державному секторі в умовах реформування системи управління публічними фінансами та зміцнення фінансової безпеки суб'єктів господарювання. *Світ фінансів*. 2022. № 4(73). С. 22-44. URL: https://archive.interconf.center/index.php/conference-proceeding/article/view/3992. (дата звернення 01.05.2024 р.).

УДК 336.71:004.056.5

Раєвська Маргарита Олександрівна, *студентка,*
Науковий керівник: Худолій Юлія Сергіївна,
кандидат економічних наук, доцент
Національний університет «Полтавська політехніка імені Юрія Кондратюка» (Україна)

КІБЕРБЕЗПЕКА БАНКІВ УКРАЇНИ В УМОВАХ ВІЙНИ

Від початку війни, в Україні збільшилась кількість кібератак, які охопили державні установи, приватні організації та громадян. Особливо важливим є готовність та реагування на інциденти для банків, які є частиною критичної інфраструктури. Таке збільшення загроз в кіберпросторі змушує підвищити рівень захисту та розробити плани реагування на кіберінциденти. Фінансова система України продовжує боротись із викликами війни, незважаючи на збитки. Боротьба із наслідками також важлива частина забезпечення економічної безпеки країни. На даний момент НБУ успішно протистоїть викликам війни.

28 червня 2017 року правління Нацбанку прийняло постанову №95, якою затверджено Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України. Саме ця постанова вперше передбачила регулювання Національним банком питань безпеки інформації і кіберзахисту, шляхом визнання обов'язкових вимог. Ці заходи включають в себе: захист від

зловмисного коду; заходи безпеки при використанні електронної пошти; контроль доступу до банківської системи; захист мережі банку; криптографічний захист. Реалізація проекту сприяє нормативно-правовому регулювання питань кіберзахисту системи банківсько бізнесу України, швидке та ефективне передавання інформації між банками країни та забезпечить комунікацію і партнерство між суб'єктами кіберзахисту та банками [1].

Проект USAID «Кібербезпека критично важливої інфраструктури в Україні» розрахований на 4 роки і має вартість 38 млн. дол., розпочав свою діяльність у 2020 році. Завдання проекту – підвищити рівень готовності критичної інфраструктури до кібератак. Є три основні напрямами: зміцнення середовища кіберзахисту, формування кадрового складу в України, створення стійкої індустрії. Діяльність проекту підвищить якість послуг за рахунок співпраці державних установ і приватного бізнесу. Після повномасштабного вторгнення Росії, було профінансовано діяльність технічних спеціалістів, які допомогли надавачам послуг державного сектору виявити і вирішити проблеми в кіберпросторі [3].

Центр кіберзахисту НБУ створений для ефективного функціонування системи кіберзахисту банківських та небанківських станов. У центрі встановлено 4 сервіси: Incident Response, Proactive Risk Monitoring, Information services, Training and education. Перший, Incident Response, це сервіс який надає допомогу банкам у вирішенні технічних питань підчас кібератак. Proactive Risk Monitoring – займається збором інформації про кіберінциденти, здійснює моніторинг ризиків, шукає потенційні вразливі місця. Information services – займається безпосереднім інформуванням банків про кіберзагрози та заходи протидії кібератак. Training and education – цей сервіс проводить тренінги та навчальні сесії, метою є підвищення обізнаності та поінформованості у сфері

кіберзахисту, протидіють актуальним кіберзагрозам. Також центр активно протидіє фішингу. А саме: блокує шахрайські ресурси на рівні хостесів та надавачів хмарних послу; обмежує фішингові домени; проводить заходи з підвищення кібергігієни користувачів банківських послуг.

15 лютого 2022 року на українські банки, державні веб-ресурси та портал електронних послуг «Дія» було здійснено масштабну кібератаку, вона тривала майже добу. Серед усіх галузей критичної інфраструктури банківська система захищена найкраще. Причиною є відповідність банків міжнародним вимогам. Якщо банки щороку не проходитимуть незалежний аудит кібербезпеки, то їх просто відключать від Visa чи Mastercard, а для банку це означає закриття.

Слабким місцем банків є люди. Працівники, яких хакають через фішингові посилання чи дзвінки, або соцмережі. Цей метод дозволяє атакувати установу не на пряму, а змусити людей самостійно зробити щілину в системі. Тому банки регулярно проводять навчання для співробітників. Важливо зазначити, IT технології постійно вдосконалюються і саме нові технології несуть у собі найбільший ризик. Наприклад, хакер після виявлення недоліку в програмному забезпеченні починає розробку шкідливого коду, який використовує виявлену вразливість для зараження окремих комп'ютерів або мереж. Інформацію або доступ до мережі потім продають на чорному ринку. В результаті на основі даних створюються нові хакерські інструменти, які дають змогу проникнути в систему ще на етапі її розробки, як результат аудит проходить успішно і система вважається безпечною.

14 січня 2022 р. була здійснена атака на постачальників, які також є слабкою ланкою. «Supply chain attack» була здійснена на ланцюжок поставок. Таке відбувається коли система є надійно захищеною, проте постачальник залишається вразливим, наприклад компанія яка розробляє

веб-сайт для організації. Якщо злом відбудеться в компанії яка створила сайт і має доступ до нього хакери отримують доступ до системи.

Від початку у 2014 році війни в Україні було здійснено 2693 кібератаки на різні об'єкти критичної інфраструктури, більша частина інцидентів відбулася після повномасштабного вторгнення в 2024 році. Тоді Європейський парламент закликав посилити допомогу Україні у сфері кібербезпеки та повною мірою використовувати санкції ЄС проти кіберзлочинців [5].

Таким чином можна зробити висновки, що банківська система проявила стійкість у боротьбі з кіберзлочинцями. Вперше політика інформаційної безпеки була оприлюднена в 2017 році і до сьогодні це питання залишається актуальним. В умовах інформаційної війни системи захисту банківських і не банківських установ продовжують вдосконалюватись. Їх розвиток активно підтримує НБУ, ним створено Центр кіберзахисту, який займається моніторингом, аналізом, протидії і боротьбі із кіберінцидентами. Не зважаючи на вжиті заходи банківські і небанківські установи мають бути у стані підвищеної готовності, адже фінансовий сектор є пріоритетною ціллю під час війни.

Література

1. Національний банк України. Кіберзахист банківської системи України має посилитися. 2021. URL: https://bank.gov.ua/ua/news/all/kiberzahist-bankivskoyi-sistemi-ukrayini-maye-posilitisya-12738.

2. Volkova, Nelia; Volkova, Valeria; Khudolii, Yuliia. Estimating credit risks impact on economic security of a bank. *Akademia zarządzania*, 1.1:108.

3. «Кібербезпека». USAID/UKRAINE, 5 серп. 2022 р. URL: Кібербезпека | Ukraine | Fact Sheet | U.S. Agency for International Development (usaid.gov).

4 Артем Жидкевич. Як побудована кіберстійкість банківської системи України. 2024. URL: https://speka.media/yak-pobudovana-kiberstiikist-bankivskoyi-sistemi-ukrayini-p1w0gx.

5. Дар'я Нинько. Що стоїть за кібератакою на українські банки та ресурси. 2022. URL: https://www.dw.com/uk/shcho-stoit-za-cherhovoiu-kiberatakoiu-na-ukrainski-banky-ta-resursy/a-60817398.

УДК 336.748

Сохань Тетяна Дмитрівна,
Нагай Дар'я Русланівна, *студентки,*
Науковий керівник: Вовченко Оксана Сергіївна,
кандидат економічних наук, доцент
Національний університет «Полтавська політехніка імені Юрія Кондратюка» (Україна)

ІНФЛЯЦІЙНІ ОЧІКУВАННЯ НАСЕЛЕННЯ ТА ЇХ ВПЛИВ НА ФІНАНСОВУ БЕЗПЕКУ КРАЇНИ

Інфляційні очікування населення відіграють ключову роль у визначенні фінансової стабільності країни. Вони впливають на рішення економічних суб'єктів щодо збереження та інвестування коштів, а також на стратегії бізнесу та макроекономічну політику держави. Дослідження цього впливу дозволяє краще зрозуміти механізми функціонування економіки та розробляти ефективні заходи для забезпечення фінансової безпеки країни.

Інфляційні очікування – це морально-психологічний стан щодо очікування споживачами, виробниками, підприємцями можливих інфляційних течій, змін у економічному середовищі, які у перспективі матимуть на них позитивний чи негативний вплив і насамперед пов'язані з