УДК 004.056:(37+001)

Іван Голуб,
науковий співробітник
відділу цифрових освітніх ресурсів
Інституту професійної освіти НАПН України,
https://orcid.org/0000-0001-9008-6255

ОСНОВНІ АКТИВИ ТА ТИПОВІ ЗАГРОЗИ КІБЕРЗАХИСТУ НАУКОВИХ УСТАНОВ ТА ЗАКЛАДІВ ОСВІТИ

Анотація: У статті розглянуто ключові аспекти кібербезпеки в науково-освітній сфері, що є об'єктом інтенсивного оброблення, зберігання та передавання значних обсягів інформації. Визначено основні цифрові активи, що потребують захисту, зокрема результати досліджень, персональні дані, освітні платформи та внутрішні інформаційні системи. Проаналізовано типові кіберзагрози, такі як крадіжка даних, кібершпигунство, саботаж досліджень, DDoS-атаки на освітні платформи та дезінформаційні кампанії. У статті наголошується на унікальному виклику для цих установ: необхідності збалансувати відкритість для наукової комунікації з потребою в конфіденційності та контролі доступу.

Ключові слова: кіберзахист, наукові та освітні установи, кіберзагрози, цифрові активи, інтелектуальна власність.

CYBERSECURITY OF SCIENTIFIC AND EDUCATIONAL INSTITUTIONS: KEY ASSETS AND TYPICAL THREATS

Ivan Golub,
Researcher of Department of Digital Educational Resources,
The Institute of Vocational Education of the
National Academy of Educational Sciences of Ukraine

Abstract: The article examines the key aspects of cybersecurity in the scientific and educational sector, which involves the intensive processing, storage, and transmission of valuable information. It identifies the main digital assets requiring protection, including research results, personal data, educational platforms, and internal information systems. Typical cyber threats are analyzed, such as data theft, cyber-espionage, research sabotage, DDoS attacks on educational platforms, and disinformation campaigns. The article emphasizes the unique challenge for these institutions: the need to

balance openness for scientific communication with the need for confidentiality and access control.

Keywords: cybersecurity, scientific and educational institutions, cyber threats, digital assets, intellectual property.

Наукові установи та заклади освіти є не лише осередком, де основним видом діяльності є наукова та освітня діяльність, а середовищем інтенсивного опрацювання, зберігання та передавання значних обсягів даних, що мають стратегічну, фінансову або інтелектуальну цінність. З огляду на вказане вище, їх кіберзахист потребує особливого підходу з урахуванням специфіки цифрових активів, відкритості академічного середовища та постійної взаємодії з зовнішніми платформами.

До ключових цифрових активів наукових установ та закладів освіти, які підлягають захисту, належать:

результати досліджень і наукові дані, включаючи бази експериментальних даних, наукові публікації, інші види інтелектуальної власності, патентна інформація;

персональні дані наукових співробітників, студентів, викладачів, дослідників, включно з інформацією про освіту, місце проживання, платіжні реквізити та ін.;

освітні платформи та онлайн системи управління навчанням (LMS), зокрема Moodle, Google Classroom, Zoom, Microsoft Teams;

корпоративна пошта, документообіг та внутрішні інформаційні системи;

вебмережі для співпраці та обміну з міжнародними партнерами.

Унікальною особливістю науково-освітнього простору є постійне балансування між відкритістю для наукової комунікації та потребою в конфіденційності та контролі доступу.

У сучасних умовах найбільш поширеними кіберзагрозами для закладів освіти та наукових установ є:

крадіжка або витік даних – атаки з метою викрадення наукових результатів, персональних даних або конфіденційної інформації, що часто пов’язані з фішингом, зараженням шкідливим ПЗ або компрометацією облікових записів;

кібершпигунство – цілеспрямоване проникнення у мережі наукових установ задля отримання інтелектуальної власності, доступу до технологічних розробок, у тому числі в оборонній або біотехнологічній сферах;

зрив або саботаж досліджень – внесення змін у наукові дані, видалення або шифрування архівів (наприклад, з використанням

ransomware), що призводить до втрати результатів багаторічних досліджень;

атаки на освітні платформи та IT-інфраструктуру – DDoS-атаки (Distributed Denial of Service), масові збої в роботі систем дистанційного навчання, несанкціоноване втручання в роботу електронного журналу, бази дисертацій, дипломів, сертифікатів та ін.;

дезінформація та маніпуляції у цифровому середовищі – поширення фальшивих даних від імені закладу, створення підроблених сторінок або листування, маніпуляції результатами академічної діяльності. Мета – підірвати довіру до інституції або викликати паніку серед студентів і викладачів (табл. 1.).

Таблиця 1.

Типові кіберзагрози для наукових та освітніх установ: наслідки і засоби протидії

Кіберзагроза	**Типові наслідки**	**Засоби протидії**
Крадіжка даних	Витік персональної або наукової інформації, порушення конфіденційності	Шифрування даних, багатофакторна автентифікація, контроль доступу, журналювання подій
Несанкціонований доступ	Крадіжка або підміна наукових даних	Управління доступом, моніторинг логів
Кібершпигунство	Втрата інтелектуальної власності, витік стратегічної інформації	Мережева сегментація, аналіз поведінки користувачів (UEBA), система виявлення вторгнень (IDS / IPS)
Зрив досліджень (sabotage)	Втрата результатів, переривання експериментів, неможливість відновлення архівів	Регулярне резервне копіювання, контроль версій, використання ізольованих середовищ
DDoS-атаки на освітні платформи	Блокування доступу до дистанційного навчання, зрив іспитів, зниження довіри, виведення сайтів з ладу	Використання CDN, систем виявлення аномалій, договір з провайдером на фільтрацію трафіку. Захист на рівні хостингу, WAF
Атаки на освітні платформи	Порушення навчального процесу, втрати оцінок	Резервне копіювання, шифрування, оновлення CMS
Фішинг	Компрометація облікових записів. Отримання несанкціонованого доступу, викрадення даних користувачів	Навчання персоналу, впровадження антифішингових фільтрів, автентифікація за двома факторами (2FA)

Дезінформаційні кампанії	Паніка, репутаційні втрати, маніпуляції у ЗМІ чи соцмережах	Моніторинг соціальних мереж, офіційні канали комунікації, інформаційна політика
Компрометація e-mail	Витік внутрішньої інформації, дезінформація	SPF, DKIM, DMARC, цифрові підписи
Публікація фейкової інформації	Підрив довіри, дестабілізація інфопростору	Контент-модерація, інформаційна політика

Європейський досвід кіберзахисту в освітньо-науковій сфері передбачає комплексний підхід до кіберзахисту, що поєднує високий рівень технічної безпеки, гнучкість доступу та освітню складову для здобувачв освіти та співробітників.

У документі «A Europe Fit for the Digital Age – Commission proposes new cybersecurity and digital resilience measures» (2025) Єврокомісія наголошує на потребі посилення цифрової безпеки та стійкості до кібератак в межах ініціативи «Європа, готова до цифрового майбутнього». Основні акценти зроблені на:

пропозиції щодо посилення Мережі центрів оперативного реагування на кіберінциденти за участю CSIRTs (Computer Security Incident Response Teams) у державах-членах ЄС;

створенні Центру з кіберзахисту та кризового реагування для швидкої координації між країнами в разі масштабних кібератак;

розширенні дії Директиви NIS (Network and Information Security) (2016; 2022), яка включає нові обов'язки з кібербезпеки для більшого кола секторів, зокрема освіти, науки, енергетики, охорони здоров'я;

забезпеченні кіберстійкості цифрових продуктів і хмарних рішень;

впровадженні механізмів перевірки та сертифікації цифрових послуг і технологій.

Такі ініціативи мають безпосередньо впливають на кіберзахист наукових установ та освітніх закладів, оскільки:

вони все частіше стають мішенню для кібератак, особливо в галузях досліджень, пов'язаних з обороною, біотехнологіями, штучним інтелектом та ін.;

розширення дії Директиви NIS передбачає, що закладам освіти та дослідницьким інституціям, в перспективі, необхідно впроваджувати стандартизовані практики кібербезпеки (ризик-менеджмент, аудит, звітність, інцидент-реагування) (2016; 2022);

координація через CSIRTs дає змогу отримувати попередження, ділитися інформацією та швидше реагувати на загрози;

сертифікація цифрових сервісів, що використовуються для зберігання чи обробки дослідницьких даних (наприклад, хмарних платформ), зміцнює довіру до захищеності таких середовищ;

участь у загальноєвропейській екосистемі кіберзахисту відкриває доступ до фінансування, інструментів і стратегічного партнерства.

Підсумовуючи їхні рекомендації можемо резюмувати, що кіберзахист у науково-освітньому середовищі повинен поєднувати:

високий рівень організації технічної безпеки (мережевий захист, шифрування, двофакторна автентифікація);

гнучкість доступу для користувачів (науковців, студентів, викладачів);

відкритість до зовнішніх наукових співпраць, що передбачає ретельне управління правами доступу та постійний моніторинг активності.

Активне розроблення рекомендацій з цифрової безпеки не зупиняється та розвивається. Важливим компонентом впровадження заходів з кібербезпеки є навчання студентів, викладачів, наукових працівників та персоналу правилам кібергігієни, етичним аспектам безпеки в мережі та проведення на практиці навчальних симуляцій кібератак (Red Team / Blue Team) (2016; 2022). З огляду на що, доцільним вважаємо введення в освітню складову підготовки здобувачів освіти дисциплін з основ кібербезпеки.

Список посилань

European Commission. (2025). A Europe fit for the digital age – Commission proposes new cybersecurity and digital resilience measures (Press Release IP/25/907). https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_25_907/IP_25_907_EN.pdf

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, 2016 O.J. (L 194) 1. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016L1148

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, 2022 O.J. (L 333) 80. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555