



**ОКСАНА ВАЛЕРІЇВНА БРУСАКОВА,**

доктор юридичних наук, доцент,  
Харківський національний університет внутрішніх справ,  
факультет № 6;

 <https://orcid.org/0000-0001-8616-0424>,  
e-mail: [advokat.brusakova@gmail.com](mailto:advokat.brusakova@gmail.com);

**ОЛЬГА ПЕТРІВНА ГЕТМАНЕЦЬ,**

доктор юридичних наук, професор,  
Харківський національний університет внутрішніх справ,  
кафедра правового забезпечення господарської діяльності;

 <https://orcid.org/0000-0003-4826-5799>,  
e-mail: [olga.getmanec12@gmail.com](mailto:olga.getmanec12@gmail.com)

## МОДЕРНІЗАЦІЯ МЕХАНІЗМУ ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ РИНКУ ФІНАНСОВИХ ПОСЛУГ

Розглянуто основні підходи до протидії загрозам кібербезпеці на ринку фінансових послуг. Запропоновано створити нові та модернізувати вже наявні правові засоби забезпечення кібербезпеки на ринку фінансових послуг, а також нові спеціальні правові режими для суб'єктів ринку фінансових послуг з метою підвищення рівня кібербезпеки. Наголошено на важливості створення єдиного державного фонду підтримки інноваційного розвитку, що має здійснювати стимулювання залучення інноваційних технологій у фінансовий сектор з метою підвищення рівня кібербезпеки ринку фінансових послуг. Наголошено на важливості створення механізму гарантування державою часткового відшкодування збитків суб'єктам ринку фінансових послуг, завданих унаслідок кібератак.

**Ключові слова:** кібербезпека, ринок фінансових послуг, економічна безпека, засоби правового забезпечення, спеціальний правовий режим.

### Оригінальна стаття

**ВСТУП.** Сьогодні, враховуючи стрімкий розвиток цифрових технологій, відбувається активне збільшення ролі інтернет-сегменту ринку фінансових послуг. Епідемія COVID-19 також активно сприяє збільшенню частки інтернет-послуг на цьому ринку. Саме тому питання забезпечення кібербезпеки ринку фінансових послуг набуває наразі загальнодержавного значення та стає критичним для національної безпеки. Враховуючи велику кількість кібератак з боку як приватних осіб, так і цілих держав (зокрема у межах гібридних війн), необхідно створити ефективно діючий правовий механізм забезпечення кібербезпеки ринку фінансових послуг, що дасть можливість повною мірою захистити вітчизняних суб'єктів ринку фінансових послуг.

Важливим завданням для нашої держави є стимулювання створення, розроблення відповідними науковими установами та впровадження суб'єктами ринку фінансових послуг новітніх інформаційних технологій з метою підвищення конкурентоздатності вітчизняних суб'єктів зазначеного ринку на міжнародних ринках та зниження загроз у сфері кібербезпеки. Особливо важливою є активізація

вітчизняних досліджень інформаційних технологій, враховуючи сучасний стан міжнародних відносин, коли через певні санкції, гібридну війну чи умисне ненадання доступу до певних технологій з метою монополізації ринку дедалі частіше розриваються окремі зв'язки споживачів технологій і виробників. Так, В. Р. Сіденко (2014, с. 92) зазначає, що політика Російської Федерації, спрямована на імпортозаміщення, призвела до неможливості трансферу технологій та інновацій, а також унеможливила передання прав на окремі об'єкти права інтелектуальної власності, що призвело до значних втрат українських товаровиробників. Це явище також посилюється через той факт, що значна кількість вартісних досліджень здійснюється великими холдингами чи транснаціональними корпораціями виключно для себе, оскільки надання відповідного продукту у вигляді новітніх технологій іншим суб'єктам негативно вплине на прибуток.

Слід наголосити, що одним з основних правових засобів забезпечення будь-якої сфери національної безпеки є створення чітких єдиних стандартів. Водночас уже існують міжнародні стандарти інформаційної безпеки

суб'єктів ринку фінансових послуг, тому одним із завдань нашої держави має стати стимулювання відповідних суб'єктів до ухвалення відповідних стандартів на локальному рівні.

Також у світі досить ефективно для досягнення окремих цілей держави наразі використовується такий правовий механізм, як спеціальні правові режими, тому вбачається перспективним використати його для підвищення рівня кібербезпеки на ринку фінансових послуг.

**МЕТА І ЗАВДАННЯ ДОСЛІДЖЕННЯ.** Метою статті є вироблення авторського механізму правових засобів забезпечення кібербезпеки на ринку фінансових послуг. Завданнями дослідження є вивчення поглядів науковців щодо правових засобів забезпечення національної безпеки та дослідження вітчизняного законодавства у сфері забезпечення кібербезпеки на ринку фінансових послуг для його подальшої модернізації.

**МЕТОДОЛОГІЯ ДОСЛІДЖЕННЯ.** Методологічна основа дослідження має системний характер, що виявляється у застосуванні різних методів наукового пізнання залежно від конкретних аспектів дослідження. Методологічну основу дослідження становить діалектичний метод пізнання явищ і процесів. У дослідженні використовувався комплексний підхід, що виявився в застосуванні різних наукових методів залежно від конкретних питань дослідження: порівняльно-правовий метод застосовувався для аналізу положень правових актів України та їх співвідношення, зокрема з метою дослідження повноважень різних державних фондів, що здійснюють стимулювання інноваційного розвитку; системно-структурний метод – для дослідження систематики відносин, пов'язаних із кібербезпекою на ринку фінансових послуг, та їх законодавчого забезпечення з метою знаходження відносин, пов'язаних з кібербезпекою на ринку фінансових послуг, які потребують більш детального й ефективного правового регулювання, та створення пропозицій з модернізації відповідного законодавства; статистичний метод – для аналізу статистики щодо кібернетичних атак у країнах Європи та у Новій Зеландії; логіко-юридичний метод активно застосовувався для формування пропозицій, викладених у дослідженні, та висновків відповідно до мети дослідження з метою створення пропозицій щодо найбільш ефективно модернізації вітчизняних нормативно-правових актів, що регулюють відносини, пов'язані з кіберзахистом суб'єктів ринку фінансових послуг, і створення ефективно діючого механізму забезпечення національної кібербезпеки на ринку фінансових послуг; фор-

мально-юридичний метод широко застосовувався під час аналізу законодавства, розроблення правових засобів забезпечення кібербезпеки на ринку фінансових послуг з метою запропонування більш ефективного правового забезпечення кібербезпеки на цьому ринку; застосування методу аналогії дало змогу на підставі досвіду інших країн щодо кількості кібератак на суб'єктів підприємницької діяльності зробити висновок про ймовірність збільшення кібератак суб'єктів національного ринку фінансових послуг; метод правового моделювання застосовувався для формування конкретних пропозицій щодо модернізації чинного законодавства України у сфері забезпечення кібербезпеки на ринку фінансових послуг.

**РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ ТА ДИСКУСІЯ.** Сьогодні однією з головних загроз як національному, так і міжнародному ринку фінансових послуг виступають різні кібератаки. Як доречно зазначають В. В. Боженко, В. В. Койбічук та М. М. Габенко (2021, с. 51), в умовах пандемії COVID-19 населення та суб'єкти ринку фінансових послуг почали більш активно використовувати онлайн-формат для процесів надання та отримання фінансових послуг, однак це підвищило кількість кібератак суб'єктів ринку фінансових послуг та відповідні ризики. За офіційною статистикою, кібернетичних атак у 2020 році зазнали 49 % компаній у Бельгії, 44 % в Іспанії, 41 % у Німеччині, 37 % у Новій Зеландії, 34 % у Франції та 30 % у Великій Британії<sup>1</sup>. Слід зазначити, що ці цифри можуть бути нижчими за реальні, оскільки існує певна ймовірність приховування юридичними особами фактів кібератак з метою недопущення певних репутаційних втрат. Із цієї статистики можна дійти висновку, що існує значний ризик здійснення кібератак на суб'єктів ринку фінансових послуг (ураховуючи недостатньо розвинуту систему кіберзахисту та низьку порівняно з країнами ЄС кіберграмотність населення, можна робити прогноз про існування можливості здійснення кібератак на понад 40 % суб'єктів ринку фінансових послуг). Також слід зазначити, що відповідно до Звіту Accenture State of Cyber Resilience (Accenture) за 2019 рік за останні п'ять років загальна кількість кібератак зросла на 65 %<sup>2</sup>.

<sup>1</sup> Share of European firms reporting a cyber attack 2020, by country // Statista : сайт. URL: <https://www.statista.com/statistics/1006664/european-firms-cyberattack-target-reporting/> (дата звернення: 26.06.2021).

<sup>2</sup> The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study // Accenture : сайт.

Водночас забезпечення стабільності ринку фінансових послуг (а отже, й захисту його від кіберзагроз), безперечно, є однією з важливих ланок національної економічної безпеки. Для ефективної протидії загрозам національній економічній безпеці у кіберпросторі необхідно створити ефективно діючий правовий механізм протидії таким загрозам. В Україні наразі діють здебільшого обмежувальні засоби у сфері забезпечення кібербезпеки ринку фінансових послуг. Тому пропонується зосередити увагу на пошуку стимулюючих (заохочувальних) правових засобів з метою модернізації механізму забезпечення кібербезпеки ринку фінансових послуг та підвищення рівня забезпечення національної безпеки в цілому.

Першочерговою ланкою протидії загрозам є їх виявлення. Для ефективного виявлення загроз національному ринку фінансових послуг необхідно створити механізм отримання даних про здійснення кібератак. Важливим фактором має стати закритість такої інформації, щоб суб'єкти ринку фінансових послуг мали можливість повідомляти про здійснення кібератак, не побоюючись зазнати репутаційних втрат через розголошення інформації про вразливість їх комп'ютерних мереж для здійснення кібератак. Також необхідно ухвалити на державному рівні Програму підвищення правової грамотності суб'єктів ринку фінансових послуг, яка має передбачати, зокрема, підвищення правової грамотності відповідних суб'єктів у разі здійснення на них кібератак. Важливість цього зумовлюється також необхідністю розбудови системи ухвалених державою централізованих програм розвитку. Так, Р. В. Яковенко та А. М. Чернега (2012, с. 435) наголошують на факті недостатнього розвитку системи формування, розгляду та затвердження програмних документів на державному рівні. Також відповідні положення мають міститись у Стратегії кібербезпеки України.

Слід зазначити, що наразі в Україні відсутній єдиний центральний орган, що здійснює реалізацію державної політики у сфері кібербезпеки та правоохоронну функцію в цій сфері. Так, у Законі України «Про основні засади забезпечення кібербезпеки України» визначаються такі суб'єкти забезпечення кібербезпеки: Президент України, Рада національної безпеки і оборони України, Національний ко-

ординаційний центр кібербезпеки як робочий орган Ради національної безпеки і оборони України, Кабінет Міністрів України, міністерства та інші центральні органи виконавчої влади, місцеві державні адміністрації, органи місцевого самоврядування, правоохоронні, розвідувальні та контррозвідувальні органи, суб'єкти оперативно-розшукової діяльності, Збройні сили України, інші військові формування, утворені відповідно до закону, Національний банк України, підприємства, установи та організації, віднесені до об'єктів критичної інфраструктури, суб'єкти господарювання, громадяни України та об'єднання громадян, інші особи, які провадять діяльність та/або надають послуги, пов'язані з національними інформаційними ресурсами, інформаційними електронними послугами, здійсненням електронних правочинів, електронними комунікаціями, захистом інформації та кіберзахистом<sup>1</sup>. Водночас, ураховуючи тенденцію до спеціалізації органів, що здійснюють правоохоронну функцію (створення Бюро економічної безпеки України, Національного антикорупційного бюро України, Державного бюро розслідувань тощо), вважаємо доцільним розглянути можливість створення єдиного органу, що здійснюватиме правоохоронну функцію у сфері забезпечення кібербезпеки. Це дасть можливість централізувати зусилля відповідних детективів і слідчих, що наразі працюють у різних органах, та уникнути розпорошення справ по відповідних органах, а отже, підвищить рівень забезпечення державної кібербезпеки. Також заслуговує на увагу думка, викладена у науковій літературі (Yazlyuk et al., 2018, р. 342) щодо важливості створення єдиного мегарегулятора у фінансовій сфері економіки, що мав би реалізовувати державну політику в економічній сфері.

Також, як зазначає К. Г. Гриценко (2020, с. 276), важливим фактором протидії загрозам у кіберсфері є запровадження суб'єктами ринку фінансових послуг міжнародних стандартів інформаційної безпеки, що дасть можливість оптимізувати витрати на здійснення заходів кіберзахисту, знизити ризики від кібератак та більш ефективно здійснювати заходи політики кіберзахисту як окремого суб'єкта, так і держави в цілому. Цю думку також підтримують

<sup>1</sup> Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII // База даних (БД) «Законодавство України» / Верховна Рада (ВР) України. URL: <https://zakon.rada.gov.ua/laws/show/2163-19> (дата звернення: 26.06.2021).

В. В. Домарєв та Д. В. Домарєв (2012), наголошуючи на необхідності приведення системи управління інформаційною безпекою банку у відповідність до міжнародних стандартів у разі, якщо банк хоче створити ефективну систему забезпечення кібербезпеки. Про важливість розроблення ефективного механізму організаційного забезпечення для досягнення високого рівня кіберстійкості зазначає і О. А. Криклій (2020), розглядаючи проблематику забезпечення кіберстійкості банків. Тому пропонується створити спеціальний стимулюючий фінансово-правовий механізм заохочення суб'єктів ринку фінансових послуг до запровадження міжнародних стандартів інформаційної безпеки. Механізми запровадження спеціальних правових режимів уже давно широко використовуються у світі та показали свою перспективність. Основними правовими заходами такого спеціального режиму мають стати податкові пільги для суб'єктів фінансового ринку, які запровадили міжнародні стандарти інформаційної безпеки та діяльність яких відповідає цим стандартам. Додатково можна створити відкритий державний реєстр суб'єктів ринку фінансових послуг, діяльність яких відповідає міжнародним стандартам інформаційної безпеки, з метою отримання такими суб'єктами репутаційних переваг та стимулювання запровадження відповідних стандартів інформаційної безпеки. Також доцільною здається думка окремих науковців (Stetsenko et al., 2019) щодо необхідності реєстрації (а отже, і створення окремого реєстру) та ліцензування всіх суб'єктів, що здійснюють операції з електронними грошима (e-money).

Розглядаючи питання забезпечення кібербезпеки банку, К. Г. Гриценко (2020, с. 277) зазначає, що в технологічному аспекті головним фактором, який позитивно впливає на стан забезпечення кібербезпеки банку, є запровадження інноваційних технологій у сфері кіберзахисту. О. М. Шевченко та Л. В. Рудич (2020), розглядаючи проблематику ринку фінансових технологій, також зазначають, що наразі можна констатувати майже повну відсутність проривних ІТ-технологій у фінансовій сфері та в цілому недостатньо ефективний розвиток фінансових технологій в Україні. Н. П. Чорна (2012, с. 41) також уважає недостатність фінансування науково-технічної та інноваційної діяльності, а також зменшення фінансового і матеріального забезпечення наукових закладів та установ чинниками, що стримують розвиток інноваційної діяльності в цілому. Погоджуючись із цим, пропонуємо створити також спеціальний правовий режим стимулю-

вання створення, розроблення та впровадження інноваційних технологій кіберзахисту у сфері фінансового ринку. Насамперед такий спеціальний режим має передбачати податкові пільги для суб'єктів, які що здійснюють діяльність зі створення, розроблення та впровадження окремих інноваційних технологій, що використовуються у сфері кіберзахисту ринку фінансових послуг, а також заходів державного замовлення здійснення діяльності зі створення та розроблення окремих інноваційних технологій, які мають критичне значення для забезпечення національної кібербезпеки в цілому та кібербезпеки ринку фінансових послуг зокрема, а також прямого фінансування відповідних наукових установ. Наразі підтримка відповідних наукових установ може здійснюватись за рахунок спеціальних фондів підтримки інновацій та наукових досліджень. Так, ст. 49 Закону України «Про наукову та науково-технічну діяльність» містить основні правові засади діяльності й умови роботи Національного фонду досліджень України, завданням якого є підтримка наукових досліджень, інноваційного розвитку та дослідницької інфраструктури, сприяння налагодженню науково-технічного співробітництва та міжнародному обміну інформацією<sup>1</sup>. Також здійснює державну підтримку інноваційних проєктів Фонд розвитку інновацій, який фінансує відповідні проєкти на підставі Постанови Кабінету Міністрів України від 12 грудня 2018 року № 1110<sup>2</sup>. Крім того, державне фінансування наукових досліджень та інновацій здійснює Державна інноваційна фінансово-кредитна установа<sup>3</sup> на підставі тієї ж Постанови Кабінету Міністрів України від 12 грудня

<sup>1</sup> Про наукову та науково-технічну діяльність : Закон України від 26.11.2015 № 848-VIII // БД «Законодавство України» / ВР України. URL: <https://zakon.rada.gov.ua/laws/show/848-19> (дата звернення: 26.06.2021).

<sup>2</sup> Про затвердження Порядку використання коштів, передбачених у державному бюджеті Міністерству фінансів для забезпечення функціонування Фонду розвитку інновацій : Постанова Кабінету Міністрів України від 12.12.2018 № 1110 // БД «Законодавство України» / ВР України. URL: <https://zakon.rada.gov.ua/laws/show/1110-2018-п> (дата звернення: 26.06.2021).

<sup>3</sup> Питання Державної інноваційної фінансово-кредитної установи : Постанова Кабінету Міністрів України від 15.06.2000 № 979 // БД «Законодавство України» / ВР України. URL: <https://zakon.rada.gov.ua/laws/show/979-2000-п> (дата звернення: 26.06.2021).

2018 р. № 1110<sup>1</sup>. Розглядаючи проблематику стимулювання інноваційних лікарських засобів, С. В. Васильєв (2021, с. 25) зазначає, що одним із напрямів удосконалення правового забезпечення є створення окремого підзаконного акта Кабінету Міністрів України, який розмежує компетенцію окремих фондів, що здійснюють підтримки інновацій, з метою уникнення дублювання повноважень та функцій таких фондів, або навіть єдиного фонду підтримки інновацій шляхом об'єднання наявних фондів. Пропонується з метою уникнення розпорошення функцій та надмірної бюрократизації процесу отримання підтримки інноваційних проєктів все ж таки об'єднати наявні фонди і створити єдиний державний Фонд підтримки інноваційного розвитку. Це дасть можливість значно підвищити рівень взаємодії між державним і приватним сектором щодо створення, розроблення та впровадження інноваційних технологій у сфері ринку фінансових послуг і дасть змогу більш ефективно забезпечувати приватних суб'єктів фінансовими ресурсами (що дасть їм можливість поліпшити кадрове й технічне забезпечення), і це відповідно до досліджень Д. В. Дубова (2014, с. 275) має бути одним із провідних напрямів діяльності держави у сфері кібербезпеки.

Окрім стимулювання діяльності суб'єктів, які здійснюють діяльність у сфері створення та розроблення критичних для кібербезпеки ринку фінансових послуг, слід запровадити спеціальний правовий механізм захисту відповідних критичних технологій. При цьому йдеться про велику кількість факторів, яким держава має протидіяти: загрозу саботажу досліджень, технологічний шпіонаж, непрозорість вітчизняного законодавства для інвесторів, правові колізії тощо. Навіть не враховуючи такого фактора, як гібридна війна, у світі спостерігається посилення технологічного шпіонажу навіть союзних держав. Саме тому вкрай важливо створити окремий нормативно-правовий акт, що регулюватиме відносини, пов'язані з інноваційною діяльністю в цілому. Це дасть можливість сконцентрувати всі норми, що регулюють відповідні відносини, в одному документі та значно полегшить правозастосування. Слід зазначити, що проєкт Інноваційного кодексу України було створено та подано на розгляд до Адміністрації Президента у 2011 р. у місті Харкові робочою групою, створеною за розпорядженням Адміністрації Президента України та президії НАПрНУ, однак відповідний документ так і не ухвали-

ли, а отже, відносини продовжують регулюватись нормами, розпорошеними по багатьох нормативно-правових актах. При цьому багато науковців, зокрема Ю. І. Остапенко (2015, с. 62), вже досить давно наголошують на необхідності подальшої кодифікації економічного законодавства та створення спеціальних кодексів, що регулюватимуть основні сфери національної економіки. Іншим варіантом кодифікації норм права, що регулюють відносини, пов'язані з інноваційною діяльністю, є запропонована окремими науковцями модернізація Господарського кодексу України, що полягатиме у виділенні окремої складової Кодексу (наприклад, розділу чи глави «Державна інноваційна політика») з метою створення більш ефективного механізму регулювання відповідних відносин (Задихайло та ін., 2013, с. 111).

Також із метою захисту критичних суб'єктів національного ринку фінансових послуг доцільно створити окремий правовий механізм часткового відшкодування державою збитків, заподіяних критичним суб'єктам ринку фінансових послуг унаслідок кібератак. Такий механізм запропонував А. І. Денисов (2017, с. 129) щодо гарантування державою часткового відшкодування збитків у певних випадках стосовно критичних суб'єктів для національної інноваційної безпеки. Принцип часткової компенсації збитків допоможе зберегти від банкрутства окремі критичні для національного ринку фінансових послуг підприємства, що може бути вкрай важливим для національної безпеки в цілому, враховуючи зростання ризиків кібератак та агресію у віртуальному просторі в умовах гібридної війни.

Для запровадження такого правового механізму часткового відшкодування державою збитків, заподіяних критичним суб'єктам ринку фінансових послуг унаслідок кібератак, необхідно створити спеціальний фонд бюджету України, а також окремий орган, що визначатиме розмір відповідного відшкодування, скласти перелік критичних суб'єктів для ринку фінансових послуг, а також установити критерії, що даватимуть можливість надавати відповідну фінансову допомогу.

Ураховуючи важливість модернізації правового механізму забезпечення кібербезпеки ринку фінансових послуг, доцільно створити окремий нормативно-правовий акт, який міститиме основні норми, що регулюють відносини у зазначеній сфері. Це допоможе уникнути розпорошення норм по багатьох окремих нормативно-правових актах і дасть можливість значно полегшити правозастосування як для суб'єктів ринку фінансових послуг, так і

<sup>1</sup> Там само.

для органів державної влади, а також полегшить розуміння відповідних норм потенційних інвесторів, що збільшить перспективи інвестування у суб'єктів ринку фінансових послуг.

**ВИСНОВКИ.** За результатами дослідження запропоновано цілісний правовий механізм забезпечення кібербезпеки ринку фінансових послуг. На основі поглядів науковців і власних досліджень запропоновано такі нові засоби забезпечення кібербезпеки на ринку фінансових послуг:

1) створення механізму отримання даних про здійснення кібератак і відповідного закритого реєстру з метою більш ефективної протидії таким кібератакам та збору інформації щодо кібератак для подальшого аналізу компетентними державними органами;

2) ухвалення на державному рівні Програми підвищення правової грамотності суб'єктів ринку фінансових послуг;

3) створення єдиного органу, що здійснюватиме правоохоронну функцію у сфері забезпечення кібербезпеки;

4) створення спеціального стимулюючого фінансово-правового механізму заохочення суб'єктів ринку фінансових послуг до запровадження міжнародних стандартів інформаційної безпеки;

5) створення відкритого державного реєстру суб'єктів ринку фінансових послуг, діяльність яких відповідає міжнародним стандартам інформаційної безпеки;

6) створення спеціального правового режиму стимулювання створення, розроблення та впровадження інноваційних технологій кіберзахисту у сфері фінансового ринку;

7) створення єдиного державного фонду підтримки інноваційного розвитку, об'єднавши на його базі інші фонди, що стимулюють інноваційний розвиток;

8) створення окремого правового механізму часткового відшкодування державою збитків, заподіяних критичним суб'єктам ринку фінансових послуг унаслідок кібератак.

Перспективи подальших досліджень полягають у встановленні конкретних правових заходів у межах запропонованих спеціальних режимів у сфері забезпечення кібербезпеки на ринку фінансових послуг, визначенні окремих загроз кібербезпеці на ринку фінансових послуг і встановленні конкретних правових засобів подолання або ліквідації таких загроз, створенні макетів і проектів нормативно-правових актів, що дадуть можливість ефективно застосовувати запропоновані правові засоби забезпечення кібербезпеки на ринку фінансових послуг.

#### СПИСОК БІБЛІОГРАФІЧНИХ ПОСИЛАНЬ

1. Боженко В. В., Койбічук В. В., Габенко М. М. Вплив кібершахрайств на фінансову систему на прикладі країн Євросоюзу. *Вісник Сумського державного університету. Серія: Економіка*. 2021. № 2. С. 47–52. DOI: <https://doi.org/10.21272/1817-9215.2021.2-6>.
2. Васильєв С. В. Правові засади державної підтримки створення інноваційних лікарських засобів. *Право і безпека*. 2021. № 2 (81). С. 21–26. DOI: <https://doi.org/10.32631/pb.2021.2.02>.
3. Гриценко К. Г. Шляхи підвищення ефективності забезпечення кібербезпеки банку. *Інфраструктура ринку*. 2020. Вип. 45. С. 274–279. DOI: <https://doi.org/10.32843/infrastruct45-44>.
4. Денисов А. І. Господарсько-правове забезпечення технологічної безпеки держави : монографія. Харків : Юрайт, 2017. 232 с.
5. Домарєв В. В., Домарєв Д. В. Управління інформаційною безпекою в банківських установах (теорія і практика впровадження стандартів серії ISO 27k). Донецьк : Велстар, 2012. 146 с.
6. Дубов Д. В. Кіберпростір як новий вимір геополітичного суперництва : монографія. Київ : НІСД, 2014. 328 с.
7. Інноваційне інвестування в Україні: проблеми правового забезпечення : монографія / за наук. ред. Д. В. Задихайла. Харків : Юрайт, 2013. 536 с.
8. Криклій О. А. Теорія та практика забезпечення кіберстійкості банків. *Ефективна економіка*. 2020. № 10. DOI: <https://doi.org/10.32702/2307-2105-2020.10.50>.
9. Остапенко Ю. І. Щодо тенденцій розвитку господарського законодавства України // Актуальні питання цивільного та господарського права : зб. матеріалів круглого столу (м. Полтава, 24 груд. 2015 р.) / редкол.: А. П. Гетьман, Н. О. Гуторова та ін. Полтава, 2015. С. 61–62.
10. Сіденко В. Деградація економічних відносин України та Росії: що далі? *Національна безпека і оборона*. 2014. № 5/6. С. 92–96.
11. Чорна Н. П. Галузеві фактори інноваційного розвитку сфери виробництва продуктів харчування. *Економічний часопис – XXI*. 2012. № 11/12. С. 40–42.
12. Шевченко О. М., Рудич Л. В. Розвиток фінансових технологій в умовах цифровізації економіки України. *Ефективна економіка*. 2020. № 7. DOI: <https://doi.org/10.32702/2307-2105-2020.7.61>.
13. Яковенко Р. В., Чернега А. М. Інноваційна діяльність в Україні: проблеми та перспективи. *Наукові праці Кіровоградського національного технічного університету. Економічні науки*. 2012. Вип. 22. С. 434–439.

14. Basic principles of financial markets regulation and legal aspects of the legislative requirements / B. Yazlyuk, A. Guley, R. Brukhanskyi et al. *Investment Management and Financial Innovations*. 2018. Vol. 15, No. 1. Pp. 337–349. DOI: [https://doi.org/10.21511/imfi.15\(1\).2018.28](https://doi.org/10.21511/imfi.15(1).2018.28).

15. Financial and legal regulation of electronic money circulation in developed countries / S. Stetsenko, O. Yu. Syniavska, M. L. Shelukhin et al. *Journal of Legal, Ethical and Regulatory Issues*. 2019. Vol. 22. Spec. Iss. 2. URL: <https://www.abacademies.org/articles/Financial-and-Legal-regulation-of-electronic-money-circulation-in-developed-countries-1544-0044-22-SI-2-377.pdf> (дата звернення: 26.06.2021).

Надійшла до редакції: 29.06.2021

### **БРУСАКОВА О. В., ГЕТМАНЕЦ О. П. МОДЕРНИЗАЦІЯ МЕХАНІЗМА ПРАВОВОГО ОБЕСПЕЧЕННЯ КИБЕРБЕЗОПАСНОСТІ РЫНКА ФИНАНСОВЫХ УСЛУГ**

Рассмотрены основные подходы к противодействию угрозам кибербезопасности на рынке финансовых услуг. Предложено создать новые и модернизировать уже существующие правовые средства обеспечения кибербезопасности на рынке финансовых услуг, а также новые специальные правовые режимы для субъектов рынка финансовых услуг с целью повышения уровня кибербезопасности. Подчеркнута важность создания единого государственного фонда поддержки инновационного развития, который должен осуществлять стимулирование привлечения инновационных технологий в финансовый сектор с целью повышения уровня кибербезопасности рынка финансовых услуг. Подчеркнута важность создания механизма гарантирования государством частичного возмещения убытков субъектам рынка финансовых услуг, причиненных в результате кибератак.

**Ключевые слова:** кибербезопасность, рынок финансовых услуг, экономическая безопасность, средства правового обеспечения, специальный правовой режим.

### **BRUSAKOVA O. V., GETMANETS O. P. MODERNIZATION OF THE MECHANISM OF THE FINANCIAL SERVICES MARKET CYBERSECURITY LEGAL SUPPORT**

Due to the rapid development of digital technologies, the role of the Internet segment of the financial services market is actively increasing. That is why the issue of cybersecurity in this market is now gaining national importance and is becoming critical to national security. The methodological basis of the study is systemic, and the study used a comprehensive approach, which is manifested in the use of different methods of scientific knowledge depending on specific aspects of the study. The methodological basis of the study is the dialectical method of phenomena and processes cognition. In particular, the comparative legal method, the system and structural method, the statistical method, the logical legal method, the formal legal method and the method of analogy were used.

The main scientific approaches to counteracting cybersecurity threats in the financial services market are considered. It is proposed to create new and modernize existing legal means to ensure cybersecurity in the financial services market. Emphasis is placed on the need to create a mechanism to stimulate entities engaged in the creation and development of information technology used in the financial services market, and a mechanism to protect such technology. It is proposed to create new special legal regimes for financial services market participants in order to increase the level of cybersecurity. The importance of creating a single state fund to support innovative development is emphasized, which should stimulate the involvement of innovative technologies in the financial sector in order to increase the level of cybersecurity of the financial services market. It is proposed to create a mechanism for the state to guarantee partial compensation to financial market entities for losses caused by cyber attacks, and to form a separate state body that will determine the amount of compensation, compile a list of critical entities for the financial services market, and establish criteria that will provide appropriate financial assistance. The importance of adopting a separate legal act, which will contain the basic rules governing relations in the field of cybersecurity of the financial services market, is emphasized.

**Key words:** cybersecurity, financial services market, economic security, legal remedies, special legal regime.

**Цитування (ДСТУ 8302:2015):** Брусакова О. В., Гетманець О. П. Модернізація механізму правового забезпечення кібербезпеки ринку фінансових послуг. *Право і безпека*. 2021. № 3 (82). С. 77–83. DOI: <https://doi.org/10.32631/pb.2021.3.08>.

**Citation (APA):** Brusakova, O. V., & Getmanets, O. P. (2021). Modernization of the Mechanism of the Financial Services Market Cybersecurity Legal Support. *Law and Safety*, 3(82), 77–83. <https://doi.org/10.32631/pb.2021.3.08>.