протидії (запобігання) злочинним проявам у банківській сфері від способів і засобів вчинення і приховування останніх. У банківському секторі поряд з ризик-менеджментом окремого банку застосовуються й прямі колективні методи забезпечення фінансової безпеки.

В умовах інтеграційних процесів вплив зовнішнього економічного середовища не може бути нівельований. На діяльність вітчизняних банків впливають не лише вимоги органів регулювання всередині країни, але й на наднаціональному рівні. На підставі аналізу нормативно-правового забезпечення фінансової безпеки банків, можна зробити висновок, що на даному етапі формування система нормативно-правових актів не відповідає необхідним вимогам і є незавершеною. Система пруденційного нагляду за банками спрямована здебільшого на реагування на негативні події, які вже сталися. На наш погляд, регулятивні заходи повинні бути розроблені таким чином, щоб передбачати і своєчасно реагувати на появу нових викликів і загроз, аніж нажорсткі репресивні дії. Доцільним є регулярне проведення стрес-тестувань з метою оцінки можливих збитків як окремих банків, так і загалом банківського сектору в умовах реалізації стресових сценаріїв.

Отже, основними напрямами забезпечення достатнього рівня фінансової безпеки банківського сектору України повинно стати в першу чергу зміна сприйняття самої філософії фінансової безпеки як елементу управління, який дозволяє забезпечити фінансово стійке її функціонування.

З цією метою необхідно вирішити питання макроекономічного та мікроекономічного спрямування.

Питання макроекономічного спрямування відносять до привілеї Національного банку України, а саме: мінімізація витрат для платників податків при капіталізації банків; створення спеціального фонду для рекапіталізації банків; розвиток третейських судів та досудового вирішення проблем між кредиторами та боржниками; підвищення відповідальності позичальників за надання в банки або кредитні бюро недостовірної інформації; створення банку «поганих активів банків»; приведення законодавства щодо процесів злиття і поглинання банків до найкращих практик Європейського Союзу, що дозволить швидше провести процес консолідації банків та знизить негативний вплив на їх ефективність; активізація політики сприяння підвищенню ролі іноземних банків в Україні та вжиття заходів задля залучення іноземного капіталу, передусім з глобальних фінансових установ.

Питання мікроекономічного спрямування націлені на створення єдиної системи фінансової безпеки у банках. Оскільки головним завданням підрозділу фінансової безпеки банку є захист його фінансових інтересів, одним з напрямків роботи по забезпеченню такого захисту є створення сприятливих умов перш за все для ведення фінансових операцій, що дозволяють отримувати максимальний дохід при мінімальних ризиках. Однак, щоб цілеспрямовано формувати такі умови, в структурі банків перш за все необхідно виділити ті об'єкти і явища, які впливають на їх фінансову безпеку, що дозволить надати роботі більш системний і комплексний характер.

4.2. Кібернетична безпека банківського сектора в системі фінансової безпеки держави

© Полторак А. С.
канд. екон. наук, доц., доц. кафедри фінансів, банківської справи та страхування, Миколаївський національний аграрний університет, м. Миколаїв, Україна
© Баришевська І. В.
канд. екон. наук, доц., доц. кафедри фінансів, банківської справи та страхування, Миколаївський національний аграрний університет, м. Миколаїв, Україна
© Мельник О. І.
канд. екон. наук, доц., доц. кафедри фінансів, банківської справи та страхування, Миколаївський національний аграрний університет, м. Миколаїв, Україна
© Боднар О. А.
канд. екон. наук, асистент кафедри фінансів, банківської справи та страхування, Миколаївський національний аграрний університет, м. Миколаїв, Україна

Система фінансової безпеки держави в умовах глобалізації не може характеризуватися оптимальним рівнем без достатнього рівня кібербезпеки банківського сектора, так, на нашу думку, саме кібернетичну безпеку банківського сектора необхідно розглядати та аналізувати як важливу частину фінансової безпеки держави. Зауважимо, що у сфері кібербезпеки

фінансового сектора проблемами пострадянських країн є: недостатня кількість галузевих центрів кібербезпеки; недостатній рівень стандартизації для суб'єктів господарювання; міжвідомча взаємодія; механізми стимулювання галузі.

У фінансовій сфері кібер-злочини часто відбуваються з метою отримання грошей в умовах вищого (у порівнянні із законним бізнесом) потенційного прибутку, що розглядається злочинниками як компенсація за ризик. Кібер-злочинність отримала стрімкий розвиток через те, що суттєвий рівень прибутку можливий в умовах суттєво нижчого ризику. Так, рентабельність фішингових повідомлень електронної пошти інколи досягає сотні або тисячі процентів, прибуток від незаконних дій у сфері крадіжок інтелектуальної вартості у фінансовій сфері взагалі важко оцінити.

Окремі аспекти оцінювання кібер-ризику в системі фінансової безпеки держави розглядали у своїх працях А. Буверет [2]; С. Байнерб, М. Елінг, Дж. Вифс [1; 7], С. Толюпа, Є. Толюпа, Є. Агапова [20]; О. Ясенко [23]; В. Л. Бурячок [12]. Деякі аспекти забезпечення кібербезпеки в системі фінансової безпеки держави розглядали у своїх працях Дж. Себула і Л. Янг [3]; В. Ліпкан та І. Діордіца [16]. Однак, необхідно зазначити, що повні дані щодо кібер-атак у світі є дефіцитними, що суттєво ускладнює механізм оцінки та аналізу стану кібер-безпеки, крім того, в будь-які офіційні дані включаються лише прямі збитки від кібер-атаки, тоді як непрямі витрати, в т. ч. відновлення бізнесу та репутації можуть становити понад 90 % від їх загального обсягу [4].

Відповідно до Закону України від 05.10.2017 р. № 2163-VIII «Про основні засади забезпечення кібербезпеки України» кібербезпека – це «захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі», а індикатори кіберзагроз – це показники, які використовуються для виявлення та реагування на них [19].

В. Ліпкан та І. Діордіца під національною системою кібербезпеки розуміють сукупність суб'єктів її забезпечення, властивих конкретній державі, які комплексно взаємодіють із метою формування сприятливих умов для реалізації інтересів індивіда, суспільства і країни загалом [16, с. 174].

На нашу думку, кібернетична безпека банківського сектора – умови, в яких функціонує банківська система країни, за яких дія внутрішніх та зовнішніх загроз у кібернетичному просторі не спричиняє негативних процесів у даній складній системі та не заважає створенню сприятливих фінансових умов для її сталого розвитку в умовах діджиталізації, безперешкодного формування, зберігання, використання, поширення та захисту інформації. Так, кібер-атаки можуть вплинути на банківську стабільність через три аспекти кібер-безпеки: цілісність, конфіденційність та доступність. Аспект цілісності пов'язаний з некоректним використанням систем аналогічно до випадків шахрайства, наслідком чого є прямі фінансові втрати. Конфіденційність порушується, коли приватна інформація розкривається третім особам, що спричиняє виникнення репутаційних ефектів та судових втрат, а питання доступності пов'язані з певними перебоями у бізнесі, в результаті яких порушується діяльність підприємства, спричиняючи виникнення збитків.

Відділ міжнародного зв'язку Організації Об'єднаних націй визначає глобальний індекс кібербезпеки (global protection index) для країн світу [9], розрахунок якого ґрунтується на аналізі технічних, організаційних заходів, що впроваджуються у певній країні, а також зміцненні потенціалу держави. Рівень кібербезпеки держав світу у рейтингу [9] розраховується за п'ятьма основними показниками: організаційний і технічний потенціали; законодавча база; кооперація; темпи нарощування потенціалу. Високий рівень індексу кібербезпеки мають переважно розвинені країни, тоді як країни з низьким та середнім рівнем розвитку характеризуються нижчими значеннями індексу кібербезпеки.

У 2017 р. глобальний індекс кібербезпеки визначався для 193 країн світу. Першість у рейтингу отримали Сінгапур, США, Малайзія, Оман. Серед європейських країн лідерами є Норвегія, Франція та Естонія. Поміж пострадянських країн Грузія займає 8 місце, Білорусь – 39 місце, а Україна, в якій сектор кібербезпеки є лише на стадії розвитку, – 56 місце.

Існує також національний індекс кібербезпеки (National Cyber Security Index, далі – NCSI), який визначається естонською Академією управління E-Governance Academy Foundation з метою оцінки здатності країн управляти кібер-інцидентами та запобігати кібер-загрозам. Відповідно до результатів розрахунку NCSI станом на 01.10.2018 р. Україна з індексом 63,64 посідає 23 місце з 114 країн світу, що представлені в рейтингу (табл. 1).

Таблиця 1

Порівняльна характеристика місця у рейтингу за NCSI країн Східної Європи, 2018 р.

Місце у рейтингу	Країна	Національний індекс кібербезпеки NCSI	Цифровий розвиток (далі – DDL)	Різниця
4.	Словаччина	80,52	66,73	13,79
10.	Чехія	74,03	69,37	4,66
14.	Польща	70,13	66,59	3,54
17.	Угорщина	66,23	66,08	0,15
23.	Україна	63,64	58,10	5,54
24.	Російська Федерація	63,64	67,49	-3,85
33.	Білорусь	55,84	75,50	-19,66
35.	Румунія	54,55	61,69	-7,14
37.	Болгарія	51,95	63,59	-11,64
42.	Молдова	48,05	60,82	-12,77

Джерело: узагальнено авторами за даними [6]

Аналізуючи дані табл. 1, доцільно зробити висновок, що позитивна різниця між NCSI-індексом та індексом цифрового розвитку (DDL), що є узагальненим показником розвитку інформаційно-комунікаційних технологій та індексу мережевої готовності, свідчить, що розвиток кібербезпеки окремих держав (Словаччина, Чехія, Польща, Угорщина, Україна) випереджає або відповідає її цифровому розвитку. Від'ємний результат означає, що цифрове суспільство певних країн (Російська Федерація, Білорусь, Румунія, Болгарія, Молдова) є більш розвиненим у порівнянні з національною сферою кібербезпеки.

В останні роки стрімкого розвитку інформаційних технологій, частіших кібератак на фінансові установи (такі як NoPetya в червні 2017 р., Wannacry у травні 2017 р.), які можуть призвести до значних збоїв та суттєвих фінансових збитків, кіберризик доцільно розглядати як одну з небезпечних та недостатньо досліджених загроз фінансовій стабільності держави, відповідно, в умовах зміни економічних умов вважаємо кібернетичну безпеку однією з підсистем фінансової безпеки держави.

Якщо порівняти сучасний професіональний рівень кібер-спеціалістів та інструментів для кібер-атак у фінансовому секторі та аналогічні дані 1990-х років, то зробимо висновок, що якщо раніше інструменти кібер-злочинців були переважно простими, виготовленими індивідуально, а їх використання вимагало високого рівня знань та професійних навичок у площині мережевих протоколів, програмування, внутрішніх компонентів операційних систем. З часом інструменти, які використовуються у процесі здійснення кібер-атак, стрімко розвивалися, а їх застосування спрощувалось. Сьогодні запуск фішингу (шахрайська практика відправлення повідомлень електронною поштою з метою розкриття конфіденційної інформації, які виглядають як листи від справжнього відправника) вимагає від кібер-злочинців виключно базове розуміння концепцій та фінансові можливості, відповідно, з підвищенням різня розвитку інструментів кібер-атаки на фінансовий сектор вимагають менше технічних професійних знань, що спрощує процедуру кібер-інциденту (рис. 1).

У процесі узагальнення теоретико-методичних засад і розроблення практичних підходів до забезпечення кібернетичної безпеки банківського сектора в системі фінансової безпеки держави було зроблено наступні висновки:

1. Опрацьовано динаміку значень глобального індексу кібербезпеки та національного індексу кібербезпеки та з'ясовано, що високий рівень індексів мають переважно розвинені країни, тоді як країни з низьким та середнім рівнем розвитку характеризуються нижчими значеннями індексів кібербезпеки. Доведено, що позитивна різниця між NCSI-індексом та індексом цифрового розвитку свідчить, що розвиток кібербезпеки окремих держав (в т. ч. Україна) випереджає або відповідає її цифровому розвитку, тоді як від'ємний результат означає, що цифрове суспільство країн є більш розвиненим у порівнянні з національною сферою кібербезпеки.

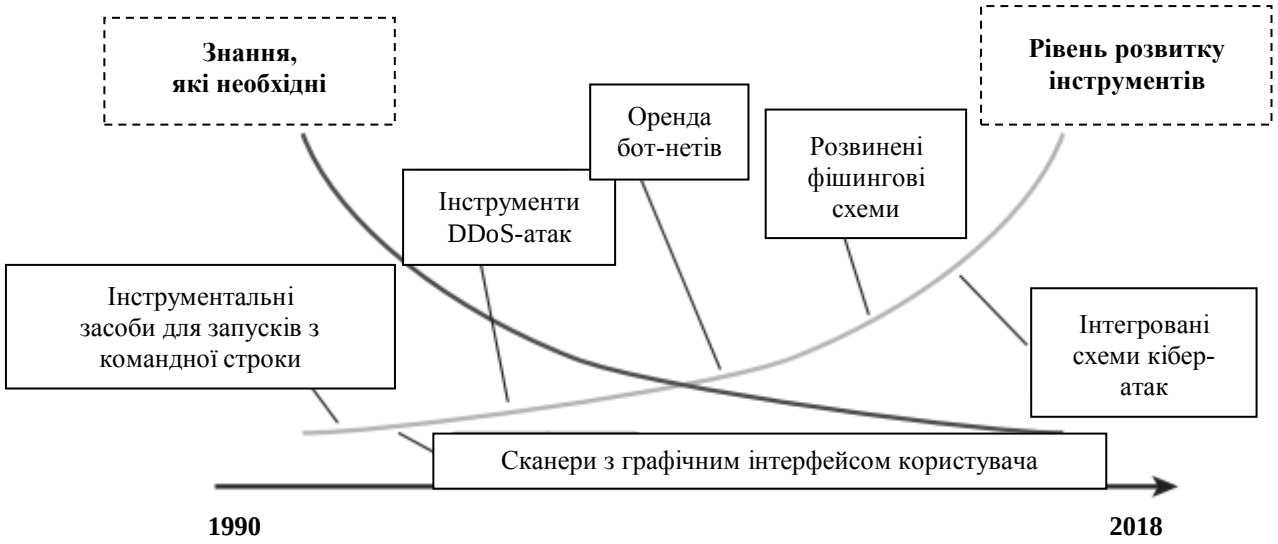

Рис. 1. Динаміка обсягу необхідних професійних знань та інструментів для здійснення кібер-атак на банківські установи

Джерело: адаптовано авторами до предмету дослідження на основі даних Carnegie Mellon University

2. Досліджено, що відповідно до результатів міжнародних опитувань, досліджень міжнародних фахівців, в т. ч. представників поважних фінансових установ, кібернетичний ризик має найвищі кількісні показники зростання у динаміці в системі ризиків глобальній фінансовій системі. Вважаємо, що небезпека загострюється, враховуючи те, що зломи систем окремих фінансових організацій можуть спричинити формування системного ризику. Крадіжка конфіденційної інформації, дезорганізація клірингової, платіжної або розрахункової системи, враховуючи тісний взаємозв'язок суб'єктів фінансового сектора, очікувано призведуть до масштабних вторинних ефектів та, відповідно, стануть реальною загрозою для фінансової безпеки. В цій потенційній ситуації сукупний ризик для економіки може суттєво перевищувати загальну суму ризиків для окремих осіб, враховуючи національний характер структур реагування, глобальний характер мереж та платформ інформаційних технологій, неефективність міжнародного співробітництва. Обґрунтовано, що найчастіше інформація про кібер-атаки розкривається лише через тривалий період часу після інциденту з побоювань шкоди для репутації, відсутності стимулів висвітлення інформації про кібер-атаки за умови відмови від страхування від кібер-ризиків.

3. Запропоновано теоретичний підхід до трактування категорії «кібернетична безпека банківського сектора», що сприятиме удосконаленню науково обґрунтованої термінології та розвитку економічної науки.

4. Зазначено, що найкращим напрямом забезпечення кібернетичної безпеки у фінансовій сфері є атака бізнес-моделі кібер-злочинності особливістю якої є специфічне співвідношення рівня ризику та потенційного прибутку, винагороди, що пов'язано з неефективністю судового переслідування, в т. ч. внаслідок тісного міжнародного співробітництва.

5. Доведено, що характер кібер-загроз швидко змінюється, що призводить до зниження важливості даних щодо минулих кібер-інцидентів для можливого прогнозування майбутніх загроз банківському сектору. Особливо це стосується негативного впливу деструктивних ідей, що поширюються в офіційному інформаційному просторі (реклама фінансових пірамід, популяризація боргової залежності, оприлюднення способів та варіантів ухилення від оподаткування, масове закликання до застосування криптовалют, розповсюдження інших теорій швидкого збагачення, псевдонаукові вчення, такі як фінансова нумерологія чи фінансова астрологія). Виділено основну серед причин активного розвитку кібер-злочинності у банківському секторі, її трансформацію в цілу індустрію, якою автори вважають розвиток інструментів, які використовуються у процесі кібер-атак, особливо співвідношення ризику та потенційної винагороди.

Враховуючи вищевикладене, вважаємо необхідним розглядати кібернетичну безпеку як важливу складову фінансової та, відповідно, національної безпеки держави. Кібернетичні загрози можуть негативно вплинути не тільки на банківський сектор, однак, як засвідчує практика, саме фінансовий сектор є найбільш вразливим стосовно кібер-атак. Банківські установи, враховуючи їх важливу місію посередників у процесі руху грошових коштів, є найбільш привабливими об'єктами для кібер-атак, в т. ч. зловмисні дії щодо роботи банкоматів, операцій з переказу грошей, знищення файлів, введення шкідливих програм в банківські системи, дії, що порушують внутрішні операції, та мають характер вимагання. Наслідками таких дій можуть бути суттєві фінансові збитки та погіршення репутації.

4.3. Бюджетна складова забезпечення фінансової безпеки держави

© Заїчко І. В.
старший викладач, Науково-дослідний інститут
Київського національного університету культури і мистецтв, м. Київ, Україна

Однією зі структурних елементів економічної безпеки держави являється фінансова безпека, що досягається якісним виконанням функціональних обов'язків уряду і визначає її ефективність на макрорівні. Рівень захисту державних інтересів на міжнародній арені характеризує ефективність організаційно-економічного механізму, який забезпечує реалізацію фінансової безпеки, що визначається сукупністю заходів держави з організації та використання способів захисту інтересів країни. Реалізація національних інтересів України можлива тільки на основі стійкого розвитку фінансової системи. Тому, національні інтереси України в цій галузі є ключовими. Саме у сфері фінансів при забезпеченні фінансової безпеки – національні інтереси полягають в забезпеченні достатності бюджетних ресурсів для повноцінного виконання державою своїх функцій, нарощування бюджетного потенціалу в умовах його збалансованості і нормалізації фінансових ресурсів.

Забезпечення фінансової безпеки входить до складу найважливіших функцій усіх держав світу. Фінансова безпека істотно впливає на розвиток економічної, соціальної, політичної системи суспільства, її готовність і можливість протистояти негативним діям. Без належного фінансового потенціалу не можна створити і забезпечити діяльність усіх сфер життя держави, суспільства і кожної окремої людини: економічних, соціальних, політичних, правових, і силових структур, здатних ефективно захищати суспільство і інтереси країни. А видозміна характеру сучасних погроз в умовах глобалізації, вибір світовою спільнотою нової основної стратегічної мети – перехід до стійкого економічного розвитку – вимагають нових підходів і механізмів до забезпечення фінансової безпеки держав. «Фінансова безпека держави є багатоаспектним явищем, її стан динамічно змінюється, тому потрібно здійснювати ретельний моніторинг фінансової системи, а також вивчати проблеми, що виникають під впливом реформування національної економіки, регіоналізації і глобалізації світової економіки, інтернаціоналізації фінансових потоків тощо» [7, с. 123]. Наприклад, З. С. Варналій, у своєму визначенні робить акцент на захищеності та керованості економічним процесом. У зв'язку з цим найбільш вдале визначення на його думку таке: «фінансова безпека держави – це захищеність інтересів держави у фінансовій сфері; такий стан бюджетної, податкової та грошово-кредитної систем, що гарантує спроможність держави ефективно формувати, зберігати від надмірного знецінення та раціонально використовувати фінансові ресурси країни для забезпечення її соціально-економічного розвитку й обслуговування фінансових зобов'язань» [7, с. 123].

Ми вважаємо слушною дану думку, оскільки порушення функціонування однієї з сфер фінансових стосунків може підірвати безпеку інших сфер і навпаки, якщо одна із сфер досить ефективно функціонує, виникнення проблем в іншій сфері необов'язково повинне нести загрозу усій фінансовій безпеці. Фінансова безпека не має на увазі, що усі сфери фінансових стосунків повинні функціонувати з максимальною ефективністю.