

**ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ КІБЕРСТРАХУВАННЯ БАЗ ДАНИХ
ДЛЯ ОСВІТНІХ УСТАНОВ СИСТЕМИ МВС УКРАЇНИ****PROBLEMS AND PROSPECTS OF CYBERINSURANCE OF DATABASES
FOR EDUCATIONAL INSTITUTIONS OF THE SYSTEM OF THE MIA OF UKRAINE**

**Кудінов В.А., к.ф.-м.н., доцент,
завідувач кафедри інформаційних технологій**
Національна академія внутрішніх справ

**Корнейко О.В., к.т.н., професор,
професор кафедри інформаційних технологій**
Національна академія внутрішніх справ

**Пакриш О.Є., к.т.н., доцент,
доцент кафедри інформаційних технологій**
Національна академія внутрішніх справ

Шуляк Б.А., студент
Національна академія внутрішніх справ

За умов прискореної цифрової трансформації усіх сфер суспільного життя в Україні, кіберстрахування – це новий та актуальний тренд сучасного бізнесу. Зі збільшенням кількості кіберінцидентів в Україні в останні роки, особливо в умовах воєнного стану, можливість страхування баз даних є гарантією мінімізації збитків організацій від зазначених кіберінцидентів. Особливо актуальним це стало також для освітньої галузі з інтенсивним використанням навчальних онлайн-платформ та веденням електронного документообігу. Міжнародний досвід свідчить про те, що страхування кіберризиків не лише дає можливість компенсувати збитки, але й стимулює розробку більш досконалих заходів безпеки, що також є важливим для розвитку цифрових технологій у сфері освіти. В роботі розглянуто потенційні ризики для баз даних в цифровому форматі освітніх установ системи МВС України, проаналізовано поняття кіберстрахування баз даних та міжнародний досвід страхових компаній, які спеціалізуються на цьому напрямі; окреслено основні проблеми застосування кіберстрахування в Україні.

Наукова новізна дослідження полягає в обґрунтуванні Концепції впровадження кіберстрахування баз даних в освітніх установах системи МВС України, яка включає чітко визначену мету та завдання, організаційну структуру взаємодії між освітніми установами, страховими компаніями та державними регуляторами. Для ефективної реалізації системи кіберстрахування в ЗВО системи МВС України запропоновано відповідний алгоритм впровадження. Надано низку рекомендацій для українських страхових компаній, які планують надавати послуги кіберстрахування для закладів освіти.

Ключові слова: кіберстрахування, бази даних, кіберінциденти, освітні установи, МВС України.

In the context of accelerated digital transformation of all spheres of public life in Ukraine, cyber insurance is a new and relevant trend in modern business. With the increase in the number of cyber incidents in Ukraine in recent years, especially under martial law, the possibility of insuring databases is a guarantee of minimizing losses of organizations from these cyber incidents. This has also become especially relevant for the education sector with intensive use of online educational platforms and electronic document management. International experience shows that cyber risk insurance not only makes it possible to compensate for losses, but also stimulates the development of more advanced security measures, which is also important for the development of digital technologies in the field of education. The paper considers potential risks for databases in digital format of educational institutions of the Ministry of Internal Affairs of Ukraine, analyzes the concept of cyber insurance of databases and the international experience of insurance companies specializing in this area; outlines the main problems of applying cyber insurance in Ukraine.

The scientific novelty of the study lies in the substantiation of the Concept of implementing cyber insurance of databases in educational institutions of the Ministry of Internal Affairs of Ukraine, which includes a clearly defined goal and objectives, an organizational structure of interaction between educational institutions, insurance companies and state regulators. For the effective implementation of the cyber insurance system in higher educational institutions of the Ministry of Internal Affairs of Ukraine, an appropriate implementation algorithm is proposed. A number of recommendations are provided for Ukrainian insurance companies that plan to provide cyber insurance services for educational institutions.

Key words: cyber insurance, databases, cyber incidents, educational institutions, Ministry of Internal Affairs of Ukraine.

Вступ. Інтенсивна цифровізація суспільного життя вимагає нових підходів до адаптації інформаційних та економічних процесів. Не винятком є і середовище освітніх установ системи МВС України, яке, спираючись на відповідну нормативно-правову базу, активно діджиталізується. Створюються платформи для онлайн-навчання та ведення електронного документообігу, що підвищує ефективність освітнього процесу закладів вищої освіти (далі – ЗВО) та зменшує витрати часу/ресурсів на підтримку його функціонування. Цифровізація освітнього середовища ЗВО системи МВС України ставить на порядок денний важливе питання щодо надійного захисту його інформаційних ресурсів. Але незалежно від застосованих заходів завжди існує ймовірність реалізації фінансових, технічних та репутаційних ризиків унаслідок кібератак, особливо в сучасних умовах широкомасштабного вторгнення РФ в Україну. Тому сьогодні, на наш погляд, є надзвичайно

актуальною проблема впровадження ефективних механізмів для кіберстрахування баз даних, які зберігаються в цифровому форматі в освітніх установах системи МВС України, що дозволить знизити фінансові ризики та втрати через реалізацію можливих кібератак.

Мета дослідження. На підставі аналізу проблеми застосування кіберстрахування баз даних в Україні створити та науково обґрунтувати Концепцію впровадження кіберстрахування баз даних в освітніх установах системи МВС України, що дозволить мінімізувати фінансові та репутаційні втрати від кіберінцидентів та підвищити рівень їх кіберстійкості в умовах цифрової трансформації.

Результати й обговорення. Інтенсивна цифровізація освітньої системи, як вже нами зазначалося, супроводжується новими ризиками. Серед ключових загроз виділяють:

1) вразливість цифрових платформ: більшість платформ, що використовуються в ЗВО, мають низький

рівень кіберзахисту (не оновлене програмне забезпечення та слабкі алгоритми шифрування);

2) використання недостатньо захищених каналів для передачі даних між структурними підрозділами ЗВО. Тому стають можливими кібератаки типу «ransomware», які блокують доступ до баз даних, вимагаючи викуп за їх відновлення. Також серед ризиків – застосування фішингових схем, які спрямовані на отримання доступу до паролів або інших конфіденційних даних [1].

Таким чином, викрадення фінансової інформації може призвести до втрати коштів або їх використання для незаконних операцій, а розголошення персональних даних викликає репутаційні та юридичні ризики.

До ризиків слід також обов'язково віднести і можливі технічні збої – у такому разі відсутність резервного копіювання електронних баз даних може призвести до повної втрати інформації.

Отже, в сучасних реаліях хакерські атаки можуть завдати значної шкоди фінансовим процесам ЗВО. Вплив таких кібератак охоплює кілька аспектів:

1) *економічні наслідки*: втрата доступу до баз даних може спричинити затримки у виплаті заробітних плат, що вплине на якість роботи персоналу, а також існує ризик розкрадання коштів з рахунків ЗВО або благодійних фондів;

2) *збої в управлінні*: відсутність доступу до фінансових звітів унеможливує оперативне прийняття рішень щодо витрат, а порушення звітності перед органами управління освітою може призвести до санкцій або припинення фінансування;

3) *репутаційні ризики*: втрата довіри з боку персоналу та здобувачів вищої освіти освітньої установи, потенційних абітурієнтів, які можуть відмовитися від вступу на навчання до ЗВО, а також негативний імідж закладу освіти в інформаційному просторі.

Питання захисту освітніх баз даних у країнах ЄС, США, Канаді стало актуальним ще в середині 1990-х років, коли почали використовуватися перші автоматизовані програмні продукти для діловодства у закладах освіти, що відповідали стандартам FERPA (Family Educational Rights and Privacy Act). У Німеччині, Великобританії, Канаді та Австралії електронні журнали в освітній системі стали обов'язковими з 2000-х років, а в Швеції – з 2005 року [2]. Поряд з їх впровадженням завжди актуальним було питання гарантій захисту даних і наразі в країнах ЄС діють чіткі вимоги для роботи з освітніми платформами відповідно до регламенту GDPR (General Data Protection Regulation), а в скандинавських країнах всі навчальні заклади користуються інтегрованими державними платформами, які забезпечують збереження усієї звітності [3].

Таким чином, захист фінансових даних ЗВО є основою для забезпечення стабільної роботи освітньої системи, оскільки це дозволить уникнути непередбачуваних витрат, забезпечить відшкодування збитків у разі порушення роботи систем. Автоматизація фінансових процесів із захищеними системами забезпечує більшу прозорість та зручність управління. Слід зазначити, що для підвищення рівня захисту інформації необхідно формувати цифрову компетентність з питань кібергігієни (уникнення підозрілих посилань, створення складних паролів тощо) науково-педагогічного складу, адміністрації та бухгалтерії ЗВО.

Сучасні онлайн-платформи для здійснення освітнього процесу намагаються гарантувати достатній рівень безпеки баз даних, але вони унеможливають повну відсутність ризиків, зокрема у випадках хакерських атак чи технічних збоїв. За даними Microsoft, Україна стала однією з країн, організацій та користувачів яких зазнавали найбільше кібератак у першій половині 2025 року. На країну припало близько 9,5% від загальної кількості

постраждалих у європейському регіоні. Заклади освіти, лікарні та місцеві органи влади все частіше стають мішенями через зберігання конфіденційних даних і обмежені ресурси на кіберзахист. Кількість кібератак на освітні заклади у світі значно зросла в останні роки. За статистикою компанії Check Point за 2025 рік, більш ніж 3,5 тисяч атак щотижня націлені на освітній сектор [4].

В Україні ситуація також викликає занепокоєння. Вона щомісяця зазнає близько 100 тисяч кібератак. При цьому кількість кібератак на освітній сектор постійно зростає. У відповідь на зростання кіберзагроз в Україні був прийнятий закон, який формує принципи з кіберзахисту держінформресурсів [5]. Ним передбачено функціонування системи оцінювання стану кіберзахисту також в закладах вищої освіти. Таким чином, увага до практичних питань забезпечення кібербезпеки в освітніх установах в Україні є достатньо високою, а практика кіберстрахування освітніх закладів станом на сьогодні відсутня.

Кіберстрахування (страхування кіберризиків або cyber insurance) – це страховий продукт для захисту бізнесу та фізичних осіб від ризиків, пов'язаних із користуванням Інтернетом, зберіганням та обробкою даних в електронному вигляді, роботою з IT-інфраструктурами. У цьому контексті страхування баз даних – це фінансовий механізм, який дозволяє закладам освіти, які користуються онлайн-платформами для ведення навчальних журналів і зберігання іншої важливої документації, захистити себе від фінансових втрат у разі витоку або знищення даних.

Враховуючи величезну цінність персональних і фінансових даних, а також можливість їхнього знищення чи викрадення внаслідок дій кіберзлочинців, такі види страхування мають стати частиною стратегії управління ризиками для освітніх організацій. Комплексне рішення страхування від кіберзагроз та кіберризиків дозволяє компенсувати можливі втрати від пошкодження, руйнування або крадіжки корпоративних та клієнтських даних, а також подолати кризу в бізнес-діяльності, яка може виникнути внаслідок дії кіберризиків. Поліси кіберстрахування як страхові продукти не мають регламентованих характеристик, у різних компаній вони мають свої умови та ліміти відповідальності. Відтак, для таких страхових полісів характерні кілька важливих аспектів: 1) типи ризиків, які покриваються страховкою; 2) страхова сума; 3) процес подачі та обробки заявок на відшкодування.

Слід зазначити, що у зв'язку з відсутністю законодавчої бази кіберстрахування в Україні врегульовувати права та обов'язки між страхувальником та страховиком можливо лише за відповідним договором. Укладання такого договору починається з комплексної оцінки закладу освіти та його систем. В основному такі договори покривають збитки страховика на відновлення даних та збитки перед третіми особами (наприклад, моральні збитки), але в розширеному варіанті можуть охоплювати витрати на кризовий менеджмент.

Сьогодні в Україні існують окремі страхові компанії, які пропонують спеціалізовані поліси для кіберстрахування, що в перспективі може бути модифікованою послугою і для закладів вищої освіти. Основною проблемою залишається визначення обсягів збитків та доказ причинно-наслідкового зв'язку між страховим випадком і заявленими збитками, а тому найскладнішим об'єктом страхування є бази даних.

Для розробки Концепції впровадження кіберстрахування для українських закладів вищої освіти необхідно вивчити досвід міжнародних страхових компаній, які спеціалізуються на цьому напрямі. Аналіз міжнародного досвіду кіберстрахування свідчить про існування еволюції від простого покриття «технологічних помилок» до складного інструменту управління ризиками, що реагує на зростання кількості кіберризиків (гібридна війна, програми-вимагачі). Міжнародний досвід також демонструє,

що закони є головним стимулом для розвитку ринку кіберстрахування, а не добровільна ініціатива.

Станом на сьогодні світовий ринок кіберстрахування можна умовно поділити на три основні регіони:

1. *США (Північна Америка)*. Найбільш розвинений ринок у світі. Лідером з питань кіберстрахування є США, оскільки приблизно 90% ринку страхування кіберризиків припадає саме на цю країну. Прийняття законів про конфіденційність даних, які змушують компанії страхувати ризики, пов'язані з витоком персональних даних, стало стимулом для розвитку ринку. AIG – це приклад американської транснаціональної страхової корпорації, що надає послуги у сферах особистого та майнового страхування, а також інші фінансові послуги у понад 80 країнах світу.

2. *Країни Європи*. Прийняття Загального регламенту захисту даних (GDPR) [6] стало стимулом для розвитку ринку. GDPR встановлює високі штрафи за витоки, що стимулює компанії купувати страховку для покриття цих потенційних витрат. GDPR створив чіткий фінансовий стимул для страхування: а) *фіксовані штрафи* (до 4% від річного світового обороту компанії або €20 млн за серйозне порушення), тому кіберстрахування стало механізмом перекладання цього ризику; б) *обов'язок повідомлення* (компанії зобов'язані повідомляти регуляторам та постраждалим особам про витік даних протягом 72 годин), тому страхові поліси включають покриття витрат на PR та кризові комунікації для дотримання цього обов'язку. Звернемо увагу на такі потужні компанії, як Beazley, Chubb, Zurich і Lloyd's of London, надають послуги для захисту від кіберризиків.

3. *Азійсько-Тихоокеанський регіон*. Вважається, що ринок знаходиться на стадії формування, але він має високий потенціал зростання через швидку цифровізацію та зростання кіберзагроз, особливо в Сінгапурі та Японії.

Розглянемо міжнародний досвід страхування у секторі освіти (США/Велика Британія). Необхідно відмітити, що освітні установи є особливо вразливими через величезну кількість персональних даних, що зберігаються в базах даних (студенти, викладачі, фінансова інформація). Крім того, освітні установи часто стають ціллю програм-вимагачів (ризики «ransomware») через відносно слабкий захист і життєву важливість швидкого відновлення даних (необхідність проведення іспитів та освітнього процесу). При цьому страхування покриває витрати на викуп і відновлення цих навчальних систем. Крім того, страховики пропонують освітнім установам спеціалізовані поліси, які включають покриття витрат на компенсацію за призупинення освітнього процесу та відновлення довіри батьків/студентів.

Необхідно відмітити, що організація кіберстрахування принципово відрізняється від традиційного страхування (наприклад, майна) через нематеріальність об'єкта та швидку зміну загроз. Існує два основні типи полісів, які покривають базу даних та пов'язані з нею ризики:

1. *Страхування першої особи*. Прямі витрати компанії-страхувальника пов'язані з інцидентом та покривають витрати на IT-криміналістику, відновлення даних, PR-комунікації, викуп за програми-вимагачі, юридичні консультації, витрати на повідомлення клієнтів про витік.

2. *Страхування третіх осіб*. Витрати компанії-страхувальника пов'язані з відповідальністю перед іншими суб'єктами (клієнтами, регуляторами) та покривають судові витрати, штрафи від регуляторних органів (наприклад, штрафи GDPR), витрати на врегулювання позовів від клієнтів або партнерів.

Страхові компанії США та країн Європи підходять до оцінки ризиків не як до пасивної процедури, а як до активного управління безпекою страхувальника:

1. *Кібергігієна як умова страхування*. Перед укладанням договору компанія (освітня установа) зобов'язана пройти аудит. Якщо в її базах даних немає базових засо-

бів захисту (двофакторна автентифікація, резервне копіювання, оновлення програмного забезпечення), то у страхуванні буде відмовлено або поліс буде значно дорожчим.

2. *Використання скорингових моделей*. Страховики використовують спеціалізовані AI-моделі для аналізу зовнішнього периметра безпеки клієнта, присвоюючи йому бал («кіберскоринг»), який визначає вартість і умови полісу.

Таким чином, аналіз міжнародного досвіду кіберстрахування дозволяє нам зробити висновок, що для успішної організації кіберстрахування баз даних в освітніх установах системи МВС України необхідне виконання двох умов:

1. *Посилення регулювання*. Створення чіткого законодавчого визначення відповідальності за недбале зберігання персональних даних (аналог GDPR) для створення фінансового стимулу.

2. *Стандартизація кіберзахисту*. Впровадження обов'язкових мінімальних стандартів кібергігієни (захист баз даних, автентифікація), як необхідної умови для придбання полісу.

Виходячи з аналізу міжнародних практик, пропонуємо *Концепцію впровадження кіберстрахування* для закладів вищої освіти системи МВС України, яка буде відповідати умовам та запитам українського ринку. Вважаємо, що ця Концепція стане основою для створення шаблонів, які можуть бути адаптовані українськими страховими компаніями для забезпечення кібербезпеки в зазначених освітніх установах, оскільки жодна компанія наразі подібних послуг не надає. А тому може бути реалізована тільки у формі персоналізованої послуги для окремого закладу освіти.

Мета Концепції впровадження кіберстрахування – створення та наукове обґрунтування організаційно-правової моделі впровадження кіберстрахування баз даних в освітніх установах системи МВС України, спрямованої на мінімізацію фінансових, репутаційних та операційних втрат від кіберризиків та підвищення рівня кіберстійкості освітнього процесу в умовах цифрової трансформації.

Завдання Концепції впровадження кіберстрахування – для досягнення поставленої мети необхідно, на наш погляд, розв'язати такі завдання, а саме:

1. Провести комплексний аналіз сучасного стану кіберзахисту баз даних та існуючої нормативно-правової бази в системі МВС України.

2. Визначити ключові кіберризики («ransomware», витік персональних даних, DDos-атаки) та їхню потенційну фінансову оцінку, специфічну для освітніх установ.

3. Розробити методологію оцінки вразливостей та розрахунку страхових премій для баз даних з урахуванням специфіки освітньої діяльності.

4. Сформулювати структуру та основні положення уніфікованого договору кіберстрахування для освітніх установ системи МВС України, що включають покриття першої та третьої сторони.

5. Обґрунтувати організаційний механізм взаємодії між освітніми установами, страховими компаніями та Держспецв'язком у разі настання страхового випадку (регулювання врегулювання збитків).

6. Запропонувати модель управління кіберризиками, яка передбачає обов'язкове дотримання мінімальних стандартів кібергігієни як передумови для укладення страхового договору.

7. Сформулювати рекомендації щодо необхідних змін у відомчих документах МВС України та законодавстві України для впровадження кіберстрахування баз даних як інструменту фінансового захисту.

Для ефективної реалізації системи кіберстрахування в ЗВО системи МВС України пропонується створити такий алгоритм впровадження (покрокову процедуру), яка включатиме наступні етапи: 1) оцінка існуючих ризи-

ків та створення стратегії захисту; 2) визначення відповідальних осіб за кібербезпеку в закладі освіти, які будуть контролювати виконання всіх норм і процедур захисту; 3) імплементація технологій для кібербезпеки; 4) вибір та укладання договору з українською страховою компанією; 5) навчання персоналу та здобувачів вищої освіти; 6) регулярні перевірки та оновлення політик: проводити регулярні перевірки ефективності системи кібербезпеки та страхування.

На основі розробленої Концепції впровадження кіберстрахування в ЗВО системи МВС України можна сформулювати низку рекомендацій для українських страхових компаній, які планують надавати послуги кіберстрахування для закладів освіти, а саме:

1) адаптація продукту під специфіку вищого навчального закладу (страхові компанії мають розробити спеціалізовані продукти для ЗВО, зокрема з урахуванням обсягу даних, кількості учасників освітнього процесу, типу інформаційних систем);

2) гнучкість у визначенні покриттів та умов (пропонувати варіанти покриття, які можна адаптувати до конкретних потреб закладу: для навчальних установ це можуть бути продукти, що включають витрати на відновлення даних, юридичні послуги, а також штрафи за порушення законодавства);

3) інтеграція з технічними рішеннями (страхові компанії повинні співпрацювати з постачальниками технологій кібербезпеки для створення комплексних рішень, які поєднують захист даних з можливістю страхування);

4) розробка освітніх програм для клієнтів (окрім самих страхових послуг, компанії можуть впроваджувати навчальні програми з кібербезпеки для своїх клієнтів, що дозволить знижувати ймовірність настання страхових випадків).

Окреслена Концепція впровадження кіберстрахування може бути перспективною за умови виділення на це субвенції з державного бюджету, а тому подібні ініціативи мають бути пріоритетними на владному рівні, алгоритмізовані та реалізовані як умова безпечної цифровізації документообігу та освітнього процесу, а на рівні страхових компаній основною задачею стає розробка нових стра-

хових продуктів, які будуть більш гнучкими і доступними для освітніх організацій. Слід також зазначити, що розвиток кіберстрахування ЗВО неможливий без об'єднаних зусиль страхових компаній, Департаменту кіберполіції Національної поліції України, Державної служби спеціального зв'язку та захисту інформації України, Національної комісії, що здійснює державне регулювання задля протидії кіберзагрозам тощо.

Також важливим є напрям співпраці страхових компаній між собою (забезпечення перестраховування у критичних випадках) та із зарубіжними колегами з метою обміну досвідом та удосконалення механізму надання подібних послуг. Для кожної страхової компанії є визначальним високий рівень захисту її власних баз даних. Це значні фінансові затрати, але вони дозволять їм у перспективі виграти конкурентну боротьбу на ринку страхових послуг.

Для закладів вищої освіти позитивним може бути і поява страхових освітніх омбудсменів, що сприятиме прозорості надання страхових послуг.

Висновки. Основними результатами роботи є узагальнення та систематизація ключових механізмів організації кіберстрахування баз даних у провідних країнах (США, ЄС), виділення найбільш релевантних моделей, придатних для адаптації в Україні (наприклад, у частині оцінки ризиків та покриття). Створено та науково обґрунтовано Концепцію впровадження кіберстрахування баз даних в освітніх установах системи МВС України, яка включає чітко визначену мету та завдання, організаційну структуру взаємодії між освітніми установами, страховими компаніями та державними регуляторами (Держспецзв'язку). Надано рекомендації щодо поетапного впровадження Концепції, починаючи з пілотних проєктів та інтеграції кіберстрахування у загальну систему управління ризиками. Сформульовано пропозиції щодо внесення змін до нормативно-правових актів України у частині стандартизації кіберполісів та створення сприятливих умов для розвитку ринку. Створено перелік мінімальних обов'язкових вимог до кіберзахисту баз даних, відповідність яким має бути обов'язковою умовою для отримання страхового полісу, що підвищить загальний рівень захисту.

ЛІТЕРАТУРА

1. Бендер Ю. В. Вплив кіберзлочинності на фінансову сферу: проблеми та можливі рішення. *Економіка і фінанси*. 2017. № 6. С. 112-120.
2. Броннер Д. Захист даних у цифрових платформах: принципи та підходи до страхування. *Економіка та інновації*. 2020. № 3(8). С. 65-70.
3. Огляд Європейського агентства з кібербезпеки: безпека електронних платформ для закладів освіти. *ENISA* : [сайт]. URL: <http://www.enisa.europa.eu>.
4. Щорічний звіт компанії Check Point «The State of Cyber Security 2025». *Datastream* : [сайт]. URL: <https://www.datastream.com.ua/ua/news/shhorichnij-zvit-kompanii-check-point-«stan-kiberbezpeki-u-2025-roczni»>.
5. Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури : Закон України від 27 берез. 2025 р. № 4336-IX // *Голос України* від 19 квіт. 2025 р. № 77.
6. Про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних): Регламент Європейського парламенту і Ради (ЄС) 2016/679 від 27 квіт. 2016 р. № 984_008-16 // Офіційний вісник Європейського Союзу від 04 трав. 2016 р. L 119. Стр. 1.

Дата першого надходження рукопису до видання: 20.09.2025
Дата прийнятого до друку рукопису після рецензування: 22.10.2025
Дата публікації: 29.10.2025