КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4(16), 2022
ISSN 2663 - 4023
DOI: 10.28925/2663-4023.2022.16.7684
УДК 004.056.5

Трофименко Олена Григорівна
кандидат технічних наук, доцент, доцент кафедри інформаційних технологій,
Національний університет «Одеська юридична академія», м. Одеса, Україна,
ORCID ID 0000-0001-7626-0886
trofymenko@onua.edu.ua

Логінова Наталія Іванівна
кандидат педагогічних наук, доцент, завідувачка кафедри інформаційних технологій,
Національний університет «Одеська юридична академія», м. Одеса, Україна,
ORCID ID 0000-0002-9475-6188
loginova@onua.edu.ua

Манаков Сергій Юрійович
кандидат технічних наук, доцент кафедри інформаційних технологій,
Національний університет «Одеська юридична академія», м. Одеса, Україна,
ORCID ID 0000-0001-5930-4592
s.manakov@meta.ua

Дубовой Ярослав Володимирович
магістр з кібербезпеки,
Національний університет «Одеська юридична академія», м. Одеса, Україна,
ORCID ID 0000-0002-3987-9409
dubovoy97@gmail.com

КІБЕЗЗАГРОЗИ В ОСВІТНЬОМУ СЕКТОРІ

Анотація. Внаслідок переходу до дистанційного та гібридного навчання, спочатку через пандемію COVID-19, а тоді через російський напад і масштабну війну, освітній сектор України стикнувся з широким спектром кіберзагроз. Усвідомлення цих загроз може допомогти університетам та їхнім співробітникам захистити себе та своїх студентів від цих уразливостей. З'ясовано, що у закладах вищої освіти циркулюють великі обсяги персональних даних і фінансової інформації про студентів, викладачів та співробітників, а також інформації про наукові дослідження. Це робить їх привабливою мішенню для кіберзлочинців. У статті проаналізовано кіберзагрози у секторі вищої освіти. Проведено класифікацію найпоширеніших кіберзагроз у секторі вищої освіти. З'ясовано, що людський фактор, тобто помилки співробітників або студентів через необізнаність або зневажання елементарними правилами кібергігієни лежать в основі більшості успішно реалізованих кібератак. Дослідження ознак кіберзагроз в галузі освіти дозволив розділили їх за дев'ятьма критеріями: загрози на пристрої IoT, загрози через людський фактор, крадіжка персональних даних, програми-вимагачі або зловмисне програмне забезпечення, фінансова вигода, шпигунство, фішинг, DDoS-атаки, загрози на CMS. Реалізована у роботі класифікація загроз кібербезпеці в галузі освіти сприятиме чіткому їх розумінню і специфіки за тією чи іншою ознакою. Знання основних загроз освітніх мереж і систем, розуміння поширених способів злому і витоків конфіденційних даних студентів, викладачів та інших співробітників дозволить вибирати й застосовувати навчальним закладам найбільш ефективні інструменти і стратегії на всіх рівнях кіберзахисту. Кібербезпека є спільною відповідальністю для всіх, а її успіх залежить від обізнаності про мотиви та методи зловмисників, дотримання належної кібергігієни кожним та контролем за дотриманням вимог.

Ключові слова: кіберризики; кібервразливості; кіберзагроза; кібератака; кіберзахист; кібербезпека; освітній сектор.

ВСТУП

Разом з повсюдною інформатизацією суспільства ІТ-інфраструктура стає все більш вразливою для кіберзлочинності. Нехтування питаннями кіберзахищеності на тлі зростаючих кіберзагроз є вкрай небезпечним, а ціна такого ігнорування є надто високою. Так, 2021 року середня глобальна вартість злому даних склала 4,24 млн доларів США, що перевищило середні витрати на злом даних у $3,86 млн у попередньому році [1]. Тому організації та компанії вимушені вживати заходів щодо своєї кібербезпеки, яка є нині пріоритетом в їхніх ІТ-бюджетах.

Не в останню чергу зростання цих показників зумовлене спалахом пандемії COVID-19, через яку за умов карантину організації по всьому світу відправляли своїх співробітників на віддалену роботу з дому. Це порушило архітектуру мережі бізнесу, зробило її набагато більш відкритою, чим створило нові вразливі місця для використання зловмисниками і відповідно операційні та фінансові ризики. Переважно кібератаки спрямовані на дані й активи фінансових установ, урядів, корпорацій, різних підприємств і компаній. Проте не стали винятком у цьому переліку університети та академічні установи.

Постановка проблеми. У закладах вищої освіти циркулюють великі обсяги персональних даних і фінансової інформації про студентів, викладачів та співробітників, а також інформації про наукові дослідження, що робить їх привабливою мішенню для кіберзлочинців [2]. Національний центр кібербезпеки (NCSC) [3] наголошує на загрозах кібератак на освітній сектор, оскільки більшість навчальних закладів за умов карантину через пандемію COVID-19 продовжує навчання в онлайн-режимі.

Це свідчить про актуальність пошуків комплексного і виваженого підходу до вирішення питань кібербезпеки закладів освіти як всеосяжної стратегії, що залучатиме дієві практики і передові технології. При цьому поняття кібербезпеки охоплює всі ресурси вишу, враховуючи студентів, співробітників, філіалів і партнерів. Адже будь-яка сфера діяльності або активності, яка може притягнути загрозу реалізації вищезазначених ризиків, формує повне охоплення кіберзагроз [4].

Аналіз останніх досліджень і публікацій. Питанням аналізу кіберзагроз присвячені різні дослідження. Так, дослідження [5] виявило, що не всі компанії навіть після злому їх систем змінюють свою поведінку щодо кібербезпеки. В роботах [6, 7, 8] наголошено на важливості людського фактора в кібербезпеці, позаяк багато кіберінцидентів та витоків даних пов’язані саме з людським фактором. Дослідження [9] вивчає рівень обізнаності пересічних респондентів щодо кібербезпеки та їхнє розуміння проблем кібербезпеки. У статті [10] розглянуто загальну модель загроз та вразливостей кібербезпеки у закладах вищої освіти. Дослідники продовжують пошуки вдалих моделей і методів для кібербезпеки, зокрема, аналізуючи різноманітні кіберзагрози. Різні підходи і специфічні аспекти у пошуках рішення проблем, пов'язаних з питаннями аналізу кіберризиків та забезпеченням кібербезпеки, свідчать про актуальність цієї тематики і потребу подальших наукових досліджень, особливо щодо специфіки можливих кіберризиків закладів вищої освіти.

Мета дослідження полягає в класифікації можливих кіберзагроз з урахуванням специфіки забезпечення кібербезпеки закладів вищої освіти.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Освітній сектор стикається з широким спектром кіберзагроз, які можуть порушувати їхню повсякденну роботу, спричинити витоки даних наукових досліджень, а також персональних та фінансових даних. Логічним є класифікувати найпоширеніші кіберзагрози щодо сектора вищої освіти, розмежовуючи їх за критеріями з урахуванням специфіки забезпечення кібербезпеки. Дослідження та аналіз ознак сучасних уразливостей і кіберризиків освітнього сектора дозволили розділили кіберзагрози на дев'ять класів (рис. 1).

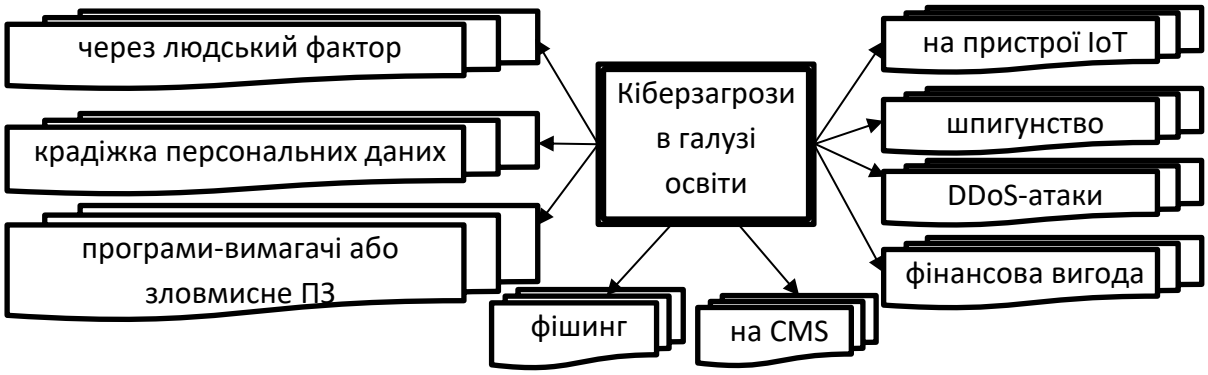

Рис. 1. Класифікація кіберзагроз у секторі вищої освіти

Загрози, націлені на пристрої інтернету речей (IoT). Ризик атак на освітні мережі зростає, оскільки вони стають все більш залежними від відкритого середовища і використання мобільних технологій та IoT. Освітній інтернет речей стосується наявних розумних дошок, інтелектуальних систем кондиціювання, вентиляції, освітлення тощо. Крім того, зараз багато навчальних програм базуються на цифровому форматі, тому студенти повинні мати доступ до підключених мобільних пристроїв. Нині поширеною практикою є те, що студенти приходять до ЗВО з декількома пристроями IoT і для своєї зручності залучають їх під час навчання та не лише. Так, за даними досліджень FortiGuard Labs [11] пристрої IoT впроваджуються в мережі з феноменальною швидкістю, до 1 мільйона пристроїв щодня. Хоча ці пристрої надають нові захопливі способи підвищення ефективності, гнучкості та продуктивності навчання і саморозвитку, також вони створюють нові ризики для мереж. Нині IoT є одним із ключових постачальників даних. Проблеми полягають в тому, що ці, здавалося б, невинні пристрої здебільшого вразливі через відсутність у них необхідних вбудованих засобів контролю безпеки для захисту від загроз. Уразливі місця в пристроях IoT дозволяють кіберзлочинцям отримати доступ до конфіденційних даних і реалізувати атаки на інші пристрої, підключені до цієї мережі. Тому пропорційно зі зростанням кількості IoT пристроїв, збільшується і число кібератак через такі пристрої. Саме тому університети нині запроваджують політику заборони використовувати особисті мобільні пристрої (телефони, планшети, ноутбуки тощо) (Bring your own device, BYOD) для доступу до корпоративних даних і систем;

Кіберзагрози через недостатню обізнаність є дуже актуальними для будь-якого сектора, у тому числі і для вищої освіти. Людський фактор, тобто помилки співробітників або студентів через необізнаність або зневажання елементарними правилами кібергігієни лежать в основі більшості успішно реалізованих кібератак. Кібербезпека є спільною відповідальністю для всіх, а її успіх залежить від обізнаності

про мотиви та методи зловмисників, дотримання належної кібергігієни кожним та контролем за дотриманням вимог. Розподіл відповідальності за кібербезпеку має бути частиною посадової інструкції кожного в організації. Кожен, від вищого керівництва до рядового працівника структурного підрозділу закладу і навіть студента, має дотримуватись визначених вимог кібербезпеки. Задля запобігання значної частки кібератак освітнім закладам варто регулярно проводити просвітницькі тренінги як для студентів, так і для працівників різних структурних підрозділів вишів щодо проблем кібербезпеки та розгляду можливих моделей поведінки при роботі з мережевими корпоративними ресурсами задля кращого захисту своєї ІТ-інфраструктури;

Крадіжка персональних даних. Цей вид кіберзагроз зачіпає всі рівні освіти, оскільки всі навчальні заклади зберігають дані студентів і співробітників, включаючи персональні дані (імена, адреси, медичні показники про стан здоров'я та багато іншого). Цей тип інформації може бути цінним для кіберзлочинців з кількох причин, незалежно від того, чи планують вони продавати інформацію третій стороні, чи використовувати її як інструмент угоди та вимагання викупу. Тривожним аспектом цього типу кіберзагрози є те, що хакери можуть залишатися непоміченими протягом тривалого проміжку часу;

Програми-вимагачі або зловмисне програмне забезпечення здебільшого заражають пристрої за допомогою вірусу-трояна або замаскованого вкладення, хоча деякі програми-вимагачі (наприклад, атаки WannaCry, Petya, NotPetya та інші) переміщуються між пристроями без взаємодії з користувачем. Постійна еволюція програм-вимагачів як послуги (Renin-Angiotensin-Aldosterone System, RaaS) означає, що академічні установи повинні захищатися від вимог кіберзлочинців, які погрожують розкрити конфіденційні дані студентів. Адже атаки програм-вимагачів і зловмисних програм спричиняють збій і перешкоджають користувачам отримати доступ до мережі або файлів. Інколи форми цієї загрози можуть призвести до того, що зловмисники тримають файли для викупу. Ця категорія кіберзагроз у секторі освіти є однією з найбільших і надалі активність програм-вимагачів стрімко зростає;

Фінансова вигода є мотивом хакерів для атак на навчальні заклади, особливо на приватні університети і коледжі через наявність у них численних студентських фінансових зборів. Студенти або батьки зазвичай оплачують навчання через онлайн-портали, часто переказуючи великі суми грошей на весь термін або рік навчання. Без належного захисту чи підготовки з боку навчальних закладів це є слабким місцем для перехоплення кіберзлочинцями;

Шпигунство. Якщо ЗВО є центром досліджень і володіє цінною інтелектуальною власністю, це може бути причиною шпигунства кіберзлочинів. Університети і коледжі мають бути належним чином захищені, щоб не стати жертвами хакерів. Інколи такі атаки замовляють і фінансують маючи професіонали відповідної галузі з метою отримання результатів інноваційних досліджень;

Фішинг. Фішингові шахрайства часто мають форму листів електронної пошти, їх мета змусити користувача довіритися джерелу в шахрайській спробі отримати доступ до їхніх облікових даних: персональних даних студентів, конфіденційних даних досліджень тощо. Цей тип атаки є найпоширенішою загрозою, з якою стикаються ЗВО під час віддаленого навчання та роботи з дому. Фішингові листи містять шкідливий програмний код, який може, наприклад, перенаправити користувача на шкідливий сайт. Під час пандемії хакери розробляють фішингові листи з такими ключовими словами, які психологічно спонукатимуть до перегляду такого повідомлення та виконання запропонованих дій щодо їх поширення і переходів за посиланнями. Тому важлива підвищена обізнаність щодо потенційних кіберзагроз. Усвідомлення цих загроз може

допомогти ЗВО та їхнім працівникам захистити себе та своїх студентів від цих уразливостей;

DDoS-атаки. Такий різновид атак є поширеним для освітніх закладів. Мотивом зловмисника є масштабне порушення роботи мереж і систем ЗВО і, як наслідок, неможливість виконувати свій повсякденний функціонал. Відмова вебсервера відбувається унаслідок розподіленої атаки, коли на нього з різних машин (ботнетів) за короткий проміжок часу надходить велика кількість запитів, що через перенавантаження уповільнює його і в решті решт робить недоступним для користувачів. Через недостатню захищеність університетських мереж і відносну легкість реалізації таких атак відомі випадки [12, 13], коли студенти або викладачі самі успішно проводили DDoS-атаки, наприклад, щоб мати вихідний чи то з інших особистих невдоволень;

Загрози, націлені на системи керування вмістом (Content Management System, CMS). Нині велика кількість вебсайтів закладів освіти створені засобами безплатних систем управління вмістом з відкритим кодом, найпоширенішими серед яких є WordPress, Joomla і Drupal. Оскільки більшість платформ CMS створені на основі відкритого вихідного коду, вони мають критичні вразливості безпеки і при цьому немає відповідального за своєчасний пошук і виправлення вразливостей безпеки. Зловмисники через виявлення вразливості в CMS можуть використовувати пошукову систему сайту, облікові дані та паролі користувачів. Так, від кібератаки 14.01.2022 постраждали понад 70 сайтів органів державної влади, а реалізувати кібератаку вдалося через а причиною цього стали вразливості системи керування вмістом вебсайтів CMS October, на якій були розроблені всі ці сайти [14]. Крім того, WordPress та інші платформи CMS використовують протокол під назвою "XML-RPC", який використовується для надання послуг, таких як pingback, trackbacks та віддалений доступ для користувачів [15]. Зловмисники можуть використовувати цей протокол для ініціювання DDoS-атак. Також через уразливості часто піддаються кібератакам численні плагіни і теми WordPress. Поширеними кібератаками на сайти, створені засобами CMS, є:

– *атаки грубої сили*: пошук логінів і паролів у систему методом перебору, адже переважно в таких системах користувачі нехтують застосуванням складних паролів, а WordPress не обмежує кількість некоректних спроб входу;

– *SQL ін'єкції*: відбуваються, коли значення в полях введення не очищені належним чином, що дозволяє потенційно виконувати будь-які запити SQL. Після успішної ін'єкції SQL зловмисник може отримати доступ або створити новий обліковий запис привілейованого користувача, який потім можна використовувати для входу та отримання повного доступу до вебсайту. Ін'єкції SQL також можна використовувати для вставлення нових даних у базу даних, зміни або видалення наявних даних;

– *міжсайтові сценарії (XSS)*: переважно використовуються для крадіжки файлів cookie сеансу користувача, що дозволяє зловмиснику впровадити на вебсторінку шкідливі сценарії, наприклад, збір даних або перенаправлення на інший шкідливий сайт;

– *DDoS атаки*: якщо вебсервер погано захищений, то такий різновид розподілених атак може реалізувати навіть кіберзлочинці-любителі;

– *експлойти долучення файлів*: трапляються, коли сайт дозволяє користувачеві надсилати дані у файли або завантажувати файли на сервер, якщо PHP-код не перевіряє введені дані. Розрізняють уразливості локального (LFI) і віддаленого долучення файлів (RFI). Уразливості LFI дозволяють зловмиснику читати, а іноді і виконувати файли на машині жертви. Якщо вебсервер неправильно налаштований або працює з високими привілеями, зловмисник може отримати доступ до конфіденційної інформації. Завдяки цій уразливості зловмисники можуть отримати доступ до файлів конфігурації на сервері;

– *обхід каталогів*: така HTTP-атака дозволяє зловмиснику отримати доступ до файлів, каталогів і команд за межами кореневого каталогу вебсервера, наприклад, переглядати файли з обмеженим доступом, що може надати зловмиснику більше інформації, необхідної для подальшої компрометації системи. Цю атаку ще називають "../" (дві крапки з косою рискою).

ВИСНОВКИ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Нині освітній сектор стикається з більш широким спектром проблем, ніж інші сектори, особливо внаслідок переходу до дистанційного та гібридного навчання. Реалізована у роботі класифікація загроз кібербезпеці в галузі освіти сприятиме чіткому їх розумінню і специфіки за тією чи іншою ознакою. Дослідження та аналіз ознак кіберзагроз в галузі освіти дозволив розділили їх за дев'ятьма критеріями: загрози на пристрої IoT, загрози через людський фактор, крадіжка персональних даних, програми-вимагачі або зловмисне програмне забезпечення, фінансова вигода, шпигунство, фішинг, DDoS-атаки, загрози на CMS. Знання основних загроз освітніх мереж і систем, розуміння поширених способів злому і витоків конфіденційних даних студентів, викладачів та інших співробітників дозволить вибрати й застосовувати навчальним закладам найбільш ефективні інструменти і стратегії на всіх рівнях кіберзахисту.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 Average cost of data breaches worldwide from 2014 to 2021. https://www.statista.com/statistics/987474/global-average-cost-data-breach/.
2 Трофименко, О. Г., Логінова, Н.І., Манаков, С. Ю., Янковський, О.Г. (2022). Кіберризики в освітньому секторі. *Сучасна спеціальна техніка,* 2 (69), 38-52. https://doi.org/10.36486/mst2411–3816.2022.2(69).2
3 Alert: Further ransomware attacks on the UK education sector by cyber criminals. https://www.ncsc.gov.uk/news/alert-targeted-ransomware-attacks-on-uk-education-sector.
4 Кіберризики: як розуміти та управляти. https://10guards.com/ua/articles/cyber-risks.
5 Geer, D., Jardine, E., Leverett, E. (2020). On market concentration and cybersecurity risk. *Journal of Cyber Policy*, 5, 1-21. https://doi.org/10.1080/23738871.2020.1728355. https://www.researchgate.net/publication/339459416_On_market_concentration_and_cybersecurity_risk.
6 Nurse, J., Creese, S., Goldsmith, M., Lamberts, K. (2011). Trustworthy and Effective Communication of Cybersecurity Risks: A Review. *Proceedings - 2011 1st Workshop on Socio-Technical Aspects in Security and Trust, STAST 2011*. https://doi.org/10.1109/STAST.2011.6059257.
7 Kadëna, E., Gupi, M. (2021). Human Factors in Cybersecurity: Risks and Impacts. *Security science journal*, 2, 51-64. https://doi.org/10.37458/ssj.2.2.3.
8 Задерейко, О.В., Трофименко, О.Г., Логінова, Н.І., Прокоп, Ю.В., Кухаренко, С.В. (2022). Захист даних користувачів в інформаційних системах. *Сучасна спеціальна техніка*, 1(70), 16-30. https //doi.org/10.36486/mst2411–3816.2022.1(68).2.
9 Rahman, M., Hamzah, M., Yasin, M., Tahar, M., Haron, Z., Ensimau, N. (2019). The UKM Students Perception towards Cyber Security. *Creative Education*, 10, 2850-2858. https://doi.org/10.4236/ce.2019.1012211.
10 Ulven, J., Wangen, G. (2021). A Systematic Review of CybersecurityRisks in Higher Education. *Future Internet*, 13, 39. https://doi.org/10.3390/fi13020039.
11 Internet of Things (IoT) Security Solutions. https://www.fortinet.com/solutions/enterprise-midsize-business/iot-solution.
12 Teenage hacker jailed for masterminding attacks on Sony and Microsoft. https://www.theguardian.com/technology/2017/apr/25/teenage-hacker-adam-mudd-jailed-masterminding-attacks-sony-microsoft.

13 Cybersecurity Considerations for Institutions of Higher Education. https://rems.ed.gov/docs/Cybersecurity_Considerations_for_Higher_ed_Fact_Sheet_508C.pdf
14 Тарасовський, Ю., Антонюк, Д., Сапітон, М. (2022). Хакери атакували українські урядові сайти. Можлива причина – вразливість у системі управління контентом. Forbes. https://web.archive.org/web/20220115001531/https://forbes.ua/news/khakeri-v-atakuvali-ukrainski-uryadovi-sayti-ne-pratsyuyut-sayti-minoboroni-mzs-dsns-dii-14012022-3212.
15 CMS Vulnerabilities: Why are CMS platforms common hacking targets? https://beaglesecurity.com/blog/article/cms-vulnerabilities.html.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (16), 2022
ISSN 2663 - 4023

Trofymenko Olena,
PhD, Associate Professor, Associate Professor at the Department of Information Technologies of the National University "Odessa Law Academy", Odesa, Ukraine,
ORCID ID: 0000-0001-7626-0886
trofymenko@onua.edu.ua

Loginova Nataliia,
PhD, Associate Professor, Head of the Department of Information Technologies of the National University "Odessa Law Academy", Odesa, Ukraine,
ORCID ID 0000-0002-9475-6188
loginova@onua.edu.ua

Manakov Serhii,
PhD, Associate Professor at the Department of Information Technologies of the National University "Odessa Law Academy", Odesa, Ukraine,
ORCID ID 0000-0001-5930-4592
s.manakov@meta.ua

Dubovoi1 Yaroslav
master in cybersecurity, the National University "Odessa Law Academy", Odesa, Ukraine,
ORCID ID 0000-0002-3987-9409
dubovoy97@gmail.com

CYBERTHREATS IN HIGHER EDUCATION

Abstract. As a result of the transition to distance and hybrid learning, first due to the COVID-19 pandemic and then due to the Russian attack and large-scale war, the education sector has faced a wide range of cyber threats. Awareness of these threats can help universities and their staff protect themselves and their students from these vulnerabilities. Large amounts of personal data and financial information about students, faculty and staff, as well as information about research circulate in higher education institutions. It makes them an attractive target for cybercriminals. The article analyzes cyber threats in the higher education sector. The classification of the most common cyber threats in the higher education sector is offered. The basis of most successfully implemented cyber attacks is the human factor, ie the mistakes of staff or students due to ignorance or disregard for the basic rules of cyber hygiene. A study of the signs of cyber threats in the field of education made it possible to divide them according to nine criteria: threats to IoT devices, threats due to human factors, identity theft, ransomware or malicious software, financial gain, espionage, phishing, DDoS attacks, threats to CMS. The implemented classification of cybersecurity threats in the field of higher education will contribute to their clear understanding and specifics on one or another basis. Knowledge of the main threats to educational networks and systems, understanding of common ways of hacking and leaking confidential data of students, teachers and other staff will allow educational institutions to choose and apply the most effective tools and strategies at all levels of cybersecurity. Cybersecurity is a shared responsibility for everyone, and its success depends on being aware of the motives and methods of attackers, maintaining good cyber hygiene by everyone, and monitoring compliance.

Keywords: cyber risks; cyber vulnerabilities; cyberthreat; cyberattack; cyber defense; cybersecurity; educational sector.

REFERENCES (TRANSLATEDAND TRANSLITERATED)

1 Average cost of data breaches worldwide from 2014 to 2021. https://www.statista.com/statistics/987474/global-average-cost-data-breach/.
2 Trofymenko, O., Loginova, N., Manakov, S., Iankovskii, O. (2022). Cyber risks in the education sector. Modern Special Technics, 2 (69), 38-52. https://doi.org/10.36486/mst2411–3816.2022.2(69).2
3 Alert: Further ransomware attacks on the UK education sector by cyber criminals. https://www.ncsc.gov.uk/news/alert-targeted-ransomware-attacks-on-uk-education-sector.

4 Cyber risks management. https://10guards.com/ua/articles/cyber-risks.
5 Geer, D., Jardine, E., Leverett, E. (2020). On market concentration and cybersecurity risk. *Journal of Cyber Policy*, 5, 1-21. https://doi.org/10.1080/23738871.2020.1728355. https://www.researchgate.net/publication/339459416_On_market_concentration_and_cybersecurity_risk.
6 Nurse, J., Creese, S., Goldsmith, M., Lamberts, K. (2011). Trustworthy and Effective Communication of Cybersecurity Risks: A Review. *Proceedings - 2011 1st Workshop on Socio-Technical Aspects in Security and Trust, STAST 2011*. https://doi.org/10.1109/STAST.2011.6059257.
7 Kadëna, E., Gupi, M. (2021). Human Factors in Cybersecurity: Risks and Impacts. *Security science journal*, 2, 51-64. https://doi.org/10.37458/ssj.2.2.3.
8 Zadereyko, A., Trofymenko, O., Loginova, N., Prokop, Y., Kuharenko, S. (2022). Protection of user data in information systems. *Modern Special Technics*, 1(70), 16-30. https://doi.org/10.36486/mst2411–3816.2022.1(68).2.
9 Rahman, M., Hamzah, M., Yasin, M., Tahar, M., Haron, Z., Ensimau, N. (2019). The UKM Students Perception towards Cyber Security. *Creative Education*, 10, 2850-2858. https://doi.org/10.4236/ce.2019.1012211.
10 Ulven, J., Wangen, G. (2021). A Systematic Review of CybersecurityRisks in Higher Education. *Future Internet*, 13, 39. https://doi.org/10.3390/fi13020039.
11 Internet of Things (IoT) Security Solutions. https://www.fortinet.com/solutions/enterprise-midsize-business/iot-solution.
12 Teenage hacker jailed for masterminding attacks on Sony and Microsoft. https://www.theguardian.com/technology/2017/apr/25/teenage-hacker-adam-mudd-jailed-masterminding-attacks-sony-microsoft.
13 Cybersecurity Considerations for Institutions of Higher Education. https://rems.ed.gov/docs/Cybersecurity_Considerations_for_Higher_ed_Fact_Sheet_508C.pdf
14 Tarasovsky, Yu., Antonyuk, D., Sapiton, M. (2022). Hackers attacked Ukrainian government sites. A possible reason is a vulnerability in the content management system. Forbes. https://web.archive.org/web/20220115001531/https://forbes.ua/news/khakeri-v-atakuvali-ukrainski-uryadovi-sayti-ne-pratsyuyut-sayti-minoboroni-mzs-dsns-dii-14012022-3212.
15 CMS Vulnerabilities: Why are CMS platforms common hacking targets? https://beaglesecurity.com/blog/article/cms-vulnerabilities.html.