

ПЕЧЕНА Анна

здобувачка першого (бакалаврського) рівня вищої освіти,
спеціальності 071 Облік і оподаткування,
Одеський національний економічний університет
nushapechena@gmail.com

ГОСТРИК Олексій

к.е.н., доцент,
кафедра економічної кібернетики та інформаційних технологій,
Одеський національний економічний університет
AlexeyGostrik@gmail.com

КІБЕРБЕЗПЕКА У ФІНАНСОВІЙ СФЕРІ

Кібербезпека в Україні є невід'ємною складовою національної безпеки, оскільки вона забезпечує захист критичної інфраструктури, інформаційних систем та даних від кібератак. У сучасному світі, де все більша кількість процесів цифровізується, кіберзагрози становлять серйозну загрозу для економічної стабільності, політичної системи та суспільства в цілому. Захист кіберпростору є необхідною умовою для збереження суверенітету країни, підтримки економічного зростання та забезпечення безпеки громадян.

У доповіді аналізується поняття кібербезпеки, кіберзагроз та кібершахрайства, а також приводяться приклади шляхів подолання загроз стосовно фінансового сектору економіки країни.

Відповідно до закону України «Про основні засади забезпечення кібербезпеки України», «кібербезпека - 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» [7].

Кіберзагрози у фінансовій сфері прямо впливають на фінансову стабільність підприємств, призводячи до матеріальних втрат та підриваючи інтереси як власників, так і інвесторів.

Науковці виділяються декілька видів кіберзагроз, що вражають фінансовий сектор, з них [1; 5, с. 31-34]:

1. Фішинг. Створення підроблених веб-сайтів, які імітують офіційні ресурси, дозволяє зловмисникам виманювати у користувачів конфіденційну інформацію для подальшого її використання в злочинних цілях.

2. Розповсюдження шкідливих програм. Зловмисники можуть підроблювати програми. Завантаживши такі програми, можна нашкодити комп'ютерній системі та передати третім особам свої особисті дані.

3. DDoS-атаки. Такі атаки спрямовані на комп'ютерну систему органу, організації, підприємства з метою з метою порушення доступності до атакованих вебресурсів. Наразі в Україні часто спостерігаються DDoS-атаки на банківську систему.

4. Скімінг. Це вид шахрайства, при якому зловмисники використовують спеціальні зчитувальні пристрої ("скіммери") для копіювання даних з магнітної смуги або безконтактного чіпа банківської картки під час її використання в банкоматі. Отримані дані потім використовуються для створення дублікатів карток та незаконного зняття коштів.

Кібератаки мають багатогранний вплив на діяльність підприємств. Окрім очевидних фінансових втрат, вони призводять до дестабілізації бізнес-процесів внаслідок порушення роботи інформаційних систем, підривають довіру клієнтів та партнерів, а також створюють загрозу для безпеки персональних даних, що зберігаються в комп'ютерних системах.

Існує безліч методів та способів, за допомогою яких можна завдати шкоди фінансовій системі. З кожним роком тенденція до урізноманітнення видів шахрайств збільшується.

Задля забезпечення фінансового та банківського сектора України від кібершахрайств Національний банк України підписав Меморандум про взаємодію та співробітництво у сфері кібербезпеки. Метою цього документа є налагодження співпраці між Національним банком України та Міністерством фінансів США для посилення кіберзахисту фінансового сектору України шляхом обміну інформацією, розвитку Центру кіберзахисту НБУ та надання міжнародної технічної допомоги [6].

Постійна еволюція кіберзагроз вимагає від України постійного вдосконалення систем кібербезпеки, особливо у фінансовому секторі, який є привабливою мішенню для кіберзлочинців через широке використання цифрових технологій. Для ефективного захисту від них необхідний комплексний підхід.

Ефективними методами боротьби з кібершахраями, на нашу думку, можна вважати наступне:

- посилення відповідальності. Державі необхідно передивитися законодавство та запровадити більш жорсткі міри покарання для шахраїв, збільшити суми до відшкодування та термін покарання;

- інформування населення. Населенню необхідно знати, з якими ризиками вони можуть зіткнутися під час здійснення фінансових операцій. Для цього банківські установи, спеціалізовані організації тощо мають доводити до суспільства можливі ризики;

- просвіта в освітніх закладах. Навчальні заклади мають звертати особливу увагу на можливості бути обманутим шахраями. Особливо це стосується закладів середньої освіти, оскільки саме діти є однією з найбільших ланок, яка може постраждати від кібершахраїв;

- загальна організація боротьби з кіберзлочинністю та правоохоронна діяльність, спрямована саме на виявлення, запобігання та розкриття кіберзлочинів. Кіберполіція має приділяти

більшу увагу новим схемам, попереджати про їх небезпечність та оперативно знаходити винних.

На нашу думку, доцільно було б додати до цього списку практику банківських установ, яка є досить ефективною, особливо в сучасних умовах. Разом з Національним банком України, РНБО (Рада національної безпеки і оборони України) запустила проєкт, спрямований на захист українців від фінансових кібератак [8]. Цей крок став необхідним через зростання кількості шахрайських схем, особливо пов'язаних з війною. Мета проєкту – перенаправляти користувачів з фішингових сайтів на сторінки з попередженнями. За перший місяць роботи тисячі українців завдяки цьому проєкту уникнули шахрайства.

Державі необхідно співпрацювати з фінансовими установами, оскільки саме вони можуть допомогти масово розповсюдити інформацію про можливі загрози під час проведення грошово-кредитних операцій тощо.

Кіберзагрози для фінансового сектору становлять складну та постійно еволюціонуючу проблему, що вимагає комплексного підходу до її вирішення. Для ефективного захисту необхідно поєднання законодавчих ініціатив, підвищення обізнаності населення, розвитку сучасних технологій захисту та міжнародного співробітництва. Запобігання кібератак є більш ефективним, ніж їхні наслідки, тому інвестиції в профілактичні заходи є

виправданими. Важливо розуміти, що кожен користувач мережі відіграє свою роль у забезпеченні кібербезпеки, дотримуючись правил кібергігієни.

Список використаної літератури

1. Гончаренко І. Г. Кіберзагрози фінансового сектора в умовах війни. Економіка та суспільство. 2022. № 50.

2. Гострик О.М. Програмні засоби бізнес-аналізу та їх застосування для оцінки розвитку бізнес-середовища. Економіко-правові аспекти господарювання: сучасний стан, ефективність та перспективи: матеріали VIII Міжнародної науково-практичної конференції(Одеса, 23-24 вересня 2022 р). - Одеса, 2022, 596 с. (с. 372-373).

[URL: http://dspace.oneu.edu.ua/jspui/handle/123456789/15236](http://dspace.oneu.edu.ua/jspui/handle/123456789/15236) (дата звернення: 02.10.2024).

3. Гострик О.М., Степаненко О.А. Визначення допустимого кредитного ризику комерційного банку з використанням методу системної динаміки. Науковий вісник Ужгородського національного університету. Серія "Міжнародні економічні відносини та світове господарство". Вип. 6, частина 3. Видавничий дім "Гельветика". Ужгород, 2016 с. 60-63. ISSN: 2413-3960. URL: <http://dspace.oneu.edu.ua/jspui/handle/123456789/4665> (дата звернення: 02.10.2024).

4. Білявська Ю., Шестак Я. Кібербезпека та кібергігієна: нова ера цифрових технологій. The international scientific-practical journal "Commodities and Markets". 2022. Т. 43, № 3. С. 47–59. URL: [https://doi.org/10.31617/2.2022\(43\)04](https://doi.org/10.31617/2.2022(43)04) (дата звернення: 03.10.2024).

5. Маковець О. П., Дрозд І. К. Кібербезпека як фактор фінансової безпеки підприємства. Економіка. Фінанси. Право. 2020. № 5/3. С. 31–35. URL: <http://efp.in.ua/uk/journal-article/442> (дата звернення: 02.10.2024).

6. Національний банк України. Національний банк України та Міністерство фінансів США продовжать обмін досвідом у сфері кібербезпеки. Національний банк України. URL: <https://bank.gov.ua/ua/news/all/natsionalniy-bank-ukrayini-ta-ministerstvo-finansiv-ssha-prodovjat-obmin-dosvidom-u-sferi-kiberbezpeki> (дата звернення: 02.10.2024).

7. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII : станом на 28 черв. 2024 р. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text> (дата звернення: 02.10.2024).

8. Національний банк України. Стартував проєкт із протидії кібершахрайству у фінансовому секторі. Національний банк України. URL: <https://bank.gov.ua/ua/news/all/startuvav-proyekt-iz-protidiyi-kibershahraystvu-u-finansovomu-sektori> (дата звернення: 06.10.2024).

9. Сопілко І. Інформаційна безпека та кібербезпека: порівняльно-правовий аспект. Scientific works of National Aviation University. Series: Law Journal "Air and Space Law". 2021. Т. 2, № 59. С. 110–115. URL: <https://doi.org/10.18372/2307-9061.59.15603> (дата звернення: 05.10.2024).