УДК 336.71:355.2.001.57.058.4

Худолій Юлія Сергіївна,
кандидат економічних наук, доцент
Андрієць Тетяна Романівна,
студентка,
Національний університет «Полтавська політехніка імені Юрія Кондратюка» (Україна)

ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ БАНКІВСЬКОЇ СИСТЕМИ УКРАЇНИ У ПЕРІОД ВОЄННОГО СТАНУ

З початком повномасштабного російського вторгнення чисельність кібератак з метою зупинення роботи системно важливих об'єктів різко зросла. Найбільше втрат зазнають державні установи, банки, фінансові організації та ІТ-компанії. Забезпечення кібербезпеки банків України є важливим напрямом захисту банківської системи від зовнішніх загроз, що можуть призвести до непередбачуваних наслідків.

Сутність кібербезпеки визначено у Законі України «Про основні засади забезпечення кібербезпеки України» [1]. Відповідно до закону кібербезпека являє собою 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.

У період воєнного стану банківські установи не зацікавленні в розкритті інформації про кібератаки, адже це може призвести до погіршення репутації. Ліквідність банку у разі розкриття такої інформації може погіршитись, оскільки спричинить відток клієнтів. Також одним з чинників приховування інформації про здійснені кібератаки є те, що ця інформація приверне увагу інших кіберзлочинців, які за

допомогою необхідних інструментів, зможуть пройти через встановлені патчі та знову здійснити успішну кібератаку на інфраструктуру банку.

Національний банк України створив окремий інструмент для збору інформації про інциденти інформаційної безпеки – MISP-NBU Центру кіберзахисту. Це спеціалізований сайт Національного банку України, створений на базі платформи з відкритим програмним кодом MISP, призначений для організації доступу банків до системи збору, обробки, зберігання і обміну інформацією загально-організаційного та технічного характеру в режимі реального часу з урахуванням вимог конфіденційності. Таким чином, регулятор та банківські установи проінформовані про всі інциденти інформаційної безпеки [2].

Також Національним банком було розроблено вимоги щодо функціонування системи кіберзахисту в банківській системі. З метою унормування питання організації та забезпечення кіберзахисту НБУ визначив основні засади функціонування системи кіберзахисту, принципи забезпечення інформаційного обміну між Центром кіберзахисту Національного банку і банками України, вимоги щодо заходів із забезпечення кіберзахисту об'єктів критичної інформаційної інфраструктури та вимоги щодо проведення незалежного аудиту інформаційної безпеки банків.

Основними напрямами НБУ щодо протидії спробам рф зашкодити кіберпростору є такі:

– адаптація нормативної бази під реалії воєнного часу (ухвалення постанови №42 «Про використання банками хмарних послуг в умовах воєнного стану в Україні»);

– тісна співпраця з правоохоронними органами, службами безпеки банків та міжнародними партнерами (зокрема плідна робота із РНБО та Кіберполіцією);

– впровадження більш гнучких політик безпеки (керування ключами, віддалений доступ і використання

хмарних систем).

Починаючи з квітня 2022 року основними напрямками кібернападів рф стали: фішингові атаки різних типів; DDOS-атаки різного характеру.

На початку 2023 року Національний координаційний центр кібербезпеки при РНБО спільно з НБУ запустили проєкт із протидії кібершахрайству у фінансовому секторі. Метою цього проекту є посилення захисту громадян України від кіберзлочинців, що активізувалися у період воєнного стану. Основним напрямком зловмисників стали фішингові кампанії, за допомогою яких вони можуть виманювати дані для доступу до банківських рахунків. Фішинг це один із відомих методів кібершахрайства, що використовують зловмисники з метою привласнення коштів та збору персональних даних. Завданням проекту є зменшення переходу користувачів на шахрайські сайти шляхом перенаправлення їх на сторінку з попередженням, що сайт створений шахраями [3].

Distributed Denial of Service (DDoS) атака є однією з найпоширеніших проблем українських банків. У період 15-16 лютого 2022 року було здійснено наймасштабнішу в історії України DDoS-атаку на урядові сайти, банківський сектор. У жовтні 2022 року хакери провели масштабну DDoS-атаку на український банк Monobank, що призвело до тривалих перебоїв у роботі. Через такі атаки банки можуть втратити доступ до критично важливих систем, клієнти не зможуть знімати кошти, здійснювати перекази тощо, а хакери у цей час зможуть отримати доступ до конфіденційної інформації. Запобігти цьому можливо за допомогою різних інструментів захисту. Так, наприклад, банки можуть скористуватися AntiDDos створений Київстар. Це багаторівневий сервіс захисту IT-інфраструктури банку від відомих і невідомих атак. AntiDDos побудований на базі рішення FortiDDoS від Fortinet і має дійсний сертифікат відповідності, зареєстрований адміністрацією Держспецзв'язку України [4].

Отже, пріоритетним напрямком Національного банку є забезпечення кібербезпеки банківських установ у період воєнного стану. Українські банки повинні бути готовими до можливості загроз їх діяльності та виконувати розпорядження регулятора. Законодавча база щодо регулювання банківської діяльності у інформаційному просторі постійно адаптується під сучасні реалії. Банківські установи повинні створювати умови щодо захисту своїх даних та встановлювати сучасні інструменти захисту, що вбережуть їх від можливих атак.

Література:

1. Онищенко С.В., Глушко А.Д. Аналітичний вимір кібербезпеки України в умовах зростання викликів та загроз. *Економіка і регіон*. 2022. № 1 (84). С. 13–20. DOI: https://doi.org/10.26906/EiR.2022.1(84).2540.

2. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII : станом на 17 серп. 2022 р. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

2. Кльоба Л., Кльоба Т. Кіберзагрози банківського сектора в умовах воєнного стану в Україні. Financial and credit activity problems of theory and practice. 2022. Т. 5, № 46. С. 19–28. URL: https://doi.org/10.55643/fcaptp.5.46.2022.3883.

3. 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.

4. Київстар. Кібербезпека у банківській сфері під час війни / Kyivstar Business Hub. Kyivstar Business Hub. URL: https://hub.kyivstar.ua/news/instrumenty-dlya-borotby-z-shahrajstvom-u-bankivskomu-sektori/#4.