potential limitations. *medRxiv*. 2023. URL : https://doi.org/10.1101/2023.02.19.23286155.

15. Grawitch M. Just how accurate is ChatGPT? *Psychology Today*. URL : https://www.psychologytoday.com/intl/blog/a-hovercraft-full-of-eels/202302/just-how-accurate-is-chatgpt.

16. Garg M., Goel A. A systematic literature review on online assessment security: Current challenges and integrity strategies. *Computers & Security*. 2022. Vol. 113. 102544. URL : https://doi.org/10.1016/j.cose.2021.102544.

17. Susnjak T. ChatGPT: The end of online exam integrity? *Cornell University*. 2022. URL : https://doi.org/10.48550/arXiv.2212.09292.

18. Kung T. H. et al. Performance of ChatGPT on USMLE: Potential for AI-assisted medical education using large language models. *medRxiv*. 2022. URL : https://doi.org/10.1101/2022.12.19.22283643.

19. Choi J. H., Hickman K. E., Monahan A., Schwarcz D. B. ChatGPT Goes to Law School. *SSRN*. 2023. URL : https://doi.org/10.2139/ssrn.4335905.

20. Fijačko N., Gosak L., Štiglic G., Picard C. T., John Douma M. Can ChatGPT Pass the Life Support Exams without Entering the American Heart Association Course? *Resuscitation*. 2023. 109732. URL : https://pubmed.ncbi.nlm.nih.gov/36775020/.

21. Azaria A. ChatGPT usage and limitations. *HAL Open Science*. 2022. URL : https://doi.org/10.13140/RG.2.2.26616.11526.

22. Gašević D., Siemens G., Sadiq S. Empowering learners for the age of artificial intelligence. *Computers and Education: Artificial Intelligence*. 2023. Vol. 4. 100130. URL : https://doi.org/10.1016/j.caeai.2023.100130.

23. Tlili A., Shehata B., Adarkwah M. A., Bozkurt A., Hickey D. T., Huang R., Agyemang B. What if the devil is my guardian angel: ChatGPT as a case study of using chatbots in education. *Smart Learning Environments*. 2023. No. 10(1). Art. num. : 15. URL : https://doi.org/10.1186/s40561-023-00237-x.

24. Is it safe to use ChatGPT in academic essay writing? *Plagexpert*. URL : https://www.plagexpert.com/is-it-safe-to-use-chatgpt-in-academic-essay-writing/.

Людмила РИБАЛЬЧЕНКО
завідувач кафедри інформаційних технологій
Дніпропетровського державного університету внутрішніх справ,
кандидат економічних наук, доцент
І. МАТВЄЄВА
студентка Дніпропетровського державного університету внутрішніх справ

ЯК НЕ ПОТРАПИТИ НА ГАЧОК ШАХРАЇВ

Нині важко уявити своє життя без електронних пристроїв, соціальних мереж, тому з кожним днем все більше і більше людей потрапляють на гачок до аферистів і шахраїв. Шахраї стають розумнішими та користуються новими

технологіями, продуктами чи послугами, щоб створювати правдоподібні історії, котрі переконають вас віддати їм свої гроші чи передати особисті дані.

Шахрайство спрямоване на людей різного походження, віку та рівня доходу. Немає жодної групи людей, котра з більшою ймовірністю може стати жертвою шахраїв – усі ми можемо бути вразливими до них. Шахрайство має успіх і застає вас зненацька, коли ви цього не очікуєте.

Для того, щоб не потрапити на гачок шахраїв, потрібно:

1. Не розголошувати особисту інформацію. Ніколи не слід повідомляти незнайомцям свої особисті дані, такі як номери банківських карток, паролі, адреси електронної пошти, номери телефонів та деталі про своє місце проживання [1];

2. Не давати гроші незнайомцям або переказом через Інтернет, не надсилати гроші на вимогу інших людей, особливо якщо немає впевненості, що вони дійсно їх потребують;

3. Перевіряти інформацію. Якщо надійшло повідомлення або електронний лист, що виглядає сумнівно, слід спробувати перевірити інформацію, використовуючи інші джерела. Наприклад, якщо надійшло повідомлення від банку, необхідно перевірте його офіційний вебсайт або зателефонувати до служби підтримки, щоб переконатися, що повідомлення дійсно звідти;

4. Не тиснути на посилання в сумнівних повідомленнях або електронних листах, інакше на комп’ютері або пристрої можуть встановитися віруси або шкідливі програми;

5. Бути обережними та пильними при отриманні запитів на особисті дані або гроші від незнайомців. Якщо є впевненість, що це шахрайська схема, слід повідомити про це відповідні служби безпеки [4];

6. Використовувати складні паролі. Використання складних паролів є важливим для захисту особистих даних і запобігання несанкціонованому доступу до облікового запису. Ось декілька порад щодо створення складних паролів:

- Довжина. Пароль повинен містити щонайменше 8 символів. Чим довшим є пароль, тим складніше його зламати;
- Складність. Пароль повинен містити різноманітні символи, такі як великі і малі літери, цифри та спеціальні символи (наприклад, !, @, #, $, %, ^, &, *, (,)). Це зробить його складнішим для тих, хто намагається його зламати;
- Не використовувати особисту інформацію, таку як ім’я, дата народження, адреса електронної пошти, номер телефону або інша особиста інформація, котру можна легко встановити;
- Не використовувати очевидні паролі, такі як «123456» або «password». Ці паролі дуже легко розгадати;
- Використовувати різні паролі для різних облікових записів. В іншому випадку, якщо один із паролів стане відомим, то решта облікових записів будуть уразливими;

- Зберігати паролі в безпечному місці, наприклад, у зашифрованому файлі на комп'ютері або в програмі для управління паролями. Ніколи не зберігайте паролі у неперевірених місцях, таких як записки або електронні повідомлення [2];

7. Встановити надійне антивірусне програмне забезпечення та регулярно його оновлювати, щоб захистити свій комп'ютер від шкідливих програм та вірусів і у такий спосіб запобігти несанкціонованому доступу до облікових записів [3];

8. Бути уважними при використанні громадських мереж Wi-Fi, оскільки зловмисники можуть перехоплювати трафік та отримувати доступ до чужих облікових записів. Тому слід уникати використання громадських мереж Wi-Fi для важливих операцій, таких як банківські операції або введення паролів [4];

9. Навчитися розпізнавати шахрайство. Шахраї намагаються обдурити своїх жертв, використовуючи різні маніпуляції та прийоми. Тому слід навчитися розпізнавати шахрайство та фішинг, щоб уникнути потенційних загроз у майбутньому. Зокрема, не вірити у схеми збагачення, що здаються занадто хорошими, аби бути правдивими, і завжди бути пильними при отриманні неперевірених повідомлень або листів [5–7].

Найбільш поширеними видами економічних злочинів та шахрайства є незаконне привласнення майна, шахрайство у сфері закупівель, у сфері управління персоналом та кіберзлочини, що пов'язані з економічною діяльністю. Україна є однією з держав, де широко розповсюджуються кіберзлочини. Хоча українські організації застосовують сучасні інформаційні технології і методи для виявлення шахрайства та його моніторингу, але все ж таки вони відстають від інших країн світу [8].

Економічна безпека країни спрямована на забезпечення захисту життєво важливих інтересів усіх жителів суспільства і держави в економічній сфері від можливих внутрішніх та зовнішніх загроз.

Більш комплексне визначення економічної безпеки передбачає досягнення такого стану економіки, що зможе забезпечити високе та стійке економічне зростання всіх економічних показників, ефективне задоволення економічних потреб, державний контроль за рухом і використанням національних ресурсів, захист економічних інтересів на національному та міжнародному рівнях [9].

Таким чином, у сучасному світі шахрайство стає все більш поширеним. Шахраї постійно знаходять нові способи обману своїх жертв. Вони можуть використовувати фальшиву ідентифікацію, соціальну інженерію, фішинг, атаки на комп'ютери тощо.

Для того щоб не потрапити на їхній гачок, потрібно бути обережним, не повідомляти особисті дані (паролі, дані банківських карт тощо), постійно змінювати паролі та тримати їх у безпечному місці, діяти розсудливо та зважено.

Список використаних джерел

1. Конфіденційна інформація: які дані можна і не можна засекречувати. *? доступ до правди.* URL : https://dostup.pravda.com.ua/explainers/publications/konfidentsiina-informatsiia-iaki-dani-mozhna-i-ne-mozhna-zasekrechuvaty.
2. Як і навіщо вигадувати надійні паролі. *Конкурент.* URL : https://konkurent.ua/publication/35337/yak-i-navischo-vigaduvati-nadiyni-paroli/.
3. Навіщо потрібні антивіруси? *ITEZ.* URL : https://itez.com.ua/why-do-you-need-antivirus.html.
4. Небезпека Wi-Fi у публічних місцях: поради IT-спеціалістів. *Шпальта.* URL : https://shpalta.media/2020/08/12/nebezpeka-wi-fi-u-publichnix-miscyax-poradi-it-specialistiv/.
5. Як розпізнати та захистити себе від онлайн-шахрайства. *fin.do.* URL : https://www.fin.do/uk/blog/215_yak-rozpiznati-ta-zahistiti-sebe-vid-onlajn-shahrajstva.
6. Rybalchenko L., Kosychenko O. Features of latency of economic crimes in Ukraine. *Scientific Bulletin of the Dnipropetrovsk State University of Internal Affairs.* 2019. Special Issue № 1(102). P. 264–267. URL : https://er.dduvs.in.ua/bitstream/123456789/3944/1/29.pdf.
7. Дисковський А. О., Косиченко О. О., Рибальченко Л. В. Основи організації захисту об'єктів та інформації від злочинних посягань : навч. посібник для слухачів магістратури. Дніпро : Дніпроп. держ. ун-т внутр. справ, 2020. 96 с.
8. Rybalchenko L., Kosychenko O. Features of latency of economic crimes in Ukraine. *Scientific Bulletin of the Dnipropetrovsk State University of Internal Affairs.* 2019. Special Issue № 1. P. 264–267.
9. Rybalchenko L., Ryzhkov E., Ohrimenco S. Economic crime and its impact on the security of the state. *Philosophy, Economics and Law Review.* 2021. No. 1(2). P. 67−80.

Валерія БЄЛОВА
студентка ННІ права
та інноваційної освіти
Науковий керівник:
к. і. н., доцент **Ірина ЄРЕМЄЄВА**
(Дніпропетровський державний університет внутрішніх справ)

ДОСВІД СТИМУЛЮВАННЯ ЕКОНОМІЧНОГО ЗРОСТАННЯ КРАЇН АЗІЇ

Економічна політика азійських країн спрямована на стимулювання економічного зростання та базується на стратегіях, що мають на меті заохочення інвестицій, підтримку підприємництва та інновацій, підвищення ефективності виробництва та якості освіти, забезпечення соціального захисту населення. Одним із ключових принципів економічної політики азійських країн є стимулювання інвестицій та підтримка підприємництва. Для досягнення цієї мети використовуються різні інструменти, такі як податкові пільги, зниження ставок податків на прибуток підприємств, зниження рівня регулювання та адміністративних перешкод для бізнесу, забезпечення доступу