Міністерство освіти і науки України
Навчально-науковий інститут фінансів, економіки, управління та права Національного університету «Полтавська політехніка імені Юрія Кондратюка» (Україна)
Варненський вільний університет Чорноризця Храбра (Болгарія)
Гентський університет (Бельгія)
Сучавський університет ім. Штефана чел Маре (Румунія)
Міжнародний науково-освітній та навчальний центр (Естонія)
Київський національний університет імені Тараса Шевченка (Україна)
Харківський національний університет імені В. Н. Каразіна (Україна)
Київський національний університет будівництва і архітектури (Україна)
Сумський державний університет (Україна)
Сумський національний аграрний університет (Україна)
Національний університет «Запорізька політехніка» (Україна)
Державна установа
«Інститут економіки та прогнозування НАН України» (Україна)
Державна установа
«Інститут демографії та проблем якості життя НАН України» (Україна)
Державна податкова інспекція у м. Полтава Головного управління Державної податкової служби у Полтавській області (Україна)
Полтавське територіальне відділення Всеукраїнської професійної громадської організації «Спілка аудиторів України» (Україна)
Торгово-промислова палата України (Україна)

ЗБІРНИК
ІІ Міжнародної науково-практичної Інтернет-конференції «СТАЛИЙ РОЗВИТОК: ВИКЛИКИ ТА ЗАГРОЗИ В УМОВАХ СУЧАСНИХ РЕАЛІЙ»

With the support of the Erasmus+ Programme of the European Union

06 червня 2024 року

ПОЛТАВА

незалежного аудитора 50% було позитивних і 50% із думкою із застереженням. Але всі причини модифікації не стосувалися дотримання принципу безперервності діяльності.

Список використаних джерел

1. Onyshchenko S. V., Masliy O. A., Buriak A. A. Threats and Risks of Ecological and Economic Security of Ukraine in the Conditions of War. 17th International Conference Monitoring of Geological Processes and Ecological Condition of the Environment, Nov 2023, Volume 2023, p.1 – 5. DOI: https://doi.org/10.3997/2214-4609.20235200721.

2. Філонич О.М., Карпенко Є.А., Крекотень І.М. Загрози економічної безпеки малих аудиторських фірм в умовах воєнного стану. *Економічна безпека: держава, регіон, підприємство: Матеріали Міжнародної науково-практичної Інтернет-конференції, 29 вересня 2022 р. Полтава: НУПП, 2022. 215 с.* С. 132-136.

УДК 338.23:004.056.5

Худолій Ю. С., к.е.н., доцент; Костиря Б. Р., Пилипенко Д. С., студенти
Національний університет «Полтавська політехніка імені Юрія Кондратюка» (Україна)

ПРОБЛЕМИ І ПЕРСПЕКТИВИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В УМОВАХ ВОЄННОГО СТАНУ

Сучасна Україна стикається з тяжкими проблемами в забезпеченні захисту своєї економічної системи та її суб'єктів під час повномасштабного вторгнення російської федерації. Як молода держава, Україна має нестачу стресостійкості у своїй економічній системі, порівняно з країнами-союзниками.

Одним з основних аспектів цієї проблеми є недостатній розвиток системи кіберзахисту, що ставить під загрозу функціонування та безпеку фінансових інститутів, інфраструктури та промислових об'єктів.

В епоху конфліктів економічна система країни відіграє ключову роль у підтримці бойової готовності її армії. Наші противники розуміють це і намагаються дестабілізувати її.

Один із яскравих прикладів таких спроб – масштабна DDoS-атака на Monobank. Але під загрозою не тільки великі банки, а й звичайні громадяни.

Протягом останніх двох років спостерігається значне поширення різноманітних махінаційних схем, які базуються на банківській системі і ґрунтуються на фішингу. Ось декілька прикладів: створення фейкових сайтів з підробленим доменом, які видають себе за реальні банківські установи, розсилка фейкових листів та гіперпосилань. Кожен з цих методів стає все більшою загрозою з кожним днем.

Фішингові атаки через фейкові сайти та електронні листи, що виглядають як листи від реальних банків, чинять шкоду не лише окремим особам, але й довірі до банківської системи в цілому. Втрата довіри призводить до репутаційних проблем для банків, що ускладнює їх повноцінну діяльність та має негативний вплив на економічну систему загалом.

Для початку розберемо цю проблему на окремі складові, досліджуючи їх комплексно.

Перше, з чого ми почнемо, це фішингові сайти та розсилки. Головна проблема полягає в тому, що у нас недостатньо впроваджено системи захисту, і населення країни недостатньо проінформоване про те, як ці системи працюють. Перші дії, які слід виконати – це інформування банками своїх користувачів через мобільні додатки та в їхніх установах. Прикладом такого додатка може служити Privat24.

Другим етапом формування системи захисту має бути забезпечення безпеки електронної пошти. Це може допомогти не тільки окремим людям, а й великим компаніям, яким приходять десятки тисяч листів в день, оскільки такі листи можуть містити як і спам, так і різні хакерські програми.

Для того, щоб запобігти цій проблемі варто використовувати сучасні протоколи

захисту, такі як DMARC. Його функціонал полягає в тому, що він надає декілька рівнів захисту, що допомагає запобігти фішингу та спуфінгу.

Основні види захисту, які DMARC може забезпечити:

1) автентифікація: DMARC використовує два протоколи автентифікації – SPF (Sender Policy Framework) та DKIM (DomainKeys Identified Mail), для перевірки, що електронний лист дійсно надіслано з домену, який він вказує. Це не дозволяє зловмисникам використовувати ваш домен та ім'я, що заважає їхнім махінаціям;

2) політики DMARC:

a. p=none: це режим моніторингу, який дозволяє відправникам отримувати звіти про перевірки, але не впливає на доставлення повідомлень;

b. p=quarantine: листи, які не проходять перевірку DMARC, можуть бути поміщені на карантин (наприклад, у теку спаму);

c. p=reject: найсуворіший рівень, який відхиляє листи, що не пройшли перевірку DMARC, запобігаючи їх доставленню;

3) звітність: DMARC також формує звіти, які надають відправникам інформацію про те, як їх електронна пошта обробляється отримувачами, і допомагають виявити потенційні проблеми. Ці механізми захисту допомагають організаціям захистити свої домени від зловживань, а своїх користувачів від шахрайських листів.

Всі наведені вище приклади будуть ефективні на рівні державних установ та окремих суб'єктів економіки, але для захисту всієї інформаційної системи в цілому потрібна велика та детально відпрацьована програма.

Прикладом для нас може слугувати програма інформаційного захисту США «Ейнштейн». Програма «Ейнштейн» – це система виявлення вторгнень, яка захищає мережеві шлюзи вищих державних органів та установ США від несанкціонованого трафіку. Програмне забезпечення було розроблено комп'ютерною командою екстреної готовності США (US-CERT), яка є оперативним підрозділом Національного управління кібербезпеки міністерства внутрішньої безпеки США.

Метою програми є сприяння виявленню та усуненню кіберзагроз і кібератак, підвищенню безпеки мережі та відмовостійкості критично важливих державних послуг.

Основні принципи її роботи:

1) збір даних: програма збирає інформацію про мережевий трафік, включаючи унікальні номери автономних систем (ASN), типи та коди ICMP, довжини мережевих пакетів, протоколи передачі даних, IP-адреси джерела і призначення, порти джерела і призначення, а також інформацію про прапори TCP;

2) аналіз трафіку: програма аналізує зібрані дані, порівнюючи їх з базовою лінією для виявлення аномалій або підозрілого трафіку, який може вказувати на кібератаки;

3) реагування на інциденти: у разі виявлення потенційної кібератаки, програма сповіщає відповідні служби, такі як US-CERT, для подальшого розслідування та реагування.

4) підтримка 24/7: служба моніторингу US-CERT працює цілодобово, щоб оцінювати дані вхідного трафіку та допомагати у вирішенні інцидентів.

Отже, забезпечення кібербезпеки є найважливішим аспектом для України в умовах вторгнення росії та збереження економічної стійкості. Підвищення освіченості громадян та впровадження сучасних технологій захисту, таких як DMARC, є першочерговими завданнями. Додатково, необхідно впровадити комплексну програму захисту, рикладом якої може бути програма «Ейнштейн» у США, для ефективного виявлення та усунення кіберзагроз.

Вважаємо, що успішна реалізація цих заходів допоможе зміцнити економічну систему та забезпечити безпеку фінансових інститутів та промислових об'єктів.

Список використаних джерел

1. Ейнштейн (програма) – Вікіпедія. *Вікіпедія*. URL: https://uk.wikipedia.org/wiki/Ейнштейн_(програма) (дата звернення: 06.05.2024).

2. dmarc.org – Domain Message Authentication Reporting & Conformance. *dmarc.org – Domain Message Authentication Reporting & Conformance*. URL: https://dmarc.org (дата звернення: 06.05.2024).

3. Худолій Ю. С. Застосування технології big data у банківському бізнесі. Актуальні проблеми розвитку фінансів в умовах цифровізації економіки України: І всеукраїнська науково-практ. конф., присвяч. 55-річчю каф. фінансів і банк. справи, м. Вінниця, 27 квіт. 2023 р. 2023. С. 144–147. URL: https://cutt.ly/DwHh0F45 (дата звернення: 04.04.2024).

4. 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

5. Onyshchenko, S., Yanko, A., Hlushko, A., Maslii, O., Skryl, V. (2023). The Mechanism of Information Security of the National Economy in Cyberspace. Proceedings of the 4th International Conference on Building Innovations, 791–803. doi: https://doi.org/ 10.1007/978-3-031-17385-1_67

УДК 336

Оленич В.П., студентка
Національний університет "Полтавська Політехніка ім. Юрія Кондратюка"
(м. Полтава, Україна)

СТАБІЛІЗАЦІЯ ФІНАНСОВОЇ СИСТЕМИ ЯК УМОВА ЄВРОІНТЕГРАЦІЇ УКРАЇНИ

Фінансова система України зазнала численних економічних та політичних криз. Однією з головних причин нової та найбільш серйозної кризи стало військова агресія рф проти України, що розпочалася наприкінці лютого 2022 року. В цьому контексті актуальним є дослідження стану фінансової системи України під час збройного конфлікту та процесів її євроінтеграції, на які був активно налаштований уряд України у довоєнні часи [1].

Внаслідок війни Україна зазнала значного економічного тиску. Фінансові ресурси довелося мобілізувати на потреби обороноздатності, що призвело до припинення функціонування багатьох підприємств і загрози руйнування критичних об'єктів інфраструктури. Тисячі людей втратили роботу та житло, а мільйони змушені були шукати притулок у безпечних місцях. Уряд відчув необхідність в радикальних економічних реформах для збереження економічної стабільності та забезпечення обороноздатності країни [1].

Але, попри численні виклики, фінансова система досить швидко адаптувалась до умов військового стану і навіть не полишила завдань євроінтеграційних процесів та робить певні успіхи.

Перш за все, для забезпечення успішного функціонування економіки України та наближення її до рівня країн ЄС, необхідна модернізація фінансової системи. У період економічних трансформацій та військового стану це стає складним завданням, що вимагає розробки нових фінансових інструментів і технологій, удосконалення нормативно-правової бази та розвиток фінансових інститутів, адже функціонування економіки без модернізації фінансової системи є неможливим [2].

Також, на мою думку, в умовах євроінтеграційних процесів було б доцільно використати досвід країн ЄС для модернізації української фінансової системи, звичайно, врахувавши наші обставини.

Оскільки українська фінансова система має банкоцентричну модель функціонування, нестабільні явища в економіці сильно відображаються на ній.

На сьогоднішній день банківський сектор стикається з численними проблемами, такими як стрімке зростання проблемних активів на балансах банків, значний відтік депозитних ресурсів, введення жорстких адміністративних заходів у зв'язку з військовим конфліктом та економічною кризою, висока доларизація кредитів та депозитів, а також незбалансована база активів та пасивів банків. Для вирішення економічних проблем країни