Використання інтернет-технологій та інших інноваційних засобів зв'язку дозволяє підприємствам легко входити на міжнародні ринки, комунікувати з партнерами та споживачами з усього світу, використовуючи електронні платформи та інструменти електронної комерції.

Одним із суттєвих ризиків під час війни у сфері зовнішньоекономічної діяльності є укладення договорів. Згідно із ст. 6 Закону України «Про зовнішньоекономічну діяльність» зовнішньоекономічний договір (контракт) укладається суб'єктом зовнішньоекономічної діяльності або його представником у простій письмовій або в електронній формі, якщо інше не передбачено міжнародним договором України чи законом. У разі експорту послуг (крім транспортних) зовнішньоекономічний договір (контракт) може укладатися шляхом прийняття публічної пропозиції про угоду (оферти) або шляхом обміну електронними повідомленнями, або в інший спосіб, зокрема шляхом виставлення рахунка (інвойсу), у тому числі в електронному вигляді, за надані послуги [3]. Тому, на нашу думку, використання електронного підпису сприяє розвитку зовнішньоекономічних зв'язків.

Застосування криптографії та блокчейн-технологій підвищує конфіденційність транзакцій. Наприклад, у сфері зовнішньоекономічної діяльності криптографію використовують для захисту передачі даних між банком і клієнтом, при здійсненні мобільних платежів. Ці технології гарантують захист від несанкціонованого доступу та забезпечують цільність і конфіденційність інформації, що є фактичними аспектами міжнародних фінансових відносин.

Загалом, інновації у зовнішній економічній діяльності відкривають нові можливості для сталого розвитку та сприяють ефективному використанню ресурсів, зниженню негативного впливу на довкілля та забезпеченню сталого росту як національних, так і глобальних економік. Однією з важливих аспектів є можливість розвинути сталі поставки ланцюгів, які сприятимуть оптимізації процесів, зменшенню викидів шкідливих речовин під час виробництва та транспортування, сприяючи збереженню навколишнього середовища.

Тому вважаємо, що інноваційні технології є важливим інструментом для підвищення ефективності управління зовнішньоекономічною діяльністю, формування більш надійного середовища для зовнішньоекономічних операцій, розвитку міжнародної торгівлі та фінансових відносин й досягнення цілей сталого розвитку,

Список використаних джерел

1. Левченко О.М., В'юник О.В. Механізми активізації зовнішньоекономічної діяльності інноваційноінтегрованих структур. *Центральноукраїнський науковий вісник. Економічні науки.* 2020. Вип. 5(38). С.152–162. DOI: https://doi.org/10.32515/2663-1636.2020.5(38).152-162

2. Бортнікова М.Г., Чиркова Ю.Л. Штучний інтелект в менеджменті зовнішньоекономічної діяльності. *Цифрова економіка та економічна безпека.* 2022. Вип. 2(02). С. 70–75. DOI: https://doi.org/10.32782/dees.2-12

3. Про зовнішньоекономічну діяльність: Закон України від 16 квітня 1991 року № 959-XII. URL: https://zakon.rada.gov.ua/laws/show/959-12#Text

УДК 330.47

Вергал К.Ю., к.е.н., доцент
Національний університет «Полтавська політехніка імені Юрія Кондратюка»
(м. Полтава, Україна)

КІБЕРНЕТИЧНІ ЗАГРОЗИ ЦИФРОВОЇ ЕКОНОМІКИ

Цифрова економіка розглядається як економіка, що базується на електронних товарах і послугах і формується електронними бізнес-моделями, що інтегровані з глобальною мережею економіки та підтримуються ІКТ [6], такими як Інтернет-технології, «Великі дані» («Big

data»), «Хмарні обчислення» («Cloud computing»), «Інтернет речей» («Internet of Things») [1], «Штучний інтелект» («Artificial Intelligence»), «Роботизація» («Robotization»). Стрімкий розвиток цифрової економіки підтрведжує статистка Світового банку: у 2022 році цифрова економіка становила понад 15% світового ВВП і за останні десять років зросла в 2,5 рази швидше, ніж ВВП фізичного світу.

Необхідність залишатися конкурентоспроможними на ринку є рушійною силою цифрової трансформації бізнесу, що полягає у впровадженні нових організаційних форм та інноваційних методів ведення бізнесу в онлайн форматі для отримання доступу до нових ринків та створення конкурентних переваг. За цих умов інформація стає агентом інтеграції та чинником інновації в бізнесі [4]. В умовах цифровізації необхідність зберігання, обробка та аналіз великих масивів в цифровому вигляді для швидкого ухвалення стратегічних рішень, гнучкого реагування на кон'юнктурні зміни, впровадження електронних сервісів створює низку кіберзагроз як для країни в цілому, так і для бізнесу. Вразливість безпеки особистої інформації називають основним ризиком цифрової економічної трансформації, оскільки це стосується безпеки персональних даних під час здійснення економічної діяльності [5]. Основним джерелом такого ризику є інформаційні активи цифровій формі (цифрові моделі бізнес-процесів, цифрові послуги, цифровий контент, цифрові бази даних, веб-ресурси, програмне забезпечення, цифрові дані з різних датчиків, електронні медіадані, інформація, що обробляється в інформаційних системах і передається по каналах передачі даних).

Кіберзлочинність обходилася світовій економіці приблизно 787 671 долар на годину згідно даних 2021 року. Середня вартість кібервзлому у 2022 році склала 4,35 мільйона доларів. У 2023 витрати пов'язані із кіберзлочинністю становили 913 мільйонів доларів на годину та 8 трильйонів доларів на рік. Прогнозується, що кіберзлочинність обійдеться світовій економіці у2025 року в розмірі 10,5 трильйона доларів [42].

Різке зростання кіберзлочинності розпочалося із пандемією Covid19 та активним переходом бізнесу на віддалений режим роботи. Порівняно з 2019 роком у 2020 році кількість атак шкідливого ПЗ зросло на 358%. Із повномасштабним вторгненням в Україну розширився ландшафт кіберзагроз. Кількість фішингових атак зі сторони росії на адреси електронної пошти європейських та американських компаній зросло у 8 разів. За даними дослідження Accenture Cost of Cybercrime Study, 43% кібератак спрямовані на малий бізнес, але лише 14% готові захистити себе. Згідно статистики 67% підприємств малого та середнього бізнесу вважають, що у них немає власних навичок для боротьби з витоками даних.

До найпоширеніших типів кібер-атак на бізнес в умовах цифрової економіки у 2022-2023 рр.:відносять

- фішинг - є найпоширенішою формою кіберзагроз, що спричиняє крадіжку облікових даних кредитних карток та іншої особистої фінансової інформації, а також дозволяє отримувати доступ до приватних баз даних або призводить до завантаження шкідливого програмного забезпечення;

- програми-вимагачі – одна з найпоширеніших форм кіберінцидентів у секторі малого та середнього бізнесу. Хакери розгортають технології, які дозволяють викрадати бази даних особи чи організації та зберігати всю інформацію з метою отримання викупу. Зростанню криптовалют, таких як біткойн сприяють зростанню кількості атак програм-вимагачів, дозволяючи вимагати викуп анонімно;

- атаки на ланцюги постачання – становлять до 40% усіх кіберзагроз у сфері бізнесу. Дослідження показують, що лише 23% керівників служб безпеки відстежують своїх партнерів та постачальників у режимі реального часу щодо ризиків кібербезпеки. Збій цифрових ланцюгів поставок або платформ хмарних сервісів (35%) є третьою за значимістю проблемою кіберризику для респондентів Allianz Risk Barometer [6];

- взломи інтернет-речей. За даними Statista.com, очікується, що до 2025 року кількість пристроїв, підключених до IoT, досягне 75 мільярдів. Потрапивши під контроль хакерів, пристрої IoT можна використовувати для перевантаження мереж або блокування основного обладнання з метою отримання фінансової вигоди;

- мобільні атаки - смартфони сприйнятливі до багатьох загроз безпеці, включаючи фішинг (особливо за допомогою текстових повідомлень), поганий захист паролів, шпигунське програмне забезпечення та шкідливі програми.

- криптоджекінг - кіберзлочинці захоплюють робочі комп'ютери з метою «майнінгу» криптовалюти. Для компаній системи, піддані шифруванню, можуть спричинити серйозні проблеми з продуктивністю та дорогі простої, оскільки IT-спеціалісти працюють над пошуком і вирішенням проблеми;

- кібершпигунство - крадіжка інтелектуальної власності компаній

Список використаних джерел

1. Кіндзерський Ю. В. Кібербезпека та становлення цифрової економіки: проблеми взаємозв'язку. Економічний вісник Дніпровської політехніки. 2020. № 3 (71). С. 18-26.

2. Cybercrime-Report 2022. URL : https://s3.ca-central-1.amazonaws.com/esentire-dot-com-assets/assets/resourcefiles/2022-Official-Cybercrime-Report.pdf

3. FBI's IC3 report: financial losses due to email fraud hit record high in 2021, March 29, 2022

4. Hemmatfar, M., M. Salehi, and M. Bayat, Competitive advantages and strategic information systems. International Journal of Business and Management, 2010. 5(7): p. 158-169.

5. McAfee. (2014). Net losses: Estimating the Global Cost of Cybercrime.California, 2014. ГКДЖ https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/attachments/140609_McAfee_PDF.pdf

6. Weill, P. and S.L. Woerner, The Future of the CIO in a Digital Economy. MIS Quarterly Executive, 2013. 12(2).

УДК 338.1

Вакуленко Д.С., студентка
Національний університет «Полтавська політехніка імені Юрія Кондратюка»
(м. Полтава, Україна)

ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІ СИСТЕМИ В УПРАВЛІННІ

Інформаційна система (ІС) – комунікаційна система, що забезпечує збирання, пошук, оброблення та пересилання інформації, необхідної в процесі прийняття управлінських рішень, завдань з будь якої області. Елементами ІС є: комп'ютери, комп'ютерні мережі, люди, інформаційне та програмне забезпечення. А головна мета – виробництво професійної інформації. ІС є невід'ємною частиною сучасного управління. З кожним роком світ прогресує, з'являються нові галузі в яких потрібні інформаційні технології (ІТ). Вони досить стрімко прогресують, люди не встигають адаптуватися до оновлень, як з'являються вже більш прогресивні технології, системи. Згадаймо одні із перших прикладів інформаційно-комунікаційних систем. Вони з'явилися у 1950-х роках XX століття. Це були електромеханічні бухгалтерські рахункові машини. Основним їх призначенням було обрахування заробітної плати, це дозволяло зробити розрахунки швидше та точніше. Далі ці системи починають використовуватися більш широко на управлінських рівнях. Так виникають перші автоматизовані системи управління підприємством (АСУП).

До кінця 80-х років XX століття ІС змінюються і використовуються вже більш масово на всіх рівнях організації будь-якого профілю. В цей період ІС допомагають організаціям вийти на нові рівні, створювати нові товари та послуги, знаходити нові ринки збуту та досягати успіху у своїй діяльності. Перехід з XX до XXI століття, є періодом динамічних змін у розвитку ІС, які підтримують управління, в першу чергу завдяки мережевим системам, корпоративним інтрамережам та системам управління даними. Обґрунтовано, що системи Business In-Intelligence (BI) є кульмінацією еволюції змін у сфері систем підтримки прийняття