Міністерство освіти і науки України

Національна академія наук України

Національний університет «Полтавська політехніка імені Юрія Кондратюка»

«Академічна й університетська наука: результати та перспективи»,

присвячена 90-річчю Національного університету «Полтавська політехніка імені Юрія Кондратюка» та пам'яті президента Національної академії наук України, академіка НАН України Бориса Євгеновича Патона

Збірник наукових праць
за матеріалами

XIII Міжнародної науково-практичної конференції

10 - 11 грудня 2020 року

Полтава 2020

УДК 339.7:[343.9.024:004.77]:616-036.21

***Онищенко В.О.**, д.е.н., професор, **Сівіцька С.П.**, к.е.н.,, доцент*
***Черв'як А.В.**, аспірант кафедри фінансів, банківського бізнесу та оподаткування*
Національний університет «Полтавська політехніка імені Юрія Кондратюка»

СТАН ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНИХ КАНАЛІВ СВІТОВОЇ ЕКОНОМІКИ У ПЕРІОД ПАНДЕМІЇ COVID-19

***Анотація.** З початку 2020 року світова економіка перебуває у шоковому стані через епідемію COVID-19. Пандемія призвела до значних людських втрат, має негативний вплив на соціально-культурне життя населення, економічну стабільність та розвиток кожної країни. У зв'язку з невизначеністю тривалості вірусу COVID-19 та пов'язаних з ним обмежень, неможливо прогнозувати подальший стан чи розвиток економічного та соціального становища в країні.*

Пандемія змусила світ переосмислити своє буття та визначити пріоритети у своїй діяльності. Суб'єкти фінансового ринку були змушені швидко адаптуватись до нових викликів і вимог, щоб рентабельно продовжувати свою діяльність. Але з освоєнням нового он-лайн способу роботи, до нових викликів пристосувалися і кіберзлочинні угрупування та хакери. Щоб отримати інформацію, як протидіяти несанкціонованим доступам до конфіденційної інформації, необхідно проаналізувати види та динаміку здійснення атак на інформаційні канали фінансових установ. Це дасть змогу сформувати реальне бачення загроз у кіберпросторі та розробити дієвий стратегічний план дій.

***Ключові слова**. Вірус, інформаційні канали, кіберзлочинність, фінансова установа, хакерська атака, несанкціонований доступ.*

Глобальне та жваве обговорення проблеми поширення коронавірусної інфекції відбувається у засобах масової інформації та соціальних мережах. Свої думки та статистичні дані оприлюднюють Міністерства та Всесвітні організації з охороним здоров'я, лідери держав, представники штабів з контролю поширення коронавірусної інфекції та статистичні відомства, провідні економісти, політологи та інші фахівці.

Через невизначеність тривалості пандемії та нові спалахи вірусної інфекції в різних куточках світу, неможливо точно стверджувати у якому стані буде світова економіка по завершенні пандемії. Проте можливо і варто робити прогнозні дослідження.

Так, прогноз рівня ВВП за інформацією Служби економічних досліджень США[1], що наведено у таблиці 1. Наведені прогнозні дані відповідають прогнозом Світового банку та консенсус прогнозом і знаходиться на рівні 3%. Це є доволі оптимістичним прогнозом у зв'язку з тим, що знову ж таки неможливо визначити тривалість пандемії.

Таблиця 1

Аналіз прогнозних темпів зростання ВВП економік світу

Країни	2016	2017	2018-2020	2021-2025	2026-2030
Розвинена економіка					
США	1,5 %	2,3 %	2,2 %	2,1 %	2,1 %
Південна Корея	2,9 %	3,1 %	2,7 %	2,0 %	2,0 %
Велика Британія	1,9 %	1,8 %	1,6 %	1,7 %	1,8 %
Німеччина	1,9 %	2,2 %	1,6 %	1,1 %	1,0 %
Японія	0,9 %	1,7 %	1,1 %	0,8 %	0,9 %
Економіка, що розвивається					
Індія	7,1 %	6,6 %	7,8 %	7,6 %	6,8 %
Китай	6,7 %	6,9 %	6,1 %	5,4 %	5,0 %
Індонезія	5,0 %	5,1 %	5,2 %	5,0 %	5,0 %
Україна	2,3 %	2,5 %	2,7 %	3,4 %	3,4 %

Варто розглянути вплив пандемії на деякі галузі економіки, відповідно до інформаційно-аналітичних даних «Програма стимулювання економіки для подолання наслідків COVID-19: «Економічне відновлення» (рис.1).

Рисунок 1. Вплив на різні сектори економіки запроваджених заходів із протидії поширенню пандемії

**складено за даними [2]*

З точки зору важливості для економіки, промисловість, оптова та роздрібна торгівля, а також сільське господарство генерують найбільше доданої вартості та створюють найбільше робочих місць.

Роздрібна торгівля непродовольчими товарами, готельно-ресторанний бізнес, сфера обслуговування та розваг, промисловість найбільше страждають від обмежень введених у відповідь на поширення вірусу, оскільки передбачають безпосередній контакт з клієнтами. Попри те, що частка готельно-ресторанного бізнесу в економіці є відносно незначною, в цьому секторі сконцентрована велика частка малих підприємств, які потребують підтримки.

Введені карантинні обмеження в усьому світі мають прямий вплив на дохідність всіх галузей економіки та її рівень зростання. Проте, важливим фактором варто виділити і зростання кіберзлочинів у інформаційному середовищі.

Інформація про нові види загроз безпеці та економічній стабільності має оновлюватися постійно. У боротьбі з кіберзлочинністю особливо важливо володіти актуальною і своєчасною інформацією. Під час пандемії COVID-19 кількість кібератак збільшилась, що пояснюється збільшенням проведення операцій у режимі он-лайн.

Передовою міжнародною компанією із протидії і розслідування кіберзлочинів та шахрайства з використанням високих технологій Group-IB [3] було сформовано Hi-Tech Crime Trends 2020/2021, де зазначались відповідні аналітичні висновки, щодо стану захищеності кіберпростору у банківському секторі (Таблиця 2).

Кіберзлочини у 2020 році перш за все базувалися на потребі людини отримати інформацію про вірус, статистичні дані захворюваності і таке інше.

У період першого півріччя 2020 року смарт-канал Trend Micro Smart Protection Network (SPN) виявив близько 9 млн загроз, пов'язаних з COVID-19. Ці загрози являли собою повідомлення на електронну адресу, які містили в собі посилання і шкідливі файли. Які прямо чи опосередковано мали відношення до пандемії. Це могли бути інформаційні додатки або сповіщення щодо затримки термінів доставки через вірус.

Таблиця 2

Стан та прогноз захищеності інформаційного простору банківської системи

Кібератаки у банківському секторі	Прогноз кіберзлочинності на ринку банківських послуг
1. Жодного публічного повідомлення щодо несанкціонованого доступу через SWIFT, ATM Switch, платіжні канали чи ATM, коли доступ до них було отримано через банківські мережі, не було зафіксовано у 2020 році.	1. Великої кількості цільових атак на банки не передбачається. Поодинокі випадки можливі але без широкого розповсюдження.
2. Група Lazarus продовжувала здійснювати хакерські атаки через SWIFT, і для першочергового проникнення вони використовували банківську бот-систему Trickbot. Були зафіксовані дії ще однієї команди, яка використовувала загальнодоступні троянські вірус без будь-яких модифікацій. Такий набір інструментів характерний лише для атак на банки з мінімальним рівнем безпеки.	2. Як і в інших галузях значну загрозу будуть нести групи, які займаються шифруванням даних, підтвердженням чого є зростання випадків продажу доступів до корпоративних каналів фінансових установ.
3. Група Silence провела успішне викрадення даних, не пов'язаних із SWIFT, у другій половині 2019 року. Але у 2020 року вони перестали здійснювати атаки.	3. Вагомою проблемою може стати викрадення інформацій про фінансові транзакції VIP-клієнтів і розміщення цих даних у відкритому доступі. Це завдасть значних фінансових збитків і змусить банки здійснювати виплати хакерам.
4. Філіппінський банк United Coconut Planters Bank (UCPB) було пограбовано у вересня 2020 року. Хакерам удалось отримати доступ до карткового процесу обслуговування і змінити ліміти, а також доступ до системи міжбанківських переводів InstaPay. У результаті вони змогли вивести з банку 3,44 млн.доларів.	4. Іншим способом вимагання коштів у фінансових установ може стати оповіщення фінансових регуляторів про наявні проблеми з безпекою та фінансовою нестабільністю відповідних установ. Це буде вести за собою більші витрати для нерозголошення подібної інформації.
5. Інструменти ціле направлених атак на банкомати слабо розвинулись. За звітний період було виявлено ATMDtrack від Lazarus і нова модифікація ATM-трояна від групи Silence, але про їх вдалі спроби викрадення інформації даних немає.	

Лідером по кількості загроз такого характеру стали США – 38% випадків із усіх виявлених кібератак, Германія – 14,6% та Франція – 9,2%. Найбільша частка випадків була ідентифікована у квітні місяці, саме під час першого спалаху захворюваності у світі [2].

Аналіз загроз у 2020 році показав, настільки швидко кіберзлочинці адаптуються під актуальні інформаційні та телекомунікаційні зміни.

Відповідно до даних Державної служби спеціального зв'язку та захисту інформації України [4] з 25 листопада по 1 грудня система кіберзахисту державних інформаційних ресурсів та об'єктів критичної інфраструктури на об'єктах моніторингу зафіксувала близько 1,4 млн підозрілих подій.

Зазначається, що урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA [5]. у цей період зареєструвала та опрацювала 1 878 кіберінцидентів, що приблизно на рівні попереднього тижня.

Експерти вважають, що поведінка людей та структура попиту після завершення пандемії зміниться, але не суттєво. Разом з тим більшість експертів вважає, що процеси діджиталізації (цифровізації), оновлення програмного забезпечення та удосконалення системи захисту інформаційних каналів прискоряться. Криза відкриє «вікно можливостей» для зміни української економіки у напрямі переходу до нової якості [1].

Висновок. Пандемія змінила не лише стиль нашого життя, але й мислення кожного.

Оцінивши нові реалії та виклики, компанії почали розробляти новий підхід до своєї діяльності та безпеки.

Складні часи вимагають застосування надійних технологій забезпечення безпеки. Однорівневої системи захисту недостатньо. Лише комплексний підхід та багаторівневий захист зможе забезпечити відповідний рівень захищеності інформаційних каналів, надаючи широкий спектр показників та статистичних даних для аналізу.

Література

1. Періодичне видання Міністерства розвитку економіки, торгівлі та сільського господарства України, «Консенсус-прогноз «Україна у 2020-2021 роках: наслідки пандемії» – 2020 рік, Київ, №51, с. – 31.

2. Кабінет Міністрів України, «Програма стимулювання економіки для подолання наслідків COVID-19: «Економічне відновлення», С - 88, Електронний ресурс – Режим доступу: https://www.kmu.gov.ua/storage/app/sites/1/18%20-%20Department/18%20-%20PDF/07.2020/programa.pdf

3. Group-IB, Hi-Tech Crime Trends 2020/2021, Електронний ресурс – Режим доступу: https://www.group-ib.ru/blog/trends20_21?fbclid=IwAR3jJ7kQD4J93SJC 13zx3D2sltaC4IdzrTQ3HiUIBQYnnvsXFjIkT_8x3U

4. Державна служба спеціального зв'язку та захисту інформації України, Електронний ресурс – Режим доступу: https://cip.gov.ua/ua

5. Урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA, Електронний ресурс – Режим доступу: https://www.unn.com.ua/uk/news/1905638-za-tizhden-na-derzhavni-informatsiyni-resursi-namagalis-zdiysniti-blizko-1-4-mln-kiberatak