УДК 007:004
DOI https://doi.org/10.32782/IT/2024-4-10

Валентин ДЯЧЕНКО
кандидат економічних наук, доцент кафедри кібербезпеки, інформаційних технологій та економіки, Київський університет інтелектуальної власності та права Національного університету «Одеська юридична академія», Харківське шосе 210, м. Київ, Україна, 02121
ORCID: *0000-0002-0055-9256*
Scopus Author ID: *57994193000*

Наталія ДЯЧЕНКО
кандидат наук з державного управління, доцент кафедри кібербезпеки, інформаційних технологій та економіки, Київський університет інтелектуальної власності та права Національного університету «Одеська юридична академія», Харківське шосе 210, м. Київ, Україна, 02121
ORCID: *0000-0002-4306-7665*
Scopus Author ID: *57216565101*

Бібліографічний опис статті: Дяченко, В., Дяченко, Н. (2024). Врахування ризиків при використанні інформаційних технологій. *Information Technology: Computer Science, Software Engineering and Cyber Security,* 4, 75–80, doi: https://doi.org/10.32782/IT/2024-4-10

ВРАХУВАННЯ РИЗИКІВ ПРИ ВИКОРИСТАННІ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

У статті досліджено ризики та загрози при використанні інформаційно-комунікаційних технологій.

Метою дослідження *є ідентифікація основних видів ризиків та загроз при хмарному збереженні даних. На виконання мети ідентифіковано комплекс заходів щодо формування засад кібербезпеки. Акцентовано, що з урахуванням викликів сьогодення потрібні не лише кіберграмотність користувачів інформаційно-комунікаційних технологій, а й координація та переорієнтація досліджень у сфері комп'ютерних розробок, адже нові покоління програмно-апаратного забезпечення повинні гарантувати безпеку діяльності та дотримання принципу конфіденційності приватної, підприємницької чи державної інформації.*

Методологія дослідження. *Методологічні аспекти дослідження враховують концепції виявлення закономірностей появи нових ризиків та загроз інформаційній та кібернетичній безпеці в сучасних умовах стрімкого розвитку інформаційних технологій. У роботі було застосовано комплекс взаємопов'язаних наукових методів, зокрема: діалектичний, компаративного аналізу та логічний під час дослідження сутності загроз інформаційній безпеці у сучасних умовах невизначеності та ризику; метод емпіричного дослідження при порівнянні особливостей надання хмарних послуг IT-сервісами; системний підхід при ідентифікації комплексу заходів щодо формування засад кібербезпеки.*

Наукова новизна *полягає в інтегрованому підході до дослідження сутності ризиків та загроз інформаційній та кібернетичній безпеці в умовах стрімкого розвитку інформаційно-комунікаційних технологій та при використанні хмарних сервісів.*

Висновки. *У результаті теоретичного дослідження було здійснено ідентифікацію ризиків та загроз кібернетичній безпеці. Наголошено, що оперативна ідентифікація нових типів загроз та ризиків, визначення їх ключових характеристик сприятиме окресленню їх сутнісних властивостей, розробці алгоритмів їх аналізу та методів управління ними.*

Ключові слова: *ризики, загрози, інформаційні технології, хмарні технології.*

Valentyn DIACHENKO
Candidate of Economic Sciences, Associate Professor at the Department of Cybersecurity, Information Technology and Economics, Kyiv University of Intellectual Property and Law of the National University «Odessa Law Academy», 210, Kharkivske highway, Kyiv, Ukraine, 02121, diachenko.v@ukr.net
ORCID: *0000-0002-0055-9256*
Scopus Author ID: *57994193000*

Natalia DIACHENKO
Candidate of Public Administration Sciences, Associate Professor at the Department of Cybersecurity, Information Technology and Economics, Kyiv University of Intellectual Property and Law of the National University «Odessa Law Academy», 210, Kharkivske highway, Kyiv, Ukraine, 02121, n.diachenko@ukr.net
ORCID: *0000-0002-4306-7665*
Scopus Author ID: *57216565101*

To cite this article: Diachenko, V., Diachenko, N. (2024). Vrakhuvannia ryzykiv pry vykorystanni informatsiinykh tekhnolohii [Considering risks when using information technology]. *Information Technology: Computer Science, Software Engineering and Cyber Security,* 4, 75–80, doi: https://doi.org/10.32782/IT/2024-4-10

CONSIDERING RISKS WHEN USING INFORMATION TECHNOLOGY

The article examines risks and threats when using information and communication technologies.

***The purpose of the study** is to identify the main types of risks and threats when storing data in the cloud. To achieve this goal, a set of measures to form the foundations of cybersecurity has been identified. It is emphasized that, taking into account today's challenges, not only cyber literacy of information and communication technology users is required, but also coordination and reorientation of research in the field of computer development, because new generations of software and hardware must guarantee the security of activities and compliance with the principle of confidentiality of private, business or state information.*

***Research methodology.** The methodological aspects of the study take into account the concept of identifying patterns of the emergence of new risks and threats to information and cyber security in modern conditions of rapid development of information technologies. The work used a set of interrelated scientific methods, in particular: dialectical, comparative analysis and logical when studying the essence of threats to information security in modern conditions of uncertainty and risk; empirical research method when comparing the features of the provision of cloud services by IT services; systematic approach when identifying a set of measures to form the foundations of cybersecurity.*

***The scientific novelty** lies in an integrated approach to studying the essence of risks and threats to information and cyber security in the context of the rapid development of information and communication technologies and when using cloud services.*

***Conclusions.** As a result of the theoretical study, risks and threats to cyber security were identified. It is emphasized that the operational identification of new types of threats and risks, the determination of their key characteristics will contribute to the delineation of their essential properties, the development of algorithms for their analysis and methods for managing them.*

***Key words:** risks, threats, information technologies, cloud technologies.*

Актуальність проблеми. Інтернет, інформаційно-комунікаційні технології (далі – ІКТ), надання послуг у цифровому форматі, що стали невід'ємною умовою сьогодення, від електронного документообігу, інтернет-магазинів, онлайн-банкінгу, інтелектуальних систем управління бізнесом передбачають необхідність не лише наявності знань, умінь та навичок використання ІКТ, а й наявність досвіду з управління системами захисту інформації та кібернетичної безпеки, оскільки кіберзагрози інтенсивно еволюціонують, кіберзлочини постійно вдосконалюються, набуваючи рис транснаціонального характеру.

Аналіз останніх досліджень і публікацій. Дослідженню ризиків, загроз та небезпек при використанні інформаційно-комунікаційних технологій присвятили увагу ряд відомих вітчизняних науковців, зокрема О. Гайдук та В. Звєрєв здійснили аналіз кіберзагроз в умовах стрімкого розвитку інформаційних технологій (Гайдук, Звєрєв, 2024, с. 229). А. Лисеюк та Т. Свінцицька дослідили правове забезпечення кібербезпеки України в умовах воєнного стану та євроінтеграції (Лисеюк, Свінцицька, 2024). К. Мовчан ідентифіковано ризики кібербезпеки в епоху робототехніки (Мовчан, 2023).

Метою дослідження є ідентифікація основних видів ризиків та загроз при хмарному зберіганні даних.

Виклад основного матеріалу дослідження. За умов сучасного правового режиму воєнного стану в Україні та стрімкого зростання кіберризиків і кіберзагроз гостро постає потреба у підготовці висококваліфікованих фахівців у цій сфері, які могли б здійснювати як аналіз уже реалізованих заходів у сфері захисту комп'ютерних і комунікаційних мереж від кібератак, так і передбачати можливі ризики й загрози та оперативно реагувати на їх прояви.

Системні перебої з електропостачанням, що мали місце у певні періоди, спричиняли збої у наданні електронних послуг. А кібератаки спричиняли блокування діяльності органів державної влади та роботи важливих для економіки та формування засад національної безпеки підприємств, установ та організацій. З метою формування засад кібербезпеки реалізовано ряд заходів для вирішення базових правових, суспільних, політичних та організаційних питань (рис. 1):

В умовах сьогодення вкрай необхідно посилити кіберзахищеність підприємств, установ, організацій та критичної інфраструктури, дотримуючись принципу «безпека понад усе» (англ. security-first thinking).

З метою формування базових знань з кібербезпеки ряд закладів освіти пропонують безоплатні курси, зокрема, заклад вищої освіти

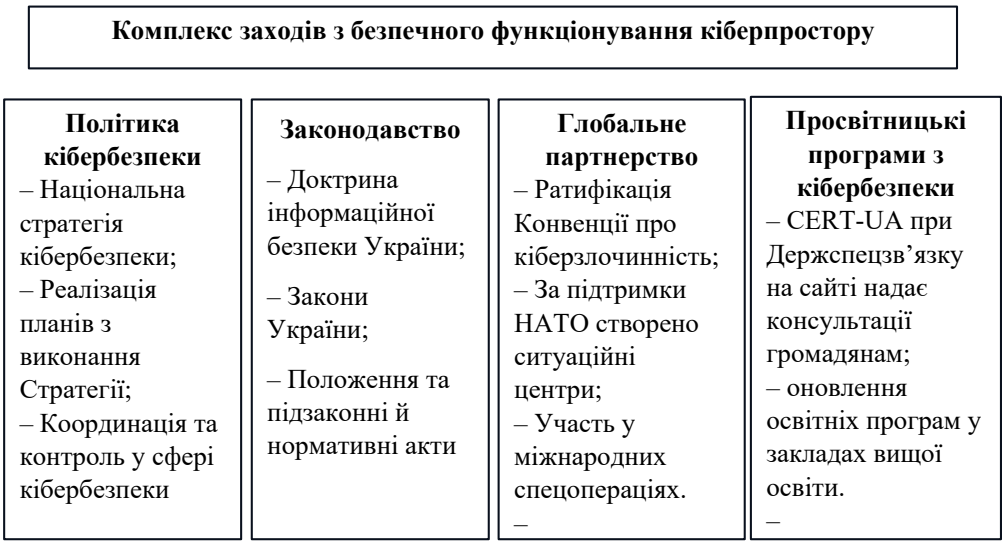

Рис. 1. Комплекс заходів щодо формування засад кібербезпеки

Вища школа публічної освіти пропонує загальну короткострокову програму «Основи забезпечення кібербезпеки та протидії дезінформації», яка передбачає дистанційну форму навчання, два напрями – інформаційна безпека та кібербезпека. Партнером-укладачем програми є «Міжнародна академія інформації». Метою програми є розвиток у слухачів компетентностей у сфері кібербезпеки, у тому числі застосування інструментів, що забезпечують конфіденційність, цілісність чи доступність даних, запобігання кібератакам та протидія дезінформації шляхом набуття професійних навичок роботи з інформацією, опанування цифрової грамотності та основ кібербезпеки.

З урахуванням викликів сьогодення потрібні не лише кіберграмотність користувачів ІКТ, а й координація та переорієнтація досліджень у сфері комп'ютерних розробок, адже нові покоління програмно-апаратного забезпечення повинні гарантувати безпеку діяльності та дотримання принципу конфіденційності приватної, господарської чи державної інформації.

Передумовою формування кола висококваліфікованих спеціалістів у сфері інформаційних технологій є підготовка здобувачів вищої освіти відповідно до освітньої програми «Управління системами захисту інформації та кібернетичної безпеки», метою якої є розвиток соціального та інтелектуального капіталу шляхом підготовки у галузі інформаційних технологій висококваліфікованих, соціально відповідальних фахівців кібербезпеки з високим рівнем етичних стандартів та професійної гідності, які, в контексті сприяння реалізації стратегій кібербезпеки та інформаційної безпеки, відповідають сучасним потребам ринку праці, суспільства та держави, сфокусовані на захисті прав, свобод і законних інтересів громадян в інформаційному просторі, володіють теоретико-практичними знаннями та вміннями, необхідними для розуміння принципів управління системами та комплексами інформаційної та/або кібербезпеки держави в цілому або окремих суб'єктів їх інфраструктури, здатні до постійного навчання і самовдосконалення, до застосування методів та засобів технічного та криптографічного захисту інформації від ризику стороннього кібернетичного впливу, що передбачає розробку нових, удосконалення або подальшого розвитку наявних розробок та досліджень.

Освітньо-професійна програма «Управління системами захисту інформації та кібернетичної безпеки» базується на загальновідомих наукових результатах в галузі інформаційних технологій та зорієнтована на формування комплексу знань, умінь та навичок щодо моделювання, проєктування, розробки, інтеграції та супроводження систем та комплексів інформаційної та/чи кібербезпеки на базі сучасних інформаційно-комунікаційних технологій, які надають здобувачами вищої освіти широкі можливості для самореалізації у сфері зайнятості та кар'єрного зростання.

Програма передбачає формування у здобувачів вищої освіти компетентностей щодо сучасних методів, методик, інформаційно-комунікаційних технологій та технологій забезпечення інформаційної та/або кібербезпеки, необхідних для розв'язання базових задач та практичних проблем в ІТ-сфері з урахуванням методології системного ІТ-аудиту щодо виявлення кібернетичних загроз та вторгнень, а також сучасних тенденцій розробки нових, удосконалення

або подальшого розвитку наявних розробок та досліджень у сфері інформаційних технологій.

Серед особливостей освітньої програми «Управління системами захисту інформації та кібернетичної безпеки» варто виокремити поєднання комплексу освітніх компонентів, що формують компетентності за фахом, враховують стратегічні напрями забезпечення кібербезпеки та інформаційної безпеки України, зорієнтовані на розвиток інтелектуального капіталу особистості, з акцентом на здатність здобувачів до розуміння змісту управління системами та комплексами інформаційної та/чи кібербезпеки, застосування сучасних концепцій та інструментарію забезпечення інформаційної безпеки, методологію системного IT-аудиту протидії кібернетичним загрозам та проєктування нових, удосконалення чи подальшого розвитку наявних розробок та досліджень.

Програмою передбачено наявність інструментів та обладнання, зокрема сучасного програмно-апаратного забезпечення інформаційно-комунікаційних технологій, яке передбачає у рамках інтерактивного навчання використовувати розроблене Microsoft лабораторне середовище SimuLand із відкритим вихідним кодом, розроблене з метою допомогти розгорнути лабораторне середовище, що відтворює добре відомі методи, які використовуються в реальних сценаріях атак, активно тестувати та перевіряти ефективність відповідних виявлень Microsoft 365 Defender, Azure Defender і Microsoft Sentinel, а також розширити дослідження загроз за допомогою телеметрії та криміналістичних артефактів, створених після кожної вправи моделювання, протестувати та поліпшити захист.

Одним з актуальних питань сьогодення є використання Інтернету, зокрема, хмарних сервісів. Хмарні технології (англ. cloud technologies) – сервіс, що дозволяє віддалено використовувати засоби накопичення, обробки та зберігання даних.

Базова концепція хмарного збереження та обробки даних базується на різних моделях надання IT-послуг, серед яких: CaaS, WaaS, SaaS, DaaS, PaaS, EaaS (табл. 1). Серед пропонованих сервісів варто виокремити SaaS (Software as a Service) – програмне забезпечення як послуга), як вигідну альтернативу придбання програмного забезпечення, адже SaaS дозволяє отримувати програмне забезпечення як послугу, а не дорого купувати ліцензійні програми.

Серед популярних продуктів SaaS є Salesforce.com (https://www.salesforce.com/) – найбільший у світі SaaS-провайдер (Salesforce, 2024), що надає доступ до власної CRM-системи (системи управління відносинами із клієнтами).

Набір додатків компанії Google Inc. (https://www.google.com/) містить поштовий сервіс з розширеними можливостями та інший ефективний функціонал для оптимізації діяльності, як приватної, так і підприємницької чи державної (Google Inc., 2024).

Серед популярних та зручних у використанні хмарних сховищ довільно виокремити:

– Google Drive – сховище даних, яке належить компанії Google Inc., дає змогу користувачам зберігати інформацію на хмарних серверах та обмінюватися нею з іншими користувачами в Інтернеті.

– OneDrive (офіційно Microsoft OneDrive) – сховище файлів, засноване на хмарній організації інтернет-сервісу зберігання файлів з додатковими функціями файлообміну (Microsoft OneDrive, 2024);

Таблиця 1

Особливості надання IT-послуг хмарними сервісами

Назва послуги	Опис
CaaS (Communication as a Service – комунікація як послуга)	Надає послуги зв'язку: IT-телефонія, поштові послуги тощо.
WaaS (Workplace as a Service – робоче місце як послуга)	Спеціалізується на наданні віртуальних робочих місць
SaaS (Software as a Service – програмне забезпечення як послуга)	Провайдер розміщує у себе додаток, а користувачі оплачують послугу за використання програми
DaaS (Data as a Service – дані як послуга)	Надання даних на вимогу користувача незалежно від його розташування
PaaS (Platform as a Service – платформа як послуга)	Надання інтегрованої IT-платформи для створення, розгортання, тестування та підтримки додатків
EaaS (Everythinge as a Service – все як послуга)	Комплекс хмарних сервісів, що задовольняє великий спектр потреб користувачів

– Dropbox файлообмінник та синхронізатор файлів від компанії Dropbox Inc., розташованої у Сан-Франциско, США (Dropbox Inc., 2024).

При використанні хмарних сервісів необхідно враховувати ризики:

– хмарні послуги надаються певною компанією, тому й збереження приватної інформації повністю залежить від неї;

– для перегляду власної інформації чи її опрацювання необхідно бути в мережі інтернет;

– зникнення напруги може спричинити тимчасову відсутність можливості доступу до власних баз даних, що зберігаються у хмарних сервісах.

Наведені вище постачальники хмарних послуг забезпечують захист персональних даних, зокрема:

– Google Drive забезпечують захист при передачі даних;

– Dropbox забезпечує захист через аутентифікацію;

– OneDrive здійснює подвійну аутентифікацію.

Однак, серед основних загроз хмарного збереження даних варто виокремити (табл. 2):

У рамках інтерактивного та практико-орієнтованого навчання здобувачів вищої освіти при опануванні ними освітніх компонентів програми «Управління системами захисту інформації та кібернетичної безпеки» доцільно використовувати кіберполігон.

Розгортання на базі кафедри кібербезпеки та інформаційних технологій *Київського університету інтелектуальної власності та права* кіберполігону – сукупності спеціальних програмно-апаратних комплексів, які об'єднані провідними та безпровідними засобами комунікацій, що можуть бути інтегрованими в мережу Інтернет та застосовуються для здійснення моніторингу впливу на системи управління, які можуть становити інтерес, для захисту власних систем від несанкціонованого доступу – сприяє формуванню у здобувачів вищої спеціальності 125 Кібербезпека навичок використання тактик передбачення кібератак, методів ідентифікації симуляції кібератак, відпрацювання методик їх відбиття. Навчальний кіберполігон сприяє формуванню у здобувачів вищої освіти системи професійних здатностей, адже дозволяє імітувати кібератаки, кібернапади на сервери, які обслуговують інфраструктури підприємства, установи чи організації для пошуку вразливих місць, усунення їх вразливості, налагодження ефективної системи захисту наявних комп'ютерних та інформаційно-комунікаційних ресурсів, відновлювати штатне їх функціонування. Програмне забезпечення та системи візуалізації кіберполігону сприяють відпрацюванню кібердій, що здійснюються у віртуальному середовищі. Системами візуалізації передбачено можливість моделювання кібератак, які можуть здійснюватись на комп'ютерні мережі, що передбачає зменшення чи й зовсім уникнення витрат на придбання ресурсів хмарних технологій.

Навчальний кіберполігон дозволяє імітувати кібератаки, кібернапади на сервери, які обслуговують інфраструктури закладу вищої освіти для пошуку вразливих місць, усунення їх вразливості, налагодження ефективної системи захисту наявних комп'ютерних та інформаційно-комунікаційних ресурсів, відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв чи відмов різного рівня та походження.

Висновки та перспективи подальших досліджень. За умов сучасного правового режиму воєнного стану в Україні та стрімкого зростання кіберризиків і кіберзагроз гостро постає потреба аналізу та визначення трендів і тенденцій перебігу кіберзагроз, їх взаємного впливу та чинників, що не пов'язані напряму з кіберпростором, що здатні сприяти появі суттєвого негативного впливу на процеси розвитку комп'ютерних та інформаційно-комунікаційних систем і мереж. Ідентифікація нових типів загроз та ризиків, визначення їх ключових характеристик сприятиме окресленню їх сутнісних властивостей, розробці алгоритмів їх аналізу та методів управління ними.

Таблиця 2

Основні види загроз хмарного збереження даних

Загроза	Опис
Крадіжка даних	Можлива при атаці на сервер, коли отримують доступ до бази email-адрес
Втрата, псування даних	Дані можуть бути втраченими чи пошкодженими внаслідок системних помилок, програмної недосконалості хмарних сервісів
Незахищеність інтерфейсів	Помилки в проєктуванні хмарних сервісів роблять їх уразливими до кібератак
Суміжна вразливість	Спільний доступ до одних і тих же ресурсів створює повторну вразливість

ЛІТЕРАТУРА:

1. Гайдук О., Звєрєв В. Аналіз кіберзагроз в умовах стрімкого розвитку інформаційних технологій. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*.2024, № 3 (24). С. 225–236. https://doi.org/10.28925/2663-4023.2024.23.225236.

2. Лисеюк А., Свінцицька Т. Правове забезпечення кібербезпеки України в умовах воєнного стану та євроінтеграції. *Право та інновації*, 2024, № 4 (48), с. 32–38. https://doi.org/10.37772/2518-1718-2024-4(48)-4.

3. Мовчан К. О. Ризики кібербезпеки в епоху робототехніки. *Вчені записки ТНУ імені В. І. Вернадського. Серія: Технічні науки*. 2023, Том 34 (73). с. 79–83. https://doi.org/10.32782/2663-5941/2023.4/13.

4. Salesforce.com. URL: https://www.salesforce.com/.

5. Google.Inc. URL: https://www.google.com/.

6. Microsoft OneDrive. URL: https://www.microsoft.com/uk-ua/microsoft-365/onedrive/online-cloud-storage.

7. Dropbox Inc. URL: https://www.dropbox.com/uk_UA/.

REFERENCES:

1. Haiduk, O., Zvieriev, V. (2024). Analysis of cyber threats in the context of rapid development of information technologies [Analysis of cyber threats in conditions of rapid development of information technologies]. *Elektronne fakhove naukove vydannia «Kiberbezpeka: osvita, nauka, tekhnika»*. https://doi.org/10.28925/2663-4023.2024.23.225236 [in Ukrainian].

2. Lyseiuk, A., Svintsytska, T. (2024). Pravove zabezpechennia kiberbezpeky Ukrainy v umovakh voiennoho stanu ta yevrointehratsii [Legal support for Ukraine's cybersecurity in the context of martial law and European integration]. *Pravo ta innovatsii*. https://doi.org/10.37772/2518-1718-2024-4(48)-4 [in Ukrainian].

3. Movchan, K. O. (2023). Ryzyky kiberbezpeky v epokhu robototekhniky [Cybersecurity risks in the age of robotics]. *Vcheni zapysky TNU imeni V. I. Vernadskoho. Seriia: Tekhnichni nauky.* https://doi.org/10.32782/2663-5941/2023.4/13 [in Ukrainian].

4. Salesforce.com. Retrieved from: https://www.salesforce.com/.

5. Google.Inc. Retrieved from: https://www.google.com/.

6. Microsoft OneDrive. Retrieved from: https://www.microsoft.com/uk-ua/microsoft-365/onedrive/online-cloud-storage.

7. Dropbox Inc. Retrieved from: https://www.dropbox.com/uk_UA/.