

Cybernetic factors of Ukraine's global security

Larisa Yemelianenko¹, Dmitriieva Oksana²

Abstract. *The modern world of distance contact contains cyber challenges that affect learning, work and leisure by putting more pressure than ever before. Smooth transition from work and study to games, doctor's appointments, happy hours, shopping for essentials, meetings, and even celebrating life events on the same devices every day. Planning for future accomplishments is happening online, and the biggest risk to future cybersecurity is the threat of ignorance. Cyber learning and awareness, implementation of human risk management will shape the trends of global security of the population of Ukraine.*

Key Words: *Internet privacy, social hostileness, phishing, digital identity, the role of BISO (Business Information Security Officer), open source security projects.*

1. ВСТУП

Безпека конфіденційності в Інтернеті формує персональне усвідомлення безпеки цифрової ідентичності. Вимірювання, управління та зменшення людського ризику для підприємств, установ, організацій, суб'єктів приватного сектору у найближчі роки стане окремою галуззю, що займатиметься розробленням стратегій того, як ми живемо, працюємо та граємо сьогодні. Індустрія кібербезпеки отримує нові, сучасні погляди, розроблені, щоб допомогти населенню змінити поведінку та зменшити ризики організацій у світі, де життя відбувається онлайн.

2. РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Існує велике прагнення освітніх закладів зробити інформаційні системи безпечнішими, змінюючи поведінку простими та при-

¹ Associate Professor. Kviv National Economic University named after Vadym Hetman, Economics and Management Faculty, Department of National Economy and Public Administration, Ukraine

² Postgraduate. Kviv National Economic University named after Vadym Hetman, Economics and Management Faculty, Department of National Economy and Public Administration, Ukraine

вабливими способами. Наполегливо підготовлюючи до запуску офіційні програми інформування про кібер учасників навчального процесу [1], майбутні кадри будуть стратегічними іорієнтованими на результат професіоналами з великим досвідом керівництва в галузі технологій та кібербезпеки. Це зробить безпеку інструментом для бізнесу, а також розробником рішень і послуг безпеки з глобальним досвідом та оперативною досконалістю. Праця над удосконаленням програм безпеки у великих масштабах відбуватиметься завдяки стратегічним інвестиціям у людей та стійким і повторюваним процесом і визначаючи інструменти, які їх підтримують. Крім того, консультування у сфері безпеки, розроблення експертизи безпеки та участь у проектах безпеки з відкритим кодом заповнить майбутнє інформаційних технологій. Стануть достатньо відомі ризики, що забезпечують цифрову трансформацію, інновації та зростання бізнесу, захищаючи дані та бренд компанії [2, 3]. Безпека ділової інформації, освітніх технологій та послуг на ринк вищої освіти, інформаційна безпека в університеті, розбудова програм відповідності в університеті, консультування працюючих у сфері внутрішньої безпеки та фінансових послуг, все це доповнює перелік планового управління у інформаційних системах [4].

Управління технологіями та ризиками секторів критичної інфраструктури. Набуття досвіду консультування глобальних компанії та їхніх найвищих керівників з питань технологій, кібербезпеки, відповідності та цифрових ризиків, пов'язаних із продуктами, послугами, важливими ініціативами та поточними операціями [5]. Глобальна безпека по управлінню формування майбутнім України на сьогодні охоплює такі фактори (табл. 1).

Кіберхист — це ланцюг логічно пов'язаних, послідовних і керованих дій, у результаті яких вхідні параметри (ресурси, інформація) перетворюються у вихідні (управлінське рішення) з метою отримання багаторівневої системи оцінювання ризиків і загроз.

Таблиця 1. Методичні підходи щодо дослідження основних глобальної кібербезпеки

Аналітика процесу безпеки	Синергія процесу безпеки	Техніки та терміни безпеки
Фактор 1. Управління подвійними ризиками		
Відповідаскерівництво організації за кібер-безпеку, щоб забезпечити готовність компа-нії запобігати, виявляти та реагувати на еволюційні кіберзагрози; а також знаходити ініціативи щодо ризику кібербезпеки комер-ційної діяльності та покращення кіберстійко-сті в підприємницьких екосистемах. Об'єднання людей різноманітністю техноло-гій та процесів[8].	Досвід роботи в IT та безпеці, а також розро-бка програмного забезпечення, архітектури безпеки, інженерії безпеки та керівництва в галузі безпеки. Кар'єрні радники з кібербез-пеки та наставники для людей по всьому світу, пристрасна допомога людям, особли-во жінкам, увійти в кібербезпеку.	Створити позитивну культуру безпеки в організаціях. Досягнення єдиної мети : зменшити ризик, зробивши людей активом безпеки, а не зобов'язанням. Кібербезпека та її прискорений вплив на організації, окремих людей, сім'ї та спільно-сті. [6,7].Новафілософія, згідно з якою роз-ширення прав і можливостей людей є най-кращим підходом до постійного усвідомлення безпеки та запобігання злов-живанням. [9]
Фактор 2. Соціальна інженерія		
Керування людьми це наука, яка дає необ-межені можливості. Це метод управління діями людини без використання технічних засобів. Метод заснований на використанні слабкостей людського фактору та вважається дуже руйнівним. Соціальну інженерію можна також використовувати і в законних цілях не тільки для отримання інформації, а й для дій конкретною людиною. Сьогодні соціальну інженерію найчастіше використовують в інтернеті, для отримання закритої інформа-ції, або інформації, що становить велику цінність. Соціальна інженерія молода наука, яка є складовою соціології, і претендує на сукуп-ність тих специфічних знань, які спрямову-ють, упорядковують та оптимізують процес створення, модернізації та відтворення нових (штучних) соціальних реальностей. [10] Певним чином вона «добудовує» соціологічну науку, завершує її на фазі перетворення нау-кових знань у моделі, проекти та конструкції	Заняття безпеки зорієнтовані на озброєння слухачів насамперед методологією аналіти-ко-синтетичного мислення та знаннями формалізованих процедур (технологій) конструкторськo-винахідницької діяльності. У характеристичні формалізованих операцій, у тому числі складається це останнє, особли-ву увагу звертається на операції складної комбінаторики. Ігнорування принципу сис-теменості в операцій комбінаторики завдає і продовжують завдавати великої шкоди усім рівням трансформційних процесів, які у нашому суспільстві. Для захисту користувачів від соціальної інженерії можна застосовувати як технічні, так і антропогенні засоби. Найпростішими методами антропогенного захисту можна назвати: — Привернення уваги людей до питань безпеки. — Усвідомлення користува-чами всієї серйозності проблеми та прийнят-тя політики безпеки системи. — Вивчення та впровадження необхідних методів та дій для	Претекстинг — це дія, відпрацьована за задалегідь складеним сценарієм (претексту). У результаті ціль має видати певну інформа-цію або вчинити певну дію. Цей вид атак застосовується зазвичай телефоном. Частіше ця техніка включає більше, ніж просто брех-ня, і вимагає будь-яких попередніх дослі-джень (наприклад, персоналізації: дата народження, сума останнього рахунку і ін.), з тим, щоб забезпечити довіру ціль. До цього ж виду належать атаки і по онлайн-месенджерам, наприклад, по ICQ,ICQ Фішинг техніка, спрямована на неправомірне отримання конфіденційної інформації. Зазви-чай зловмисник посилав ціль, підроблений під офіційний лист від банку або платіжної систе-ми, що вимагає «перевірки» певної інформації або вчинення певних дій. Цей лист зазвичай містить посилання на фальшиву веб-сторінку, що імітує офіційну, з корпоративним логоти-пом та наповненням, і містить форму, що вимагає ввести конфіденційну інформацію

соціальних інститутів, цінностей, норм, алгоритмів діяльності, відносин, поведінки т. п. Але, припустимо, співробітники не виконали заплановані заходи і виявили наступні ознаки. На електронну пошту вашим співробітникам приходить занадто багато спаму. Сервери сповільнюють роботу. Наприклад, відповідають протягом хвилини (при звичайному часу відповіді 3–4 секунди). ПК повільно виконує звичні дії, так як еревантажений вірусним трафіком. Сайт недоступний. Потрібно занадто багато часу, щоб зайти на сайт. Ви бачите великий стрибок трафіку, але для цього немає підстав. Якщо є можливість, відразу ж звернутися до фахівця з кібербезпеки, потрібно це зробити негайно. Якщо миттєво відреагувати на інцидент не вдається, співробітникам варто вжити кількя заходів.	підвищення захисту інформаційного забезпечення. Ці засоби мають один загальний недолік: вони пасивні. До технічного захисту можна віднести інформацію та засоби, що заважають користуватися отриманою інформацією. Найбільшу поширеність серед атак в інформаційному просторі соціальних мереж з використанням слабкостей людського фактора набули атаки за допомогою електронних листів, а саме: і внутрішні пошта мережі. Боротьба — автоматизація у системі Cartesa, коли у якості паролів потрібно вибрати вказанераніше зображення або частину зображення, але у сильно спотвореному вигляді. Щоб не втратити дані, потрібно поставити сайт в режим обслуговування. Варто повідомити про подію керівництву, інтернет-провайдеру і будь-яким третім особам, які відповідають за надання послуг і периметр безпеки. Також потрібно постаратися зафіксувати час початку DDoS, тривалість інциденту, статистику по трафіку, логі з помилками сервера і відзначити будь-які зміни, що відбуваються в системі під час DDoS. Якщо співробітники виконують ці нескладні дії, технічного фахівця буде легше вирішити проблему і відновити дані.	від домашньої адреси до пін-коду банківської картки. Троянський кінь Ця техніка експлуатує інтерес, цікавість або жадібність мети. Зловмисник відправляє «цікавий» скрін-сейвер, важливий апгрейд антивірусу або навіть свіжий компромат на співробітника. Така техніка залишається ефективною, поки користувачі сліпо клікатимуть за будь-якими вкладеннями [11]. Дорожнє абулюко Цей метод атаки є адаптацією троянського коня і полягає у використанні фізичних носіїв. Зловмисник може підкинути інфікований CD або флеш у місію, де носій можна легко знайти (туалет, ліфт, парковка). Носій підробляється під офіційний та супроводжується підписом, покликаним викликати цікавість. Кві про кво Зловмисник може зателефонувати за випадковим номером до компанії та представитися співробітником техпідтримки, який опитує, чи є якісь технічні проблеми. У випадку, якщо вони є, в процесі їх вирішення мета вводити команди, які дозволяють хакеру запустити шкідливе програмне забезпечення.
Добріка інформації, отриманої в результаті онлайн-діяльності особи. До неї належать: імена користувачів і паролі, операції пошуку в Інтернеті, дата народження, соціальне забезпечення та історія покупок тощо	Прагнення залучити кінцевих користувачів і викликати захоплення своїм освітнім досвідом і вимірними результатами[12].	Створення й оптимізація програм безпеки в державному та приватному секторах. Навчання ефективним стратегіям боротьби з кіберзлочинністю і отримання найвищих рейтингів безпеки в уряді.

Фактор 4. Роль BISO		
Відводиться роль сполучної ланки між топ-менеджментом, бізнес-підрозділами, IT-службою та службою інформаційної безпеки (ІБ). BISO може допомогти бізнесу в досягненні цілей, представляючи ефективну безпекову стратегію, дорожню карту робіт і проєктів з ІБ на майбутнє.	Застосування глибоких знань для зниження корпоративних і особистих ризиків, розробляючи науково-обґрунтовані, спільні програми підвищення обізнаності щодо безпеки. Забезпечення успіхів ролі головного директора з інформаційної безпеки (CISO) Створення трансформаційних стратегій кібербезпеки; а також створення програм поінформованості про безпеку, поведінки та культури в основі стратегії безпеки. Покороги різноманітності та залученість в безпеку дослідження. Практичну локальну та глобальну перспективу та культуру.	Міжнародним доповіді, захоплення своєю метою у сфері безпеки. Створення команд з кібернавчання та поінформованості в організації з кібербезпеки. Сюди входять розгортання імітованих фішингових кампаній, розробка навчання на основі ролей та забезпечення виконання тренінгів усіх вимог до відповідності та нормативних вимог. Розглядаються такі питання: що таке конфіденційна інформація, як її захищати, відповідні норми законодавства, безпеки, які чекають в Інтернеті, а також рекомендації як користуватися особистим комп'ютером та телефоном щоб зберегти конфіденційність своїх даних. Захист даних. Конфіденційність в Інтернеті.

Джерело: складено авторами [6,7,8,9,10,11,12].

Очікуваний результат кібер безпекової діяльності, має забезпечити ефективний загальнонаціональний інструмент спільного протистояння кіберзагрозам. Систематизацію безпекових заходів доцільно відобразити такими їх видами: операційні (основні); підтримуючі (забезпечуючі та допоміжні), управлінські (загальнокорпоративні та процеси розвитку) [13]. Об'єкти критичної інфраструктури, урядових та військових ресурсів, які можуть стати об'єктами посягань ворожих хакерів приєднувати до платформ (систем моніторингу). Де фактично в режимі онлайн, отримують індикатори кіберзагроз.. Надається можливість поділитись із закритою спільнотою власними даними посягань у кіберпростір. Пропонуємо на підприємствах проводити кібераналіз з метою оцінки безпекового стану інформаційних систем за такими напрямками (рис. 1).



Рис. 1. Аналіз даних кібернетичних глобальних викликів

Джерело: складено авторами.

3. ВИСНОВКИ

Оформлення процедури захисту підприємств, аналіз кібернетичних факторів безпеки в управлінні глобальними викликами інформаційних технологій України вбачаємо за трьома напрямками:

1. експрес-аналіз кібернетичних загроз,
2. повний аналіз кібернетичних загроз і результатів кібербезпеки підприємств, установ, організацій,
3. оцінка стану системи інформаційних технологій підприємств, установ, організацій.

Для реалізації останнього напрямку запропоновано застосовувати показники-індикатори оцінки стану інформаційно технологічних систем підприємств, установ, організацій до складу яких входять показники-індикатори глобальних кібер загроз і міжнародної практики і показники-індикатори корпоративної кібербезпекової спроможності [14]. Ефективне управління кіберпроцесами на підприємствах, установах, організаціях передбачає їх постійне поліпшення і оптимізацію, тому дуже важливе формування системи удосконалення процесів безпеки інформаційних систем.

ЛІТЕРАТУРА

1. Law of Ukraine «on information protection in automated systems» <https://zakon.rada.gov.ua/laws/show/2594-15>(Accessed 25 May 2022)
2. DECREE OF THE PRESIDENT OF UKRAINE NO. 447/2021 On the decision of the national security and Defense Council of Ukraine of May 14, 2021 «on the cybersecurity strategy of Ukraine»
3. On the decision of the national security and Defense Council of Ukraine of May 14, 2021 “on the cybersecurity strategy of Ukraine”: decree of the president of Ukraine of 26.08.21 No. 447. URL: <https://www.president.gov.ua/documents/4472021-40013> (Accessed 15 May 2022)
4. On the decision of the national security and Defense Council of Ukraine of May 20, 2016 “on the Strategic Defense Bulletin of Ukraine”: decree of the president of Ukraine of 06.06.16 No. 240. URL: <https://zakon.rada.gov.ua/laws/show/240/2016>(Accessed 01 May 2022) (Accessed 02 June 2022)
5. On the basic principles of ensuring cybersecurity of Ukraine: Law of Ukraine No. 2163-VIII of 05.10.17. Clause 4 of Article 9 URL: <https://zakon.rada.gov.ua/laws/show/2163-19>(Accessed 05 May 2022)

6. Cooperation in the field of cybersecurity URL:<https://cert.gov.ua/> (Accessed 15 June 2021).

7. Dovgan O.D., Tkachuk T.Yu. Information Security system of Ukraine: ontological dimensions. Information and law.No. 1 (24)/2018, pp. 89–103.

8. Lukyanchuk R. v. State strategic planning in the field of ensuring cybersecurity: realities of the present. Bulletin of the National Academy of Public Administration under the president of Ukraine. Series: Public Administration. 2016. № 3, pp. 131–137.

9. National Risk and Threat Assessment Systems: best World practices, new opportunities for Ukraine: analytical add./ Reznikova O.O., Voitovsky K.E. Lepikhov A.V.; for general information. edited by O.O. Reznikova. Kiev: nisi, 2020. 84 p.

10. Solodkaya a.m. priorities for improving information security in Ukraine. Information and law.No. 3 (15)/2015, pp. 36–42.

11. Tikhomirov A. A. ensuring information security as a function of the modern state: monograph; general. edited by R. A. Kalyuzhny. Kiev: Center for academic and scientific practice. vid. na SB Ukrainy, 2014. 196 P.

12. Tkachuk N. State and problematic issues of implementation of the cybersecurity strategy of Ukraine. Information and law.No. 1 (28)/2019. pp. 129–134.

13. on national security of Ukraine: Law of Ukraine No. 2469-VIII of 21.06.18. URL: <https://zakon.rada.gov.ua/laws/show/2469-19#Text14>. Rinaldi S., Peerenboom J., and Kelly T. "Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies". IEEE Control Systems Magazine, IEEE, December 2001, pp. 11–25.

14. Priority assessment of threats and risks: which issues require extra focus. URL: <https://english.nctv.nl/topics/national-security-strategy/priority-assessmentof-threats-and-risks> (Accessed 01 June 2022)