УДК *657.6*
JEL Code *G21, G22, L86, M42*

О.А. КРИКЛІЙ*
(Сумський державний університет, м. Суми, Україна)

Л.Д. ПАВЛЕНКО**
(Сумський державний університет, м. Суми, Україна)

Внутрішній аудит як превентивна складова в системі кібербезпеки банку

Сектор фінансових послуг є найбільш привабливим для кібератак та кібершахрайств через можливість отримання зловмисниками значних фінансових та нефінансових вигід. Для підвищення ефективності забезпечення кібербезпеки банку необхідним є посилення ролі превентивних інструментів, одним з основних яких є внутрішній аудит. Мета статті полягає у розробці теоретико-методичних основ системи внутрішнього аудиту кібербезпеки банку, з деталізацією її складових та науковому обґрунтуванні принципів функціонування, на основі чого можна було б вирішувати завдання забезпечення ефективного контролю кібербезпеки. Уточнено сутність інформаційних активів банку як об'єктів внутрішнього аудиту кібербезпеки. Для формування комплексного розуміння контрольного середовища систематизовано загрози кібербезпеки банку та способи їх реалізації в розрізі різних об'єктів кібербезпеки. Розкрито організаційно-управлінську підсистема забезпечення кібербезпеки банку. Визначено, що система внутрішнього аудиту кібербезпеки являє собою сукупність взаємопов'язаних елементів (цілі та завдання, об'єкт, суб'єкт, механізм), що функціонують на основі загальних та спеціальних принципів та дозволяють об'єктивно оцінити рівень захищеності та збереження властивостей інформаційних активів та інформаційної інфраструктури банку в умовах постійного впливу зовнішніх та або / внутрішніх загроз, а також дотримання вимог національного та міжнародного законодавства. Наведено перелік завдань, які повинен здійснити персонал служби внутрішнього аудиту для оцінки ефективності системи забезпечення кібербезпеки банку. Виділено елементний склад системи внутрішнього аудиту та визначено принципи, яких необхідно дотримуватись для досягнення його цілей та завдань.

Ключові слова: *внутрішній аудит в банку, кібербезпека банку, кібер-ризики банку, загроза втрати кібербезпеки банку, аудит кібербезпеки банку.*

DOI: https://doi.org/10.33146/2307-9878-2019-2(84)-124-133

O.A. KRYKLIY
(Sumy State University, Sumy, Ukraine)

L.D. PAVLENKO
(Sumy State University, Sumy, Ukraine)

Internal Audit as a Preventive Component in the Bank's Cybersecurity System

The financial services sector is the most attractive for cyber-attacks and cyber fraud because there is the possibility to receive the financial and non-financial benefits. In order to increase the efficiency of ensuring cybersecurity of the bank, it is necessary to strengthen the role of preventive tools, one of the main of which is internal audit. The purpose of the article is to develop the theoretical and methodical foundations of the internal audit system of a cybersecurity bank. In particular, the authors carry out the detalization of the components of internal audit system and the scientific substantiation of the principles of it operation, on the basis of which it would be possible to solve the problem of ensuring effective monitoring of cybersecurity. The essence of the bank's information assets as objects of

* **Криклій Олена Анатоліївна**, доцент кафедри фінансів, банківської справи та страхування Навчально-наукового інституту бізнес-технологій «УАБС» Сумського державного університету (м. Суми), кандидат економічних наук, доцент.

** **Павленко Людмила Дмитрівна**, асистент кафедри фінансів, банківської справи та страхування Навчально-наукового інституту бізнес-технологій «УАБС» Сумського державного університету (м. Суми), кандидат економічних наук.

internal audit of cybersecurity was clarified. To form a comprehensive understanding of the control environment, cybersecurity threats of the bank and ways to implement them in the context of various cybersecurity objects were systematized. The organizational and managerial subsystem for ensuring cybersecurity of the bank was disclosed. It was determined that the internal audit system of cybersecurity is a set of interrelated elements (goals and objectives, object, subject, mechanism) operating on the basis of general and special principles and allow an objective assessment of the level of security and preservation of the information assets and information infrastructure of a bank under constant impact external and / or internal threats, as well as compliance with national and international legislation. A list of tasks to be performed by the internal audit service to assess the effectiveness of the cybersecurity system of the bank was provided. The elemental composition of the internal audit system was highlighted and the principles that must be followed to achieve its goals and objectives were defined.

Keywords: *internal audit in bank, banking cybersecurity, cyber risk in banking, emerging cybersecurity threats, audit of the banking cybersecurity.*

Постановка проблеми. Сектор банківських та фінансових послуг є найбільш привабливим для кібератак та кібершахрайств через можливість отримання зловмисниками значних фінансових та нефінансових вигід.

За даними IBM, фінансовий сектор у 2016 році атакований на 65 % частіше, ніж будь-який інший, у результаті чого втрачено більш, ніж 200 мільйонів записів (на 937 % більше, ніж у 2015 році) [28]. У 2016 році 8,5 % зареєстрованих інцидентів витоку інформації зафіксовано в фінансовому секторі, при чому фінансові установи постраждали від цих інцидентів у 300 разів частіше, ніж підприємства інших галузей [37].

У дослідженні глобальних банків, проведеному Інститутом міжнародних фінансів у партнерстві з Ernst & Young, як голови рад директорів, так і відповідальні за ризик-менеджмент, вважали забезпечення кібербезпеки ключовим стратегічним пріоритетом [33].

Попри значну увагу банків до дослідження видів кіберзагроз, причин, що обумовлюють їх появу, ландшафт загроз постійно розвивається, приводячи до складнішої кібер-екосистеми, а наслідки реалізації кіберзагроз експоненційно зростатимуть. Це, насамперед, обумовлено розвитком цифрової інфраструктури, впровадженням фінансових технологій та активною діяльністю FinTech-фірм, що розмиватиме кордони між традиційними банківськими та небанківськими послугами, загострюватиме конкуренцію та створюватиме нові джерела загроз для кібербезпеки банків. Проблема посилюватиметься тим, що банківські інформаційні системи ставатимуть все більш взаємопов'язаними, операційні процеси – більш автоматизованими, при цьому вже наявна інфраструктура інформаційних та комунікаційних технологій не була розроблена з пріоритетом кібербезпеки, що потребуватиме її адаптації до нових умов діяльності.

Зважаючи на це, формування заходів для запобігання настанню ситуацій, що класифікуються як кіберзагроза або шахрайство, є важливою науковою та прикладною задачею. У рамках дослідження рейтингового агентства PwC Україна виявлено, що «… більшість корпоративних рад директорів не дотримуються превентивного підходу до формування стратегій забезпечення кібербезпеки чи інвестиційних планів її розвитку» [20]. Відтак актуальним для банків України є створення превентивної системи забезпечення кібербезпеки, одним з важливих елементів якої є внутрішній аудит.

Аналіз останніх досліджень і публікацій. Вагомий внесок у становлення та розвиток теоретико-методологічних засад внутрішнього аудиту в банках, на яких мають базуватись розробки у сфері внутрішнього аудиту кібербезпеки, зробили такі вітчизняні та іноземні вчені, як: А. Герасимович [17], О. Кірєєв [3], Л. Костирко [5], М. Маркевич [11], М. Письменна [18], О. Сарахман [3, 5], А. Арсланбеков-Федоров [1], С. Банк [4], Г. Бєлоглазова та інші [2], Н. Соколинська [22], А. Баракат (*A. Barakat*) [26], К. Россітер (*C. Rossiter*) [34] та інші.

Важливість ефективної системи внутрішнього аудиту для попередження шахрайства у сфері електронних банківських послуг та інформаційних банківських систем досліджувало багато іноземних науковців, серед них: О.Дж. Акіньомі (*O.J. Akinyomi*) [25], А.А. Боатенг, Г.О. Боатенг та Х. Акуа (*A.A. Boateng, G.O. Boateng, H. Acquah*) [27], С. Пальфі та М. Мурешан [30], Д. Петрашку та А. Тіану (*D. Petraşcu and A. Tieanu*) [31], Р. Саламе, Г. Аль-Вешах, М. Аль-Нсур та А. Аль-Хіяри (*R. Salameh, G. Al-Weshah, M. Al-Nsour, A. Al-Hiyari*) [35], М. Ула, З. Ісмаїл та З.М. Сідек (*M. Ula, Z. Ismail, Z.M. Sidek*) [38], А.К. Усман та М.Х. Шах (*A.K. Usman and M.H. Shah*) [39] та інші.

Переважна більшість досліджень цих та інших іноземних науковців ураховують специфіку банківських систем та загроз кібербезпеки, притаманних конкретним країнам та регіонам. Тому отримані наукові результати можуть лише частково бути враховані при формуванні системи внутрішнього аудиту для запобігання загрозам втрати кібербезпеки в банках України.

Комплексні теоретичні розробки, що обґрунтовують систему внутрішнього аудиту кібербезпеки як превентивну складову в системі кібербезпеки банку, у вітчизняній науковій літературі практично відсутні.

Увага науковців, в основному, зосереджується на окремих об'єктах системи забезпечення кібербезпеки банку. Так, О. Мельниченком у [12-16] досліджено аудит інформаційної безпеки банку при роботі з електронними грошима. Основна увага акцентується на ключових напрямах перевірки, зокрема, організаційно-технічній та правовій забезпеченості банків для запобігання загрозам стабільного

функціонування систем електронних грошей. Крім того, дослідник розглядає методи соціальної інженерії та способи попередження цього типу загроз кібербезпеці.

О. Попович та К. Войновська у [19] розробили методологію аудиту електронних грошей в банках України як складової системи контролю інформаційної безпеки, зокрема, ними висвітлено ключові напрями аудиту.

Високо оцінюючи вклад вітчизняних та іноземних авторів у дослідження питань запобігання кіберзагрозам в банківській діяльності, у тому числі з застосуванням внутрішнього аудиту, слід зазначити про необхідність подальшого поглиблення цих теоретичних досліджень з урахуванням специфіки діяльності банків України.

Мета статті полягає у розробці теоретико-методичних основ системи внутрішнього аудиту кібербезпеки банку, з деталізацією її складових та науковому обґрунтуванні принципів функціонування, на основі чого можна було б вирішувати завдання забезпечення ефективного контролю кібербезпеки.

Методика дослідження. Для досягнення поставленої мети авторами проведено систематичний, логічний та порівняльний аналіз та узагальнення наукової літератури, використано такі методи й прийоми теорії пізнання, як аналіз та синтез, встановлення причинно-наслідкових зв'язків розвитку процесів та явищ, табличний та графічний методи.

Виклад основного матеріалу. Зважаючи на зростання зовнішніх та внутрішніх загроз, що впливають на рівень кібербезпеки банків України, постала необхідність розбудови системи внутрішнього аудиту як превентивної складової в системі кібербезпеки. Парадигма превентивності реалізується на основі незалежної та об'єктивної оцінки поточного рівня захищеності банку від зовнішніх та внутрішніх кіберзагроз, розробки рекомендацій з усунення виявлених недоліків у системі забезпечення кібербезпеки та моніторингу їх своєчасного впровадження.

Внутрішній аудит кібербезпеки банку пропонуємо розглядати як періодичну систему збору та оцінки інформації для визначення того, чи забезпечують всі системи банку належний стан захищеності інформаційних активів та інформаційної інфраструктури, збереження властивостей інформаційних активів (доступності, цілісності чи конфіденційності) на цільовому рівні відповідно до встановлених критеріїв в умовах постійного впливу зовнішніх та або / внутрішніх загроз з дотриманням вимог національного та міжнародного законодавства.

Систему внутрішнього аудиту пропонуємо розглядати як невіддільну складову забезпечення кібербезпеки банку, що являє собою сукупність взаємопов'язаних елементів (цілі та завдання, об'єкт, суб'єкт, механізм), що функціонують на основі загальних та спеціальних принципів та дозволяють об'єктивно оцінити рівень захищеності та збереження властивостей інформаційних активів та інформаційної інфраструктури банку в умовах постійного впливу зовнішніх та або / внутрішніх загроз, а також дотримання вимог національного та міжнародного законодавства.

Об'єктами внутрішнього аудиту є інформаційні активи – матеріальні або нематеріальні об'єкти, що є інформацією або містять інформацію, слугують для обробки, зберігання або передачі інформації та мають цінність для банку.

Для формування об'єктного середовища внутрішнього аудиту в системі забезпечення кібербезпеки банку необхідно враховувати загрози, що генерується як зовнішнім, так і внутрішнім середовищем (табл. 1).

Перелік способів реалізації загроз кібербезпеки банку, на яких має концентруватись аудит, наведено в таблиці 2.

Таблиця 1

Класифікація загроз кібербезпеки банку

Ознака	Вид загрози
1	2
За джерелом	– внутрішні (втрата, знищення, викрадення, викривлення або розголошення інформації, витік інформації); – зовнішні (модифікація змісту, порушення конфіденційності, порушення логічної цілісності, порушення прав власності на інформацію, порушення фізичної цілісності, природні та техногенні катастрофи, що порушують нормальний режим роботи інформаційних систем тощо)
За походженням	– об'єктивні (природні), що характеризуються впливом на об'єкт захисту фізичних процесів або стихійних природних явищ, що не залежать від людини; – суб'єктивні, що характеризуються впливом на об'єкт захисту діяльністю людини; – результати соціальної інженерії (фішинг, фармінг, претекстинг, скрімінг та ін.)
За ступенем впливу на інформаційну систему	– пасивні без впливу на стан інформаційної системи; – активні з порушенням нормального процесу функціонування інформаційної системи банку
За цілеспрямованістю	– ненавмисні (помилкові, випадкові, необдумані, без злого наміру та корисливих цілей) дії персоналу та користувачів банківських послуг; – навмисні (в корисливих цілях, з примусу третіми особами, зі злим умислом тощо) персоналу, користувачів банківських послуг, злочинних груп та формувань, політичних і економічних структур, а також окремих осіб

Продовження табл. 1

1	2
За способом реалізації	– розголошення; – витік; – несанкціонований доступ.
За ступенем сформованості	– реальні; – потенційні.
За можливістю прогнозування	– прогнозовані; – не прогнозовані;
За ймовірністю виникнення	– реальна; – ймовірна; – малоймовірна; – неймовірна.
За характером впливу	– явна, пряма (загрози, реалізація яких порушує безпеку інформаційних активів); – неявна, опосередкована (загрози, що створюють умови для появи прямих загроз);
За масштабами наслідків	– катастрофічні; – критичні; – середні; – незначні.
За можливістю нейтралізації	– можливо нейтралізувати; – можливо частково нейтралізувати; – нейтралізувати неможливо.

Джерело: розроблено авторами на основі [7, 9].

Таблиця 2

Перелік способів реалізації загроз кібербезпеки банку

Рівні кібербезпеки	Способи реалізації загроз
Фізичний рівень	– витік інформації; – знищення / руйнування / диверсії; – несанкціонований фізичний доступ; – розкрадання / крадіжка.
Мережевий рівень	– атаки «відмова в обслуговуванні»; – впровадження апаратних закладок; – підміна довіреного об'єкта мережі та передача за каналами зв'язку; повідомлень від його імені з присвоєнням його прав доступу; – порушення штатних режимів роботи мережевого обладнання.
Рівень мережевих додатків і сервісів	– аналіз трафіку; – атаки «відмова в обслуговуванні»; – використання спеціалізованих програм; – впровадження шкідливого програмного забезпечення; – порушення штатних режимів роботи мережевих додатків; – сканування мережі, спрямоване на виявлення відкритих портів та служб, відкритих з'єднань.
Рівень операційних систем та систем управління базами даних	– копіювання; – крадіжка / втрата паролів; – модифікація / видалення даних; – неправильна (неповна) конфігурація систем захисту інформації; – несанкціонований логічний доступ до операційних систем/ систем управління базами даних з використанням спеціалізованого програмного забезпечення; – підміна ідентифікаторів користувача; – поширення шкідливих програм.
Рівень банківських технологічних процесів та програм	– модифікація / видалення даних; – розповсюдження / передача даних; – друк документів; – крадіжка документів та карток; – крадіжка паролів.
Рівень бізнес-процесів	– саботаж; – халатність та помилки; – шкідництво.

Джерело: розроблено авторами.

Зважаючи на збільшення кількості операційних процесів, у тому числі ключових, що передаються стороннім організаціям (наприклад, інтернет-провайдери, підрядники, що здійснюють монтаж обладнання), зростає залежність банків від кібербезпеки цих сторін. У відповідь на це, в банку має бути передбачена можливість аудиту кібербезпеки сторонніх організацій для забезпечення того, щоб їх діяльність відповідала встановленим стандартам та не створювала загрози втрати кібербезпеки.

До реалізації завдань внутрішнього аудиту кібербезпеки долучається служба внутрішнього аудиту банку. Аудит також може бути проведено шляхом залучення юридичних / фізичних осіб із належним рівнем компетенції та досвіду (аутсорсинг).

Слід наголосити на тому, що служба внутрішнього аудиту є третьою лінією захисту від кібер-ризиків, при цьому не бере безпосередньої участі в управлінні ними, а її роль зводиться до оцінки адекватності системи забезпечення кібербезпеки цілям та задачам банку [24], оцінки загальної ефективності дій, що виконуються першою та другою лініями захисту (підрозділи менеджменту та інформаційної безпеки, відповідно) в управлінні та зниженні ризиків кібербезпеки.

Взаємозв'язок суб'єктів забезпечення кібербезпеки банку зі службою внутрішнього аудиту наведено на рисунку 1.

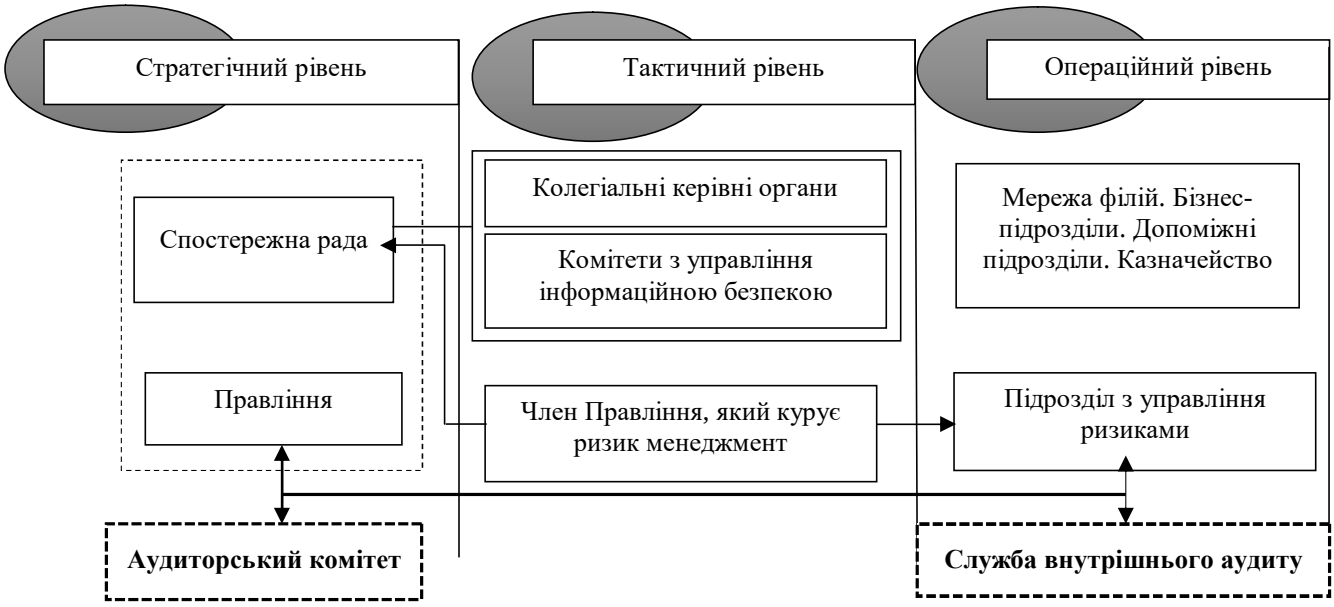

Рис. 1. **Організаційно-управлінська підсистема забезпечення кібербезпеки банку**
Джерело: побудовано авторами.

Отже, внутрішній аудит кібербезпеки має спрямовуватись на оцінку ефективності системи забезпечення кібербезпеки для того, щоб визначити, чи відповідає вона стратегії та цілям діяльності банку на ринку в поточних умовах кібер-екосистеми. Для досягнення поставленої мети слід виконати значну кількість різноспрямованих завдань, а саме [19, 21, 28, 30, 32]:

– перевірити відповідність наявної політики кібербезпеки чинному законодавству, міжнародним стандартам та рекомендаціям;

– виявити недоліки та оцінити ефективність політики кібербезпеки банку, внутрішньобанківських стандартів, регламентів та процедур;

– оцінити поточний рівень захищеності інформаційних активів банку;

– провести аналіз ризиків, пов'язаних з можливістю реалізації загроз кібербезпеки щодо інформаційних активів;

– оцінити ефективність управління кібер-ризиками;

– на основі результатів аналітичної роботи виявити можливі вразливості інформаційних активів банку до зовнішніх та внутрішніх загроз втрати кібербезпеки;

– вивчити наявні засоби контролю кібербезпеки за операційними, адміністративними та управлінськими аспектами, забезпечити ефективне виконання норм кібербезпеки та відповідність встановленим стандартам кібербезпеки;

– розробити рекомендації щодо впровадження нових та підвищення ефективності наявних механізмів забезпечення кібербезпеки.

У число додаткових завдань служби внутрішнього аудиту можуть також входити розробка політик кібербезпеки та інших нормативних документів щодо захисту інформаційних активів та участь в їх впровадженні; постановка завдань для персоналу, що стосуються забезпечення захисту інформаційних активів та попередження реалізації внутрішніх та зовнішніх загроз кібербезпеці; участь у навчанні персоналу у сфері забезпечення кібербезпеки банку тощо [19, 21, 28, 30, 32].

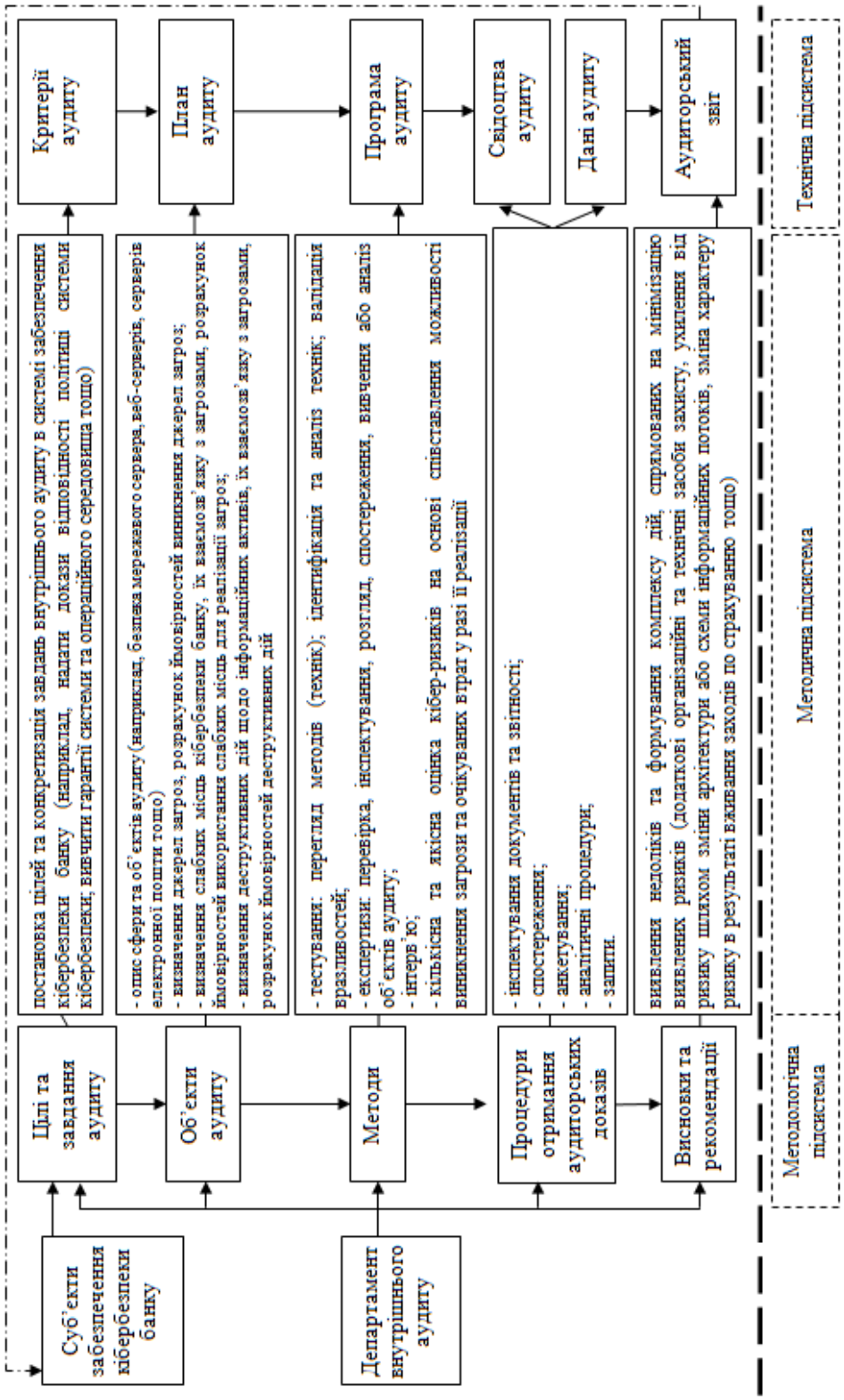

Рис. 2. **Механізм внутрішнього аудиту в системі забезпечення кібербезпеки банку**

Джерело: розроблено авторами на основі [21, 23, 29, 32, 36].

Досягнення цих цілей та завдань забезпечується через створення та постійну модернізацію механізму внутрішнього аудиту кібербезпеки.

Узагальнюючи розробки науковців, механізм внутрішнього аудиту у сфері забезпечення кібербезпеки пропонуємо визначати як сукупність методологічної, методичної та технічної підсистем, що забезпечують ідентифікацію та структуризацію об'єктів, постановку цілей та завдань, вибір методів та процедур для отримання достатніх та належних аудиторських доказів, які дозволяють аргументувати висновки та рекомендації для забезпечення необхідного рівня кібербезпеки банку, як це представлено на рисунку 2.

Цей механізм має функціонувати на основі системи принципів внутрішнього аудиту. При цьому загальні принципи внутрішнього аудиту залишаються важливими. При структуризації принципів вважаємо за доцільне використовувати підхід Ю. Слободяник та виділяти:

– основоположні принципи, що відбивають сутність внутрішнього аудиту як суспільного явища (теоретична складова): незалежність; об'єктивність; системність; комплексність; компетентність; ефективність;

– методологічні принципи, що є основою його практики:

1) принципи професійної етики: чесність; об'єктивність; конфіденційність; професійна компетентність;

2) принципи організації: систематичність; оперативність; планування; збалансованість; документація; комунікація [6].

Окрім наведених вище принципів, доцільно враховувати також більш специфічні принципи, орієнтовані на аудит в системі забезпечення кібербезпеки банку:

– актуальність: відповідність механізму внутрішнього аудиту чинній нормативно-правовій базі, міжнародним рекомендаціям та стандартам та кібер-екосистемі;

– повнота: аудит має охоплювати всі об'єкти та сфери аудиту кібербезпеки, враховувати всі загрози та фактори, що можуть вплинути на ефективність механізму забезпечення кібербезпеки банку;

– надійність: наявні підсистеми механізму внутрішнього аудиту дозволяють зробити послідовну оцінку кібер-ризиків або вимірювання об'єкта аудиту та обґрунтувати аудиторські висновки;

– періодичність відповідно до цілей внутрішнього аудиту: ефективна система внутрішнього аудиту має передбачати можливість проведення попереднього, регулярного, випадкового та нічного (неробочого) аудиту [21, 23, 29, 32, 36].

Висновки. За результатами дослідження виявлено, що ландшафт кібер-екосистеми постійно змінюється, створюючи нові загрози втрати кібербезпеки банків та призводячи до зростання рівня кібер-ризиків. У цих умовах банки мають мати ефективну систему забезпечення кібербезпеки для усунення наявних та потенційних зовнішніх та внутрішніх загроз.

Важливу роль для попередження кіберзагроз відіграє внутрішній аудит, що надає об'єктивну оцінку поточному рівню кібербезпеки в банку, виявляє слабкі місця в системі забезпечення кібербезпеки та управління кібер-ризиками та виробляє рекомендації щодо їх усунення.

Внутрішній аудит кібербезпеки визначено як періодичну систему збору та оцінки інформації для визначення того, чи забезпечують всі системи банку належний стан захищеності інформаційних активів та інформаційної інфраструктури, збереження властивостей інформаційних активів (доступності, цілісності чи конфіденційності) на цільовому рівні відповідно до встановлених критеріїв в умовах постійного впливу зовнішніх та або / внутрішніх загроз з дотриманням вимог національного та міжнародного законодавства.

Автори визначили, що система внутрішнього аудиту кібербезпеки являє собою сукупність взаємопов'язаних елементів (цілі та завдання, об'єкт, суб'єкт, механізм), що функціонують на основі загальних та спеціальних принципів та дозволяють об'єктивно оцінити рівень захищеності та збереження властивостей інформаційних активів та інформаційної інфраструктури банку в умовах постійного впливу зовнішніх та або / внутрішніх загроз, а також дотримання вимог національного та міжнародного законодавства.

4 Список використаних джерел

1. Арсланбеков-Федоров А. А. Система внутреннего контроля коммерческого банка: монография / Под ред. А. М. Тавасиева. М.: Юнити-Дана, 2004. 191 с.

2. Аудит банков: учебное пособие / Г. Н. Белоглазова, Л. П. Кроливецкая, Е. А. Лебедев [и др.]. / Под ред. Г. Н. Белоглазовой, Л. П. Кроливецкой. Изд. 2-е, перераб. и доп. М.: Финансы и статистика, 2005. 413 с.

3. Аудит у банках: навчальний посібник / За заг. ред. О. М. Сарахман. К.: УБС НБУ, 2007. 334 с.

4. Банк С. В. Аудит в коммерческих банках: учебное пособие. М.: Экономистъ, 2007. 156 с.

5. Внутрішній аудит у банку: навчальний посібник / О. М. Сарахман та ін. К.: УБС НБУ, 2015. 239 с.

6. Внутрішній аудит: навчальний посібник / за ред. Ю. Б. Слободяник. Суми: ТОВ «ВПП «Фабрика друку», 2018. 248 с.

7. Кібальник Л. О., Напора І. Ю. Впровадження політики інформаційної безпеки банківських установ. *Причорноморські економічні студії*. 2016. Вип. 12(2). С. 119-122. URL: http://nbuv.gov.ua/UJRN/bses_2016_12(2)__23 (дата звернення: 01.05.2019).

8. Кірєєв О. І. Внутрішній аудит у банку: навчальний посібник для студентів вищих навчальних закладів. К: Центр навчальної літератури, 2006. 220 с.

9. Король О. Г. Аналіз загроз і механізмів забезпечення безпеки інформації в системі електронних платежів комерційного банку України. *Системи обробки інформації*. 2015. Вип. 9. С. 88-95. URL: http://nbuv.gov.ua/UJRN/soi_2015_9_21

10. Костырко Л. А. Банковский аудит : учебное пособие. Луганск: [б. в.], 1998. 220 с.

11. Маркевич М. А. Організація і методика внутрішнього аудиту в банку: дис. ... канд. екон. наук: 08.00.09; Університет банківської справи Національного банку України. К., 2011. 301 с.

12. Мельниченко О. В. Аудит систем електронних грошей на основі інтегрованої звітності банків. *Бізнес Інформ.* 2013. № 12. С. 301-305.

13. Мельниченко О. В. Аудит договірної роботи та методологічного забезпечення банків з організації обігу електронних грошей. *Вісник Житомирського державного технологічного університету. Серія: Економічні науки*. 2014. № 2. С. 68-74.

14. Мельниченко О. В. Аудит інформаційної безпеки банку при роботі з електронними грошима. *Проблеми економіки*. 2013. № 4. С. 341-347.

15. Мельниченко О. В. Теорія, методологія та практика обліку, аналізу і аудиту електронних грошей в банках: монографія. Житомир: ЖДТУ, 2015. 383 с.

16. Мельниченко О. В. Аудит електронних грошей у банках України. *Вісник Національного банку України*. 2013. № 3. С. 41-45.

17. Облік і аудит у банках: підручник / А. М. Герасимович, Л. М. Кіндрацька, Т. В. Кривов'яз та ін. / За заг. ред. А. М. Герасимовича. К.: КНЕУ, 2004. 536 с.

18. Письменна М. С. Внутрішній аудит в банківській системі: дис. ... канд. екон. наук: 08.00.09; Одеський державний економічний університет. Одеса, 2011. 265 с.

19. Попович О. В., Войновська К. О. Особливості аудиту інформаційної безпеки банку при роботі з електронними грошима. *Формування ринкових відносин в Україні*. 2014. № 12. С. 127-130.

20. Посилення цифрового середовища проти кібер-загроз. Дослідження глобальних тенденцій інформаційної безпеки за 2018 рік: основні висновки. *PwC Україна. Міжнародне рейтингове агентство*. URL: https://www.pwc.com/ua/uk/survey/2018/pwc-2018-gsiss-strengthening-digital-society-against-cyber-shocks-ukr.pdf (дата звернення: 01.05.2019).

21. Рой Я. В., Мазур Н. П., Складанний П. М. Аудит інформаційної безпеки – основа ефективного захисту підприємства. *Кібербезпека: освіта, наука, техніка*. 2018. № 1. С. 86-93.

22. Соколинская Н.Э. Банковский аудит. М.: Перспектива, 1994. 118 с.

23. Хох В. Д., Мелешко Є. В., Смірнов О. А. Дослідження методів аудиту систем управління інформаційною безпекою. *Системи управління, навігації та зв'язку*. 2017. Вип. 1. С. 38-42.

24. Щодо організації та функціонування систем ризик-менеджменту в банках України: методичні рекомендації, схвалені Постановою Правління Національного банку України від 02.08.2004 р. № 361 [Електронний ресурс]. URL: http://zakon.nau.ua/doc/?uid=1045.5945.1&nobreak=1

25. Akinyomi O. J. Examination of fraud in the Nigerian banking sector and its prevention. *Asian Journal of Management Research.* 2012. № 3 (1), pp. 182-194. URL: https://mtu.edu.ng/mtu/oer/journals/31-EIJMRS3015.pdf (дата звернення: 01.05.2019).

26. Barakat A. Banks Basel II norms requirement regarding internal control. *Delhi Business Review*. 2009. № 10(2). pp. 35-49.

27. Boateng A. A., Boateng G. O., Acquah H. A literature review of fraud risk management in micro finance institutions in Ghana. *Research Journal of Finance and Accounting.* 2014. № 5(11). URL: https://ssrn.com/abstract=2537768 (дата звернення: 01.05.2019).

28. Boer M., Vazquez J. Cyber Security & Financial Stability: How cyber-attacks could materially impact the global financial system. URL: https://www.iif.com/Portals/0/Files/IIF%20Cyber%20Financial%20Stability%20Paper%20Final%2009%2007%202017.pdf?ver=2019-02-19-150125-767 (дата звернення: 01.05.2019).

29. Conteh N. Y., Schmick P. J. Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks. *International Journal of Advanced Computer Research*. 2016. № 6. pp. 31-38.

30. Palfi C., Muresan M. Survey on Weaknesses of Banks Internal Control Systems. *Journal of International Finance and Economics.* 2009. № 9 (1). pp. 106-116.

31. Petraşcu D., Tieanu A. The role of internal audit in fraud prevention and detection. *Procedia Economics and Finance.* 2014. № 16. pp. 489-497. URL: https://www.sciencedirect.com/science/article/pii/S2212567114008296 (дата звернення: 01.05.2019).

32. Practice Guide for Security Risk Assessment & Audit [ISPG-SM01] / Office of the Government Chief Information Officer. URL: https://www.ogcio.gov.hk/en/our_work/information_cyber_security/government/doc/ISPG-SM01.pdf (дата звернення: 01.05.2019).

33. Restore, rationalize and reinvent. A fundamental shift in the way banks manage risk: Eighth annual global EY/IIF bank risk management survey. URL: https://www.ey.com/Publication/vwLUAssets/ey-eighth-annual-global-eyiif-bank-risk-management-survey/$FILE/ey-eighth-annual-global-eyiif-bank-risk-management-survey.pdf (дата звернення: 01.05.2019).

34. Rossiter C. Top 10 priorities for internal audit in a changing environment: new realities lead to a larger, more central and more visible role for internal audit. *Bank Accounting & Finance.* Aug.-Sept. 2007. pp.34-40.

35. Salameh R., Al-Weshah G., Al-Nsour M., Al-Hiyari A. Alternative Internal Audit Structures and Perceived Effectiveness of Internal Audit in Fraud Prevention: Evidence from Jordanian Banking Industry. *Canadian Social Science.* 2011. № 7(3). pp. 40-50. URL: http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=79201535&site=ehost-live (дата звернення: 01.05.2019).

36. Scarfone K., Souppaya A., Cody A., Orebaugh M. Technical Guide to Information Security Testing and Assessment: Recommendations of the National Institute of Standards and Technology (NIST Special Publication 800-115). Gaithensburg: NIST, 2008. 80 p.

37. The impact of cybersecurity incidents on financial institutions. URL: https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_Generali_The-Impact-of-Cybersecurity-Incidents-on-Financial-Institutions-2018.pdf (дата звернення: 01.05.2019).

38. Ula M., Ismail Z., Sidek Z. M. A Framework for the governance of information security in banking system. *Journal of Information Assurance & Cyber Security*. 2011. 1-12. URL: https://ibimapublishing.com/articles/JIACS/2011/726196/726196.pdf (дата звернення: 01.05.2019).

39. Usman A. K., Shah, M. H. Critical success factors for preventing e-banking fraud. *The Journal of Internet Banking and Commerce*. 2013. № 18(2). URL: http://www.icommercecentral.com/open-access/critical-success-factors-for-preventing-ebanking-fraud-1-14.php?aid=38196 (дата звернення: 01.05.2019).

4 References

1. Arslanbekov-Fedorov, A. A. (2004). Sistema vnutrenneho kontrolia kommercheskoho banka [Internal control system of a commercial bank]. Moskva: Yuniti-Dana.

2. Belohlazova, H. N., Krolyvetskaia, L. P., Lebedev, E. A. at al. (2005). Audyt bankov [Bank audit] (2nd edition by H. N. Belohlazova, L. P. Krolyvetska). Moskva: Finansy i statistika.

3. Sarakhman, O. M. (ed.). (2007). Audyt u bankakh [Bank audit]. Kyiv: UBS NBU.

4. Bank, S. V. (2007). Audyt v kommercheskykh bankakh [Audit in Commercial Banks]. Moskva: Ekonomist.

5. Sarakhman, O. M. at al. (2015). Vnutrishnii audyt u banku [Internal audit at the bank]. Kyiv: UBS NBU.

6. Slobodianyk, Yu. B. (ed.). (2018). Vnutrishnii audyt [Internal audit]. Sumy: TOV «VPP «Fabryka druku».

7. Kibalnyk, L. O., Napora, I. Yu. (2016). Vprovadzhennia polityky informatsiinoi bezpeky bankivskykh ustanov [Implementation of information security policy of banking institutions]. *Prychornomorski ekonomichni studii*, 12(2), 119-122. Retrieved from http://nbuv.gov.ua/UJRN/bses_2016_12(2)__23

8. Kirieiev, O. I. (2006). Vnutrishnii audyt u banku [Internal audit at the bank]. Kyiv: Tsentr navchalnoi literatury.

9. Korol, O. H. (2015). Analiz zahroz i mekhanizmiv zabezpechennia bezpeky informatsii v systemi elektronnykh platezhiv komertsiinoho banku Ukrainy [Analysis of threats and mechanisms for ensuring information security in the electronic payment system of the commercial bank of Ukraine]. *Systemy obrobky informatsii*, (9), 88-95. Retrieved from http://nbuv.gov.ua/UJRN/soi_2015_9_21

10. Kostyrko, L. A. (1998). Bankovskii audit [Bank audit]. Luhansk.

11. Markevych, M. A. (2011). Orhanizatsiia i metodyka vnutrishnoho audytu v banku [Organization and method of internal audit in a bank] (Candidate dissertation). Kyiv: Universytet bankivskoi spravy Natsionalnoho banku Ukrainy.

12. Melnychenko, O. V. (2013). Audyt system elektronnykh hroshei na osnovi intehrovanoi zvitnosti bankiv [Audit of electronic money systems based on integrated reporting of banks]. *Biznes Inform*, (12), 301-305.

13. Melnychenko, O. V. (2014). Audyt dohovirnoi roboty ta metodolohichnoho zabezpechennia bankiv z orhanizatsii obihu elektronnykh hroshei [Audit of contractual work and methodological provision of banks for the organization of circulation of electronic money]. *Visnyk Zhytomyrskoho derzhavnoho tekhnolohichnoho universytetu. Seriia: Ekonomichni nauky*, (2), 68-74.

14. Melnychenko, O. V. (2013). Audyt informatsiinoi bezpeky banku pry roboti z elektronnymy hroshyma [Audit of information security of the bank when working with electronic money]. *Problemy ekonomiky*, (4), 341-347.

15. Melnychenko, O. V. (2015). Teoriia, metodolohiia ta praktyka obliku, analizu i audytu elektronnykh hroshei v bankakh [Theory, methodology and practice of accounting, analysis and audit of electronic money in banks]. Zhytomyr: ZhDTU.

16. Melnychenko, O. V. (2013). Audyt elektronnykh hroshei u bankakh Ukrainy [Аудит електронних грошей у банках України]. *Visnyk Natsionalnoho banku Ukrainy*, (3), 41-45.

17. Herasymovych, A. M. (ed.), Kindratska, L. M., Kryvoviaz, T. V. at al. (2004). Oblik i audyt u bankakh [Accounting and auditing in banks]. Kyiv: KNEU.

18. Pysmenna, M. S. (2011). Vnutrishnii audyt v bankivskii systemi [Internal audit in the banking system] (Candidate dissertation). Odesa: Odeskyi derzhavnyi ekonomichnyi universytet.

19. Popovych, O. V., Voinovska, K. O. (2014). Osoblyvosti audytu informatsiinoi bezpeky banku pry roboti z elektronnymy hroshyma [Features of audit of information security of the bank when working with electronic money]. *Formuvannia rynkovykh vidnosyn v Ukraini*, (12), 127-130.

20. PwC Ukraina. (2018). Posylennia tsyfrovoho seredovyshcha proty kiber-zahroz. Doslidzhennia hlobalnykh tendentsii informatsiinoi bezpeky za 2018 rik: osnovni vysnovky [Strengthening the digital environment against cyber threats. Study of Global Information Security Trends for 2018: Key Findings]. Retrieved from https://www.pwc.com/ua/uk/survey/2018/pwc-2018-gsiss-strengthening-digital-society-against-cyber-shocks-ukr.pdf

21. Roi, Ya. V., Mazur, N. P., Skladannyi, P. M. (2018). Audyt informatsiinoi bezpeky – osnova efektyvnoho zakhystu pidpryiemstva [Information security audit is the basis of effective protection of the enterprise]. *Kiberbezpeka: osvita, nauka, tekhnika*, (1), 86-93.

22. Sokolinskaya, N. E. (1994). Bankovskyi audit [Bank audit]. Moskva: Perspektiva.

23. Khokh, V. D., Meleshko, Ye. V., Smirnov, O. A. (2017). Doslidzhennia metodiv audytu system upravlinnia informatsiinoiu bezpekoiu [Investigation of audit methods of information security management systems]. *Systemy upravlinnia, navihatsii ta zviazku*, (1), 38-42.

24. Pravlinnia Natsionalnoho banku Ukrainy. (02.08.2004). Shchodo orhanizatsii ta funktsionuvannia system ryzyk-menedzhmentu v bankakh Ukrainy: metodychni rekomendatsii [Methodical recommendations regarding the organization and functioning of risk management systems in Ukrainian banks]. Retrieved from http://zakon.nau.ua/doc/?uid=1045.5945.1 &nobreak=1

25. Akinyomi, O. J. (2012). Examination of fraud in the Nigerian banking sector and its prevention. *Asian Journal of Management Research*, 3(1), 182-194. Retrieved from https://mtu.edu.ng/mtu/oer/journals/31-EIJMRS3015.pdf

26. Barakat, A. (2009). Banks Basel II norms requirement regarding internal control. *Delhi Business Review*, 10(2), 35-49.

27. Boateng, A. A., Boateng, G. O., Acquah, H. A (2014). Literature review of fraud risk management in micro finance institutions in Ghana. *Research Journal of Finance and Accounting*, 5(11). Retrieved from https://ssrn.com/abstract=2537768

28. Boer, M., Vazquez, J. (2017). Cyber Security & Financial Stability: How cyber-attacks could materially impact the global financial system. Retrieved from https://www.iif.com/Portals/0/Files/IIF%20Cyber%20Financial%20Stability%20Paper%20Final%2009%2007%202017.pdf?ver=2019-02-19-150125-767

29. Conteh, N. Y., Schmick, P. J. (2016). Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks. *International Journal of Advanced Computer Research*, (6), 31-38.

30. Palfi, C., Muresan, M. (2009). Survey on Weaknesses of Banks Internal Control Systems. *Journal of International Finance and Economics*, 9(1), 106-116.

31. Petraşcu, D., Tieanu, A. (2014). The role of internal audit in fraud prevention and detection. *Procedia Economics and Finance*, (16), 489-497. Retrieved from https://www.sciencedirect.com/science/article/pii/S2212567114008296

32. Office of the Government Chief Information Officer. (November 2017). Practice Guide for Security Risk Assessment & Audit [ISPG-SM01]. Retrieved from https://www.ogcio.gov.hk/en/our_work/information_cyber_security/government/doc/ISPG-SM01.pdf

33. Restore, rationalize and reinvent. A fundamental shift in the way banks manage risk: Eighth annual global EY/IIF bank risk management survey. (2017). Retrieved from https://www.ey.com/Publication/vwLUAssets/ey-eighth-annual-global-eyiif-bank-risk-management-survey/$FILE/ey-eighth-annual-global-eyiif-bank-risk-management-survey.pdf

34. Rossiter, C. (2007). Top 10 priorities for internal audit in a changing environment: new realities lead to a larger, more central and more visible role for internal audit. *Bank Accounting & Finance*, Aug.-Sept, 34-40.

35. Salameh, R., Al-Weshah, G., Al-Nsour, M., Al-Hiyari, A. (2011). Alternative Internal Audit Structures and Perceived Effectiveness of Internal Audit in Fraud Prevention: Evidence from Jordanian Banking Industry. *Canadian Social Science*, 7(3), 40-50. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=79201535&site=ehost-live

36. Scarfone, K., Souppaya, A., Cody, A., Orebaugh, M. (2008). Technical Guide to Information Security Testing and Assessment: Recommendations of the National Institute of Standards and Technology (NIST Special Publication 800-115). Gaithensburg: NIST.

37. The impact of cybersecurity incidents on financial institutions. (2018). Retrieved from https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_Generali_The-Impact-of-Cybersecurity-Incidents-on-Financial-Institutions-2018.pdf

38. Ula, M., Ismail, Z., Sidek, Z. M. (2011). A Framework for the governance of information security in banking system. *Journal of Information Assurance & Cyber Security*, 1-12. DOI: 10.5171/2011.726196. Retrieved from https://ibimapublishing.com/articles/JIACS/2011/726196/726196.pdf

Usman, A. K., Shah, M. H. (2013). Critical success factors for preventing e-banking fraud. *The Journal of Internet Banking and Commerce*, 18(2). Retrieved from http://www.icommercecentral.com/open-access/critical-success-factors-for-preventing-ebanking-fraud-1-14.php?aid=38196