УДК 336.02 JEL Classification D81, E44, G15, G18, G21

КОМПАРАТИВНИЙ АНАЛІЗ НАГЛЯДОВО-РЕГУЛЯТОРНОГО ЗАБЕЗПЕЧЕННЯ ПРОЦЕДУР ФІНАНСОВОГО МОНІТОРИНГУ ТА КІБЕРБЕЗПЕКИ[1]

Лєонов С. В.,
доктор економічних наук, професор, Сумський державний університет,
e-mail: s.leonov@biem.sumdu.edu.ua
http://orcid.org/ 0000-0001-5639-3008
Кузьменко О. В.,
доктор економічних наук, професор, Сумський державний університет,
e-mail: o.kuzmenko@biem.sumdu.edu.ua
https://orcid.org/0000-0001-8520-2266
Койбічук В. В.,
кандидат економічних наук, доцент,
Сумський державний університет
e-mail: v.koibichuk@biem.sumdu.edu.ua
http://orcid.org/ 0000-0002-3540-7922
Горай Д. С.,
студентка
Сумський державний університет
e-mail: d.horai@student.sumdu.edu.ua
https://orcid.org/0000-0002-9668-6822

Шляхи покращення процедур фінансового моніторингу, організацій кібербезпеки за умов переходу економіки держави на цифровий формат, розвитку процесів інноваційної цифровізації, рівня інформаційної обізнаності суспільства є постійно актуальною задачею сьогодення. За відсутності загального консенсусу щодо застосування конкретних міжнародно-правових норм у сфері кібербезпеки окремі держави в односторонньому порядку визначають свої національні позиції. Тому важливим є питання визначення особливостей кожної системи для безпечної та коректної організації взаємо корисної співпраці, з одного боку, та покращення власних практик та процедур протидії відмиванню кримінальних доходів, отримання якісно нових знань щодо найменших проявів ризиків та їх упередження, застосування відповідних превентивних заходів ще на стадії зародження, з іншого боку. В статті проведено компаративний аналіз правого забезпечення кіберзахисту та кібербезпеки фінансової системи та інформаційно-комунікаційних технологій Німеччини, Польщі, України, Сполучених Штатів Америки, Швейцарії, Європейського Союзу. Узагальнюючий алгоритм фінансового моніторингу розглянуто в розрізі країн-членів Євросоюзу, що ґрунтується на діючих положеннях Директиви 2018/843/EU Європейського Парламенту та Ради Європейського про запобігання використанню фінансової системи з метою відмивання коштів та фінансування тероризму. Основними положеннями, на яких ґрунтується алгоритм Єврокомісії є: відкритий доступ до реєстрів бенефіціарних власників компаній, що посилює прозорість аналізованої інформації про фінансові транзакції; прозорість інформації про трасти і подібних до них структур; розширення кола зобов'язаних суб'єктів (постачальників електронних гаманців та платформи обміну віртуальних валют), посилення можливостей компетентних органів фінансової розвідки країн Євросоюзу в частині запиту, отримання і використання інформації від зобов'язаних суб'єктів; дотримання критеріїв перевірки фінансових операцій, що здійснюються із залученням країн, які мають високий ступінь ризику.

Ключові слова: кібербезпека, фінансовий моніторинг, цифрові дані, контент-аналіз, компаративний аналіз, нормативно-регуляторне забезпечення.

DOI: 10.21272/1817-9215.2021.3-18

ВСТУП

Процеси технологізації фінансових інструментів, стрімке впровадження інноваційних інформаційних технологій в бізнес-процеси національних економік, банківську сферу, соціально-політичну сферу, освітні системи з одного боку сприяють соціальному розвитку, економічному зростанню, процвітанню та

[1] Робота виконана в рамках дослідження за фінансування Національного фонду досліджень України № 2020.01/0185 "Оптимізація та автоматизація процесів фінансового моніторингу для зростання інформаційної безпеки України".

конкурентоспроможності країн на світовій арені, а з іншого – викликають зростання масштабів транскордонної економічної злочинності, збільшення та розповсюдження різноманітних схем кіберзлочинності, збільшення кількості обсягів нелегально отриманих доходів, що супроводжується вдосконаленням механізмів відмивання кримінальних коштів. Легалізація кримінальних доходів чинить деструктивний вплив як на стійкість окремо взятої фінансової установи, так і на стабільність фінансової системи країни, її інвестиційну привабливість, а також на довіру з боку міжнародних партнерів та організацій. За аналітичними даними провідної компанії «Cybersecurity Ventures» [1], що займається дослідженням глобальної кіберекономіки, статистикою кібербезпеки, у 2021 р. збитки від кібершахрайств складають: 6 трильйонів дол. США на рік, 500 млн. дол. США – на місяць, 115,4 млн дол. США – на тиждень, 16, 4 млн. дол. США – на день, 684,9 млн. дол. США – на годину, 11, 4 млн. дол. США – на хвилину, 190 тис. дол. США – на секунду. Атаки на бізнес у 2021 році будуть здійснюватися кожні 11 секунд, порівняно з 40 секундами у 2016. Якщо провести аналогію поняття «кіберзлочинність» з поняттям «економіка країни», то кіберзлочинність є третьою за величиною економікою світу після США та Китаю. У міру того, як інформаційні технології все більше інтегруються в операції з фізичною інфраструктурою, зростає ризик масштабних подій або наслідків, які можуть завдати шкоди або порушити роботу послуг, від яких залежить економіка країн та повсякденне життя мільйонів громадян. Отже, надзвичайно важливим та актуальним є питання вивчення передових практик світу в розрізі організації та особливостей процедур фінансового моніторингу, систем кібербезпеки з метою посилення стійкості національних економік до викликів кібершахрайств.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ ТА ПУБЛІКАЦІЙ

Питання якісної організації кібербезпеки даних є багатоаспектним та мультизадачним, дослідженням якого активно займаються науковці світу протягом минулого десятиліття.

Перелік ключових слів, що в характеризують фінансову кібербезпеку зображено на рисунку 1, який сформовано за результатами проведеного бібліометричного аналізу 500 наукових публікацій за період з 2018 по 2021 рік, проіндексованих базою даних Web of Science.

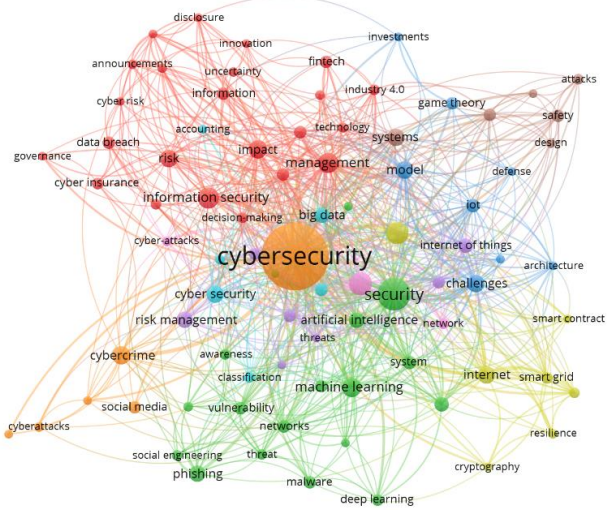

Рисунок 1 – Бібліометричний аналіз наукових публікацій за тематикою фінансової кібербезпеки

Джерело: побудовано авторами інструментарієм Vosviewer 1.6.15 на основі публікацій, індексованих базою даних Web of Science

Граф містить 84 ключових слова, що використовують спільно науковці світу в мінімальній кількості 5 одиниць, містить розподіл на 9 кластерів та має 807 взаємозв'язків (рис. 1).

Велику зацікавленість викликає праця науковців [2], де автори акцентують на необхідності стабільного фінансування науково-дослідної діяльності в галузі кібербезпеки як довгострокової інвестиції для отримання майбутніх прибутків і захисту суспільства від наслідків кібератак та кібершахрайств, що є важливою частиною національної стратегії безпеки. Їх дослідження ґрунтується на статистичних даних компаній-лідерів з кібербезпеки США та Великої Британії за період з 2016 по 2020 рік. Результати показують, що керівники з кібербезпеки використовують зовнішні кошти для фінансування науково-дослідних робіт, щоб досягти високих майбутніх прибутків, навіть за умов впливу факторів невизначеності. Аналіз факторів, які здійснюють мінімізацію впливу комунікаційних загроз, в роботі [3] вчені пропонують здійснювати за рахунок удосконалення фінансової звітності систем обліку з використанням механізмів зворотних комунікацій.

ПОСТАНОВКА ЗАВДАННЯ

Метою даного дослідження є проведення компаративного аналізу діючого правового регуляторного та наглядового забезпечення провідних систем фінансового моніторингу та кіберзахисту як потенційно важливих джерел щодо посилення рівня національної безпеки.

МЕТОДИ ДОСЛІДЖЕННЯ

У процесі дослідження використовувались методи макропруденційного аналізу, компаративного аналізу, контент-аналізу, систематизації, порівняння, логічного узагальнення, структурного аналізу, бібліометричного аналізу (з використанням інструментарію Vosviewer).

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Формування безпечного та сучасного цифрового середовища, здатного забезпечити надійну, економічно вигідну та безпечну інфраструктуру та послуги, в ногу з новими методами роботи та спільної роботи, що узгоджуються із очікуваннями персоналу, громадян, бізнесу та зацікавлених сторін, запропоновано Європейською комісією, яка є вищим органом виконавчої влади Європейського союзу (відповідає за підготовку законопроектів, виконання рішень Європарламенту та Ради, здійснює контроль за дотриманням договорів ЄС та інших правових актів та поточних справ союзу), здійснювати наступним алгоритмом дій та процедур.

Відліковою точкою є стандартний набір правил Європейської системи фінансового нагляду [4] для регулювання та нагляду за банківською діяльністю у всіх країнах ЄС, адже саме банківська система є найбільш вразливою для використання великої кількості різноманітних витончених шахрайських схем із залученням всіх учасників фінансових операцій: клієнтів банку (фізичних чи юридичних осіб), співробітників банків, економічних агентів (підприємства, фірми), держава. Європейський банківських орган (ЕВА) є незалежним органом ЄС, який працює над забезпеченням ефективного та послідовного рівня пруденційного регулювання та нагляду в усьому європейському банківському секторі. Його загальні цілі – підтримка фінансової стабільності в ЄС та забезпечення цілісності, ефективності та впорядкованого функціонування банківського сектору. Крім того, ЕВА є частиною Європейської системи фінансового нагляду (ESFA), до складу якої входять також наглядові органи: Європейський орган з цінних паперів і ринків (ESMA) та Європейський орган страхування та пенсійного забезпечення (EIOPA). Система також включає Європейську раду з системних ризиків (ESRB), а також Спільний комітет європейських наглядових органів та національних наглядових органів. Отже ЕВА

встановлює рекомендації щодо нагляду за фінансовими установами та виявляє порушення законодавства ЄС.

В Європі станом на січень 2020 р. активно функціонували 5411 банківських установ. Це потужна кількість в порівнянні з переліком інших соціально-економічних об'єктів. Та значний внесок в розвиток фінансових систем країн Європи здійснює саме банківська система. Кількість банків у Німеччині – 1531, у Польщі – 627, в Австрії – 522, в Італії – 485, у Франції – 406, у Великобританії – 401, в Ірландії – 312, у Фінляндії – 241, в Іспанії – 196, у Швеції – 154, у Португалії – 147, у Люксембурзі – 127, у Данії – 100, у Нідерландах – 93, у Бельгії – 84, у Литві – 83, у Румунії – 75, у Чехії – 58, у Латвії – 54 , в Угорщині – 46, в Естонії – 38, у Греції – 35, у Словаччині – 27, на Мальті – 25, у Болгарії – 25, у Хорватії – 24, у Словенії – 17.

Так, динаміку стану банківської системи країн ЄС на основі значень банківських структурних показників, що характеризують якість банківської системи, а саме кількості акцій 5 найбільших кредитних установ в загальному обсязі активів (CI5) за минуле десятиліття наведено в таблиці 1, яку сформовано на основі статистичних даних, що офіційно публікуються Європейським центральним банком [5].

Таблиця 1 – Банківські структурні індикатори: частка 5 найбільших кредитних установ у загальних активах (CR5, відсотки)

Країна ЄС / Рік	2020	2019	2018	2017	2016	2015	2014	2013	2012	2011	2010	Спарклайн
Австрія	38,52	36,01	36,02	36,07	34,45	35,76	36,84	36,72	36,49	38,38	35,87	
Бельгія	75,3	73,98	73,4	68,8	66,19	65,45	65,79	63,99	66,35	70,77	74,86	
Болгарія	67,1	62,51	59,69	56,48	58,03	57,64	55,03	49,85	50,38	52,58	55,17	
Кіпр	86,48	85,7	86,92	84,16	65,78	67,51	63,4	64,06	62,55	60,68	64,23	
Чехія	65,26	64,77	64,49	63,68	63,89	62,51	60,86	62,04	61,38	61,9	62,63	
Німеччина	34,03	31,22	29,1	29,71	31,35	30,56	32,12	30,59	33,01	33,55	32,6	
Данія	67,1	66,2	64,5	65,65	68,33	67,78	68,08	68,38	65,61	66,3	64,42	
Естонія	93,73	92,95	90,97	90,3	88,04	88,63	89,85	89,71	89,6	90,64	92,26	
Іспанія	66,43	67,42	68,53	63,73	61,8	60,2	58,3	54,4	51,4	48,1	44,3	
Фінляндія	80,07	80,36	81,61	73,46	80,52	88,02	89,73	87,11	85,95	86,9	89,17	
Франція	49,17	48,66	47,73	45,38	45,95	47,23	47,64	46,74	44,62	48,27	47,4	
Велика Британія	31,05	31,21	31,82	36,88	35,49	36,99	38,85	43,67	42,82	43,55	42,52	
Греція	97,03	97,35	96,83	96,98	97,28	95,23	94,06	94,01	79,47	71,99	70,64	
Хорватія	80,52	79,79	79,42	72,79	73	72,65	72,27	72,85	73,94	72,13	71,05	
Угорщина	50,09	52,72	50	49,64	49,83	49,38	49,3	51,89	54,02	54,63	54,64	
Ірландія	55,68	49,71	46,13	45,51	44,27	45,93	47,56	47,83	46,4	46,72	49,88	
Італія	49,34	47,88	45,59	43,43	43	41	41	39,6	39,68	39,46	39,84	
Литва	91,85	90,44	90,93	90,13	87,1	86,85	85,7	87,1	83,63	84,75	78,83	
Люксембург	31,6	27,68	26,31	26,18	27,63	31,27	31,95	33,72	33,08	31,21	31,11	
Латвія	87,77	83,18	80,93	73,6	66,6	64,58	63,6	64,13	64,05	59,57	60,43	
Мальта	74,81	75,14	77,52	80,85	80,27	81,32	81,49	76,48	74,44	71,96	71,28	
Нідерланди	84,32	84,71	84,67	83,84	84,72	84,59	85,01	83,83	82,07	83,56	84,2	
Польща	54,28	49,8	49,51	47,51	47,73	48,63	48,31	45,24	44,4	43,69	43,37	
Португалія	73,56	73,34	72,95	73,12	71,2	72,32	69,23	70,26	69,95	70,76	70,86	
Румунія	62,4	62,6	61,6	59,5	59,1	57,4	54,2	54,4	54,7	54,6	52,7	
Швеція	55,15	54,83	54,28	58,17	56,28	57,83	58,54	58,26	57,42	57,81	57,78	
Словенія	67,34	60,93	60,79	61,53	60,99	59,15	55,61	57,08	58,35	59,33	59,27	
Словаччина	76,78	75,69	75,57	74,54	72,72	72,3	70,69	70,32	70,72	72,23	72,03	

Джерело: побудовано авторами на основі статистичних даних [5]

Далі органи нагляду за боротьбою з відмиванням грошей контролюють, на скільки добре зобов'язані суб'єкти виконують свої завдання. Такими зобов'язанами організаціями є фінансові установи, визначені нефінансові підприємства та професійні спілки. Також здійснюється перевірка операцій в ЄС та третіх країнах через банківських юристів, бухгалтерів.

Перш ніж допустити проведення транзакцій в країнах EU або через країну чи декілька країн здійснюється ретельна перевірка клієнтів: моніторинг з боку зобов'язаних суб'єктів, які повинні переконатися, що вони знають, хто є їхнім клієнтом [6]. Якщо підозріла операція ідентифікована, то зобов'язана організація

надсилає звіт до відділу фінансової розвідки (FIU) відповідної держави-члену ЄС. Відділ фінансової розвідки має спеціальні інструменти для здійснення якісного аналізу. Такими інструментами є доступ до реєстрів бенефіціарних власників, де зазначається, хто є справжнім бенефіціаром компанії чи тресту, а також доступ до реєстрів рахунків Центрального банку з відображенням детальної інформації у кого який рахунок і де він розміщується. Якщо аналіз щодо небезпечності фінансових транзакцій підтверджується, то відділ фінансової розвідки надсилає його до правоохоронних органів, наглядового чи іншого компетентного органу.

Особливо ретельно здійснюються зобов'язаними суб'єктами фінансових установ моніторинг транзакцій, які проводяться через країни із високим рівнем ризику, які мають стратегічні недоліки у своїх режимах протидії відмиванню коштів та фінансуванню тероризму, та які становлять значну загрозу для фінансової системи Євросоюзу. Перелік цих країн згідно діючої 5 Директиви Євросоюзу щодо відмивання коштів станом на 2020 р. наступний [7]: Багамські острови, Барбадос, Ботсвана, Камбоджа, Гана, Ямайка, Маврикій, М'янма, Нікарагуа, Панама, Зімбабве. При цьому такі країни як Афганістан, Корейська Народно-Демократична Республіка (КНДР), Іран, Ірак, Сирія, Уганда, Вануату, Ємен знаходять у списку високоризикованих з 2016 року, а Пакистан, Тринідад і Тобаго – з 2018 року.

Переходячи до питання організації кібербезпеки фінансових систем країн зупинимося на діючих державних системах кібербезпеки в розрізі окремих країн та країн-членів ЄС. Так, якщо розглядати діяльність державних органів країн Євросоюзу, які здійснюють фінансовий моніторинг та мають забезпечувати кіберзахист як фінансового сектору, так і ІТ сектору, що безпосередньо є ключовим ланцюгом при здійсненні цифрових транзакцій, то, наприклад, в Германії з 2011 року створено Національний центр кібербезпеки (NCAZ), основними задачами якого є збір інформації та упередження кібератак на ІТ-системи на ранній стадії [8].

Стратегічним документом у постійному процесі дій урядової адміністрації на 2017-2022 роки, спрямованих на підвищення рівня кібербезпеки Польщі є Національна рамка політики кібербезпеки [9]. Основною його метою є забезпечення високого рівня безпеки державного та приватного секторів, а також громадян у процесі надання або використання основних послуг та цифрових послуг. Крім того, положення Національної рамки політики кібербезпеки спрямовані на збільшення спроможності до національно скоординованих дій щодо запобігання, виявлення, боротьби та мінімізації впливу інцидентів, які ставлять під загрозу безпеку інформаційно-комунікаційних технологій, життєво важливих для функціонування держави; посилення спроможності протидіяти кіберзагрозам; підвищення національного потенціалу та компетенції у сфері безпеки у кіберпросторі; побудову міцних міжнародних позицій в галузі кібербезпеки. Зокрема, між Польщею та НАТО підписано угоду в сфері кібербезпеки в липні 2019 року, яка є правовою нормативною базою для можливого використання альянсом команд та швидкого реагування на загрози в кіберпросторі [10]

В Україні у 2017 році створено Центр кіберзахисту Національного банку України, який поєднує та координує зусилля у сфері забезпечення кібербезпеки та кіберзахисту в банківському та фінансовому секторах України. З 2018 року у складі Центру кіберзахисту Національного банку України функціонує команда реагування на кіберінциденти в банківській системі (CSIRT-NBU). У серпні 2019 року Центр кіберзахисту Національного банку України та Державний центр кіберзахисту Державної служби спеціального зв'язку та захисту інформації України підписали Меморандум про взаємодію та співробітництво в сфері кібербезпеки та кіберзахисту, спрямовану на попередження, виявлення, ефективне реагування та протидію актуальним кіберзагрозам, підвищення рівня інформаційної безпеки та ситуаційної обізнаності у сфері кібербезпеки та кіберзахисту.

Агентство кібербезпеки та безпеки інфраструктури (CISA), створене наприкінці 2018 року, є федеральною агенцією США та оперативним компонентом Міністерства

внутрішньої безпеки [11]. Основною метою діяльності Агентства кібербезпеки та безпеки інфраструктури є надання оперативної довідкової інформації зацікавленим сторонам про конкретні кібер- або фізичні загрози для певної критичної інфраструктури країни на основі даних розвідувальних служб США, проведення операцій з управління інцидентами та ризиками з використанням програмного інструментарію, технічних послуг, регуляторного забезпечення (якщо це дозволено на законодавчому рівні), надання оцінки вразливості інформації, а також розроблення комплексного набору заходів щодо упередження можливих кібератак чи фізичних загроз, а у випадку їх настання – розроблення стратегій щодо пом'якшення наслідків. Наразі в Україні у вересні 2021 року розпочато співпрацю з Агентством з кібербезпеки та безпеки інфраструктури США, що є надзвичайно важливим кроком у посиленні національної безпеки України [12]. В розрізі даної співпраці до кінця року буде укладено угоду, де передбачається: здійснити побудову платформи взаємообміну інформацією про кіберінциденти в інтересах системи управління інцидентами та відновлення після них; здійснювати спільні дії щодо захисту об'єктів критичної інформаційної інфраструктури та надання сторонам-партнерам відповідної інформації для покращення системи реагування на кіберінциденти; здійснювати обмін досвідом у рамках системи управління ризиками, що дозволить забезпечити національну стійкість України; використання досвіду США з організації взаємодії у сфері кібербезпеки з приватним сектором; формування кадрового потенціалу з кібербезпеки шляхом проведення навчальних курсів на базі CISA, тренінгів, спільних навчань.

У 2016 р. з метою забезпечення захисту конфіденційних даних при здійсненні трансатлантичних операцій при передачі персональних даних з Європейської економічної зони (ЄЕЗ) до США Міністерством торгівлі США, Європейською комісією та Швейцарською адміністрацією було розроблено програму Privacy Shield. У січні 2017 року Федеральний уряд Швейцарії оголосив про схвалення даної програми як дійсний юридичний механізм для дотримання швейцарських вимог під час передачі персональних даних зі Швейцарії до Сполучених Штатів [13]. Програма Privacy Shield надає ряд важливих переваг організаціям США та їх партнерам в Європі: вимоги щодо відповідності фінансових транзакцій регламентуючим документам чітко викладені та економічно ефективні, що особливо має приносити користь малим та середнім підприємствам. Також гарантується, що організації-учасники забезпечують «адекватний» захист конфіденційності, в тому числі з використанням технологій блокчейн [14]. Детальні рекомендації про заходи, які доповнюють інструменти передачі для забезпечення відповідності рівню захисту персональних даних ЄС були розроблені Європейською радою із захисту даних (GDPR) у 2020 та прийняті до використання у 2021. Комплексний опис подано алгоритмом щодо дотриманням 6 кроків: «Знати, що передається», «Ідентифікувати інструменти передачі, до яких є довіра», «Оцінити, чи ефективний інструмент передачі відповідно до статті 46 GDPR, до якого є довіра», «Застосувати додаткові заходи», «Здійснити процедурні дії, якщо визначено ефективні додаткові заходи», «Повторно оцінювати через відповідні проміжки часу».

ВИСНОВКИ

В результаті проведеного макропруденційного аналізу наведено тенденції розвитку та змісту провідних систем фінансової кібербезпеки та кіберзахисту інформації. Контент-аналіз нормативно-регулюторного забезпечення процедур фінансового моніторингу фінансових транзакцій дозволив визначити їх особливості в розрізі економіко-політичного забезпечення для протидії відмивання кримінальних доходів та організації кібербезпеки фінансово-інформаційної сфери. Безпечна співпраця вимагає, щоб сторони, які співпрацюють, застосовували правильні політики для своєї взаємодії. Отримані результати щодо організації якісно розробленої дорожньої карти фінансового моніторингу на прикладі країн Євросоюзу слугують підґрунтям в

коротко- та довгостроковій перспективі кіберкультурим модифікаціям як для економічних агентів, так і держави.

SUMMARY

S. Lyeonov, O. Kuzmenko, V. Koibichuk, D. **Horai Comparative analysis of supervisory and regulatory support of financial monitoring and cyber security procedures**

Ways to improve the procedures of financial monitoring, cybersecurity organizations in the transition of the state economy to digital format, the development of innovative digitization, the level of information awareness of society is an urgent task today. In the absence of a consensus on the application of specific international law in the field of cybersecurity, individual states unilaterally determine their national positions. Therefore, it is important to determine the specifics of each system for safe and correct organization of mutually beneficial cooperation, on the one hand, and to improve their own practices and procedures to combat money laundering, gain qualitatively new knowledge on the least manifestations of risks and their prevention. stage of origin, on the other hand. The article presents a comparative analysis of the legal support of cyber defense and cybersecurity of the financial system and information and communication technologies of Germany, Poland, Ukraine, the United States, Switzerland, and the European Union. The generalized algorithm of financial monitoring is considered in the context of EU member states, based on the current provisions of Directive 2018/843 / EU of the European Parliament and of the Council of Europe on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing. The main provisions on which the European Commission's algorithm is based are: open access to the registers of beneficial owners of companies, which increases the transparency of the analyzed information on financial transactions; transparency of information about trusts and similar structures; expanding the range of obligated entities (suppliers of e-wallets and virtual currency exchange platform); strengthening the capacity of the competent Financial Intelligence Units of the European Union to request, receive and use information from obligated entities; compliance with the criteria for verification of financial transactions carried out with the involvement of countries with a high degree of risk. The results obtained on the organization of a well-developed roadmap for financial monitoring on the example of the European Union serve as a basis for short- and long-term cybercultural modifications for both economic agents and the state.

Keywords: cybersecurity, financial monitoring, digital data, content analysis, comparative analysis, regulatory support.

СПИСОК ЛІТЕРАТУРИ

1. Cybercrime To Cost The World $10.5 Trillion Annually By 2025 : Cybersecurity Ventures. URL : https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/
2. Ponce G., Gonzales Ch., Al-Mohareb M. (2021). Sustainable finance in cybersecurity investment for future profitability under uncertainty. *Journal sustainable finance & investment, Ahead-of-Print*, 1-20. https://doi.org/10.1080/20430795.2021.1985951
3. Zadorozhnyi, Z.-M., Ometsinska, I., & Muravskiy, V. (2021). Determinants of Firm's Innovation: Increasing the Transparency of Financial Statements. *Marketing and Management of Innovations, 2*, 74-86. http://doi.org/10.21272/mmi.2021.2-06
4. European Banking Authority: regulation and policy. URL : https://www.eba.europa.eu/regulation-and-policy
5. Statistical Data Warehouse: European Central Bank. Eurosystem. URL: https://sdw.ecb.europa.eu/
6. Holobiuc, A.-M. (2021). Determinants of economic growth in the European Union. An empirical analysis of conditional convergence. *SocioEconomic Challenges, 5*(2), 26-34. https://doi.org/10.21272/sec.5(2).26-34.2021
7. EU policy on high-risk third counties: European Commission. URL : https://ec.europa.eu/info/business-economy-euro/banking-and-finance/financial-supervision-and-risk-management/anti-money-laundering-and-countering-financing-terrorism/eu-policy-high-risk-third-countries_en
8. Federal Ministry of the Interior, Building and Community. URL : https://www.bmi.bund.de/EN/home/home_node.html;jsessionid=D13F8E960D4B632B90E39479212306A6.2_cid295
9. National framework of cybersecurity policy of the Republic of Poland for 2017-2022. URL : https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Cybersecuritystrategy_PL.pdf
10. Новини, політика, технології. URL : https://mind.ua/news/20199350-polshcha-i-nato-vpershe-pidpisali-ugodu-v-sferi-kiberbezpeki
11. Cybersecurity and Infrastructure Security Agency. URL: https://www.cisa.gov/cybersecurity
12. Розпочинаємо співпрацю з Агентством з кібербезпеки та безпеки інфраструктури США: Державна служба спеціального зв'язку та захисту інформації України. URL : https://cip.gov.ua/ua/news/rozpochinayemo-spivpracyu-z-agentstvom-z-kiberbezpeki-ta-bezpeki-infrastrukturi-derzhdepu-ssha
13. The EU-U.S. and Swiss-U.S. Privacy Shield Frameworks: International Trade Administration. URL : https://www.privacyshield.gov/
14. Holobiuc, A.-M. (2021). Determinants of economic growth in the European Union. An empirical analysis of conditional convergence. SocioEconomic Challenges, 5(2), 26-34. https://doi.org/10.21272/sec.5(2).26-34.2021

REFERENCES

1. Cybercrime To Cost The World $10.5 Trillion Annually By 2025 : Cybersecurity Ventures. URL : https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

2. Ponce G., Gonzales Ch., Al-Mohareb M. (2021). Sustainable finance in cybersecurity investment for future profitability under uncertainty. Journal sustainable finance & investment, Ahead-of-Print, 1-20. https://doi.org/10.1080/20430795.2021.1985951
3. Zadorozhnyi, Z.-M., Ometsinska, I., & Muravskiy, V. (2021). Determinants of Firm's Innovation: Increasing the Transparency of Financial Statements. Marketing and Management of Innovations, 2, 74-86. http://doi.org/10.21272/mmi.2021.2-06
4. European Banking Authority: regulation and policy. URL : https://www.eba.europa.eu/regulation-and-policy
5. Statistical Data Warehouse: European Central Bank. Eurosystem. URL: https://sdw.ecb.europa.eu/
6. Holobiuc, A.-M. (2021). Determinants of economic growth in the European Union. An empirical analysis of conditional convergence. SocioEconomic Challenges, 5(2), 26-34. https://doi.org/10.21272/sec.5(2).26-34.2021
7. EU policy on high-risk third counties: European Commission. URL : https://ec.europa.eu/info/business-economy-euro/banking-and-finance/financial-supervision-and-risk-management/anti-money-laundering-and-countering-financing-terrorism/eu-policy-high-risk-third-countries_en
8. Federal Ministry of the Interior, Building and Community. URL : https://www.bmi.bund.de/EN/home/home_node.html;jsessionid=D13F8E960D4B632B90E39479212306A6.2_cid295
9. National framework of cybersecurity policy of the Republic of Poland for 2017-2022. URL : https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Cybersecuritystrategy_PL.pdf
10. Novyny, polityka, tekhnolohii. URL : https://mind.ua/news/20199350-polshcha-i-nato-vpershe-pidpisali-ugodu-v-sferi-kiberbezpeki
11. Cybersecurity and Infrastructure Security Agency. URL: https://www.cisa.gov/cybersecurity
12. Rozpochynaiemo spivpratsiu z Ahentstvom z kiberbezpeky ta bezpeky infrastruktury SShA: Derzhavna sluzhba spetsialnoho zviazku ta zakhystu informatsii Ukrainy. URL : https://cip.gov.ua/ua/news/rozpochinayemo-spivpracyu-z-agentstvom-z-kiberbezpeki-ta-bezpeki-infrastrukturi-derzhdepu-ssha
13. The EU-U.S. and Swiss-U.S. Privacy Shield Frameworks: International Trade Administration. URL : https://www.privacyshield.gov/
14. Holobiuc, A.-M. (2021). Determinants of economic growth in the European Union. An empirical analysis of conditional convergence. SocioEconomic Challenges, 5(2), 26-34. https://doi.org/10.21272/sec.5(2).26-34.2021