УДК 004.056:[005.934:658.14]
DOI: https://doi.org/10.31617/zt.knute.2021(116)09
JEL Classification: M20, M21

НОСОВА Євгенія
E-mail: euvgenianosova@knu.ua
ORCID: 0000-0002-7975-0984
к. е. н., доцент, доцент кафедри фінансів Київського національного університету імені Тараса Шевченка
вул. Володимирська, 60, м. Київ, 01033, Україна

МУГУЄВ Кирил
E-mail: kirill.muguev@gmail.com
ORCID: 0000-0002-2393-2551
бакалавр з фінансів та кредиту Київського національного університету імені Тараса Шевченка
вул. Володимирська, 60, м. Київ, 01033, Україна

РУСІНОВ Володимир
E-mail: volodymyr.r.v@ukr.net
ORCID: 0000-0002-4362-0248
бакалавр з комп'ютерної інженерії Київського політехнічного інституту імені Ігоря Сікорського
просп. Перемоги, 37, м. Київ, 03056, Україна

ІНФОРМАЦІЙНА СКЛАДОВА У МЕХАНІЗМІ ФІНАНСОВОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

Визначено важливість механізму забезпечення інформаційної безпеки в контексті забезпечення фінансової безпеки підприємства в умовах функціонування в інформаційному середовищі та тісній взаємодії зі сферою інформаційних технологій. Встановлено, що комплексом інформаційних ризиків і ризиків транзакцій, який загрожує підприємству під час провадження його операційної діяльності, можливо управляти лише за наявності спеціалізованої служби управління інформаційними ризиками на підприємстві.

Ключові слова: фінансова безпека, інформаційна безпека, ризик транзакцій, інформаційний ризик, механізм управління ризиком.

Постановка проблеми. Цифровізація господарської діяльності зумовлює велику кількість ризиків, що загрожують фінансовій безпеці та безперервності діяльності підприємств. Під час переходу обігу комерційної інформації на електронні носії в механізмі забезпечення фінансової безпеки підприємств з'явилась нова складова – інформаційна безпека, забезпечення якої стало необхідною передумовою ефективного функціонування підприємств у довгостроковій перспективі. Нехтування процесами управління інформаційними ризиками може спричинити втрату підприємством нематеріальних активів, що призведе до дестабілізації фінансового стану підприємства та неможливості підтримання ним власної конкурентоспроможності у майбутньому. Для деяких галузей електронна комерційна інформація є найціннішим активом, без якого підприємство не може продовжувати свою господарську діяльність. До того ж в останні роки все частіше виникають масові кібератаки, які своїм впливом загрожують стабільності економічної

системи всієї країни, тож найдієвішим шляхом подолання таких загроз є забезпечення інформаційної безпеки (ІБ) у складі механізму фінансової безпеки (ФБ) на рівні підприємства.

Аналіз останніх досліджень і публікацій. Проведений огляд наукових джерел щодо теми статті показав, що багато дослідників розглядають ФБ підприємства в контексті її ролі у фінансовій безпеці держави [1; 2]. Деякі вчені приділяють більшу увагу питанню визначення та класифікації складових механізму забезпечення фінансової безпеки підприємства [3; 4]. Закордонні автори виокремлюють ІБ та управління нею в окрему функцію, яку має забезпечувати дієвий механізм забезпечення фінансової безпеки підприємства [5–8].

Однак питання застосування сучасних засобів контролю та мінімізації інформаційних ризиків і потенційних наслідків реалізації інформаційних ризиків залишаються недостатньо дослідженими.

Метою статті є обґрунтування необхідності формування механізму управління інформаційними ризиками для сучасного підприємства.

Матеріали та методи. Методологічну основу дослідження становлять загальнонаукові методи. Зокрема системний підхід використано під час розкриття сутності фінансової безпеки як економічної категорії; методи наукового абстрагування та синтезу – для визначення напрямів потенційного впливу інформаційних ризиків; узагальнення – для формування висновків. Інформаційною базою слугували праці вітчизняних і закордонних науковців.

Результати дослідження. Інформаційна безпека підприємства є складовою його ФБ. Тож для розуміння ролі ІБ спершу варто визначити поняття інформаційної та фінансової безпеки. *Фінансова безпека* підприємства – це система управління та організації відносин з приводу ідентифікації та мінімізації впливу фінансових ризиків, які загрожують стабільній діяльності підприємства [1]. Під *фінансовими ризиками* розуміють сукупність зовнішніх і внутрішніх чинників, реалізація яких може негативно вплинути на господарську діяльність підприємства, зменшити його витрати або недоотримати ним доходу [1]. Для забезпечення повного розуміння функцій фінансової безпеки доцільно розглядати поняття фінансової безпеки підприємства як стан, що характеризується захищеністю фінансових інтересів підприємства, забезпеченістю достатнім обсягом і зваженим використанням ресурсів, наявністю стійкої динаміки зростання в поточному та перспективному періодах, що досягається шляхом розробки і реалізації раціональної фінансової стратегії підприємства, гнучкістю у прийнятті фінансових рішень, вчасним реагуванням на небезпеки та загрози зовнішнього й внутрішнього характеру й ефективним управлінням фінансовими ризиками підприємства [2]. *Інформаційну безпеку* варто розуміти як систему відносин зі створення та підтримки комплексної системи

контролю використання, розповсюдження та захисту комерційної інформації на підприємстві.

До основних *складових ФБ* належать:

грошова – пов'язана з врегулюванням відносин підприємства, що виникають у процесі здійснення грошових розрахунків;

кредитна – направлена на врегулювання взаємовідносин підприємства з банками та іншими кредитними інститутами;

інвестиційна – пов'язана з регулюванням діяльності підприємства в інвестиційній сфері;

бюджетно-податкова – спрямована на врегулювання взаємовідносин підприємства з бюджетом і позабюджетними фондами [3].

Через швидке розповсюдження переносу інформації, що використовується підприємством, на електронні носії, а власних операційних процесів – у цифровий простір, постає питання розширення наведеної класифікації шляхом додавання до неї інформаційної складової. Сучасні підприємства широко застосовують електронні бази даних у власній діяльності. Пошкодження або виведення з ладу таких баз може мати значні фінансові та операційні наслідки для функціонування підприємств, а для деяких з них – взагалі стати причиною припинення діяльності.

Оскільки підприємства стають дедалі залежнішими від своїх комп'ютерних інформаційних систем, які є важливою частиною їхніх ділових операцій, управлінський персонал цих підприємств має бути дедалі обізнанішим щодо безпеки таких систем. Інформація – наразі ключовий ресурс багатьох підприємств. Інформаційна безпека стає критичним і пріоритетним фактором успіху навіть найбільших організацій.

Отже, основними сферами діяльності комерційного підприємства, що є вразливими до впливу інформаційних ризиків, є:

- системи електронних платежів, адже несанкціонований доступ до інформації працівниками підприємства або обслуговуючого банку, пов'язаними з такими системами, створює можливості для інформаційної маніпуляції діяльністю підприємства;
- системи доступу до комерційних таємниць підприємства, що зберігаються на електронних носіях;
- програмне забезпечення, що використовується підприємством для власних операційних процесів і вразливості в такому програмному забезпеченні;
- системи обігу управлінської й облікової інформації та контроль доступу працівників підприємства і третіх осіб до таких систем;
- контроль використання працівниками операційної інформації підприємства для унеможливлення застосування такої інформації в інсайдерських цілях.

Системи електронних рахунків можуть мати інформаційні ризики навіть за умови підтримання операційної транзакційної безпеки. Якщо працівник банку, що відповідає за проведення платежів у системі електронних рахунків, бачить нестачу ліквідності на рахунку підприємства, він може використати цю інформацію з метою власної вигоди або маніпулювання вартістю фінансових інструментів, що випущені компанією. До того ж працівники, що відповідають за підтримку та захист баз даних підприємства, можуть застосовувати інформацію, яка є власністю підприємства, у власних цілях. На практиці такі випадки особливо розповсюджені у комерційних відділах компанії, коли працівники під час звільнення копіюють базу клієнтів свого попереднього роботодавця з метою отримання грошової винагороди або кращих умов працевлаштування у компанії-конкурента. Подолання ризиків, пов'язаних з такими інцидентами, можливо лише шляхом запровадження комплексної системи захисту баз даних підприємства.

Використання інформації у власних цілях трапляється й з боку працівників підприємства – як для цілей інсайдерської торгівлі, так і для маніпуляцій звітними даними з метою штучного поліпшення показників діяльності цього підприємства. Через спрощення процесів копіювання та пересилання інформації застосування сучасних технологій значно ускладнює контроль за інформацією, що є в розпорядженні працівників. У разі користування децентралізованими *P*2*P* мережами для пересилання інформації, майже неможливо відслідкувати втрачену інформацію. Задля подолання проблеми такого використання інформації підприємство має запровадити багаторівневу систему контролю та захисту інформації, особливо за її копіювання на зовнішні носії та пересилання її поза корпоративної мережі. Найдієвішим рішенням є запровадження серверного забезпечення, що автоматично документує всі операції з копіювання та пересилання інформації, а отже дає змогу знайти відповідальну особу в разі втрати інформації або її застосування працівником у власних цілях. Особливу увагу варто приділити захисту та контролю за використанням електронних поштових скриньок і систем обігу управлінської інформації, адже саме ці системи найвразливіші до фішингових й вірусних атак.

У разі запровадження багаторівневої системи контролю та захисту інформації з метою оптимального використання ресурсів підприємство має чітко розподіляти зовнішніх та внутрішніх користувачів такої інформації на групи за рівнями ризику. Доцільно виділити такі групи:

особи, що мають прямий інтерес у діяльності компанії – акціонери, постачальники, замовники, кредитори та працівники компанії. У цій групі варто також особливо виокремити управлінський персонал компанії, адже саме він має доступ до найважливішої інформації підприємства;

особи, що мають непрямий інтерес у діяльності компанії – контролюючі органи, учасники фондових і товарних ринків, обслуговуючі банки та працівники таких установ;

особи, що не мають прямого фінансового інтересу – судові органи, фінансові аналітики та громадські організації.

Ризики, що загрожують безпеці комерційної інформації підприємства, з кожним роком стають нагальними для дедалі більшого кола підприємств. Унаслідок розширення інформаційних технологій стає зрозумілим, що їхнє використання може надавати конкурентні переваги, хоча запровадження їх на підприємстві пов'язане зі значними ризиками як з боку зовнішніх факторів, так і від самих технологій та процесу впровадження.

Управління інформаційними ризиками (УІР) – це процес, що передбачає здатність підприємства в особі його управлінського та професійного персоналу розпізнавати існування загроз, визначати міру їхнього впливу на господарську діяльність підприємства в разі реалізації загрози та застосування необхідних модифікацій до існуючої стратегії мінімізації ризиків від виявлених загроз економічно ефективним способом, щоб утримати можливі негативні наслідки на мінімально можливому рівні [4]. На практиці великі підприємства можуть використовувати різноманітні види інформаційного аудиту у вигляді тестування контролів і систем авторизації зміни та копіювання інформації, що вказують на існуючі недоліки цих систем і мінімізації ризиків, пов'язаних із управлінням комерційною інформацією підприємства.

У разі запровадження системи УІР на підприємстві одним з найпрактичніших рішень з позицій ефективності використання ресурсів та покриття потреб за масштабування операційних процесів підприємства є нейронні мережі [5]. На сьогодні встановлено, що застосування нейронних мереж для створення предиктивної моделі оцінки ризику витоку інформації дає змогу поліпшити безпеку в рамках багатошарового механізму захисту інформації. Такий спосіб захисту є першою лінією протидії пасивному збору інформації, до якого підприємства є вразливими. До того ж є низка статей, в яких розроблена предикативна модель аналізу облікових даних може з точністю на 80–95 % встановити можливість виконання контракту суб'єктом господарської діяльності. Висока точність таких моделей обумовлює їхнє широке впровадження в різні сфери діяльності, зокрема й фінансову. Сучасні здобутки в обчислювальній техніці дають змогу швидко розробляти, розгортати та масштабувати системи, в основі яких закладені моделі нейронних мереж [6].

Управління ризиками на підприємстві вимагає формування складних систем, що включають як безпосередньо бази даних, так і механізми авторизації користувачів та контролю змін і копіювання

інформації, що знаходиться у системі. Такі системи охоплюють ділових партнерів, контрагентів, які надають послуги підприємству на умовах аутсорсингу, а також консультантів, партнерів і підрядників. Тож ефективне функціонування інформаційної системи залежить від практики в галузі безпеки та зазвичай від управління ІБ [7].

Один з ключових процесів управління безпекою на сучасному підприємстві – управління *IT*-ризиками, що є процесом досягнення та підтримання балансу між постійним моніторингом системи на появу нових загроз і провадження діяльності з метою захисту інформаційних ресурсів.

Метою управління *IT*-ризиками є захист інформації та *IT*-інфраструктури підприємства, до яких належать дані, обладнання, програмне забезпечення, персонал та елементи комерційної інформації, втрата або поширення яких може призвести до виникнення економічних збитків або втрати потенційних прибутків. Отже, забезпечення ІБ є неодмінною частиною підтримання фінансової безпеки підприємства на належному рівні.

У сучасному інформаційному просторі підприємство фактично змушене інвестувати у створення власного або закупівлю вже розробленого програмного забезпечення, що дасть йому змогу створювати, опрацьовувати, зберігати, контролювати та захищати інформацію, що виникає за провадження ним власної операційної діяльності [8]. Сучасні процеси обліку господарських процесів на підприємстві неможливі без відповідного програмного забезпечення. Використання ж такого програмного забезпечення обумовлює необхідність побудови системи захисту такої інформації від кіберзагроз. Підприємство має регулярно архівувати свою інформацію та зберігати її окремо від загальної системи для можливого відновлення такої інформації у разі атаки на систему.

Для окремих підрозділів (відділів) втрата або пошкодження інформації підприємства можуть призвести до таких негативних наслідків:

підрозділи обліку та бухгалтерії – втрата бухгалтерської інформації, що може спричинити значні витрати на аудит та відновлення інформації щодо господарських операцій підприємства;

відділ продажів – втрата бази даних клієнтів та подальше зниження продажів;

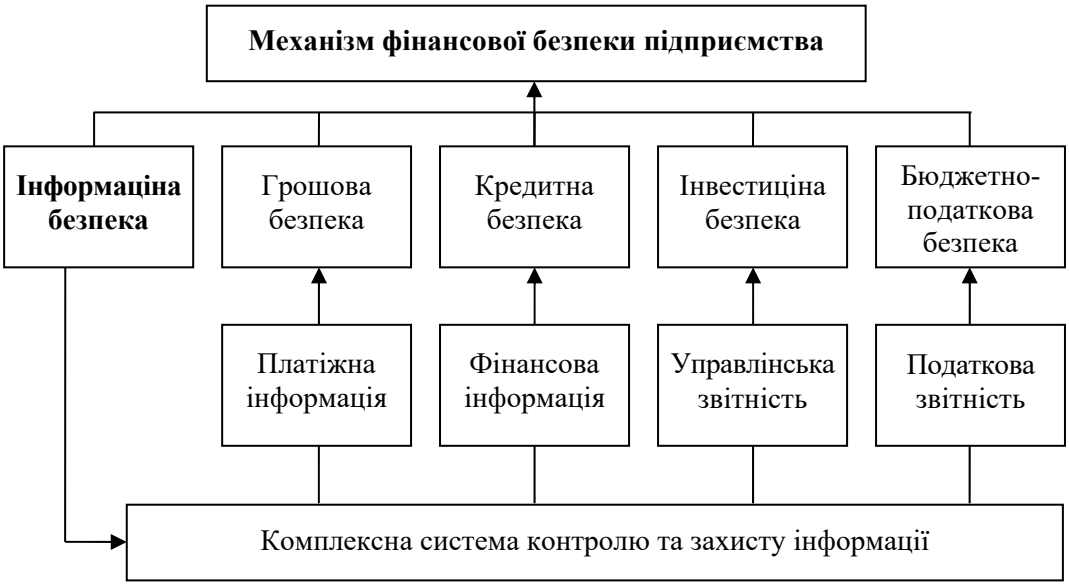
юридичний відділ – втрата документів і контрактів, що може зумовити значні витрати на їхнє відновлення. До того ж втрата юридичних документів може призвести до невиконання покупцями та постачальниками власних зобов'язань перед підприємством та розголошення ними комерційної інформації, використання якої було регламентовано втраченими документами;

виробничі підрозділи – втрата програмного забезпечення комп'ютерних систем, що може спричинити значні витрати на їхнє відновлення та налаштування;

складський відділ – втрата складських реєстрів, що призведе до значних витрат праці на проведення загальної інвентаризації. До того ж збій у складському господарстві може зумовити переривання процесу виробництва, що своєю чергою може призвести до невиконання підприємством власних контрактних зобов'язань і припинення діяльності.

Сучасні підприємства не можуть функціонувати на конкурентному рівні без використання *IT* та доступу до інформаційної інфраструктури, що збільшує потребу у розвитку адекватної системи управління інформаційними ризиками. Така система має містити чотири основні компоненти управління ризиками, спрямовані на: ідентифікацію ризику; аналіз ризику; мінімізацію ризиків; моніторинг ризиків.

Отже, інформаційна безпека доповнює інші складові ФБ та забезпечує виконання ними своїх функцій через дію комплексної системи контролю та захисту інформації, якою оперують інші складові фінансової безпеки. Місце ІБ у складі механізму ФБ підприємства проілюстровано на *рисунку*.



Місце інформаційної безпеки у складі механізму фінансової безпеки підприємства

Джерело: побудовано авторами.

Варто зазначити, що витрати на впровадження такої системи можуть бути значними у короткостроковій перспективі, проте вони дадуть змогу уникнути набагато більших витрат у разі втрати бази даних або її пошкодження, а також забезпечити стабільне функціонування підприємства у майбутньому.

Висновки. Вплив інформаційної безпеки на ФБ підприємства доцільно вимірювати через оцінку фінансових ризиків, аби визначити

розмір прямих і непрямих витрат від впровадження того чи іншого рішення у сфері управління фінансовою безпекою підприємства.

Інформаційні системи на сучасному етапі є необхідними для функціонування всіх підрозділів підприємства. Збереження цілісності таких систем і забезпечення їхнього безперервного функціонування є надзвичайно важливим для підтримання належного рівня фінансової безпеки підприємства у довгостроковій перспективі. Задля забезпечення інформаційної безпеки підприємство має створити цілісну систему контролю та захисту інформації у формі спеціалізованої служби управління інформаційними ризиками на підприємстві.

Механізм управління ІБ забезпечує функціонування підприємства на конкурентному рівні в умовах сучасного комп'ютеризованого обігу інформації. Саме завдяки такому механізму стає можливим ефективне управління інформаційними ресурсами та прийняття своєчасних управлінських рішень. Без чітко налагодженого механізму управління інформаційною безпекою підприємство є вразливим до зовнішніх і внутрішніх загроз, що у довгостроковій перспективі може загрожувати його прибутковості та безперервності діяльності.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Койло В. В. Теоретико-методологічні підходи до оцінки поняття фінансової безпеки в умовах зростання загроз країни. *Науковий вісник Херсонського державного університету*. 2017. Вип. 23. Ч. 2. С. 38-42.
2. Лиса О. В., Ярощук О. В. та інш. Фінансова безпека суб'єктів господарювання в сучасних умовах. *Економічний аналіз: збірник наукових праць*. Тернопіль: Економічна думка, 2016. Т. 26. № 1. С. 58-64.
3. Киш Л. М. Фінансова стійкість компанії в сучасних умовах. Одеса. *Причорноморські економічні студії.* 2018. № 36. С. 75-79.
4. Краснокутська Н. С., Коптєва Г. М. Дефініція поняття «фінансова безпека підприємства»: основні підходи та особливості. *Бізнесінформ*. 2019. № 7. С. 14-19.
5. Global Survey of Confidential Information Origins. 2017. URL: https://www.ec–rs.ru/novosti/utechki–konfidentsialnoy–informatsii–v–2017–godu–globalnoe–issledovanie–infowatch.
6. Ali O., Shrestha A., Chatfield A., Murray P. Assessing information security risks in the cloud: A case study of Australian local government authorities. *Government Information Quarterly*, 2020. Elsevier. URL: https://wroya.com.
7. Veiga A., Astakhova L., Botha A., Herselman M. Defining organisational information security culture. Perspectives from academia and industry. *Computers & Security*, 2020. URL: https://www.researchgate.net.
8. Brunner M., Sauerwein C., Felderer M., Breu R. Risk management practices in information security: Exploring the status quo in the DACH region. *Computers & Security*, 2020. Elsevier. URL: https://arxiv.org/pdf/2003.07674.pdf.

Стаття надійшла до редакції 06.05.2021.

Nosova Eu., Muhuiev K., Rusinov V. Information component in the financial security mechanism of the enterprise.

Background. *The digitalization of economic activity causes a large number of risks that threaten the financial security and continuity of enterprises. For some industries, electronic commercial information is the most valuable asset, without which the company cannot continue its business.*

Analysis of recent research and publications *has shown that despite the availability of some scientific achievements, an important scientific and practical problem of the application of modern means of control and minimization of information risks and the potential consequences of information risks remains unresolved.*

The ***aim*** *of the article is to substantiate the need to form a mechanism for managing information risks for a modern enterprise.*

Materials and methods. *In the course of the research the methods of scientific abstraction, synthesis, generalization and systematization were used.*

Results. *Modern enterprises cannot operate at a competitive level without the use of IT and access to information infrastructure, which increases the need to develop an adequate information risk management system. Such a system should contain four main components of risk management, aimed at: risk identification; risk analysis; risk minimization; risk monitoring.*

Thus, information security complements other components of the FS and ensures that they perform their functions through a comprehensive system of control and protection of information, which is operated by other components of financial security.

Conclusion. *The impact of information security on the company's FS should be measured through the assessment of financial risks to determine the amount of direct and indirect costs of implementing a solution in the field of financial security management of the enterprise.*

The IS management mechanism ensures the functioning of the enterprise at a competitive level in the conditions of modern computerized information circulation. It is thanks to this mechanism that effective management of information resources and timely management decisions becomes possible. Without a well-established information security management mechanism, the company is vulnerable to external and internal threats, which in the long run may threaten its profitability and business continuity.

Keywords: financial security, information security, transaction risk, information risk, risk management mechanism.

REFERENCES

1. Kojlo, V. V. (2017). Teoretyko-metodologichni pidhody do ocinky ponjattja finansovoi' bezpeky v umovah zrostannja zagroz krai'ny [Theoretical and methodological approaches to assessing the concept of financial security in the face of growing threats to the country]. *Naukovyj visnyk Hersons'kogo derzhavnogo universytetu – Scientific Bulletin of Kherson State University*, (Issue 23), (part. 2), (pp. 38-42) [in Ukrainian].

2. Lysa, O. V., & Jaroshhuk, O. V. (et al.). (2016). Finansova bezpeka sub'jektiv gospodarjuvannja v suchasnyh umovah [Financial security of business entities in modern conditions]. *Ekonomichnyj analiz: zbirnyk naukovyh prac' – Economic analysis: a collection of scientific papers*. Ternopil': Ekonomichna dumka. (Vol. 26), *1*, 58-64 [in Ukrainian].
3. Kysh, L. M. (2018). Finansova stijkist' kompanii' v suchasnyh umovah [Financial stability of the company in modern conditions]. *Prychornomors'ki ekonomichni studii' – Black Sea Economic Studies*. Odesa, *36*, 75-79 [in Ukrainian].
4. Krasnokuts'ka, N. S., & Koptjeva, G. M. (2019). Definicija ponjattja «finansova bezpeka pidpryjemstva»: osnovni pidhody ta osoblyvosti [Definition of the concept of «financial security of the enterprise»: basic approaches and features]. *Biznesinform – Businessinform*, *7*, 14-19 [in Ukrainian].
5. Global Survey of Confidential Information Origins. (2017). Retrieved from https://www.ec–rs.ru/novosti/utechki–konfidentsialnoy–informatsii–v–2017–godu–globalnoe–issledovanie–infowatch [in English].
6. Ali, O., Shrestha, A., Chatfield, A., & Murray, P. (2020). Assessing information security risks in the cloud: A case study of Australian local government authorities. Government Information Quarterly, Elsevier. Retrieved from https://wroya.com [in English].
7. Veiga, A., Astakhova, L., Botha, A., Herselman, M. (2020). Defining organisational information security culture. Perspectives from academia and industry. *Computers & Security*. Retrieved from https://www.researchgate.net [in English].
8. Brunner M., Sauerwein C., Felderer M., & Breu R. (2020). Risk management practices in information security: Exploring the status quo in the DACH region. *Computers & Security*. Elsevier. Retrieved from https://arxiv.org/pdf/ 2003.07674.pdf [in English].