Міністерство освіти і науки України
Сумський державний університет
Навчально-науковий інститут бізнесу, економіки та менеджменту
Кафедра економічної кібернетики

ВИКЛИКИ КІБЕРБЕЗПЕКИ ІНДУСТРІЇ ФІНАНСОВИХ ПОСЛУГ

Матеріали
наукової онлайн-конференції

(Суми, 07 вересня 2023)

Суми
Сумський державний університет
2023

004.056.5:336(082)
В43

Затверджено Вченою Радою Сумського державного університету (протокол № 2, 14.09.2023)

S62 Виклики кібербезпеки індустрії фінансових послуг: Матеріали наукової онлайн-конференції, Суми, 07 вересня 2023. Збірник матеріалів тез наукової онлайн-конференції / за загальною редакцією доц. Койбічук В.В. – Суми : Сумський державний університет, 2023. – 183 с.

Матеріали наукової онлайн-конференції " Виклики кібербезпеки індустрії фінансових послуг" присвячені пошуку системного вирішення проблем у сфері протидії кібеззагрозам у сфері фінансових послуг, підвищенню рівня кіберзахисту об'єктів критичної інфраструктури.

Видання розраховане на науковців, викладачів, студентів вищих навчальних закладів, аспірантів, докторантів та інших зацікавлених осіб.

004.056.5:336(082)

ЗМІСТ

ТЕНДЕНЦІЇ МОДЕЛЮВАННЯ DUE DILIGENCE ДЛЯ ПРОТИДІЇ ФІНАНСОВИМ КІБЕРШАХРАЙСТВАМ

TRENDS IN DUE DILIGENCE MODELING TO COUNTER FINANCIAL CYBER FRAUD

Тетяна Доценко, *доктор філософії*
Технічний університет Берліну, Німеччина
Дарина Бережна, *студентка*
Сумський державний університет, Україна

Суттєвим ризиком для фінансово-економічної безпеки та стабільності сучасних суб'єктів господарювання є фінансові шахрайства, що можуть статися через відсутність чіткої ясності функціонування організації, неналежну діяльність установи, недоліки інформаційного та технічного забезпечення, фінансові питання. Для запобігання шахрайствам, виходячи із специфіки функціонування підприємств, потрібно проводити їх перевірки, такі як аудит, оцінка, податкові перевірки. А в сучасних цифровізованих умовах функціонування суб'єктів господарювання, особливої актуальності набуває удосконалення системи фінансового захисту, в тому числі через застосування такої процедури перевірки як Due diligence, що є особливо ефективною в аспекті протидії фінансовим кібершахрайствам.

Поняття due diligence є відносно новою категорією, що набуває активного використання серед сучасних науковців світу: Елбел Дж., Бозе О'Рейлі С., Грзіч Р., Дева С., Ліеса К.Р.Ф., Седано Т. Г., Літвін Д., Гуаніпа Х. Дж., Чіма Дж. Т., Камолетто С., Корацца Л., Піцці С., Сантіні Е., та ін. Однією з головних причин проведення перевірок виступають ризики та загрози фінансових злочинів та, згідно останніх тенденцій, кібершахрайств, що досліджуються науковцями: Ніколлс Дж., Куппа А., Ле-Хак Н., Хіран К. К., Рао С.С., Шарма Р., Міна Р., Ліонов С., Главічка Р., Бойко А., Миненко С., Гарай- Фодор М., Кузьор А., Брожек П., Кузьменко О., Яровенко Х., Васильєва Т., Белло М., Гріффітс М., та ін. При чому, у напрямку протидії фінансовим шахрайствам, в тому числі й кібершахрайствам, практики починають використовувати елементи методики due diligence підприємств: Калина І., Хурдей В., Шевчук В., Власюк Т., Леонідов І., Читіміра Х., Мунедзі С.

Особливу роль у дослідженні економічних процесів відводять моделюванню. Досліджуючи поняття due diligence, не можливо не відмітити важливість моделювання його процесів та етапів, що висвітлюють наступні фахівці: Каранланте М., Д'Амато В., Ферсіні П., Форте С., Мелісі Г., Рой В., Дежарден Д., Фертел К., Уелле-Пламондон К., Аман А., Реджі Д. Дж., Лі З. , Лю В., Сунь Ю., Юксель С., Дінсер Х., Лю Ю., Фен Ю., Чжоу Б. (Carannante et al., 2023;

Aman et al., 2022; Li et al., 2022). Додатково слід зупинитися на моделюванні в аспекті протидії фінансовим кібершахрайствам, як визначальної складової досліджуваного питання, що представлені у роботах: Лінь К., Гао Ю., Васильєва Т.А., Кузьменко О.В., Стоянець Н.В., Артюхов А.Є., Боженко,В.В.; Кузьор А., Васильєва Т., Кузьменко О., Койбічук В., Брожек П., Кузьменко О.В., Кубалек Й., Боженко В.В., Кушнерьов О.С., Віда І., Вахід С.Д. М., Буя А.Г., Хасрол Йоно М.Н.Х., Азіз А.А. , Буджа А.Г., Вахід С.Д.М., Рахман Т.Ф.А., Дераман Н.А., Джоно М.Н.Х.Х., Азіз А.А. (Vasilyeva et al., 2022; Kuzior et al., 2022; Kuzmenko et al., 2021).

Проаналізувавши літературні надбання з досліджуваного питання, було сформульовано поняття Due Diligence – як наукової категорії, що передбачає проведення сукупності дій: різновекторне дослідження та оцінка роботи суб'єкта, з глибоким вивченням фінансового стану, оцінкою ризиків (в тому числі фінансових, інвестиційних), аналіз місця об'єкта на ринку, з особливим акцентом на питання, пов'язані з безпекою, правами людини та навколишнього середовища - для формування комплексного висновку щодо фінансового, юридичного, інвестиційного стану суб'єкта дослідження, наявних ризиків. Due Diligence включає наступні етапи: проведення консультаційної діяльності із зацікавленими сторонами; процеси збору та використання експертиз; проводиться пошук та збір даних (в тому числі щодо політики кібербезпеки); здійснюється вивчення, консолідація та аналіз даних, аналіз потенційних ризиків, перевірка відповідності загальним і специфічним галузевим стандартам; формування висновку щодо стану підприємства з досліджуваного питання, прийняття відповідного рішення.

Важливою складовою оцінки функціонування підприємств є моделювання таких вищеописаних процесів due diligence: модель due diligence на основі машинного навчання передбачає оцінку прибутковості операцій з проблемними кредитами на вторинному ринку, моделювання складних взаємозв'язків між показниками; вдосконалення процесу належної перевірки шляхом розробки алгоритму штучного інтелекту; модель due diligence на основі оцінки ризиків передбачає комплексну методологію виконання належної перевірки ризиків багатонаціональної інженерно-будівельної організації третіми сторонами; модель due diligence на основі глибокого активного навчання НЛП передбачає формування моделі належної перевірки та прогнозування навколишнього середовища; адаптацію та розширення існуючих моделей обробки інформації природною мовою НЛП шляхом додавання даних екологічної сфери (EDD); моделі NAP, mHRDD, BHR оптимальності оцінки впровадження керівних принципів ООН щодо бізнесу та прав людини. National Action Plans Model – модель національних планів дій щодо бізнесу та прав людини, національна політична стратегія з урахуванням практик держав, що передбачає запропоновану урядом систему «м'яких» політичних інструментів, що описують пріоритети уряду, за яких майбутні дії орієнтовані на сприяння виконанню юридичних або реалізації політичних зобов'язань щодо перевірки прав людини, усунення

негативних наслідків прав людини внаслідок господарської діяльності; модель консенсусної багатовимірної перевірки інвестиційних проектів на основі фінансових технологій передбачає груповий підхід до оцінки фінансових альтернатив для інвестиційних проектів; комп'ютерна модель due diligence через AHP та big data передбачає кількісну оцінку поточної технічної належної перевірки.

Розглядаючи питання моделювання процесів due diligence, зупинимося на актуальних тенденціях цієї процедури перевірки в аспекті моделювання протидії фінансовим кібершахрайствам. Так, вартими детального розгляду є наступні моделі: модель зображення жертви кіберзлочину передбачаэ створення фазового зображення жертви кіберзлочину на основі методів систематизації, порівняння, групування, логічного узагальнення, бібліометричного аналізу, регресійного аналізу (метод сигма-обмеженої параметризації), алгоритм асоціативних правил; економетрична модель впливу цифровізації на економічні трансформації на основі розроблених квантильних регресій (з урахуванням національного показника кібербезпеки) - передбачає обґрунтування існування процесів конвергенції у напрямку цифровізації країн, враховуючи певні індикатори - рівень національної кібербезпеки, легкість отримання електроенергії, легкість ведення бізнесу, індекс протидії відмиванню грошей, рівень цифрового розвитку країни; модель машинного пов'язаного навчання (SVM) для захисту фінансового сектору від кіберзлочинності - передбачає забезпечення управління кібербезпекою за допомогою аналізу великих обсягів даних, що дозволяє на ранніх стадіях виявити та оцінити потенційні чинники кіберзагроз; моделі оцінки оцінки впливових факторів поінформованості про кібербезпеку передбачає кількісне дослідження факторів організаційного, соціального та індивідуального вплив на обізнаність про кібербезпеку; модель обізнаності про кібербезпеку для людей похилого віку передбачає розробку організаційної, соціальної та індивідуальної моделі поінформованості про кібербезпеку (Osicsam) для людей похилого віку.

Аналіз результатів світових і вітчизняних досліджень дозволяє виявити та оцінити пріоритети та тренди на сучасному фінансовому ринку, зміщення вектору досліджень у напрямку вивчення проблем кіберзлочинності. Так, модернізація процесів забезпечення фінансової, а особливо кібербезпеки підприємств, стає пріоритетним напрямком для керівництва сучасних суб'єктів господарювання. При чому, дієвим інструментом для протидії фінансовим кібершахрайствам є застосування процесів due diligence підприємств, як новітньої системи перевірки стану діяльності суб'єкта, моделювання таких процесів. Використання на підприємствах методик і моделей due diligence, дозволить сформувати керівні принципи та політику фінансової безпеки підприємств, що в свою чергу допоможе знизити рівень негативних наслідків в тому числі і фінансових кіберзагроз, фінансових кіберризиків, що можуть бути присутні у бізнес процесах;

максимізувати можливі позитивні ефекти від прийняття сформованих з урахуванням ряду факторів, управлінських рішень.

Роботу виконано в межах науково-дослідної теми «Data-Mining для протидії кібершахрайствам та легалізації кримінальних доходів в умовах цифровізації фінансового сектору економіки України», № держреєстрації: 0121U100467; «Моделювання механізмів детінізації та декорумпізації економіки для забезпечення національної безпеки: вплив трансформації фінансових поведінкових патернів», № держреєстрації: 53.16.01-22/24.3П-01; «Національна безпека через конвергенцію систем фінансового моніторингу та кібербезпеки: інтелектуальне моделювання механізмів регулювання фінансового ринку» № держреєстрації: 0121U109559. The article was written during a research stay at the Technical University of Berlin, Department of Health Care Management.

Список літератури

1. Aman, A., & Reji, D. J. (2022). Environmental due diligence data: A novel corpus for training environmental domain NLP models. Data in Brief, 45 doi:10.1016/j.dib.2022.108579
2. Carannante, M., D'Amato, V., Fersini, P., Forte, S., & Melisi, G. (2023). Machine learning due diligence evaluation to increase NPLs profitability transactions on secondary market. Review of Managerial Science, doi:10.1007/s11846-023-00635-y
3. Kuzior, A., Vasylieva, T., Kuzmenko, O., Koibichuk, V., & Brożek, P. (2022). Global digital convergence: Impact of cybersecurity, business transparency, economic transformation, and AML efficiency. Journal of Open Innovation: Technology, Market, and Complexity, 8(4) doi:10.3390/joitmc8040195
4. Kuzmenko, O. V., Kubálek, J., Bozhenko, V. V., Kushneryov, O. S., & Vida, I. (2021). An approach to managing innovation to protect financial sector against cybercrime. [Podejście do zarządzania innowacjami w celu ochrony sektora finansowego przed cyberprzestępczością] Polish Journal of Management Studies, 24(2), 276-291. doi:10.17512/pjms.2021.24.2.17
5. Li, Z. (2022). Operationalising the UN guiding principles on business and human rights through human rights due diligence: A critical assessment of current states practices. Academic Journal of Interdisciplinary Studies, 11(4), 8-21. doi:10.36941/ajis-2022-0094
6. Vasilyeva, T. A., Kuzmenko, O. V., Stoyanets, N. V., Artyukhov, A. E., & Bozhenko, V. V. (2022). THE DEPICTION OF CYBERCRIME VICTIMS USING DATA MINING TECHNIQUES. [Побудова портрету кібержертви з використанням технологій data-mining] Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetu, (5), 174-178. doi:10.33271/nvngu/2022-5/174