

УДК 336.7

Андрющенко І.Є.¹, Лотарьова С.О.²

¹д-р економ.наук, проф. НУ «Запорізька політехніка»

²студ. гр. ФЕУ-110 НУ «Запорізька політехніка»

КІБЕРБЕЗПЕКА В БАНКІВСЬКІЙ СФЕРІ: ВИКЛИКИ ТА ЗАХОДИ ПРОТИДІЇ

Кібербезпека - це забезпечення безпеки електронних систем, мереж та інформації від зловживання, несанкціонованого доступу, крадіжки даних, вірусів та інших загроз віртуального простору. Деякі науковці стверджують, що кібербезпека - це стан захищеності інформаційного простору, який забезпечує захист від неправомірного зовнішнього і внутрішнього втручання і забезпечує формування та розвиток інформаційного простору в інтересах громадян, організацій і держави в цілому. Вона також охоплює стан інформаційної інфраструктури та процесів, при яких інформація використовується відповідно до призначення і не має негативного впливу на інформаційні та інші системи держави та інших країн при її використанні [1, с. 11].

Забезпечення кібербезпеки є одним з найважливіших завдань в банківській сфері, оскільки фінансові установи містять значну кількість конфіденційної інформації про клієнтів та їх фінансові операції. Атаки на банки стають все більш витонченими, після чого зловмисники постійно вдосконалюються свої методи злому і шахрайства. Порушення кібербезпеки може призвести до серйозних наслідків для банків та їх клієнтів, таких як втрата коштів, виток конфіденційної інформації, порушення репутації тощо. Тому банки

повинні постійно вирішувати питання кібербезпеки та оновлювати свої методи захисту для забезпечення безпеки своїх систем та клієнтів від теперішніх загроз. Щоб захистити себе від таких загроз, банки повинні дотримуватися високих стандартів кібербезпеки, які включають у себе захист від хакерських атак, вірусів та шкідливого програмного забезпечення. Банки також повинні забезпечувати безпеку своїх мереж та серверів і навчати співробітників про правила безпечного користування комп'ютерами та мережами. Для забезпечення безпеки вони можуть використовувати різні технології, такі як криптографічні протоколи, біометричну аутентифікацію та моніторинг мережі. Крім того, вони можуть співпрацювати зі спеціалізованими компаніями з кібербезпеки, щоб забезпечити найвищий рівень захисту своїх систем та даних.

Для забезпечення кібербезпеки в банківській сфері застосовуються комплексні заходи, що включають керування паролями, двофакторну автентифікацію, шифрування даних, моніторинг мережі та додатків, використання механізмів захисту від DDoS-атак, підвищення свідомості співробітників щодо кібербезпеки, розробку планів дій у випадку інцидентів тощо. Важливою складовою кібербезпеки є також встановлення та дотримання правил користування інформаційно-комунікаційними системами та навчання користувачів безпечному використанню комп'ютерів і мережі. Технології машинного навчання також можуть бути використані для виявлення та запобігання кібератакам [2].

В реаліях, коли Україна захищає свою національну безпеку та цілісність від агресії з боку РФ, кіберпростір – це стратегічно важливий фронт. Наша країна щоденно продовжує бути мішенню хакерських атак, спрямованих на державні установи критичної інфраструктури, приватний бізнес та на українських громадян. За даними Державної служби спеціального зв'язку та захисту інформації України, від початку повномасштабної війни, Росія здійснила 796 кібератак проти України, що втричі більше у порівнянні з аналогічним періодом минулого року. В цілому, за даними звіту від Microsoft, у 2021 році майже 20% усіх кібератак у світі були спрямовані проти України, що, після США, посідає друге місце в цьому «анти-рейтингу».

Не дивлячись на складну ситуацію і численні виклики кібербезпеки, Україна посіла 24 місце із 160 в рейтингу Національного індексу кібербезпеки, який щорічно складає Фонд електронного урядування Естонії. У цьому списку Україна випередила частину європейських країн, зокрема: Австрію, Ірландію та Норвегію. Можемо впевнено трактувати отримані результати як досить оптимістичні, але не варто забувати, що кіберзахист нашої держави все ще має слабкі місця у протистоянні потенційним загрозам [3].

Основні загрози кібербезпеки для України включають: гібридну агресію РФ, яка може дестабілізувати інформаційні системи, спричинити хаос у роботі державних установ, фінансових та ділових центрів; кібератаки з боку

інших країн, які мають за мету викрасти конфіденційну інформацію; кіберзлочинність, яка завдає шкоди інформаційним ресурсам та громадянам; високу технологічну залежність від іноземних виробників ІТ-продукції, включаючи з РФ та РБ; вразливість ІТ-інфраструктури компаній та відсутність належного контролю з боку державних органів; недосконалість нормативно-правової бази та повільна імплементація релевантних нормативних актів ЄС [3].

Банківська сфера є однією з найбільш привабливих цілей для кіберзлочинців, оскільки банки містять велику кількість цінної інформації та грошових коштів. Деякі з основних викликів кібербезпеки в банківській сфері включають: фішинг та соціальний інжиніринг, які можуть використовувати кіберзлочинці, щоб виманити логін та пароль до банківського облікового запису від користувача; кібератаки на мережу банку такі як DDoS-атаки, щоб перенавантажити мережу банку та зробити її недоступною для користувачів; злам банківської програми для отримання конфіденційної інформації про клієнтів; кібершахрайство, яке використовується щоб отримати доступ до рахунків користувачів та здійснювати незаконні перекази грошей; внутрішні загрози; кібершпигунство, тобто коли інші держави використовують кібератаки для збирання конфіденційної інформації про банківську систему та клієнтів банку [3].

Для забезпечення кібербезпеки в банківській сфері застосовуються різноманітні заходи технічного, організаційного та правового характеру. Основні з них такі: розробка та впровадження комплексної системи кіберзахисту, що включає в себе застосування антивірусного програмного забезпечення, фаєрволів, інструментів для виявлення вторгнень та інші технічні рішення; вдосконалення системи автентифікації та авторизації користувачів, що означає впровадження двофакторної аутентифікації, біометричних технологій та інших методів для забезпечення захисту від несанкціонованого доступу до банківських систем; підвищення кваліфікації персоналу; моніторинг та аналіз відхилень в роботі системи; захист інформації та даних; розробка та впровадження політики кібербезпеки [4].

Отже, все вищесказане підкреслює важливість забезпечення кібербезпеки в інформаційному просторі, який є стратегічно важливим фронтом в боротьбі з кіберзагрозами. В особливості відзначено, що банки є особливо уразливими до кібератак через конфіденційну інформацію, яку вони містять про своїх клієнтів та їх фінансові операції. Порушення кібербезпеки може мати серйозні наслідки для банків та їх клієнтів, такі як виток конфіденційної інформації, втрата коштів та порушення репутації. Приділення належної уваги кібербезпеці та використання сучасних технологій захисту можуть зменшити ризики від кібератак і забезпечити стійкий захист інформації.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Лісовська Ю.П. Кібербезпека: ризики та заходи: навч. посібник. — К.: Видавничий дім «Кондор», 2019. — 272 с. URL: <http://dcmaup.com.ua/assets/files/kiberbezpeka.pdf>
2. Інтернет-портал «Спека»: Кібербезпека: як українському бізнесу захиститися від атак російських хакерів під час війни: поради ІТ-фахівців, 2022. URL: <https://speka.media/>
3. Інтернет-ресурс «PwC Україна»: Публікації: Кібербезпека бізнесу в умовах нестабільності, 2022. URL: <https://www.pwc.com/ua/uk>
4. Інтернет-портал «Financial Club»: Пряма мова: Як банкам встояти у випадку кібератаки, 2019. URL: <https://finclub.net/ua/>