства, багато видів таких злочинів (§ 263а «Computer fraud», § 266b «Зловживання чеками та кредитними картками») і нові правопорушення, що охоплюють найнебезпечніші дії, що посилюються в інформаційній сфері, комунікаційні технології (§202-а «Дії, спрямовані на отримання інформації», § 303-а «Computer sabotage» і § 269 «Фальсифікація даних, що мають доказову силу») включені законодавцем до Кримінального кодексу такими законами: від 15 травня 1985 року Другий закон «Про боротьбу з економічною злочинністю» [9] та від 22 грудня 2003 року; Тридцять п'ятий Закон про зміни в кримінальному законодавстві [9]. Стаття 263а Кримінального кодексу Німеччини, яка передбачає кримінальну відповідальність за комп'ютерне шахрайство, передбачає, що той, хто діє з метою отримання для себе або третьої особи незаконної майнової вигоди і тим самим завдає шкоди майну іншої особи, впливаючи на результат обробки комп'ютерних даних, виробляючи неправильні програми з використанням неправильних або неповних даних, Зловживання даними або вплив на такий процес будь-якими іншими неналежними діями караються позбавленням волі на строк до п'яти років або штрафом. Це діяння є найнебезпечнішим в системі комп'ютерних кримінальних правопорушень.

Винуватцем є особа, яка завдала шкоди своєму майну з метою отримання матеріальної вигоди як собі, так і іншій особі, вплинула на результати обробки даних шляхом створення неправильних комп'ютерних програм, будь-якого іншого протиправного впливу на результат обробки: введення недостовірних, неповних даних у комп'ютер, неправомірне використання даних або навмисне, переважний вплив на процес обробки. Спосіб вчинення діяння – це не обман, а негативний інформаційний ефект: у першому випадку він впливає на особу (жертву, іншу пов'язану особу), у другому – процес обробки даних, вироблених комп'ютерними технологіями. Відповідно до § 266b КК Німеччини «Зловживання чеком і кредитними картками» передбачає кримінальну відповідальність за зловживання довірою кредитної організації, яка видала чек або кредитну картку, яка надається особі, яка отримала таку картку на законних підставах. Виходячи із законодавчої структури цього правила, «Кожен, хто зловживає можливостями, наданими йому чеком або кредитною картою, і змушує власника картки здійснити платіж, завдаючи йому шкоди, карається позбавленням волі на строк до трьох років або грошовим штрафом». При вчиненні шахрайства особа зловживає довірою банку-емітента платіжних карток, використовуючи в обігу суми, більші за довірені їй [8]. Таке посягання спрямоване на заподіяння шкоди охоронюваному благу – майну, сприяючи виникненню негативних правових наслідків.

Однак Кримінальний кодекс Німеччини розрізняє кримінальні правопорушення, вчинені у сфері комп'ютерного шахрайства, у сфері незаконних дій із чеками та кредитними картками, та дії майнового характеру, вчинені шляхом обману, а також зловживання довірою, визначаючи ці злочини в окремому абзаці національного кодифікованого джерела права. Цим посяганням приділяється особлива увага в нормативно-правових актах інших держав романо-германської правової сім'ї.

Кримінальний кодекс Франції 1992 року змінив систему юридичної відповідальності за кримінальні правопорушення проти власності, розрізняючи форми посягань, створюючи ознаки таких посягань і посилюючи покарання за дії та правопорушення [10]. Французьке законодавство, що регулює просту крадіжку та крадіжку при обтяжуючих обставинах (том. I Книга III Кримінального кодексу Франції), передбачаючи кваліфікацію діянь, не включає в себе диференціацію крадіжки з банківського рахунку, а також щодо електронних коштів. Кримінальний кодекс Франції містить окремі положення про кримінальну відповідальність за кримінальні правопорушення у сфері інформаційно-комунікаційних технологій. Кримінальний кодекс Франції, який не містить конкретних правових положень щодо розкрадання або розкрадання електронних коштів, відповідно передбачає кримінальний захист як персональних даних і телекомунікаційних систем, криміналізує шахрайські дії, які можуть бути вчинені проти електронних грошей.

Питання кримінальної відповідальності у зв'язку з крадіжкою електронних коштів вирішуються у Франції на рівні спеціального нормативно-правового акту – Закону 91-1383 «Про безпеку чеків і платіжних карток», який передбачає кримінальну відповідальність за такий вид шахрайства: за підробку, модифікацію та свідоме використання платіжної картки, за свідоме волевиявлення прийняти неналежну оплату такою картою. При цьому дане джерело права держателю платіжної картки (до моменту повідомлення про втрату або крадіжку) несе кримінальну відповідальність за збитки, завдані їй несанкціонованим використанням (до 150 євро). Однак таке правило не застосовується у разі недбалості, грубої помилки власника платіжної картки, а також за відсутності повідомлення про блокування картки [11].

Країни Балтії, які належать до романо-германської правової сім'ї, приєдналися до Європейського Союзу (ЄС) у 2004 році під

час великого п'ятого розширення інтеграційної групи за рахунок Східної Європи. Процес політичної інтеграції країн Балтії реалізовувався через комплекс економічних і правових заходів, тобто в рамках протидії кіберзлочинності. Ці держави у 2001 році ратифікували Конвенцію про комп'ютерну інформаційну злочинність (ETS 185) (Конвенція про кіберзлочинність CETS) [2], встановила кримінальну відповідальність за кіберзлочини та інші злочинні дії, пов'язані з торгівлею електронними платіжними засобами (шахрайство). Інформація в країнах Балтії, як і в усьому цивілізованому світі, є ключовою складовою розвитку суспільства, але злочинці вміло користуються недоліками безпеки у використанні сучасних засобів комунікації, Інтернету, кіберзлочинності, які завдають шкоди суспільству та громадянам.

В Естонській Республіці кримінальна відповідальність за шахрайство регулюється положеннями Пенітенціарного кодексу 20 у підрозділі 1 «Fraud» розділу 2 «Кримінальні дії проти власності в цілому» (ст. 210-213 ПК Естонія). с 209 CC Estonia розкриває визначення загального шахрайства як «заподіяння майнової шкоди іншій особі шляхом створення завідомо хибного уявлення про фактичні обставини з метою отримання майнової вигоди». Законодавець Естонської Республіки розрізняє шляхом диференціації спеціальні види шахрайства: шахрайство з виплатами (с 210), шахрайство з інвестиціями (с 211), шахрайство зі страхуванням (с 212) та комп'ютерне шахрайство (ст. 213). Ця категорія визначається як «заподіяння майнової шкоди іншій особі шляхом незаконного введення, зміни, видалення, пошкодження, блокування комп'ютерних програм, даних, шляхом незаконного втручання в процес обробки даних іншим способом з метою отримання майнової вигоди» (ст. 213) [12]. Водночас Кримінальний кодекс не передбачає кримінально-правових норм про розкрадання іноземного майна, набуття права на таке майно, встановлення кримінальної відповідальності

за заподіяння майнової шкоди чи отримання майнової вигоди [13].

Латвійський законодавець (ст. 177.1 УК21), подібно до позиції Естонії (с 213 Кримінального кодексу Естонії), встановлює кримінальну відповідальність за комп'ютерне шахрайство як кримінальне правопорушення, вчинене шляхом свідомого введення неточної інформації в автоматизовану систему обробки даних (незаконне втручання в процес обробки) [14].

Кримінальний кодекс Литовської Республіки 22 у розділі XVIII «Злочини проти власності» норми, в яких передбачена кримінальна відповідальність за умисне посягання на майно або майнові права чи обов'язки шляхом введення неправдивих даних в автоматизовану систему обробки даних. Кримінальна відповідальність за незаконне використання електронних платіжних засобів встановлюється в гл. XXXII Кримінальний кодекс Литви «Злочини та кримінальні злочини проти фінансової системи», де встановлено кримінальну відповідальність за завідомо незаконне використання платіжних засобів, за незаконну передачу його ідентифікаційних даних, за використання автентичних і шахрайських ідентифікаційних даних при ініціюванні, при здійсненні фінансової операції електронними платіжними засобами, Кримінальний кодекс Литовської Республіки передбачає шахрайство в с 182 гл. XXVII «Злочини та кримінальні злочини проти власності, майнових прав та майнових інтересів». Під шахрайством литовський законодавець, як і в Кримінальному кодексі Латвії, передбачав придбання іноземного майна, прав на таке майно шляхом зловживання довірою, обману (ст. 177 КК Латвії, 182 КК Литви), ухилення від майнового зобов'язання, його скасування (ст. 182 КК Литви) [15]. Таким чином, розвиток суспільства в нинішній період пов'язаний з цифровізацією майже всіх сфер життя в усіх цивілізованих країнах.

Таким чином, кіберзлочинності приділяється особлива увага в усьому світовому

співтоваристві. На офіційному сайті Міжнародного валютного фонду (МВФ), спеціалізованої організації ООН розміщується статистична інформація, шляхи вирішення найактуальніших проблем, пов'язаних з розкраданням з використанням ІТ-технології, легалізацією доходів, одержаних злочинним шляхом, як протиправними діями, спрямованими на приховування джерела походження коштів і надання юридичної форми доходам, одержаним злочинним шляхом. В результаті правопорушники вкладають гроші в різні кримінальні сфери суспільства, завдають шкоди державі, всьому світовому співтовариству і глобальним фінансовим системам, підриваючи тим самим економіку, валюти і міжнародну безпеку. Цими актуальними питаннями активно займається міжнародна організація «Positive Technologies», європейський лідер у цій галузі, у тому числі розробка алгоритму дій уповноважених органів у сфері запобі-

гання цим видам злочинних діянь, виконання багаторівневого аналізу необхідної безпеки відповідних систем, їх відповідності визначеним стандартам захисту. Експерти цієї організації стверджують, що на загальну статистику таких кримінальних правопорушень впливає сукупність факторів, які повинні дозволити сформувати новий алгоритм дій щодо запобігання злочинності. По-перше, в інформаційному просторі спостерігається збільшення кількості фахівців, що належать до злочинних кібергруп, з високим рівнем кваліфікації, а також мають значне технологічне оснащення і, по-друге, державна політика в галузі інформаційної безпеки вимагає прогресивних правових та інших контрзаходів, спрямованих на посилення контрзаходів щодо виявлення, попередження, попередження та локалізації злочинності, в тому числі, комп'ютерного шахрайства, протиправних посягань з використанням електронних платіжних засобів.

Анотація

Статтю присвячено дослідженню регулювання кримінальної відповідальності за правопорушення, вчинені з використанням електронних платіжних засобів, що відносяться до корисливої кіберзлочинності, в законодавстві окремих іноземних держав романо-германської правової сім'ї. У статті зазначається, що романо-германська правова сім'я істотно відрізняється від інших тільки тим, що має в силу історичних традицій багато рис права давньоримської юриспруденції, але й правові особливості кримінального законодавства щодо кіберзлочинності. Актуальним є питання кіберзлочинності, її диференціація на основі Конвенції про комп'ютерні злочини (ETS 185), а також спеціальні кримінальні положення, що регулюють правопорушення, вчинені за допомогою електронних платіжних засобів у Швеції, Німеччині, Франції, Іспанії, Нідерландах, в країнах Балтії. Вказано, що питання про такі кримінальні правопорушення мають особливе значення в усіх країнах романо-германської правової сім'ї. Незважаючи на розбіжності в позиції законодавців щодо криміналізації діянь, пов'язаних з електронними платіжними засобами, в усіх країнах посягання на майно вважається посяганням на основи держави, і захист від такого посягання визначається як одна з найважливіших державних функцій.

Зазначено, що незважаючи на розбіжності в позиції законодавців щодо криміналізації діянь, вчинених з використанням інформаційно-комунікаційних технологій, у всіх цивілізованих країнах посягання на власність розглядаються як такі, що підривають основи держави, а захист від таких посягань є одним з найважливіших суспільних обов'язків. У зв'язку з цим кримінальні кодекси більшості держав романо-германської правової сім'ї містять заборони: комп'ютерного шахрайства; крадіжки комп'ютера; отримання інформації, що становить комерційну та банківську таємницю, шляхом незаконного доступу до комп'ютерної інформації (комерційна справа, банківське шпигунство); комп'ютерне вимагання.

Ключові слова: романо-германська правова сім'я, злочинність, кіберзлочинність, шахрайство, обман, крадіжка, комп'ютерна інформація, кримінальне законодавство, кримінальна відповідальність, кримінальне правопорушення.

Kulyk A.V. Regulation of liability for violations committed by electronic means of payment in the legislation of the romano-germanic legal system

Summary

The article is devoted to the study of the regulation of criminal liability for crimes committed using electronic means of payment related to cybercrime in the legislation of certain foreign countries of the Romano-Germanic legal family. The article notes that the Romano-German legal system is significantly distinguished from other families not only by the fact that it possesses, due to historical traditions, many characteristics of the law of ancient Roman jurisprudence, but also by the legal peculiarities of criminal legislation on cybercrime. The relevance of cybercrime, its differentiation based on the Convention on Crime in the Field of Computer Information (ETS № 185) and the peculiarities of the criminal regulation of crimes committed using electronic means of payment in Sweden, France, Germany, Spain, Netherlands, China and the Baltic States are noted. It is pointed out that the issues of combating such crimes are of particular importance in all countries of the Romano-Germanic legal family. Despite differences in the position of legislators with regard to the criminalization of acts committed by electronic means of payment, in all countries attacks on property are considered as attacks on the foundations of the State, and protection against such attacks is one of the most important State functions.

It is noted that despite the differences in the position of legislators regarding the criminalization of acts committed using information and communication technologies, in all civilized countries encroachments on property are considered as undermining the foundations of the state, and protection against such encroachments is one of the most important social duties. In this regard, the criminal codes of most states of the Romano-Germanic legal family contain prohibitions: computer fraud; computer theft; obtaining information constituting commercial and banking secrets through illegal access to computer information (commercial business, bank espionage); computer extortion.

Key words: Romano-Germanic legal family, crime, cybercrime, fraud, deception, theft, computer information, criminal law, criminal liability, criminal offence.

Список використаних джерел:

1. David R. Les grands systems de droit contemporains (Droit comparé). Paris: Dalloz, 1964. P. 133
2. Конвенція про злочини у сфері комп'ютерної інформації (ETS 185). URL: https://zakon.rada.gov.ua/laws/show/994_575#Text
3. 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>
4. 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>
5. The Swedish Criminal Code. Brottsbalk (1962:700). URL: https://www.riksdagen.se/sv/dokument-lagar/dokument/svenskforfattningssamling/brottsbalk-1962700_sfs-1962-700
6. Кримінальний кодекс Нідерландів від 03.03.1881 р. станом на 28.02.2024 р. URL: <https://wetten.overheid.nl/BWBR0001854/2024-01-01>
7. Кримінальний кодекс Іспанії від 24.05.1996 р. станом на 28.02.2024 р. URL: <https://www.boe.es/buscar/act.php?id=BOE-A-1995-25444>

8. Кримінальний кодекс Німеччини від 23.01.1974 р. станом на 28.02.2024. Федеральний вісник законів. № 60, 1974 р. URL: <https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10002296>
9. Hilgendorf, E., Valerius, B. (2022). Computer– und Internetstrafrecht. 3. Auflage.: Springer. Rund 250 S. Bibliographien
10. Кримінальний кодекс Франції від 22.07.1992 р станом на 28.01.2024 р. URL: https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006070719/LEGI_SCTA000006117598/#LEGISCTA000006117598
11. French national digital security strategy. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/France_Cyber_Security_Strategy.pdf
12. Пенітенціарний кодекс Естонської Республіки. URL: <https://www.juristaitab.ee/sites/default/files/seaduste-tolked/пенитенциарный%20кодекс%2001.01.2024.pdf>
13. Кримінальний кодекс Естонської Республіки. URL: <https://www.wipo.int/wipolex/ru/legislation/details/16677>
14. Кримінальний кодекс Латвійської республіки від 08.07.1998 р. станом на 28.02.2024 р. URL: <https://likumi.lv/ta/id/318953-latvijaskriminalkodekss>
15. Кримінальний кодекс Литовської Республіки / переклад К. В. Менченя; під ред. О. В. Коротюк. К. : ОВК, 2021. 158 с.