

DOI: [https://doi.org/10.26642/jen-2024-4\(110\)-125-144](https://doi.org/10.26642/jen-2024-4(110)-125-144)
УДК 321:004.056:007(061.1ЄС)

Д.О. Грицишен, д.е.н., д.н.держ.упр., проф.
С.І. Соха, к.ю.н., докторант
С.В. Корзун, аспірантка
Державний університет «Житомирська політехніка»

Удосконалення державної політики протидії кіберзлочинності на основі досвіду країн Європейського Союзу

У статті здійснено аналіз кримінальних кодексів деяких країн Європейського Союзу, а саме: Республіки Польща, Республіки Болгарія, Чеської Республіки, Литовської Республіки. Досвід цих країн для України є принципово важливим, адже вони також перебували під радянським окупаційним режимом. Детально проаналізовано тенеу формування кримінальної системи в Республіці Польща в цілому та визначено відповідальність за кіберзлочини зокрема. Досліджено історичні віхи формування системи кримінального права в Чеській Республіці, починаючи з часів Середньовіччя і до сьогодення. Досвід Болгарії у встановленні кримінальної відповідальності за кіберзлочини комплексно проаналізований у контексті дослідження Кримінального кодексу, де особлива увага зосереджена на розгляді обтяжуючих обставин, що є дуже важливим при необхідності протидії гібридним війнам та інформаційного захисту критичної інфраструктури. Проаналізувавши Кримінальний кодекс Литовської Республіки, зосереджено увагу на різноманітності покарань за кіберзлочини. Крім того, відмінністю литовського законодавства є наявність кримінальної відповідальності юридичних осіб.

У результаті наукового дослідження було визначено основні історичні етапи формування політики протидії кіберзлочинності Республіки Польща, Республіки Болгарія, Чеської Республіки, Литовської Республіки. Здійснено комплексний аналіз основних нормативних документів, що встановлюють кримінальну відповідальність за злочини, пов'язані з кіберзлочинністю, та визначено відмінні особливості кожної з країн. Доведено, що під час реформування кримінального законодавства в Україні в контексті євроінтеграційних процесів є нагальна потреба у врахуванні досвіду європейських країн, однак варто враховувати специфічні особливості кримінального права визначених країн, а тому підходити до цього процесу поступово та вибірково.

Ключові слова: державна політика; протидія кіберзлочинності; кіберпростір; кримінальна відповідальність.

Актуальність теми. Забезпечення ефективних процесів європейської інтеграції неможливе без вивчення досвіду країн-членів у формуванні та реалізації різних видів політик, особливо тих, що визначають певний рівень безпеки держави. «Масштаби кібератак є проблемою для національної безпеки держав та їхньої внутрішньої стабільності. За даними Pew Research Center, у 2018 р. кібератаки на міжнародному рівні посіли третє місце серед глобальних загроз. Масштаби проблеми засвідчує динаміка заражень шкідливим програмним забезпеченням, що є найбільш поширеним видом кіберзлочинів» [5]. Україна не може бути поза межами міжнародної системи інформаційної безпеки, а в контексті обрання євроінтеграційного шляху має відповідати певним нормам Європейського Союзу. Зазначимо, що кожна країна обирає власні інструменти відповідності вимогам Європейського Союзу, а тому врахування їх досвіду під час формування вітчизняної політики протидії кіберзлочинності є вкрай важливим.

Аналіз останніх досліджень. Питання трансформації державної політики в сфері протидії різним видам злочинів, правоохоронної діяльності та інформаційної безпеки порушувалися в працях таких вітчизняних вчених, як: О.М. Бодунова, Т.А. Білобров, Т.В. Барановська, Д.О. Грицишен, А.П. Дикий, М.О. Думчиков, В.В. Євдокимов, М.М. Забарний, О.С. Кушнерьов, К.В. Малишев, О.І. Миргородський, Е.В. Малютін, В.В. Нонік, С.О. Перхун, В.В. Сисолятин, І.В. Супрунова, Б.Б. Теплицький, М.Ю. Яцишин. Незважаючи на значні досягнення вітчизняних вчених у цьому напрямі, залишилося багато невирішених проблемних питань, які стосуються в першу чергу обрання власної моделі інтеграції в європейський правовий простір, адже, незважаючи на спільне законодавство Європейського Союзу, кожна країна обирає свою правову модель.

Викладення основного матеріалу. В цьому дослідженні приділимо увагу країнам, що вже є членами Європейського Союзу відносно недавно, а також мають з Україною спільне минуле, зокрема перебували під окупацією Радянського Союзу. Отже, здійснимо аналіз кримінальних кодексів Республіки Польща, Республіки Болгарія, Чеської Республіки, Литовської Республіки.

Республіка Польща. «Перший сучасний Кримінальний кодекс Польщі (ККП) діяв із 1932 р. Він був першим європейським кримінальним кодексом міжвоєнної доби і вважався найпрогресивнішим у Європі. Саме цей нормативно-правовий акт заклав прогресивні європейські тенденції кримінального

законотворення і став важливим кроком для створення сучасної Польщі – правової європейської держави. Наступним був ККП 1969 р., що також взяв за основу положення класичної і соціологічної шкіл кримінального права, серед яких: принцип рівності всіх перед законом, гуманізму, індивідуалізації кримінальної відповідальності та багато інших. Цей кримінальний кодекс набув чинності 1970 р. У 1971 р. були прийняті Кодекс про проступки і Кодекс про провадження у справах про проступки. Із 1982 р. діяв Закон про провадження у справах неповнолітніх. Це був загальний вигляд кримінального законодавства Польщі до 1997 р. Із 1987 р. у Польщі відбувалася кодифікація права, яка закінчилася через 10 років. Вона усунула багато недоліків і вплинула на розв'язання питань, які раніше не були регламентовані [1]. Це своєю чергою вплинуло на сучасний кримінальний Кодекс Республіки Польща.

«Визначально на історію становлення держави Республіки Польща вплинула зміна устрою держави, а, відповідно, і зміна кримінального права та карної політики. Кримінальне право Республіки Польща зазнало нових реформ, що обумовило прийняття 6 червня 1997 р. нового Кримінального кодексу. Того ж дня було прийнято також Кримінально-процесуальний та Кримінально-виконавчий кодекси, які остаточно набули чинності 1 вересня 1998 р.» [2].

Особливістю Кримінального Кодексу Республіки Польща [8; 10] є три розділи, а саме: загальна частина, особлива частина та військова частина. В контексті об'єктно-предметного поля цього дослідження особлива частина передбачає кримінальну відповідальність за такі види злочинів: злочини проти миру, людства та військові злочини; злочини проти Республіки Польща; злочини проти оборони; злочини проти життя і здоров'я; злочини проти суспільної безпеки; злочини проти безпеки дорожнього руху; злочини проти навколишнього середовища; злочини проти свободи; злочини проти свободи совісті та віросповідання; злочини проти статевої свободи і моральності; злочини проти сім'ї та опіки; злочини проти гідності та тілесної недоторканості; злочини проти прав людей, виконуючих оплачувану працю; злочини проти діяльності державних установ і органів місцевого самоврядування; злочини проти здійснення правосуддя; злочини проти виборів та референдуму; злочини проти публічного порядку; злочини проти охорони інформації; злочини проти достовірності документів; злочини проти власності; злочини проти господарського обороту; злочини проти обігу грошових коштів та цінних паперів. Особливістю зазначеного нормативного документа є особлива побудова, а саме встановлення особи, яка вчинила чи не вчинила певні дії.

Питання встановлення кримінальної відповідальності розглядається у Розділі XXXIII – Злочини проти охорони інформації [8; 10], яким передбачено такі види злочинів:

- розголошення або всупереч закону використання закритої інформації, що відноситься до «таємної» або «абсолютно таємної» (ст. 265, § 1);
- неумисне розповсюдження інформації, що відноситься до «таємної» або «абсолютно таємної», яка стала відома у зв'язку з виконанням публічних функцій чи отриманими уповноваженнями (ст. 265, § 1);
- розкриття чи використання інформації всупереч приписам закону або прийнятим на себе зобов'язанням, яку особа дізналася у зв'язку з виконуваними функціями, виконуваною роботою, публічною, соціальною, господарською чи науковою діяльністю (ст. 266, § 1);
- розкриття посадовою особою неповноважній особі інформації, що не підлягає розголошенню як «обмежена» або «конфіденційна», чи інформації, яку отримала у зв'язку з виконанням службових обов'язків та розкриття якої може завдати шкоди охоронюваним законом інтересам (ст. 266, § 2);
- отримання доступу до інформації без повноважень, що для особи не призначена, відкриття закритих листів, підключившись до телекомунікаційної мережі або зламавши чи оминувши електричний, магнітний, інформаційний або інший спеціальний її захист (ст. 267, § 1);
- отримання доступу до частини або до всієї інформаційної системи без повноважень, що для особи не призначена (ст. 267, § 2);
- підкладання або використання підслуховуючого, візуального пристрою або іншого пристрою чи програмування, з метою отримання інформації, для отримання якої не має повноважень (ст. 267, § 3);
- знищення, пошкодження, відміна чи зміна запису важливої інформації або в інший спосіб розладнання чи ускладнення доступ до неї для особи, яка має повноваження на ознайомлення з такою інформацією, особою, що немає на це повноваження (ст. 268, § 1);
- знищення, пошкодження, відміна чи зміна запису важливої інформації на інформаційному носії даних або в інший спосіб розладнання чи ускладнення доступ до неї для особи, яка має повноваження на ознайомлення з такою інформацією, особою, що не має на це повноваження (ст. 268, § 2);
- знищення, пошкодження, відміна, зміна або ускладнення доступу до інформаційних даних або істотним чином порушення чи унеможливлення автоматичної обробки, накопичення чи передачі таких даних, особою без повноважень на такі дії (ст. 268 а);
- знищення, пошкодження, відміна або зміна інформаційних даних, що мають спеціальне значення для оборони держави, безпеки комунікації, функціонування урядової адміністрації, іншого державного органу або державної інституції, або територіального органу місцевого самоврядування чи закладу, або унеможливує автоматичну обробку, накопичення чи передачу таких даних (ст. 269, § 1);

– знищення або заміна інформаційного носія даних, або знищення чи пошкодження пристрою, що слугує для автоматичної обробки, накопичення чи передачі інформаційних даних (ст. 269, § 1);

– порушення роботи комп'ютерної системи або телекомунікаційної мережі особою, яка не має таких повноважень, шляхом передачі, знищення, відміни, пошкодження, ускладнення доступу або зміни інформаційних даних істотним чином (ст. 269 а);

– виробництво, придбання, збут чи забезпечення інших осіб пристроями або комп'ютерними програмами, пристосованими для вчинення злочину комп'ютерними паролями, кодами доступу чи іншими відомостями, що уможливають доступ до інформації, яка зберігається в комп'ютерній системі чи телекомунікаційній мережі (ст. 269 б).

На відміну від Кримінального Кодексу Грузії, Республіки Узбекистан та Республіки Таджикистан, Кримінальним Кодексом Республіки Польща передбачено кримінальну відповідальність саме за злочини, пов'язані зі створенням, обігом, використанням та зберіганням інформації без прив'язки лише до комп'ютерного середовища. Звісно, в умовах інформаційного суспільства більшість інформації зберігається в цифровому вигляді. Розглянемо більш детально питання покарання за визначені злочини, що представлено в таблиці 1.

Основними видами покарання за скоєння кіберзлочинів у Республіці Польща є обмеження або позбавлення волі, штраф, а у окремих випадках конфіскація майна. Найбільший строк позбавлення волі від 6 місяців до 8 років передбачено за такі види кіберзлочинів: 1) знищення, пошкодження, відміна або зміна інформаційних даних, що мають спеціальне значення для оборони держави, безпеки комунікації, функціонування урядової адміністрації, іншого державного органу або державної інституції, або територіального органу місцевого самоврядування чи закладу, або унеможливує автоматичну обробку, накопичення чи передачу таких даних (ст. 269); 2) розголошення або всупереч закону використання закритої інформації, що відноситься до «таємної» або «абсолютно таємної» за умови, що розголошена особі, що діє від імені або в інтересах іноземної юридичної особи (ст. 265 3).

Досліджуваним нормативно-правовим документом передбачено обтяжуючі обставини, зокрема:

– за статтею 265 щодо розголошення інформації – інформація розголошена особі, що діє від імені або в інтересах іноземної юридичної особи;

– за статтею 266 щодо розкриття чи використання інформації – розкриття посадовою особою неповноважній особі інформацію, що не підлягає розголошенню як «обмежена» або «конфіденційна», чи інформацію, яка отримала у зв'язку з виконанням службових обов'язків, та розкриття якої може завдати шкоди охоронюваним законом інтересам;

– завдання значної матеріальної шкоди за статтями 268 та 268 а;

– запис даних, здійснений на інформаційний носій за статтею 268.

Представлене вказує на існування двох ключових напрямів здійснення кіберзлочинів:

– по-перше, розголошення інформації, щодо якої є обмеження її використання;

– по-друге, порушення роботи систем збору, обробки, передачі та зберігання інформації;

– по-третє, виробництво та збут пристроїв, що дозволяють вчинити кіберзлочин.

Чеська Республіка. Чеська Республіка має давню історію формування системи кримінального права. Це обумовлено насамперед становленням держави та еволюцією її політичного розвитку. Зважаючи на політичну історію Чеської республіки та історичні епохи розвитку суспільства, можна виокремити такі етапи: 1) Середньовіччя, що характеризуються значим впливом правових традицій Священної Римської імперії; 2) Новий час (або Модерна доба), що пов'язано із втратою незалежності та входженням до складу Австрії; 3) Австро-Угорський період, що обумовлений створенням Австро-Угорщини та використанням системи Права Австрії; 4) Чехословаччина (1918–1993), систему кримінального права якої можна розділити на дорадянський та радянський періоди; 5) сучасний період, який характеризується розпадом на Чеську Республіку та Словаччину.

Середньовічна система права в цілому та кримінального права зокрема характеризувалася значним впливом правової системи Священної Римської імперії. Відповідно основними джерелами права були звичаєві норми, а в окремих випадках укази Короля. Вважається, що важливим фактором у кодифікації та систематизації права стало заснування Празького університету у 1348 р. Засновником університету вважається Карл IV, король Богемії та імператор Священної Римської імперії. Саме тоді почалося викладатися римське право, що неабияк впливало на усю правову систему країни. Формування правової системи в Новий час є досить дискусійним з позиції розвитку країни та державотворення. Насамперед це пов'язано із тим, що Фердинанд II увів у дію дві провінційні конституції Богемії (від 10 травня 1627 р.) та Моравії (від 10 травня 1628 р.) без згоди сейму. Як вказують чеські дослідники «оновлена провінційна конституція зовсім не була, як ми часто читаємо, конституцією. Це сучасний термін, що не підходить для давньої історії, до того ж провінційні конституції взагалі містили, крім державного права, процесуальне, кримінальне або спадкове право, тому ми могли б скоріше назвати їх провінційними кодексами з певним ступенем спрощення» [11]. З позиції цього дослідження така конституція є цікавою з позиції першої спроби кодифікації, зокрема визначені такі галузі права, як: державне, приватне та кримінальне.

Кримінальна відповідальність за кіберзлочини в Республіці Польщі

Злочин	Покарання	Обтяжуючі та/або пом'якшуючі обставини	
		обставина	покарання
1	2	3	4
Стаття 265			
Розголошення або всупереч закону використання закритої інформації, що відноситься до «таємної» або «абсолютно таємної»	Позбавлення волі на строк від 3 місяців до 5 років	Інформація, розголошена особі, що діє від імені або в інтересах іноземної юридичної особи	Позбавлення волі на строк від 6 місяців до 8 років
		Неумисне розповсюдження інформації	Штраф, обмеження волі або позбавлення волі на строк до 1 року
Стаття 266			
Розкриття чи використання інформації, всупереч приписам закону або прийнятим на себе зобов'язанням, яку особа дізналася у зв'язку з виконуваними функціями, виконуваною роботою, публічною, соціальною, господарською чи науковою діяльністю	Штраф, обмеження волі чи позбавлення волі на строк до 2 років	Розкриття посадовою особою неповноважній особі інформації, що не підлягає розголошенню як «обмежена» або «конфіденційна», чи інформації, отриманої у зв'язку з виконанням службових обов'язків, та розкриття якої може завдати шкоди охоронюваним законом інтересам	Позбавлення волі на строк до 3 років
Стаття 267			
Отримання доступу до інформації без повноважень, що для особи не призначена, відкриття закритих листів, підключившись до телекомунікаційної мережі або зламавши чи оминувши електричний, магнітний, інформаційний або інший спеціальний її захист	Штраф, обмеження волі або позбавлення волі на строк до 2 років	Не передбачено	
Отримання доступу до частини або до всієї інформаційної системи без повноважень, що для особи не призначена	Штраф, обмеження волі або позбавлення волі на строк до 2 років	Не передбачено	
Підкладання або використання підслуховуючого, візуального пристрою або іншого пристрою чи програмування, з метою отримання інформації, для отримання якої немає повноважень	Штраф, обмеження волі або позбавлення волі на строк до 2 років	Не передбачено	
Стаття 268			
Знищення, пошкодження, відміна чи зміна запису важливої інформації або в інший спосіб розладнання чи ускладнення доступ до неї для особи, яка має повноваження на ознайомлення з такою інформацією, особою, що немає на це повноваження	Штраф, обмеження волі або позбавлення волі на строк до 2 років	Запис даних здійснений на інформаційний носій	Позбавлення волі на строк до 3 років
		Завдано значної матеріальної шкоди	Позбавлення волі на строк від 3 місяців до 5 років

1	2	3	4
Стаття 268 а			
Знищення, пошкодження, відміна, зміна або ускладнення доступу до інформаційних даних або істотним чином порушення чи унеможливлення автоматичної обробки, накопичення чи передачі таких даних, особою без повноважень на такі дії	Позбавлення волі на строк до 3 років	Завдано значної матеріальної шкоди	Позбавлення волі на строк від 3 місяців до 5 років
Стаття 269			
Знищення, пошкодження, відміна або зміна інформаційних даних, що мають спеціальне значення для оборони держави, безпеки комунікації, функціонування урядової адміністрації, іншого державного органу або державної інституції, або територіального органу місцевого самоврядування чи закладу, або унеможливорює автоматичну обробку, накопичення чи передачу таких даних	Позбавлення волі від 6 місяців до 8 років	Не передбачено	Не передбачено
Стаття 269 а			
Порушення роботи комп'ютерної системи або телекомунікаційної мережі істотним чином без уповноваження на це через передачі, знищення, відміни, пошкодження, ускладнення доступу або зміни інформаційних даних	Позбавлення волі на строк від 3 місяців до 5 років	Не передбачено	Не передбачено
Стаття 269 б			
Виробництво, придбання, збут чи забезпечення інших осіб пристроями або комп'ютерними програмами, пристосованими для вчинення злочину, комп'ютерними паролями, кодами доступу чи іншими відомостями, що уможливлюють доступ до інформації, яка зберігається в комп'ютерній системі чи телекомунікаційній мережі	Позбавлення волі на строк до 3 років	Не передбачено	Не передбачено

Джерело: сформовано автором на основі [8; 10]

У подальшому втрата незалежності Чехії та її входження до складу Австрії обумовили реформування кримінального права, що переважно пов'язано із виданням Терезіанського кримінального кодексу (1768 р., за часів правління Марії-Терезії) та Йозифінського кримінального кодексу (1787 р., за часів правління Йосифа II). Терезіанський кодекс був досить дискусійним, що й обумовило реформування та прийняття через два десятиліття Йозифінського кримінального кодексу. Зазначений кодекс складався з частин процесуального та матеріального права, а усі злочини поділялися на дуже тяжкі, тяжкі та легкі. За перші два застосувалися смертна кара та тілесні покарання, а за легкі злочини – штрафи та конфіскація майна.

Австро-Угорський період розвитку кримінального права на території сучасної Чехії пов'язаний з Австрійським кримінальним кодексом 1852 р., який ще називають Кримінальним Кодексом Франца-Йосифа. Цей кодекс передбачав регулювання процесуального та матеріального кримінального права. «Австрійський кримінальний кодекс 1852 р. був основним джерелом кримінального права, одним із засобів протидії злочинності, важливим регулятором кримінально-правових відносин у Галичині і Буковині як складової Австрійської імперії, а з 1867 р. – Австро-Угорської монархії, а також у Першій Австрійській республіці (1918–1938 рр.) на території Австрії, яка була у складі Третього Рейху, і на території незалежної Австрійської республіки, утвореної у 1955 р. Цей Кодекс врегульовував лише питання матеріального кримінального права. Незважаючи на значну кількість актів, якими у нього вносилися зміни та доповнення, він діяв аж до 1975 р. Цей факт пояснюється не досконалістю норм цього Кодексу, а лише відсутністю волі правлячої верхівки до прийняття нового Кодексу» [9]. Проте зазначений нормативно-правовий документ визначає еволюцію системи кримінального права.

Чехословаччина є країною, що утворилася в 1918 р. в результаті відділення від Австро-Угорщини, що отримала поразку в Першій світовій війні. Варто зазначити, що ця країна має три періоди свого розвитку, а саме: I) 1918–1939 рр. як Чехословацька республіка; II) 1939–1945 рр. Чехословацька республіка в складі нацистської Німеччини; III) Чехословацька соціалістична республіка, яка перебувала під впливом Радянського Союзу. Період до другої світової війни кримінальне право базувалося на австрійській правовій традиції, з відповідними реформами. У 1950 р. до влади в країні прийшли комуністи із соціалістичною ідеологією. Зміна політичного режиму та необхідність становлення нової соціалістичної ідеології обумовили прийняття нового кримінального кодексу у 1950 р., що визначив покарання за загрозу соціалістичному політичному режиму. Цей кодекс діяв до реформи 1961 р., коли було прийнято новий кримінальний кодекс. Варто зазначити, що менше ніж за рік до цього був прийнятий Кримінальний кодекс Української РСР та інших країн-членів СРСР.

Після розпаду у 1993 р. Чехія та Словаччина стали на шлях формування власних правових систем, які своєю чергою відповідали їх прагненню вступу до Європейського Союзу. Так у 2009 р. був прийнятий новий Кримінальний Кодекс (закон № 40/2009 Sb.). Структура Кримінального кодексу Чеської Республіки становить дві частини: загальну та особливу. Загальна визначає систему регулювання кримінальної відповідальності; обставини, що виключають протиправність дій; звільнення від кримінальної відповідальності; кримінальні стягнення; зняття судимості; особливі положення щодо окремих видів суб'єктів кримінальних правопорушень.

Варто зазначити, що сьогоденні питання кібербезпеки та протидії кіберзлочинам є особливо важливим для Чехії. Опитування населення, що проведено «Zlatá koruna» під назвою «KYBERNETICKÁ RIZIKA», вказує на такі особливості:

- в частині банківського захисту: «Результати опитування показують, що чехи вірять, що банки захистять свої фінанси. Загалом банкам довіряють 89 % респондентів, з них дуже довіряють 38 %, а скоріше – 51 %. Цікаво, що найбільше довіри виявляють молоді люди віком 25–34 рр. (95 %), а також жителі великих міст з населенням понад 100 тис. (94 %) і жителі Праги (97 %);»

- щодо кібератак: «Третина респондентів (31 %) стикалися з тією чи іншою формою кібератаки. Найпоширенішими були фішинг (47 %), зловмисне програмне забезпечення (26 %) і крадіжка особистих даних (31 %). Викликає тривогу те, що більше п'ятої частини (21 %) цих жертв втратили свої кошти під час нападу;»

- в напрямі усвідомлення кіберризиків: «Інформацію про кіберризики люди найчастіше отримують із ЗМІ (42 %), соціальних мереж (27 %) та банків (27 %). Незважаючи на те, що 82 % респондентів вважають, що банки достатньо інформують про ці ризики, все ще є можливості для покращення;»

- щодо самооцінки та запобіжних заходів: «Більше половини респондентів (57 %) оцінюють себе як помірно обізнаних у кіберризиках, тоді як 5 % вважають себе експертами. З тих, хто вважає себе експертами, 78 % використовують двофакторну автентифікацію, а 72 % використовують надійні паролі, що вище, ніж серед населення (62 % і 58 % відповідно);»

- встановлення відповідальності за кібератаки: «Опитування також вивчало погляди на те, хто повинен нести відповідальність за шкоду, заподіяну кібератакою. Більшість респондентів (41 %) вважають, що метою атаки має бути фінансова установа. Ще 29 % звинувачують особу в недотриманні вказівок з безпеки, а 26 % звинувачують уряд і регуляторів;»

– щодо електронних атак: «Згідно з опитуванням, 36 % респондентів коли-небудь відкривали підозрілий електронний лист, а 44 % з них не усвідомлювали, що це був підозрілий електронний лист. Навпаки, 64 % респондентів не відкривали підозрілий електронний лист, з яких 51 % видаляли лист, не відкриваючи його, а 32 % перемістили його до спаму»;

– в частинні ролі уряду: «Що стосується урядових заходів щодо боротьби з кіберзагрозами у фінансовому секторі, то респонденти віддають перевагу освіті та підвищенню обізнаності щодо кібербезпеки (33 %). Далі йдуть створення та застосування законів (22 %), співпраця з банками та іншими фінансовими установами (22 %) і підтримка досліджень і розробок (20 %)».

Ключовими складовими формування та реалізації державної кримінально-правової політики щодо протидії кіберзлочинності в Чеській Республіці є два нормативно-правові акти, а саме: Кримінальний кодекс Чеської Республіки [14] та Закон Чеської Республіки «Про кібербезпеку» [13]. Зміст зазначених нормативно-правових актів розглянемо більш детально.

Кримінальний кодекс Чеської Республіки, що прийнятий у 2009 р., піддавався деяким змінам протягом останніх 15 років та складається з загальної та особливої частин. Питання встановлення кримінальної відповідальності за різні види злочинів, в тому числі і кіберзлочини, визначені в особливій частині.

Особлива частина Кримінального кодексу Чеської Республіки [7] визначає сукупність злочинів та кримінальну відповідальність за їх скоєння, зокрема передбачає такі кримінальні правопорушення:

– злочини проти життя та здоров'я (Глава I), що визначають такі види кримінальних правопорушень: проти життя, проти здоров'я, проти вагітних жінок, що створюють загрозу життю або здоров'ю, пов'язані із незаконним обігом тканин та органів людини, людського ембріона та геному людини;

– кримінальні правопорушення проти свободи, особистих прав, недоторканності приватного життя і таємниці кореспонденції (Глава II) включають кримінальні правопорушення проти: свободи та прав на захист особистості, приватного життя та таємниці кореспонденції;

– кримінальні правопорушення проти людської гідності у сексуальній сфері (Глава III);

– злочини проти сім'ї та дітей (Глава IV);

– злочини проти власності (Глава V);

– економічні кримінальні правопорушення (Глава VI), що включають кримінальні правопорушення щодо: валютних цінностей та засобів платежу; податків, зборів та іноземної валюти; обов'язкових правил ринкової економіки та обігу товарів при співробітництві з іноземними державами; промислових прав та авторського права;

– загальнонебезпечні кримінальні правопорушення (Глава VII), які полягають у створенні небезпеки для суспільства та небезпеки для повітряного судна, цивільних кораблів та нерухомої платформи;

– кримінальні правопорушення проти навколишнього середовища (Глава VIII);

– кримінальні правопорушення проти Чеської Республіки, іноземних держав та міжнародних організацій (Глава VIII) враховують кримінальні правопорушення проти: основ Чеської Республіки, іноземних держав та міжнародних організацій; безпеки Чеської Республіки, іноземної держави та міжнародної організації; оборони держави;

– кримінальні правопорушення проти порядку у публічних питаннях (Глава X), де передбачено кримінальну відповідальність за такі правопорушення: проти здійснення повноважень органами державної влади та службовими особами; скоєні службовими особами; корупція; інше втручання у діяльність органів державної влади; порушують спільне проживання людей; інші порушення публічного порядку; скоєні організованою злочинною групою; інші форми злочинного співробітництва;

– кримінальні правопорушення проти військової служби (Глава XI);

– військові кримінальні правопорушення (Глава XII). Так Кримінальним Кодексом Чеської Республіки передбачені такі види військових злочинів: проти військової субординації та військової честі; проти обов'язку проходження військової служби; проти порядку здійснення охорони, нагляду або виконання інших обов'язків; які створюють загрозу для боєздатності або збройних сил; проти обов'язків членів сил оборони;

– кримінальні правопорушення проти людства, миру та військові злочини (Глава XIII), що включають: проти людства; проти миру та військові злочини.

Питання протидії кіберзлочинам частково регулюються Розділом 2 – Кримінальні правопорушення проти прав на захист особистості, приватного життя та таємниці кореспонденції, II Глави – Кримінальні правопорушення проти свободи, особистих прав, недоторканності приватного життя і таємниці кореспонденції.

Зазначеним розділом передбачено кримінальну відповідальність за:

– незаконне розповсюдження особистих даних (ст. 180);

– посягання на права іншої особи (ст. 181);

– порушення таємниці кореспонденції (ст. 182);

Проте основною складовою встановлення кримінальної відповідальності за кіберзлочини є Розділ V – Злочини проти власності [14]. Зокрема в цій частині кримінального кодексу встановлена кримінальна відповідальність за такі види кіберзлочинів:

- несанкціонований доступ до комп'ютерної системи та несанкціоноване втручання в комп'ютерну систему чи носій інформації (ст. 230). Такий вид злочину характеризується Кримінальним кодексом Чеської Республіки з двох позицій: 1) подолання заходів безпеки і таким чином отримання несанкціонованого доступу до комп'ютерної системи або її частини; 2) втручання в комп'ютерну систему або носій інформації шляхом: а) несанкціонованого використання даних, що зберігається в комп'ютерній системі або на носії інформації; б) незаконне видалення або іншим чином знищення, пошкодження, зміна, приховування, зниження їх якості або робити їх непридатними для використання даних, що зберігаються в комп'ютерній системі або на носії інформації; с) фальсифікація або зміна даних, що зберігаються в комп'ютерній системі або на носії інформації, таким чином, що вони вважаються справжніми або діють так, ніби це справжні дані, незалежно від того, чи є дані безпосередньо розбірливими та зрозумілими; г) несанкціоноване введення або передача даних в комп'ютерну систему чи на носій інформації або здійснює інше втручання в програмне чи технічне обладнання комп'ютерної системи чи інше технічне обладнання для обробки даних;

- надання та зберігання пристрою доступу до комп'ютерної системи, пароля та інших подібних даних (ст. 231). Цей злочин характеризується як виробництво, введення в обіг, імпорт, експорт, транспорт, пропозиція, посередництво, продаж або іншим чином надання, збір або зберігання для себе чи іншої особи: а) пристрій або його компонент, процедура, інструмент або будь-який інший засіб, враховуючи комп'ютерну програму, створений або адаптований для несанкціонованого доступу до електронної комунікаційної мережі, до комп'ютерної системи або її частини або для несанкціонованого втручання в комп'ютерну систему або носій інформації; б) комп'ютерний пароль, код доступу, дані, процедуру або будь-які інші подібні засоби, за допомогою яких можна отримати доступ до комп'ютерної системи або її частини;

- несанкціоноване втручання в комп'ютерну систему або носій інформації через необережність (ст. 232). Передбачається кримінальна відповідальність за грубу недбалість, через порушення обов'язків, що випливають із роботи, професії, посади чи функції, або накладених законом або прийнятих за контрактом: а) знищення, пошкодження, зміна або дія, що робить непридатними для використання дані, що зберігаються в комп'ютерній системі або на носії інформації; б) втручання в технічне або програмне обладнання комп'ютерної системи або інше технічне обладнання для обробки даних.

Міра покарання за зазначеними кіберзлочинами представлена в таблиці 2.

Відповідно до наданих результатів аналізу Кримінального кодексу Чеської Республіки, можна визначити, що найбільше покарання за кіберзлочини є позбавлення волі до 8 років. Досліджуванім нормативно-правовим документом визначено такі обтяжуючі обставини:

- намір заподіяти шкоду чи іншу шкоду іншій особі або отримати несанкціоновану вигоду для себе чи іншої особи (застосовуються до статей: 230);

- намір незаконно обмежити функціональність комп'ютерної системи чи іншого технічного пристрою для обробки даних (застосовуються до статей: 230);

- дії, вчинені членом організованої групи (застосовуються до статей: 230, 231);

- діяння завдає значної шкоди (застосовуються до статей: 230);

- діяння могло б серйозно впливати на функціонування держави, здоров'я людей, безпеку, економіку або забезпечення основних життєвих потреб населення (застосовуються до статей: 230);

- отримує значну вигоду для себе чи іншої особи (застосовуються до статей: 230, 231);

- діяння спричинило серйозні порушення в діяльності юридичної особи або фізичної особи-підприємця (застосовуються до статей: 230);

- завдає шкоди великого масштабу (застосовуються до статей: 230, 232);

- отримує велику вигоду для себе або для іншої особи (застосовуються до статей: 230, 231).

Окремо увагу варто приділити відповідальності за шахрайство. Цей вид злочину визначений у статті 209 – Шахрайство Кримінального кодексу Чеської Республіки. Хоча нормативним документом не визначено власне питання комп'ютерного шахрайства, проте юридична практика в Чехії вказує на значні досягнення в цьому напрямі. В частині порушень громадського порядку в практиці кримінального процесу та притягнення до відповідальності в Чехії є приклади, засудження за кіберзлочини в частині статті 357 – Поширення тривоги. Цією статтею передбачено покарання за: навмисне викликання небезпеки серйозного занепокоєння принаймні частини населення, поширюючи повідомлення про тривогу, яке є неправдивим.

Кримінальна відповідальність за кіберзлочини в Чеській Республіці

Злочин	Покарання	Обтяжуючі та/або пом'якшуючі обставини	
		обставина	покарання
Стаття 230			
Несанкціонований доступ до комп'ютерної системи та несанкціоноване втручання в комп'ютерну систему чи носій інформації	(1) Позбавлення волі на строк до 2 років, заборона діяльності або конфіскація майна. (2) Позбавлення волі на строк до 3 років із заборonoю діяльності або конфіскацією майна	Намір заподіяти шкоду чи іншу шкоду іншій особі або отримати несанкціоновану вигоду для себе чи іншої особи	Позбавлення волі на строк від 6 місяців до 4 років із заборonoю діяльності або конфіскацією майна
		Намір незаконно обмежити функціональність комп'ютерної системи чи іншого технічного пристрою для обробки даних	
		Дії вчинені членом організованої групи	Позбавлення волі на строк від 1 до 5 років або штраф
		Діяння завдає значної шкоди	
		Діяння могло б серйозно впливати на функціонування держави, здоров'я людей, безпеку, економіку або забезпечення основних життєвих потреб населення	
		Отримує значну вигоду для себе чи іншої особи	
		Діяння спричинило серйозні порушення в діяльності юридичної особи або фізичної особи-підприємця	
		Завдає шкоди великого масштабу	Позбавлення волі на строк від 3 до 8 років або штраф
		Отримує велику вигоду для себе або для іншої особи	
Стаття 231			
Надання та зберігання пристрою доступу до комп'ютерної системи, пароля та інших подібних даних	Позбавлення волі на строк до 2 з конфіскацією майна або заборonoю займатися діяльністю	Дії вчинені членом організованої групи	Позбавлення волі на строк від 3 років із заборonoю займатися діяльністю або конфіскацією майна
		Отримує значну вигоду для себе чи іншої особи	
		Отримує велику вигоду для себе або для іншої особи	Позбавлення волі на строк від 6 місяців до 5 років
Стаття 232			
Несанкціоноване втручання в комп'ютерну систему або носій інформації через необережність	Позбавлення волі на строк до 6 місяців із заборonoю займатися діяльністю або конфіскацією майна	Завдає шкоди великого масштабу	Позбавлення волі на строк до 2 років з конфіскацією майна або заборonoю займатися діяльністю

Закон Чеської Республіки «Про кібербезпеку» [13] був затверджений у 2014 р., а поточна редакція діє від 6 серпня від 2022 р. Зазначений закон переважно регулює кіберпростір та діяльність у кіберпросторі для забезпечення кібербезпеки держави, не встановлюючи відповідальність за його порушення. Зокрема, сферою дії зазначеного закону є регулювання прав та обов'язків осіб та повноваження і компетенції органів державної влади в сфері кібербезпеки. Ним встановлюються вимоги до безпеки електронних комунікаційних мереж. Прийняття цього закону обумовлене необхідністю відповідності національної системи кіберзахисту нормам Європейського Союзу, зокрема директиви NIS. «Головною метою закону є: встановити базовий рівень заходів безпеки; покращити виявлення інцидентів кібербезпеки; запровадити звітність про інциденти кібербезпеки; запровадити систему заходів реагування на інциденти кібербезпеки; коригувати діяльність наглядових робочих місць» [13]. Таким чином, Закон Чеської Республіки «Про кібербезпеку» визначає правове поле функціонування кіберпростору, а кримінальний кодекс встановлює відповідальність за його порушення. Варто зазначити, що система державного управління кібербезпекою є інституціалізованою, адже у 2017 р. було утворено спеціалізований орган – Національне управління з кібербезпеки та інформаційної безпеки (NÚKIB).

Республіка Болгарія. Болгарія одна з небагатьох країн постсоціалістичного табору, що використовує Кримінальний кодекс другої половини минулого століття. Це можна пов'язати із багатьма політичними, соціально-економічними та правовими аспектами. Хоча й кримінальне право в Республіці Болгарія має давню історію, проте розвивалося революційно, що унеможливило відстеження певних національних особливостей в сучасному кримінальному законодавстві.

Розвиток та трансформація системи кримінального права Болгарії відбувався за такими етапами: 1) Болгарське Царство (VII–XIV ст.); 2) Османський період (1396–1878 рр.); 3) Національне відродження та визволення (XVIII–XIX ст.); 4) Князівство та Царство Болгарії (1878–1944 рр.); 5) Соціалістичний період (1944–1989 рр.); 6) Сучасний період (після 1989 р.).

Особливостями Першого Болгарського Царства, яке припадає на 681–1018 рр. та другого Болгарського Царства, що припадає на 1185–1396 рр., є те що основою кримінального права були звичаєві норми та церковні канони, що відігравали найбільшу роль. Так поєднання візантійського права та слов'янських традицій спостерігається в нормативному акті, прийнятому в період правління князя Бориса I – «Закон судний людьми» [3], що вважається одним з перших нормативних актів серед слов'янських народів, що регулював багато аспектів процесуального характеру. «“Закон судний людьми” став помітним рубежем у розвитку болгарського феодального права. В основу його покладено кілька джерел, зокрема болгарське звичаєве право. Другим джерелом для укладача слугувала Еклога. При укладанні “Закон судний людьми” активно перероблялися візантійські формули з метою привести їх у відповідність до болгарської дійсності. Термінологія пам'ятки – суто слов'янська. Норми “Закон судний людьми” дозволяють судити про суспільний лад Болгарії IX ст. Основна маса болгарського народу складалася з вільних землеволодільців, які жили громадами. Однак відносини громад вже було значною мірою підточено розвитком приватної власності. Селяни періоду “Закон судний людьми” вільно розпоряджалися своїми “маєтками”. Болгарське суспільство було вже розшарованим. Особи, які належали до землевласної аристократії, як видно із “Закон судний людьми”, користувалися у суді привілеями перед простими людьми. В “Закон судний людьми” відбився процес збідніння і розорення значної частини вільних селян. У ньому постійно згадуються злидарі, йдеться про покарання за крадіжки або за напад з метою грабежу. Все це свідчить про наявність людей, які втратили зв'язки з громадою, були позбавлені землі та засобів виробництва і перетворилися на бездомних бродяг. Злидарі та безземельні “свободники” потрапляли у боргову кабалу: “Закон судний людьми” згадує не тільки боржника, а й “мзденника”, який повинен був відпрацювати борг. У Болгарії у VIII–IX ст. продовжувало існувати патріархальне рабство: у пам'ятці є багато згадок про рабів, яких протиставлено “свободникам”. Раб не міг свідчити в суді проти свого пана. Раба, який скоїв крадіжку, передавали тому, у кого він украв, якщо його пан не погоджувався відшкодувати вкрадене. Рабами ставали військовополонені, діти рабині; вільні люди ставали рабами за борги або злочини» [4].

Варто зазначити, що цей документ переважно регулював питання відповідальності за злочини в сфері економіки та господарських відносин, які мали б відповідати християнським цінностям. Відповідно покарання найчастіше мали релігійний характер та реалізовувалися у вигляді страти, тілесних покарань та вигнання. Варто зазначити, що «Закон судний людьми», на думку багатьох вчених, був використаний при укладанні Уставу Ярослава Мудрого та «Руської правди».

Релігійний характер кримінального права в Болгарії не змінився і після завоювання Османською Імперією. Османське правління припадає на 1396–1878 рр., що характеризуються відповідністю кримінального права нормам Шаріату та указам Султана. Лише в окремих місцевих громадах зберіглося звичаєве болгарське право в обмеженому вигляді. Зазначимо, що основними формами покарання залишилися: смертна кара, тілесні покарання та конфіскація майна.

Сучасна правова система почала формуватися після визволення Болгарії від Османської Імперії, що відбулося у 1878 р. В цей період формуються та розвиваються революційні налаштування, що в історії

характеризується як національне відродження. Саме революціонери заклали основи уявлення про право, а Болгарський революційний центральний комітет почав обговорювати принципи справедливості та покарань.

Перший кримінальний кодекс Болгарії був прийнятий в період Князівства та Царства Болгарії, що припадали на 1878–1944 рр. Так у 1896 р. був прийнятий кримінальний кодекс, основні положення якого базувалися на кримінальному кодексі російської імперії 1845 р., та регулював протидію злочинам проти особи, власності, громадського порядку та держави. Така ситуація пов'язана з російською підтримкою при визволенні Болгарії. Європейський вплив на Болгарію цього періоду став причиною реформування кримінального законодавства.

Прихід комуністів до влади в Болгарії у 1944 р. визначив вектор політичного та правового розвитку на відповідність соціалістичним положенням. Особливим був Кримінальний кодекс, що було прийнято у 1951 р. Ключовими нововведеннями зазначеного Кримінального кодексу стала кримінальна відповідальність за контрреволюційну діяльність та проти соціалістичної держави.

Основними формами покарань було визначено довготривале ув'язнення, смертну кару, ув'язнення у трудових таборах та заслання.

Новий кодекс за часів соціалістичної Болгарії був прийнятий у 1968 р., який, до речі, в реформованому вигляді діє досі. Цей кодекс був значно реформований після європейського вектора розвитку Болгарії з 1989 р., коли відбулося падіння комуністичного політичного режиму. Приєднання Болгарії у 2007 р. до Європейського Союзу визначало необхідність реформування Кримінального кодексу, особливо в частині протидії корупції, торгівлі людьми, транснаціональній злочинності та організованих злочинності.

Структура сучасного Кримінального кодексу Болгарії [6] передбачає загальну та спеціальну частину. Загальна частина визначає: завдання та межі дії кримінального кодексу; характеристику злочинів підготовку та досвід їх здійснення; розуміння співучасті та множинності злочинів; визначення кримінально відповідальної особи; особливості встановлення покарання; особливості відповідальності неповнолітніх; порядок звільнення від покарання; порядок помилування; особливості звільнення від кримінальної відповідальності; особливості реабілітації та примусових медичних заходів.

Особлива частина визначає кримінальну відповідальність за такі види злочинів:

- злочини проти республіки: державний переворот; зрада та шпигунство; саботаж та диверсія; інші злочини;

- злочини проти особистості: вбивство, тілесні ушкодження, зловживання; викрадення людини та незаконне позбавлення волі; примус, розголошення чужої таємниці; образа і наклеп; розпуста; торгівля людьми;

- злочини проти прав громадян: злочини проти рівноправності громадян; злочини проти свободи віросповідання; злочини проти політичних прав громадян; порушення недоторканності житла, приміщення або транспортного засобу; порушення таємниці листування; злочини проти трудових прав громадян; злочини проти інтелектуальної власності; злочини проти свободи зборів, мітингів і демонстрацій; злочини проти права робітників і службовців об'єднуватися в профспілки;

- злочини проти шлюбу, сім'ї та молоді: злочини проти шлюбу та сім'ї; злочини проти молоді;

- злочини проти власності: крадіжка; грабіж; привласнення; шахрайство; вимагання; приховування чужого майна; знищення та пошкодження; зловживання довірою;

- злочини проти підприємництва (бізнесу): загальногосподарські злочини; злочини проти кредиторів; злочини в окремих галузях економіки; злочини проти митного режиму; злочини проти грошово-кредитної системи;

- злочини проти фінансової, податкової та страхової систем;

- злочини проти діяльності державних органів, громадських організацій та осіб, що виконують державні функції: злочини проти державного управління; службові злочини; злочини проти правосуддя; хабарництво;

- злочини проти спорту;

- злочини щодо документів;

- комп'ютерні злочини;

- злочини проти громадського порядку та спорту;

- загальнонебезпечні злочини: злочини, вчинені загальнонебезпечним способом або загальнонебезпечними засобами; злочини у сфері транспорту та зв'язку; злочини проти здоров'я населення та проти довкілля; інші загальнонебезпечні злочини; злочини при використанні атомної енергії в мирних цілях;

- злочини проти обороноздатності республіки, проти відомостей, що складають державну таємницю, проти іноземної секретної інформації: злочини проти відомостей, що становлять державну таємницю, та проти іноземної секретної інформації; злочини проти військової служби; злочини проти проходження альтернативної служби в мирний час; інші злочини;

- військові злочини: злочини проти порядку підпорядкування та військової честі; ухилення від військової служби; службові злочини; злочини проти вартової, постової, патрульної, внутрішньої та

прикордонної служби; інші військові злочини; військові злочини, вчинені у воєнний час або в бойовій обстановці, або під час участі в місії чи операції за межами країни; злочини у зв'язку з воєнними діями;

– злочини проти миру та людства: злочини проти миру; порушення законів та звичаїв війни; знищення груп населення (геноцид) і апартеїд.

В контексті об'єктного поля зазначеного дослідження кримінальна відповідальність за кіберзлочини встановлюється Главою 9 а – Комп'ютерні злочини. Ця глава була введена в дію у 2002 р. та передбачає кримінальну відповідальність за такі діяння:

– отримання доступу до інформаційної системи або її частин у малозначних випадках;

– неправомірне додання, копіювання, використання, зміна, передача, видалення, пошкодження, псування, приховування, знищення комп'ютерних даних в інформаційній системі або припинення доступу до таких даних у малозначних випадках;

– неправомірне додання, копіювання, використання, зміна, передача, видалення, пошкодження, псування, приховування, знищення комп'ютерних даних в інформаційній системі або припинення доступу до таких даних, які можуть бути передані на підставі закону, в електронному вигляді або на електронному чи іншому носії;

– внесення комп'ютерного вірусу в інформаційну систему або комп'ютерну мережу;

– створення, закупівля для себе чи іншої особи, імпорт, експорт, передача, транспортування, надання чи поширення іншим чином комп'ютерної програми, паролів, кодів чи інших подібних даних для доступу до інформаційної системи або її частини з метою вчинення злочину;

– порушення закону про електронний документообіг під час надання інформаційних послуг та послуг електронної автентифікації.

Покарання за вказанні злочини та особливі умови їх скоєння визначені в таблиці 3.

Відповідно до представлених даних за кожним видом комп'ютерних злочинів передбачено позбавлення волі на певний строк, а за окремими видами ще й штраф. Якщо не аналізувати обтяжуючі обставини найжорсткіше покарання – позбавлення волі на строк до семи років, передбачено за такі злочини, як: а) неправомірне додання, копіювання, використання, зміна, передача, видалення, пошкодження, псування, приховування, знищення комп'ютерних даних в інформаційній системі або припинення доступу до таких даних, які можуть бути передані на підставі закону, в електронному вигляді або на електронному чи іншому носії; б) внесення комп'ютерного вірусу в інформаційну систему або комп'ютерну мережу. Варто зазначити, що за цими видами злочинів передбачено як загальні обтяжуючі обставини, що визначені в загальній частині, так і специфічні обтяжуючі обставини.

Зокрема до обтяжуючих обставин належать:

– були завдані значні збитки або настали інші тяжкі наслідки;

– внаслідок діяння настали тяжкі наслідки;

– відбулося розголошення персональних даних, секретної інформації чи іншої таємниці, що охороняється законом, якщо вчинене не становить більш тяжкого злочину;

– діяння було вчинено повторно

– діяння було вчинено проти інформаційної системи або комп'ютерної мережі, яка є частиною критичної інфраструктури;

– діяння було здійснено за допомогою комп'ютерної програми, пароля, коду доступу чи інших даних доступу до інформаційної системи або до її частини, призначених для впливу на більше ніж одну інформаційну систему, і були завдані значні збитки або настали інші тяжкі наслідки;

– діяння вчинене двома або більше особами, які заздалегідь домовилися вчинити таке діяння;

– діяння вчинене особою, яка діяла на замовлення або на виконання рішення організованої злочинної групи;

– діяння вчинене повторно або щодо даних для створення електронного підпису;

– діяння вчинені щодо інформації, що становить державну чи іншу охоронювану законом таємницю;

– діяння вчинено з метою отримання майнової вигоди (корисливих цілей);

– діяння завдало значної шкоди;

– діяння має на меті перешкодити виконанню зобов'язання.

Увага до досвіду Болгарії у встановленні кримінальної відповідальності за кіберзлочини має бути приділена саме у розширенні специфічних та загальних обтяжуючих обставин. Це є вкрай важливим при необхідності протидії гібридним війнам та інформаційного захисту критичної інфраструктури.

Таблиця 3

Кримінальна відповідальність за кіберзлочини в Болгарії

Злочин	Покарання	Обтяжуючі та/або пом'якшуючі обставини	
		обставина	покарання
1	2	3	4
Отримання доступу до інформаційної системи або її частин, у малозначних випадках	Позбавлення волі на строк до 6 років і штраф до 3 тисяч левів	Діяння вчинене двома або більше особами, які заздалегідь домовилися вчинити таке діяння	Позбавлення волі на строк до 6 років і штраф до 5 тисяч левів
		Діяння вчинене повторно або щодо даних для створення електронного підпису	Позбавлення волі на строк до 7 років і штраф до 20 тисяч левів
		Діяння вчинені щодо інформації, що становить державну чи іншу охоронювану законом таємницю	Позбавлення волі на строк від 4 до 8 років, якщо не передбачено більш суворе покарання
		Діяння було вчинено проти інформаційної системи або комп'ютерної мережі, яка є частиною критичної інфраструктури	
		Внаслідок діяння настали тяжкі наслідки	Позбавлення волі від 5 до 12 років
Неправомірне додання, копіювання, використання, зміна, передача, видалення, пошкодження, псування, приховування, знищення комп'ютерних даних в інформаційній системі або припинення доступу до таких даних у малозначних випадках	Позбавлення волі на строк до 6 років і штраф до 10 тисяч левів	Були завдані значні збитки або настали інші тяжкі наслідки	Позбавлення волі на строк до 7 років і штраф до 20 тисяч левів
		Діяння вчинено з метою отримання майнової вигоди	Позбавлення волі на строк від 5 до 7 років і штраф до 10 тисяч левів
		Діяння було здійснено за допомогою комп'ютерної програми, пароля, коду доступу чи інших даних доступу до інформаційної системи або до її частини, призначених для впливу на більше ніж одну інформаційну систему, і були завдані значні збитки або настали інші тяжкі наслідки	Позбавлення волі від 5 до 8 років і штраф до 20 тисяч левів
		Діяння вчинене особою, яка діяла на замовлення або на виконання рішення організованої злочинної групи	Позбавлення волі від 9 до 12 років і штраф до 30 тисяч левів
		Діяння було вчинено проти інформаційної системи або комп'ютерної мережі, яка є частиною критичної інфраструктури	

1	2	3	4
Неправомірне додання, копіювання, використання, зміна, передача, видалення, пошкодження, псування, приховування, знищення комп'ютерних даних в інформаційній системі або припинення доступу до таких даних, які можуть бути передані на підставі закону, в електронному вигляді або на електронному чи іншому носії	Позбавлення волі на строк до 7 років і штраф до 5 тисяч левів	Діяння має на меті перешкодити виконанню зобов'язання	Позбавлення волі від 5 до 7 років і штраф до 7 тисяч левів
Внесення комп'ютерного вірусу в інформаційну систему або комп'ютерну мережу	Позбавлення волі на строк до семи років і штраф до п'яти тисяч левів	Діяння завдало значної шкоди	Позбавлення волі до 9 років і штраф до 20 тисяч левів
		Діяння було вчинено повторно	
		Діяння вчинене проти інформаційної системи або комп'ютерної мережі, яка є частиною критичної інфраструктури	Позбавлення волі на строк від 5 до 12 років і штраф до 20 тисяч левів
Створення, закупівля для себе чи іншої особи, імпорт, експорт, передача, транспортування, надання чи поширення іншим чином комп'ютерної програми, паролів, кодів чи інших подібних даних для доступу до інформаційної системи або її частини з метою вчинення злочину	Позбавлення волі на строк до 6 років	Відбулося розголошення персональних даних, секретної інформації чи іншої таємниці, що охороняється законом, якщо вчинене не становить більш тяжкого злочину	Позбавлення волі на строк від 4 до 7 років
		Діяння вчинено з метою отримання майнової вигоди	Позбавленням волі на строк до 9 років
		Діяння вчинене особою, яка діяла на замовлення або на виконання рішення організованої злочинної групи	
		Діяння завдало значної шкоди	
		Внаслідок діяння настали тяжкі наслідки	
Порушення закону про електронний документообіг під час надання інформаційних послуг та послуг електронної автентифікації	Позбавлення волі на строк до 6 років і штраф у розмірі до 5 тисяч левів, якщо не підлягає суворішому покаранню	Не передбачено	Не передбачено

Литовська Республіка. Правова історія Литовської Республіки визначається сукупністю соціально-економічних, політичних та міжнародних факторів. За всю історію свого існування Литовська республіка пережила епохи незалежності при різних політичних режимах та епохи анексії частини територій та окупації. Своєю чергою історію кримінально-правової системи Литви умовно можна розділити на такі етапи:

1) Велике князівство Литовське, що припадає на XIII–XVI століття. Особливістю зазначеного періоду розвитку правової системи на території сучасної Литви є орієнтація та звичаєві норми та значний вплив руського права. Проте на перетині XIII–XIV століть система права починає кодифікуватися, що ознаменувалися прийняттям Литовських статутів у 1529, 1566 та 1588 рр. Зазначені статuti визначали особливості державного, цивільного, сімейного, кримінального та процесуального права. Положення статутів базувалися на положеннях римського, польського, руського та німецького права. Зокрема в першому, або як його прийнято називати Старий литовський статут, що був прийнятий 29 вересня 1529 р., правові положення, що регулювали кримінальне, цивільне та господарське право, а також визначали судово-процесуальні особливості. Варто зазначити, що особливості права, навіть в частині кримінальної відповідальності, надавалися шляхті. Особливістю Другого Литовського Статуту (1566 р.) (в деяких джерелах його називають Волинським, через особливу роль волинської шляхти) є те, що він мав релігійну основу, адже до його утворення було залучено 5 католиків та 5 православних. Цей статут був направлений переважно на реалізацію адміністративної реформи в країні. Третій або Великий Литовський статут був введений в дію у 1588 р. та мав 14 розділів, які включали 488 артикулів. Цим статутом у частині кримінального права були закріплені положення щодо навмисних злочинів та злочинів з необережності. В частині процесуальних дій було визначено, що суд мав враховувати вік злочинця, зокрема вводилося поняття «покарання неповнолітніх осіб». Значна увага приділялася співучасті в скоєнні злочинів, яка поділялася на просту та складну. Вводить поняття «рецидиву». В той же час злочин, вчинений шляхтичами, карався значно меншими мірами покарання;

2) розвиток у складі Речі Посполитої, що припадає на період з другої половини XVI по кінець XVIII століття. Люблінська унія 1569 р. передбачала входження Литви до складу Речі Посполитої, що значно вплинула на правову систему сучасної території Литви в цілому та системи кримінального права зокрема, незважаючи на те, що Великий Литовський статут залишався чинним. Великий вплив мало польське право, що передбачало значною мірою покарання за злочини проти релігії, держави та власності;

3) окупаційний період у складі російської імперії (з кінця XVIII до початку XX століття). Зазначений період пов'язаний із поділами Речі Посполитої (1772, 1793 та 1795 рр.) між Австрією, Пруссією та росією. Відповідно до вказаних поділів сучасні литовські території відійшли російській імперії. Варто зазначити, що великий Литовський статут 1588 р. із відповідними змінами в результаті впливу польського законодавства діяв до 1840 р. Відповідно з 1840 р. усі закони були замінені на закони російської імперії, кримінальний кодекс якої передбачав найбільші покарання за злочини проти імперії;

4) міжвоєнний період або період незалежності Литви, що припадає на роки між Першою та Другою світовою війнами. Зазначений період характеризується значними політичними змінами. В частині права варто наголосити на прийнятті конституції 1922 р.;

5) період радянської окупації, що припадає з початку другої світової війни до 1990 р. В липні 1940 р. було утворено Литовську радянську соціалістичну республіку. Питання долі Литовської республіки вирішувалося в серпні 1939 р. підписанням пакту Молотова–Ріббентропа, згідно з яким території Литви мали знаходитися під впливом Німеччини. Проте розв'язання Другої світової війни Німеччиною та напад на Польщу сприяв обміну Литви на частину Польщі. Після нападу Німеччини на Радянський Союз сучасна територія Литви була окупована, проте у 1944 р. Литва опинилася знову під впливом Радянського Союзу, а вже 1946 р. відбулися перші вибори, і Литовська радянська соціалістична республіка представила своїх представників до Верховної Ради СРСР. В цей період система кримінального права відповідала радянським положенням, а тому як в більшості країн– членів СРСР у 1961 р. був прийнятий новий кримінальний кодекс, більшість уваги якого була сконцентрована на захисті ідеологічних положень соціалістичної держави та захист державної власності;

6) сучасний період, який розпочався з проголошення незалежності та виходу зі складу Радянського Союзу. Отримання незалежності Литви у 1990 р. стало початком політичних змін, а саме демократизації усіх суспільних процесів у державі. У 2000 р. в Литві був прийнятий новий кримінальний кодекс. Стаття 1 Кримінального кодексу Литовської республіки визначає: «Кримінальний кодекс Литовської Республіки є єдиним кримінальним законом, метою якого є захист прав і свобод людини і громадянина, інтересів суспільства і держави від злочинних діянь засобами кримінального права. Цей кодекс: 1) визначає, які діяння є злочинами та проступками, і забороняє їх; 2) визначає покарання, заходи стягнення та виховного характеру за діяння, передбачені цим Кодексом, та примусові заходи медичного характеру; 3) визначає підстави та умови кримінальної відповідальності, а також підстави та умови, за яких особи, які вчинили злочинні діяння, можуть бути звільнені від кримінальної відповідальності чи покарання. Положення цього

Кодексу гармонізовано з положеннями законодавства Європейського Союзу» [12]. Аналізуючи структуру кодексу, визначимо особливості загальної та особливої частини.

Загальна частина містить положення, що регулюють: сферу дії кодексу та загальні положення кримінальної відповідальності; тривалість кримінальної відповідальності; чинність положень кримінального кодексу щодо осіб, які вчинили злочинні діяння на території Литовської держави або на морських чи повітряних суднах під прапором чи знаками розрізнення Литовської держави; кримінальна відповідальність за злочини, що вчинені резидентами за кордоном; кримінальна відповідальність іноземців за злочинні дії, вчинені за кордоном проти громадян Литовської Республіки та інших осіб, які постійно проживають у Литві; кримінальна відповідальність іноземців за злочини проти Литовської держави, вчинені за кордоном; кримінальна відповідальність за злочини, передбачені міжнародними договорами; кримінальна відповідальність за злочинні діяння, вчинені за кордоном; екстрадиція; передача особи за європейським ордером на арешт; характеристика злочинності та кримінальних правопорушень; стадій та форми злочинних дій; обставини виключення кримінальної відповідальності; звільнення від кримінальної відповідальності; призначення та види покарання; міри злочинно правового наслідку; зупинення відбування покарання та звільнення від покарання; строки давності кримінальної відповідальності; примусові заходи медичного характеру.

Особлива частина Кримінального кодексу Литовської республіки [12] визначає специфічні риси кримінальної відповідальності за різні види злочинів, зокрема:

- злочини проти людяності та воєнні злочини;
- злочини проти незалежності, територіальної цілісності та конституційного ладу Литви;
- злочини проти життя людини;
- злочини проти здоров'я людини;
- злочини, небезпечні для здоров'я та життя людини;
- злочини та кримінальні порушення проти свободи людини;
- злочини та кримінальні правопорушення проти статевої свободи;
- злочини проти честі та гідності особи;
- злочини та кримінальні правопорушення проти дитини та сім'ї;
- злочини проти особистого приватного життя;
- злочини та кримінальні правопорушення проти рівності та свободи совісті;
- проти виборчих прав осіб та процедури виборів або референдумів Президента, Сейму, Європейського парламенту, Муніципальних рад та мерів, процедури фінансування політичних організацій, аналітичних центрів і політичні кампанії;
- злочини та кримінальні порушення проти особистих соціальних прав;
- злочини і проступки проти власності, майнових прав і майнових інтересів;
- злочини проти інтелектуальної власності;
- злочини проти безпеки електронних даних та інформаційних систем;
- злочини та кримінальні правопорушення проти економіки та порядку бізнесу;
- злочини та кримінальні правопорушення для фінансової системи;
- злочини та кримінальні правопорушення для публічної служби та суспільних інтересів;
- злочини та проступки для правосуддя;
- злочини проти громадської безпеки;
- злочини та кримінальні правопорушення, пов'язані з зберіганням зброї, боєприпасів, вибухових речовин, вибухових пристроїв або радіоактивних матеріалів, або військової техніки;
- злочини та кримінальні правопорушення, пов'язані зі зберіганням наркотичних та психотропних, токсичних або сильнодіючих речовин;
- злочини та кримінальні правопорушення проти навколишнього середовища та здоров'я людини;
- злочини та кримінальні правопорушення за безпеку руху;
- злочини та кримінальні порушення проти громадського порядку;
- злочинна діяльність проти державного службовця або особи, що виконує функції державного управління;
- злочини та кримінальні правопорушення проти державного порядку;
- злочини та кримінальні правопорушення щодо підробки документів або іншої інформації;
- злочини та кримінальні порушення проти моралі;
- злочини та кримінальні правопорушення щодо пам'яті померлих;
- злочини та кримінальні правопорушення проти служби в нацгвардії та мобілізації.

Кримінальна відповідальність щодо кіберзлочинів встановлена розділом XXX – Злочини проти безпеки електронних даних та інформаційних систем, яким визначено такі види злочинів та кримінальних правопорушень:

- незаконний доступ до електронних даних (стаття 196), якою передбачено кримінальну відповідальність особи, до речі як фізичної, так і юридичної, яка незаконно знищила, пошкодила, вилучила

або змінила електронні дані або обмежила використання таких даних за допомогою апаратних, програмних чи інших засобів, що завдають шкоди;

- протиправний вплив на інформаційну систему (ст. 197). Цією статтею визначено кримінальну відповідальність фізичної та юридичної особи, яка незаконно порушила або перервала роботу інформаційної системи шляхом заподіяння шкоди;

- незаконне перехоплення та використання електронних даних (ст. 198), що характеризують як незаконне відстеження, записування, перехоплення, отримання, зберігання, привласнення, поширення або іншим чином використання непублічних електронних даних фізичною та/або юридичною особою;

- незаконний доступ до інформаційної системи (ст. 198.1), що передбачає відповідальність особи, яка незаконно підключилася до інформаційної системи або її частини з порушенням заходів захисту інформаційної системи;

- незаконна утилізація пристроїв, програмного забезпечення, паролів, кодів та інших даних (ст. 198.2), зміст якої полягає в тому, що будь-хто, хто зі злочинною метою або іншим чином незаконно виготовляв, транспортував, імпортував, продавав, надавав доступ або іншим чином поширював, придбав або зберігав пристрої чи програмне забезпечення, безпосередньо призначені або адаптовані для вчинення злочинних дій, а також паролі, коди чи інші подібні дані для реєстрації в інформаційну систему або її частину.

В таблиці 4 визначено особливі наслідки скоєння таких злочинів та види покарань, що передбачені Кримінальним кодексом.

Відповідно до зазначеного покарання за кіберзлочини можуть бути у формі:

- громадських робіт;
- накладання штрафу;
- обмеження волі;
- арешту;
- позбавлення волі.

Щодо позбавлення волі найбільший строк передбачено, якщо не зважати на обтяжуючі обставини за статті: незаконне перехоплення та використання електронних даних (ст. 198) та незаконна утилізація пристроїв, програмного забезпечення, паролів, кодів та інших даних (ст. 198.1). Основними складовими, що визначають обтяжуючі обставини за кіберзлочини в Литовській Республіці, є такі:

- злочин скоєно щодо інформаційної системи, що має стратегічне значення для національної безпеки;
- злочин скоєно щодо інформаційної системи, що має важливе значення для державного управління;
- злочин скоєно щодо інформаційної системи, що має важливе значення для економіки чи фінансової системи;

- в результаті були використані або оприлюднені чужі персональні дані;

- в результаті злочину було завдано великої шкоди.

Досвід Литовської Республіки вказує на різноманітність покарання за кіберзлочини. Особливістю досліджуваного Кримінального кодексу Литовської Республіки, є встановлення кримінальної відповідальності юридичних осіб, що відрізняється від інших кримінальних кодексів досліджуваних країн.

Кримінальна відповідальність за кіберзлочини в Литовській Республіці

Злочин	Покарання	Обтяжуючі та/або пом'якшуючі обставини	
		обставина	покарання
Стаття 196. Незаконний доступ до електронних даних			
Незаконне знищення, пошкодження, вилучення або зміна електронних даних або обмеження використання таких даних за допомогою апаратних, програмних чи інших засобів, що завдають шкоди	Громадські роботи або штраф, або обмеження волі, або арешт, або позбавлення волі на строк до 2 років	Діяння вчинене, щодо електронних даних багатьох інформаційних систем або електронних даних інформаційної системи, що має стратегічне значення для національної безпеки або має важливе значення для державного управління, економіки чи фінансів системи, або використовуючи чужі персональні дані, або завдаючи великої шкоди	Штраф або обмеження волі, або арешт, або позбавлення волі на строк до 6 років
Стаття 197. Протиправний вплив на інформаційну систему			
Незаконне порушення або припинення роботи інформаційної системи шляхом заподіяння шкоди	Громадські роботи або штраф, або обмеження волі, або арешт, або позбавлення волі на строк до 2 років	Діяння вчинене щодо ряду інформаційних систем або інформаційної системи, що має стратегічне значення для національної безпеки, або щодо інформаційної системи, яка має велике значення для державного управління, економіки чи фінансової системи, або використовуючи чужі персональні дані, або завдаючи великої шкоди	Штраф або обмеження волі, або арешт, або позбавлення волі на строк до 6 років
Стаття 198. Незаконне перехоплення та використання електронних даних			
Незаконне відстеження, записування, перехоплювання, отримування, зберігання, привласнення, поширення або іншим чином використання непублічних електронних даних	Штраф або обмеження волі, або арешт, або позбавлення волі на строк до 4 років	Діяння скоєно, щодо закритих електронних даних, що мають стратегічне значення для національної безпеки або мають важливе значення для державного управління, економіки чи фінансової системи	Штраф або обмеження волі, або арешт, або позбавленням волі на строк до 6 років
Стаття 198.1. Незаконний доступ до інформаційної системи			
Незаконне підключення до інформаційної системи або її частини з порушенням заходів захисту інформаційної системи	Громадські роботи або штраф, або обмеження волі, або арешт, або позбавлення волі на строк до 2 років	Діяння скоєне щодо інформаційної системи, що має стратегічне значення для національної безпеки або важливе для державного управління, економіки чи фінансової системи	Громадські роботи або штраф, або обмеження волі, або арешт, або позбавлення волі на строк до 3 років
Стаття 198.1. Незаконна утилізація пристроїв, програмного забезпечення, паролів, кодів та інших даних			
Зі злочинною метою або іншим чином незаконне виготовлення, транспортування, імпортування, продаж, надання доступу або іншим чином поширення, придбання або зберігання пристроїв чи програмного забезпечення, безпосередньо призначених або адаптованих для вчинення злочинних дій, а також паролі, коди чи інші подібні дані для реєстрації в інформаційну систему або її частину	Штраф або обмеження волі, або арештом, або позбавлення волі на строк до 4 років	Не передбачено	Не передбачено

Висновки. В результаті дослідження було ідентифіковано особливості еволюції кримінального права країн Європейського Союзу (Литва, Болгарія, Чехія, Польща), що були в складі Радянського Союзу або соціалістичного табору. Здійснено структурний та змістовний аналіз основних нормативних документів, що встановлюють кримінальну відповідальність за злочини. Визначено, що кіберзлочинам у кримінальних кодексах досліджуваних країн приділені окремі розділи, зокрема в: Польщі – Розділ XXXIII Злочини проти охорони інформації; Чехії – Розділ V Злочини проти власності; Болгарії – Главою 9 а Комп'ютерні злочини; Литви – Розділ XXX Злочини проти безпеки електронних даних та інформаційних систем. Варто зазначити, що в Польщі досліджувані злочини визначають як злочини проти охорони інформації, а в Чехії злочини проти власності. Своєю чергою у Кримінальних кодексах Литви та Болгарії ці злочини є відокремленими. Встановлено, що в досліджуваних країнах, незважаючи на їх членство в Європейському Союзі, немає єдиного підходу до покарання за кіберзлочини, що можливо пояснити національними правовими традиціями та увагою політиків до інформаційної безпеки держави. При реформуванні кримінального права в Україні в умовах євроінтеграційних процесів є потреба у врахуванні досвіду зазначених країн лише часткового. Адже вже майже десятиліття точиться дискусія щодо необхідності прийняття нового кримінального кодексу, який має врахувати сучасні методи скоєння злочинів, їх класифікацію та групування. Адже кіберзлочини можуть бути скоєнні в різних сферах суспільного життя та матимуть різні наслідки як соціальні, економічні, політичні, правові, що визначатиме їх родову ознаку.

Список використаної літератури:

1. *Бондар В.* Порівняльна характеристика кримінальних кодексів України та Республіки Польща / *В.Бондар* // Правозахисний рух: історія і сучасність : матеріали X Всеукр. студ. наук.-практ. конф. – Полтава : ПНПУ імені В.Г. Короленка. – 2017. – С. 116–117 [Електронний ресурс]. – Режим доступу : <http://dspace.pnpu.edu.ua/bitstream/123456789/9379/1/Bondar.pdf>.
2. *Вакула І.Ю.* Стадії вчинення злочину за кримінальним правом України та Республіки Польща: порівняльно-правове дослідження : дис. на здобуття наук. ступеня канд. юрид. наук : 12.00.08 / *І.Ю. Вакула*. – Львів : Львівський державний університет внутрішніх справ, 2019. – 209 с. [Електронний ресурс]. – Режим доступу : https://dspace.lvduvs.edu.ua/bitstream/1234567890/3544/1/vakula_d.pdf.
3. *Вілкул Т.Л.* Закон судний людям / *Т.Л. Вілкул* // Енциклопедія історії України ; редкол. *В.А. Смолій* (голова) та ін. ; НАН України, Інститут історії України. – К. : Наукова думка, 2005. – Т. 3 : Е–Й. – 672 с. [Електронний ресурс]. – Режим доступу : http://www.history.org.ua/?termin=Zakon_sudny_ljudem.
4. *Гончаренко В.Д.* Закон судний людям / *В.Д. Гончаренко* // Юридична енциклопедія : в 6 т. ; редкол. *Ю.С. Шемшученко* (голова редкол.) та ін. – К. : «Укр. енцикл.», 1998 [Електронний ресурс]. – Режим доступу : https://leksika.com.ua/16631116/legal/zakon_soudnyu_lyudm.
5. *Грубінко А.* Особливості формування політики кібербезпеки Європейського Союзу: правові аспекти / *А.Грубінко* // Актуальні проблеми правознавства. – 2021. – № 1 (25). – С. 5–10 [Електронний ресурс]. – Режим доступу : <http://dspace.wnu.edu.ua/handle/316497/42023>.
6. *Коротюк О.В.* Кримінальний кодекс Республіки Болгарія / *О.В. Коротюк*. – К. : ОВК, 2024. – 294 с.
7. *Коротюк О.В.* Кримінальний кодекс Чеської Республіки / *О.В. Коротюк* ; переклад на українську мову *О.В. Коротюк*. – К. : ОВК, 2020. – 264 с.
8. *Станіч В.С.* Кримінальний кодекс Республіки Польща / *В.С. Станіч* ; під ред. *В.Л. Менчинського* ; переклад на українську мову *В.С. Станіч*. – К. : ОВК, 2022. – 164 с.
9. *Шуп'яна М.Ю.* Кодифікація австрійського кримінального законодавства у другій половині XIX ст. – на початку XX ст. / *М.Ю. Шуп'яна* // Науковий вісник Ужгородського національного університету. Серія : Право. – 2016. – Вип. 37, Т. 1. – С. 47–50.
10. *USTAWA z dnia 6 czerwca 1997 r. / Kodeks karny* [Electronic resource]. – Access mode : <https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU19970880553/U/D19970553Lj.pdf>.
11. *Kubeš J.* Obnovené zřízení zemské: Zákoník, ústava nebo základ absolutismu? / *J.Kubeš* [Electronic resource]. – Access mode : <https://www.stoplusejednicka.cz/>.
12. Lietuvos Respublikos baudžiamojo kodekso patvirtinimo ir įsigaliojimo. Baudžiamasis kodeksas : įstatymas 2000 m. rugsėjo 26 d. Nr. VIII-1968 / Lietuvos Respublikos Seimas [Electronic resource]. – Access mode : <https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.111555/JYbvMjklSa>.
13. O kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) : Zákon č. 181/2014 Sb. / NÚKIB [Electronic resource]. – Access mode : <https://nukib.gov.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/legislativa/>
14. Zákon trestní zákoník ze dne 8 ledna 2009 : Zákon č. 40/2009 Sb. / *Zákony pro lidi PLUS* [Electronic resource]. – Access mode : <https://www.zakonyprolidi.cz/cs/2009-40>.

References:

1. Bondar, V. (2017), «Porivnialna kharakterystyka kryminalnykh kodeksiv Ukrainy ta Respubliky Polshcha», *Pravozakhysnyi rukh: istoriia i suchasnist*, materialy X Vseukr. stud. nauk.-prakt. konf., PNPu imeni V.H. Korolenka, Poltava, pp. 116–117, [Online], available at: <http://dspace.pnpu.edu.ua/bitstream/123456789/9379/1/Bondar.pdf>
2. Vakula, I.Yu. (2019), «Stadii vchynennia zlochynu za kryminalnym pravom Ukrainy ta Respubliky Polshcha: porivnialno-pravove doslidzhennia», Ph.D. Thesis of dissertation, 12.00.08, Lvivskyi derzhavnyi universytet vnutrishnikh sprav, Lviv, 209 p., [Online], available at: https://dspace.lvduvs.edu.ua/bitstream/1234567890/3544/1/vakula_d.pdf

3. Vilkul, T.L. (2005), «Zakon sudnyi liudiem», *Entsyklopediia istorii Ukrainy*, in Smolii, V.A. (holova) et al. (ed.), NAN Ukrainy, Instytut istorii Ukrainy, Naukova dumka, K., Vol. 3. E–Y, 672 p., [Online], available at: http://www.history.org.ua/?termin=Zakon_sudny_liudem
4. Honcharenko, V.D. (1998), «Zakon sudnyi liudiem», *Yurydychna entsyklopediia*, v 6 t., in Shemshuchenko, Yu.S. (holova redkol.) et al. (ed.), «Ukr. entsykl.», K., [Online], available at: https://leksika.com.ua/16631116/legal/zakon_soudnyy_lyudm
5. Hrubinko, A. (2021), «Osoblyvosti formuvannia polityky kiberbezpeky Yevropeiskoho Soiuzu: pravovi aspekty», *Aktualni problemy pravozaivstva*, No. 1 (25), pp. 5–10, [Online], available at: <http://dspace.wnu.edu.ua/handle/316497/42023>
6. Korotiuk, O.V. (2024), *Kryminalnyi kodeks Respubliky Bolhariia*, OVK., K., 294 p.
7. Korotiuk, O.V. (2020), *Kryminalnyi kodeks Cheskoï Respubliky*, Translated by Korotiuk, O.V., OVK, K., 264 p.
8. Stanich, V.S. (2022), *Kryminalnyi kodeks Respubliky Polshcha*, in Menchynskyi, V.L. (ed.), Translated by Stanich, V.S., OVK, K., 164 p.
9. Shupiana, M.Iu. (2016), «Kodyfikatsiia avstriiskoho kryminalnoho zakonodavstva u druhii polovyni XIX st. – na pochatku XX st.», *Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu. Seriya. Pravo*, Issue 37, Vol. 1, pp. 47–50.
10. «USTAWA z dnia 6 czerwca 1997 r.», *Kodeks karny*, [Online], available at: <https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU19970880553/U/D19970553Lj.pdf>
11. Kubeš, J., «Obnovené zřízení zemské: Zákoník, ústava nebo základ absolutismu?», [Online], available at: <https://www.stoplusjednicka.cz/>
12. Lietuvos Respublikos Seimas (2000), *Lietuvos Respublikos baudžiamojo kodekso patvirtinimo ir įsigaliojimo įstatymas*, Baudžiamasis kodeksas 2000 m. rugsėjo 26 d. No. VIII–1968, [Online], available at: <https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.111555/JYbvMjklSa>
13. NÚKIB (2014), *O kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)*, Zákon č. 181/2014 Sb., [Online], available at: <https://nukib.gov.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/legislativa/>
14. «Zákon trestní zákoník ze dne 8 ledna 2009» (2009), Zákon č. 40/2009 Sb., *Zákony pro lidi PLUS*, [Online], available at: <https://www.zakonyprolidi.cz/cs/2009-40>

Грицишен Дмитрій Олександрович – доктор економічних наук, доктор наук з державного управління, професор Державного університету «Житомирська політехніка».

<https://orcid.org/0000-0002-1559-2403>.

Наукові інтереси:

- протидія економічній злочинності;
- протидія кіберзлочинності;
- національна безпека.

Соха Станіслав Ігорович – кандидат юридичних наук, докторант Державного університету «Житомирська політехніка».

<https://orcid.org/0009-0004-2606-1263>.

Наукові інтереси:

- протидія економічній злочинності;
- протидія кіберзлочинності.

Корзун Світлана Вікторівна – аспірантка Державного університету «Житомирська політехніка».

Наукові інтереси:

- протидія кіберзлочинності.

Grytsyshen D.O., Sokha S.I., Korzun S.V.

Improving the state policy of combating cybercrime based on the experience of the European Union countries

The article analyzes the Criminal Codes of some European Union countries, namely: the Republic of Poland, the Republic of Bulgaria, the Czech Republic, and the Republic of Lithuania. The experience of these countries is fundamentally important for Ukraine, since they were also under the Soviet occupation regime. The genesis of the formation of the criminal system in the Republic of Poland as a whole is analyzed in detail, and responsibility for cybercrimes in particular is determined. The historical milestones of the formation of the criminal law system in the Czech Republic from the Middle Ages to the present day are studied. Bulgaria's experience in establishing criminal liability for cybercrimes is comprehensively analyzed in the context of studying the Criminal Code, where special attention is focused on considering aggravating circumstances, which is very important when it is necessary to counteract hybrid wars and provide information protection for critical infrastructure. Having analyzed the Criminal Code of the Republic of Lithuania, attention was focused on the variety of punishments for cybercrimes. In addition, a distinctive feature of Lithuanian legislation is the presence of criminal liability of legal entities.

As a result of the scientific research, the main historical stages of the formation of the policy of combating cybercrime in the Republic of Poland, the Republic of Bulgaria, the Czech Republic, and the Republic of Lithuania were identified. A comprehensive analysis of the main regulatory documents establishing criminal liability for crimes related to cybercrime was carried out and the distinctive features of each country were identified. It is proved that during the reform of criminal legislation in Ukraine in the context of European integration processes there is an urgent need to take into account the experience of European countries, however, the specific features of the Criminal Law of certain countries should be taken into account, and therefore this process should be approached gradually and selectively.

Keywords: state policy; combating cybercrime; cyberspace; criminal liability.

Стаття надійшла до редакції 25.10.2024.