Шуляк Богдан Андрійович
Студент н.гр. 102_СПД ННІ права та психології НАВС

Науковий керівник:
Кудінов Вадим Анатолійович
кандидат фізико-математичних наук, доцент, завідувач кафедри інформаційних технологій ННІ права та психології НАВС

ВПЛИВ МІЖНАРОДНОГО ДОСВІДУ ТА УКРАЇНСЬКИХ РЕАЛІЙ НА ВПРОВАДЖЕННЯ КОНЦЕПЦІЇ КІБЕРСТРАХУВАННЯ БАЗ ДАНИХ В ОСВІТНІХ УСТАНОВАХ СИСТЕМИ МВС УКРАЇНИ

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, яке пов'язане з онлайн-навчанням та веденням електронного документообігу, у тому числі фінансової документації, ставить на порядок денний важливе питання щодо надійного захисту його інформаційних ресурсів. Однак, 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 ЗВО системи МВС України, що дозволить знизити фінансові ризики та втрати через реалізацію можливих кібератак.

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 ІТ-інфраструктурами [1]. 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 [2].

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.

Метою роботи є вивчення впливу міжнародного досвіду та українських реалій на впровадження Концепції кіберстрахування баз даних в освітніх установах системи МВС України, спрямованої на мінімізацію фінансових та репутаційних втрат від кіберризиків та підвищення рівня кіберстійкості в умовах цифрової трансформації та широкомасштабного вторгнення рф в Україну.

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. Прийняття законів про конфіденційність даних, які змушують компанії страхувати ризики, пов'язані з витоком персональних даних, стало стимулом для розвитку ринку.

2. *Країни Європи*. Прийняття Загального регламенту захисту даних (GDPR) [3] стало стимулом для розвитку ринку. GDPR встановлює високі штрафи за витоки, що стимулює компанії купувати страховку для покриття цих потенційних витрат.

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 (ризик «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 засобів 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.

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 (у 2021 році обсяг страхових виплат внаслідок атак вірусами зріс у 4 рази, а ринок кіберстрахування зростає щорічно на 25-50%) [2]. 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.

Висновки. За умов прискореної цифрової трансформації усіх сфер суспільного життя в Україні, кіберстрахування – це новий та актуальний тренд сучасного бізнесу. Зі збільшенням кількості кібератак в Україні, особливо спричинених сьогодні діями країни-агресора, можливість страхування баз даних є гарантією мінімізації збитків організацій від зазначених кіберінцидентів. Особливо актуальним це стало 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. Однак для забезпечення належного рівня страхового покриття необхідно створити в Україні чітке нормативно-правове регулювання, яке б враховувало специфіку освітніх установ та особливості їхньої фінансової діяльності, зокрема, освітніх установ системи МВС України.

Підхід до впровадження страхування у цьому напрямі є перспективним, тому окремі українські страхові компанії вже мають досвід кіберстрахування, але подібну практику для освітніх установ ще не впроваджують. Інноваційними є розробки полісів, які покриватимуть не тільки фінансові втрати, але й витрати на відновлення роботи освітніх платформ після кібератак, а також можливість надання консультацій і допомоги в розслідуванні таких кіберінцидентів.

Список використаних джерел:

1. Страхування кіберризиків. Cyber insurance. *FORINSURER* : [сайт]. URL: https://forinsurer.com/theme/48 (дата звернення: 18.10.2025).

2. Кіберстрахування: що це і чому це важливо для бізнесу та освітніх організацій? INSURANCE : [сайт]. URL: www.insurance.ua (дата звернення: 18.10.2025).

3. 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. Стор. 1.