УДК 004.056: 351.718.37

Шестак Ярослав Іванович
доктор філософії, доцент кафедри інженерії програмного забезпечення та кібербезпеки, Державний торговельно-економічний університет, Україна
ORCID: https://orcid.org/0000-0002-5102-9642
E-mail: shestack@knute.edu.ua

Цюцюра Світлана Володимирівна
доктор технічних наук, професор, професор кафедри інженерії програмного забезпечення та кібербезпеки,
Державний торговельно-економічний університет, Україна
ORCID: https://orcid.org/0000-0002-4270-7405
E-mail: svtsutsura@dteu.edu.ua

Криворучко Олена Володимирівна
доктор технічних наук, професор, професор кафедри комп'ютерних систем, мереж та кібербезпеки,
Національний університет біоресурсів і природокористування України
ORCID: https://orcid.org/0000-0002-7661-9227
E-mail: o.kryvoruchko@nubip.edu.ua

Лахно Валерій Анатолійович
доктор технічних наук, професор, професор кафедри комп'ютерних систем, мереж та кібербезпеки,
Національний університет біоресурсів і природокористування України
ORCID: http://orcid.org/0000-0001-9695-4543
E-mail: lva964@nubip.edu.ua

Касаткін Дмитро Юрійович
кандидат педагогічних наук, доцент, завідувач кафедри комп'ютерних систем, мереж та кібербезпеки,
Національний університет біоресурсів і природокористування України
ORCID: https://orcid.org/0000-0002-2642-8908
E-mail: d.kasatkin@nubip.edu.ua

КІБЕРСТІЙКІСТЬ ЗАКЛАДІВ ВИЩОЇ ОСВІТИ УКРАЇНИ В УМОВАХ ВОЄННОГО СТАНУ

***Анотація**. У статті досліджується проблема забезпечення кіберстійкості закладів вищої освіти (ЗВО) шляхом розроблення та впровадження комплексної архітектури кіберзахисту. Показано, що ефективність такої системи визначається здатністю інтегрувати освітні, адміністративні та ресурсні підсистеми, враховуючи їх взаємозалежність і специфіку функціонування. Розглянуто основні ризики та наслідки кібератак. Окреслено принципи побудови захищеної інформаційної інфраструктури й критерії, яким має відповідати надійна й ефективна система кібербезпеки ЗВО. Запропоновано модель управління інформаційними потоками ЗВО та ресурсами із застосуванням нейромережевих технологій та інтелектуальних систем підтримки рішень. Результати дослідження демонструють доцільність використання інструментів моделювання для прогнозування загроз, оптимізації розподілу ресурсів і підвищення стійкості освітнього середовища до кіберризиків.*

***Ключові слова**: кіберзахист, інформаційна інфраструктура, траєкторії розвитку, системи кіберзахисту, кіберстійкість інфраструктури, нейромережеві технології, комунікаційні мережі.*

Актуальність. В умовах воєнного стану діяльність закладів вищої освіти (ЗВО) неможлива без надійної та ефективної системи кібербезпеки. Вона забезпечує безперервність

DOI:/10.31548/itees.2025.01.058
ISSN 3083-7502

освітнього процесу, захист конфіденційних даних і стійкість інформаційної інфраструктури до зростаючого спектра кіберзагроз. Система кіберзахисту ЗВО поєднує організаційні, технічні та аналітичні заходи, спрямовані на виявлення вразливостей, запобігання атакам та мінімізацію наслідків інцидентів. Її розвиток регламентується положеннями національної стратегії кібербезпеки України та міжнародними стандартами. Інформаційна інфраструктура ЗВО є складною функціональною системою. Вона включає освітні, адміністративні та ресурсні компоненти. Її стійке функціонування визначається ефективною взаємодією всіх підсистем, застосуванням релевантних протоколів захисту та впровадженням релевантних архітектур безпеки. Саме тому в статті запропоновано модель управління інформаційними потоками ЗВО та ресурсами із застосуванням нейромережевих технологій та інтелектуальних систем підтримки рішень.

Аналіз останніх досліджень та публікацій. Різні дослідники по-різному підходили до вивчення проблематики кіберзахисту у ЗВО, зокрема в аспекті впровадження та використання технологій і систем захисту. Цим питанням присвячені праці А. Андрощука, В. Афанасьєва, В. Григи, С. Іванової, О. Дубача, О. Косенка, М. Шишкіної, Ю. Носенка, Л. Забродської, В. Кременя, Б. Одягайла, П. Орлова, Л. Фішмана, С. Лондаря, О. Бринюка, С. Дворецької, О. Шпака, В. Лужецького, О. Білика та інших науковців.

У процесі синтезу ефективної системи кіберзахисту інформаційної інфраструктури ЗВО ключове значення має використання методів моделювання, які дають можливість відобразити складні інформаційні процеси, оцінити потенційні загрози та спрогнозувати наслідки впровадження новітніх технологій. Зокрема, цікавим є підхід, запропонований А. Прусом [1, с. 58–59], який розглядає математичне моделювання як «лінзу реального світу» та виділяє чотири групи компетенцій, які визначають якість цього процесу.

Перша група стосується глибокого розуміння проблеми, формування реалістичних припущень і відокремлення релевантної інформації від другорядної. Це необхідно для аналізу актуальних кіберзагроз. Друга передбачає побудову математичної моделі, спрощення складних процесів і застосування візуалізації для відображення архітектури інфраструктури та її вразливостей. Третя група компетенцій орієнтована на інтерпретацію результатів моделювання у реальних умовах функціонування ЗВО. Четверта - на перевірку адекватності моделі, її гнучкість і здатність адаптуватися до змін кіберсередовища.

Отже, використання моделювання у сфері кіберзахисту ЗВО варто розглядати не лише як технічний інструмент, а як комплексну компетентнісну діяльність, що охоплює етапи аналізу, формалізації, інтерпретації та критичного осмислення результатів.

Мета дослідження. Впровадження інтелектуальних систем у внутрішню інфраструктуру ЗВО відкриває можливості для глибокої трансформації процесів управління ресурсами, організації навчального процесу та обслуговування користувачів. Завдяки застосуванню багаторівневої автентифікації, персоналізованого доступу до сервісів і постійному збору аналітичних даних формується динамічне цифрове середовище, яке здатне адаптуватися до індивідуальних потреб кожного учасника освітнього процесу – викладача чи адміністративного працівника.

Матеріали і методи дослідження. Інформаційна інфраструктура ЗВО включає сукупність інформаційних систем, засобів комунікації, користувачів, баз даних, серверів, шлюзів та систем контролю доступу. Для підвищення її стійкості можуть використовуватися сучасні криптографічні протоколи (AES-256, SSL/TLS), які зменшують ризики кібератак. Водночас стабільність функціонування вимагає постійного моніторингу стану систем, регулярної перевірки вразливостей, своєчасного оновлення захисних механізмів, а також дотримання правил кібергігієни. Серед ключових практик - зміна й генерація надійних паролів, своєчасне блокування підозрілих користувачів, повідомлення про спроби несанкціонованого доступу, аналіз інцидентів і прогнозування їх наслідків.

Для підсилення зазначених процесів дедалі частіше застосовуються інструменти штучного інтелекту. Вони дозволяють здійснювати глибокий аналіз даних, створювати прототипи можливих кібернападів і прогнозувати їх наслідки за допомогою нейромережевих

технологій. Це відкриває перспективи для побудови адаптивних систем кіберзахисту, здатних до самонавчання та оперативного реагування на нові загрози.

Результати дослідження та їх обговорення.

Організаційні підходи до захисту інформаційної інфраструктури закладу вищої освіти. Для забезпечення високої якості освітніх послуг, проведення наукових досліджень, ефективного управління та збереження конкурентоспроможності на ринку, ЗВО мають гарантувати викладачам, дослідникам, співробітникам і здобувачами вищої освіти (далі ЗдВос) надійний та безперервний доступ до власного цифрового середовища. Це середовище формується інформаційною інфраструктурою, яка охоплює цифрові платформи, комунікаційні мережі, системи обробки та передавання даних, а також засоби кіберзахисту.

Водночас цілісність функціонування ЗВО та рівень довіри з боку всіх зацікавлених сторін безпосередньо залежать від здатності університету забезпечити кібербезпеку, конфіденційність інформації та стійкість до кібератак. Саме тому концепція кіберстійкості набула статусу стратегічного пріоритету для ЗВО.

Підтримання безперервності, надійності й безпеки академічних та адміністративних процесів зумовлює зростаючу залежність ЗВО від комплексних інформаційних інфраструктур. Вони включають адміністративні, освітні та ресурсні системи. Водночас така залежність підвищує рівень вразливості до широкого спектра кіберзагроз. Тому першочерговим завданням є ідентифікація та класифікація стрижневих елементів цифрового середовища, що дозволить розробити гнучкі та ефективні заходи кіберзахисту.

У таблиці 1 наведено основні компоненти інформаційної інфраструктури ЗВО.

Таблиця 1 – основні компоненти інформаційної інфраструктури ЗВО

Категорія систем	Приклади компонентів	Основні функції
Ресурсні системи	Сервери, сховища даних, мережеві шлюзи, системи резервного копіювання, хмарні сервіси.	Забезпечення обробки, зберігання та захисту даних; підтримка обчислювальних ресурсів і комунікаційних сервісів.
Адміністративні системи	Системи управління документообігом, кадрові та фінансові системи, електронний деканат, інформаційні портали для співробітників.	Підтримка управлінських і організаційних процесів, доступ до адміністративної інформації, автоматизація внутрішніх процедур.
Освітні системи	Системи дистанційного навчання (LMS), електронні бібліотеки, платформи відеоконференцій, наукові бази даних, репозитарії.	Підтримка навчального процесу та досліджень, забезпечення доступу до освітніх ресурсів, організація взаємодії між викладачами та ЗдВос.

Дослідження [2–4] свідчать, що у 2024 році ЗВО стали однією з основних цілей кіберзлочинців. Так 66% опитаних представників повідомили про кібератаки, а 79% зазнали щонайменше одного інциденту. Хоча витік даних траплявся рідше (лише 18% ЗВО офіційно підтвердили такі випадки), загальний вплив атак виявився значним і у багатьох випадках критичним. Найсерйознішою загрозою залишається програмне забезпечення-вимагач: більшість постраждалих університетів сплачували до 122% від початкових вимог зловмисників, а середній розмір викупу сягав 5,85 млн доларів США, що є третім за величиною показником серед усіх галузей економіки. Крім того, половина закладів відзначила прямі пошкодження своєї ІКТ-інфраструктури, понад 60% зазнали серйозних операційних і фінансових перебоїв. У 77% випадків дані були зашифровані, а у 95% – зловмисники намагалися отримати доступ до резервних копій, що значно ускладнювало відновлення [2–4].

DOI:/10.31548/itees.2025.01.058
ISSN 3083-7502

В умовах таких викликів постає необхідність чітко визначити принципи, на яких повинна базуватися комплексна система кібербезпеки ЗВО, здатна забезпечити всебічний захист ресурсів та інфраструктури. До головних належать [5, с. 140–142]: принцип конфіденційності; принцип цілісності; принцип доступності даних та ресурсів для уповноважених користувачів у потрібний час; принцип постійного моніторингу та оцінювання ефективності системи; принцип дотримання законодавчих норм; принцип підзвітності дій у цифровому середовищі; принцип управління ризиками; принцип підвищення обізнаності користувачів; принцип адаптивної архітектури безпеки; концепція «нульової довіри»; принцип стійкості інформаційних систем; принцип суверенітету даних; а також принцип інтегрованого аналізу внутрішніх і зовнішніх загроз для проактивного реагування.

Отже, архітектура системи кібербезпеки ЗВО має розглядатися як цілісний набір правил, інструментів, процедур і механізмів контролю, що діють у комплексі для захисту інформаційних активів від кібератак. Вона визначає дизайн, методи впровадження, взаємозв'язки та управління компонентами захисту, забезпечуючи доступність, конфіденційність, цілісність і стійкість адміністративних, ресурсних та освітніх систем. Комплексна архітектура кіберзахисту ЗВО повинна відповідати академічній місії та стратегічним цілям цифрової трансформації; ґрунтуватися на ризик-орієнтованому підході з регулярними оцінками ризиків і моделюванням загроз; включати багаторівневі засоби захисту для мережі, кінцевих пристроїв, застосунків і даних; відповідати національним та міжнародним стандартам; бути масштабованою.

Крім того, така система має передбачати інтеграцію SIEM-рішень і аналітичних інструментів для автоматизованого виявлення та реагування на загрози у реальному часі, підтримувати механізми резервування й аварійного відновлення, а також забезпечувати сувору автентифікацію користувачів і пристроїв. Не менш визначальною є інтеграція внутрішніх та зовнішніх джерел даних кіберрозвідки, регулярний аудит і перевірка відповідності, чіткий розподіл ролей та відповідальності. Нарешті, система повинна гарантувати суверенітет даних закладу, зберігаючи їх конфіденційність і водночас підтримуючи безпечний обмін інформацією, командну роботу та наукові дослідження.

Процес формування комплексної системи кібербезпеки ЗВО передбачає послідовне проходження низки етапів, кожен з яких має власні завдання та очікувані результати.

1) *Попередня оцінка та стратегічне планування.* На цьому етапі здійснюється початкове розуміння поточного рівня кіберзахисту ЗВО та визначаються стратегічні орієнтири для побудови архітектури. До пріоритетних завдань належать: класифікація критичних компонентів інформаційної інфраструктури (освітні, адміністративні та ресурсні системи), аналіз чинних політик і технологій захисту, вивчення нормативних вимог, а також визначення цілей кібербезпеки відповідно до місії та цифрової стратегії університету. Реалізація цього етапу часто ускладнюється недостатньою підтримкою з боку керівництва, відсутністю повного реєстру цифрових активів, фрагментованістю системи управління, обмеженими ресурсами, слабкою обізнаністю щодо регуляторних норм, а також відсутністю офіційної системи управління кібербезпекою.

2) *Оцінка ризиків та моделювання загроз.* Метою цього етапу є ідентифікація, аналіз і пріоритезація потенційних кіберзагроз та вразливостей, властивих середовищу ЗВО. Основні завдання включають: проведення комплексної оцінки ризиків для всіх систем університету, розроблення моделі внутрішніх і зовнішніх загроз, визначення ймовірності та наслідків можливих інцидентів, виявлення зон підвищеної небезпеки й формування реєстру ризиків. Серед чинників, що ускладнюють цей процес, варто відзначити відсутність стандартизованих методик аналізу ризиків, недостатнє документування попередніх інцидентів, слабке врахування специфічних для освіти кіберзагроз, занижену увагу до внутрішніх ризиків, залежність від застарілих моделей, а також обмежений доступ до даних у режимі реального часу.

3) *Архітектурне проєктування та створення «каркасу» системи.* Цей етап передбачає розроблення багаторівневої та структурованої системи кіберзахисту, яка визначає як

функціональні, так і технічні компоненти безпеки. До центральних завдань належать: проєктування багаторівневої моделі захисту (мережевої, програмної, даних, ідентифікації та кінцевих точок), визначення доменів безпеки та політик доступу, інтеграція основних безпекових технологій, застосування базових принципів захисту, а також забезпечення відповідності міжнародним стандартам і кращим практикам. Виконання цього етапу може бути ускладнене дефіцитом фахівців із архітектурного проєктування систем безпеки, недостатнім залученням зацікавлених сторін, нечіткістю у розмежуванні прав доступу, залежністю від одного постачальника технологій, відсутністю належної документації, а також неврахуванням перспектив масштабування та модульності архітектури.

4) *Впровадження та інтеграція.* На цьому етапі здійснюється практичне розгортання інструментів і політик кібербезпеки відповідно до затвердженої архітектури та інституційних вимог. Основні завдання включають закупівлю, налаштування та інтеграцію технологічних рішень, впровадження систем управління ідентифікацією та доступом, застосування механізмів шифрування, автентифікації, моніторингу та захисту кінцевих точок, а також встановлення протоколів реагування на інциденти та резервного копіювання. Суттєвим є також узгодження дій між усіма підрозділами університету. Основні виклики цього етапу пов’язані з операційними перебоями у навчальних та адміністративних процесах, недостатньою координацією між ІТ-персоналом і підрозділами ЗВО, проблемами сумісності нових і застарілих систем, неповною конфігурацією інструментів безпеки, затримками у закупівлях, недостатнім тестуванням перед впровадженням та відсутністю стратегії управління системними змінами.

5) *Тестування, перевірка та оптимізація.* Мета цього етапу – оцінити функціональність, надійність та ефективність впровадженої архітектури кібербезпеки. До основних завдань належать проведення тестувань на проникнення, аудитів безпеки, перевірка відповідності внутрішнім політикам і зовнішнім стандартам, аналіз журналів інцидентів, оцінювання поведінки системи в умовах навантаження, виявлення слабких місць і оптимізація конфігурацій. Виконання цього етапу може ускладнюватися обмеженими ресурсами для повномасштабного тестування, небажанням планувати простої в навчальний час, відсутністю чітких показників ефективності, використанням застарілих інструментів моніторингу, низькою готовністю до впровадження змін за результатами перевірки та недостатнім залученням незалежних аудиторів.

6) *Навчання та підвищення обізнаності користувачів***.** Завдання цього етапу полягає у формуванні культури кібергігієни шляхом систематичного навчання персоналу, далі ЗдВос та адміністраторів правилам безпеки й відповідальності у цифровому середовищі. Реалізація включає організацію тренінгів, підготовку інструкцій і політик у доступних форматах, заохочення повідомлень про підозрілу активність. Основні труднощі пов’язані з низькою мотивацією до участі у тренінгах, використанням застарілих або одноразових програм навчання, слабкою інтеграцією знань у корпоративну культуру, відсутністю системного контролю дотримання політик безпеки та механізмів зворотного зв’язку для оцінювання ефективності навчання.

7) *Безперервний моніторинг та управління життєвим циклом.* Цей етап спрямований на підтримання постійної ефективності, стійкості й адаптивності архітектури кібербезпеки. Він включає використання інструментів безперервного моніторингу, оновлення політик та баз знань про загрози, регулярний перегляд архітектури з урахуванням нових ризиків і змін в інституційному середовищі, проведення аудитів і перевірок відповідності. Основними проблемами можуть бути обмежена видимість мережевої активності в реальному часі, недостатня інтеграція з системами виявлення загроз, дефіцит ресурсів для оновлення інфраструктури, надмірна залежність від ручного моніторингу, затримки у реагуванні на інциденти, фрагментарність систем нагляду та відсутність регулярних аудитів безпеки.

Тоді модель оцінки рівня кіберстійкості ЗВО подамо багатокритеріальну оптимізацію. Нехай

x$\in X \subseteq R^m$ – вектор рішень (конфігурація системи кіберзахисту),

DOI:/10.31548/itees.2025.01.058
ISSN 3083-7502

$F1(x)$ – рівень надійності (ймовірність відбиття атаки, max),
$F2(x)$ – продуктивність системи (час відгуку, max),
$F3(x)$ – вартість впровадження та обслуговування (min),
$F4(x)$ – масштабованість та гнучкість (max).
Задача:

$$\max_{x \in X} \left(F1(x), F2(x), F3(x), \quad \min_{x \in X} F4(x) \right). \tag{1}$$

Розв'язки оцінюються за принципом Парето-оптимальності:

$$x \in X, \nexists y \in X : F(y) \succ F(x^*). \tag{2}$$

Тобто, формалізуючи задачу кіберстійкості ЗВО, доцільно розглядати її як багатокритеріальну оптимізацію, де одночасно враховуються показники надійності, продуктивності, вартості та масштабованості. У цьому випадку оптимальними є такі конфігурації архітектури кіберзахисту, які належать до множини Парето-ефективних рішень, що дозволяє збалансувати суперечливі вимоги різних груп користувачів і обмеження ресурсів.

Моделювання інформаційної інфраструктури ЗВО

Одним із головних викликів у створенні ефективної системи кіберзахисту ЗВО є відсутність уніфікованих стандартів щодо структурування даних. Кожен заклад має власну специфіку, внутрішні правила й регламентовані процедури, що потребує використання додаткових інтерфейсів, запитів і засобів комунікації для забезпечення взаємодії між підсистемами та контрольованого доступу до ресурсів. Сучасні засоби передавання інформації вже функціонують у межах протоколів безпеки, проте цього недостатньо для забезпечення комплексної кіберстійкості.

У моделюванні систем кіберзахисту слід враховувати, що стійкість інформаційних ресурсів до атак, несанкціонованого доступу чи руйнування є визначальним критерієм їхньої надійності. Це потребує визначення організаційних заходів безпеки, проєктування захищених каналів зв'язку, обов'язкової автентифікації користувачів, а у випадках підвищеного ризику – багатофакторної ідентифікації (SMS, мобільні застосунки, електронні ключі, КЕП, біометричні дані тощо). Важливим інструментом підвищення кіберстійкості є впровадження ефективних криптографічних протоколів (AES-256, SSL/TLS), однак навіть вони не гарантують ефективності без постійного моніторингу, своєчасного оновлення захисних механізмів, аналізу інцидентів та впровадження заходів реагування.

Провідну роль у цьому процесі відіграють інструменти штучного інтелекту, які дозволяють моделювати прототипи кібератак, прогнозувати їх наслідки та формувати гнучкі механізми реагування. Використання нейромережевих технологій розширює можливості класичного моделювання, що узгоджується з концепцією моделювання як інструменту пізнання складних систем, запропонованою Прусом А. [1]. Поєднання інтелектуальних алгоритмів із базами знань створює умови не лише для аналізу даних, але й для їх фільтрації, генерації та добору ефективних варіантів розвитку інформаційних систем. Це забезпечує безперервність, гнучкість та прогнозованість функціонування цифрової інфраструктури.

Нейронні мережі мають стратегічне значення й для управління освітнім процесом. Вони здатні адаптувати інфраструктуру ЗВО до нових викликів, сприяти цифровій трансформації, розширювати спектр освітніх послуг, підвищувати рівень індивідуалізації та доступності освітніх ресурсів. Формування інтелектуальної системи на основі нейромереж і баз знань створює потужне середовище підтримки прийняття рішень, що включає функції автентифікації користувачів, адаптацію контенту, маршрутизацію даних до зовнішніх інфраструктур – цифрового міста (Smart City), електронного урядування, міжнародних наукових платформ тощо. Це суттєво розширює межі функціонування від локального рівня до національного й глобального освітнього кіберпростору [10].

Тобто, інформаційна інфраструктура ЗВО розглядається як динамічна система, здатна до адаптації, інтеграції з міжнародними стандартами, забезпечення безпечного обміну даними й

розгортання ізольованих підсистем для наукових експериментів, випробування захисних протоколів та моделювання кіберзагроз (рис. 1). Це визначає її подальший сталий розвиток у напрямі стійкості.

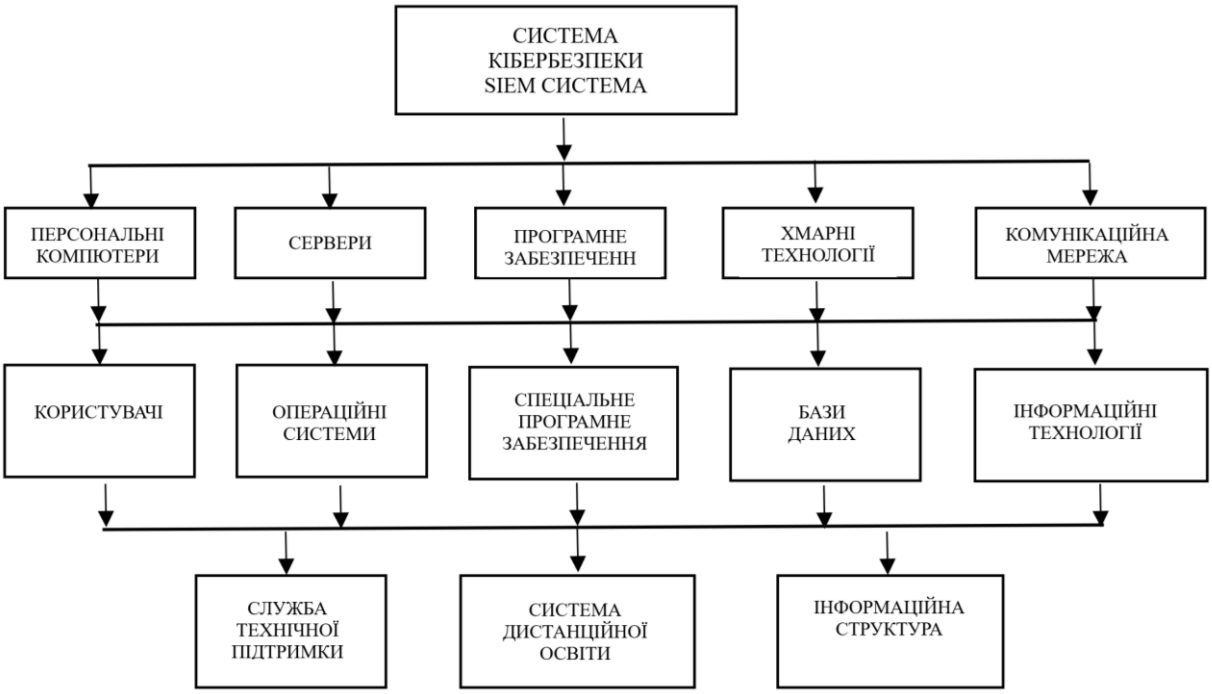

Рисунок 1 – Ієрархічна структура системи кібербезпеки ЗВО
Джерело: розроблено авторами

Окрім ресурсів, які ЗВО розподіляє між своїми користувачами, у його розпорядженні є кероване інформаційне середовище, яке забезпечує захищене з'єднання та контроль за потоками даних. У цьому середовищі функціонують шлюзи та файрволи, які виконують розподіл навантаження між ресурсами в межах інформаційної інфраструктури ЗВО.

На рисунку 2 представлено модель інформаційних ресурсів ЗВО та оптимальних шляхів комунікації між ними. Незважаючи на велику кількість комп'ютерної техніки, мережевого обладнання, баз даних і зовнішніх інформаційних ресурсів, учасники цієї інфраструктури стикаються з низкою обмежень щодо доступу до ресурсів. Відсутня уніфікація в роботі інформаційних систем, що ускладнює їхнє адміністрування: кожна система обслуговується окремо, а доступ до ресурсів надається індивідуально. При зміні організаційної структури, посадових обов'язків або ролей виникають труднощі з оновленням прав доступу в різних системах, що свідчить про неузгодженість та фрагментованість автоматизованих систем у межах єдиної інфраструктури.

Модель також демонструє, що електронна мережа ЗВО охоплює весь кампус, є складною в адмініструванні та надає можливість кожному користувачу взаємодіяти з нею відповідно до свого рівня доступу. Життєздатність та функціонування мережі регулюються нормативно-правовими актами — як державними, так і внутрішніми документами ЗВО.

Система захисту інформаційних ресурсів будується з урахуванням специфіки діяльності ЗВО. Інфраструктура включає фізичну комунікаційну мережу, мережеві комутатори, бездротові точки доступу, комп'ютери, сервери, FireWall та підключення до Інтернету. Для захисту окремих компонентів використовуються багаторівневі керовані комутатори з вбудованими функціями захисту, що дозволяє створити надійні засоби оборони інформаційних ресурсів.

В наших дослідженнях зокрема увагу приділено безпечному доступу до мережі Інтернет. Всі елементи інфраструктури з'єднані дротовими та бездротовими комунікаційними засобами,

DOI:/10.31548/itees.2025.01.058
ISSN 3083-7502

а ресурси доступні незалежно від фізичної присутності працівників на робочому місці. Сервери з критичними ресурсами розміщені всередині корпоративної мережі та адмініструються фахівцями ЗВО. Для віддаленого та захищеного доступу до ресурсів застосовуються VPN-з'єднання.

Зауважимо, що на моделі, поданій на рис. 2, не деталізовано та не структуровано механізми управління окремими компонентами інформаційної інфраструктури ЗВО. Водночас рисунок також демонструє модель системи захисту інформаційних ресурсів ЗВО.

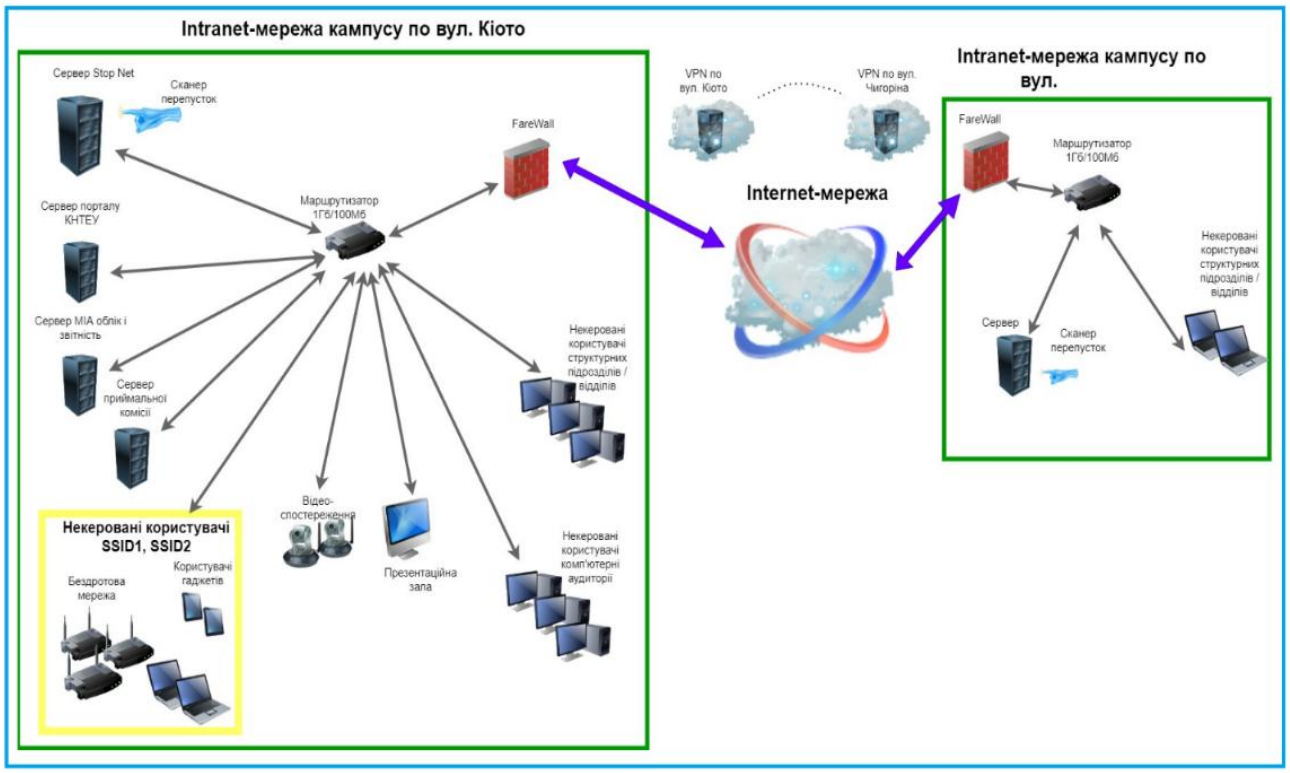

Рисунок 2 – Модель інформаційної інфраструктури ЗВО (засобів комунікації, ресурсів ЗВО) Джерело: [22]

На сьогодні впроваджено модель програмного захисту з функціями аудиту навантаження на ресурси інфраструктури. Основною – і водночас єдиною — перевагою цієї моделі є можливість ручного управління окремими автоматизованими освітніми системами через прямий доступ. Однак ця перевага водночас стає значним недоліком: для підтримки такої системи потрібні кваліфіковані працівники, які володіють навичками адміністрування різних автоматизованих систем, а також здатні узгоджувати їхню роботу з іншими внутрішніми та зовнішніми інформаційними системами. Це робить інфраструктуру ресурсоємною і дорогою в обслуговуванні.

Отже, цифрове управління ЗВО є лише частково автоматизованим і потребує значної кількості технічних узгоджень. Крім того, ускладнено побудову ефективної системи кіберзахисту через відмінності в налаштуваннях та розподілах прав доступу в різних системах. Відсутність єдиного підходу до управління базами даних, автоматизованими системами та механізмами доступу ускладнює аналіз інформації та оперативну зміну прав користувачів відповідно до їхньої присутності — очної або дистанційної.

Більшість процесів управління в ЗВО виконується вручну, що ускладнює моніторинг і контроль виконання завдань через відсутність ефективного зворотного зв'язку. Для підтримки функціонування інфраструктури необхідна велика кількість IT-фахівців із різними технічними компетенціями. Доступ до інформаційних ресурсів може бути нестабільним через технічні

чинники, зокрема збої в роботі комутаторів або відсутність електроживлення, що напряму впливає на функціонування всієї інфраструктури.

Усі пристрої (гаджети, ноутбуки, бездротове обладнання) пов'язані між собою через комутаційне обладнання, яке виконує постійний моніторинг та контроль мережі. Для формування повної картини функціонування інформаційної системи ЗВО необхідно проаналізувати всі елементи інфраструктури, зокрема бази даних. При цьому фіксується відсутність належного рівня захисту персональних даних користувачів.

Для забезпечення узгодженості інформаційних потоків необхідне втручання оператора — зокрема, для формування пропозицій, прийняття рішень і вирішення типових запитів у діалоговому режимі. Одним із суттєвих недоліків є також відсутність чіткої інформації про фізичних користувачів ЗВО в системі.

Модель інформаційної інфраструктури закладу вищої освіти: інтелектуальний доступ, аналітика потреб і кібербезпека

Усі вищезазначені недоліки можна усунути шляхом впровадження інтелектуального центру управління інформаційною інфраструктурою ЗВО, побудованого на основі централізованої системи керування з використанням нейромережевих алгоритмів. Запропонована модель інформаційної інфраструктури передбачає наявність такого інтелектуального центру, який завдяки нейромережам здатен оперативно й комплексно аналізувати стан інфраструктури та пропонувати оптимальні рішення щодо управління ресурсами та усунення проблем.

На рис. 3 представлено модель інформаційної інфраструктури ЗВО з урахуванням функціонування інтелектуального центру управління, реалізовану на прикладі Державного торговельно-економічного університету.

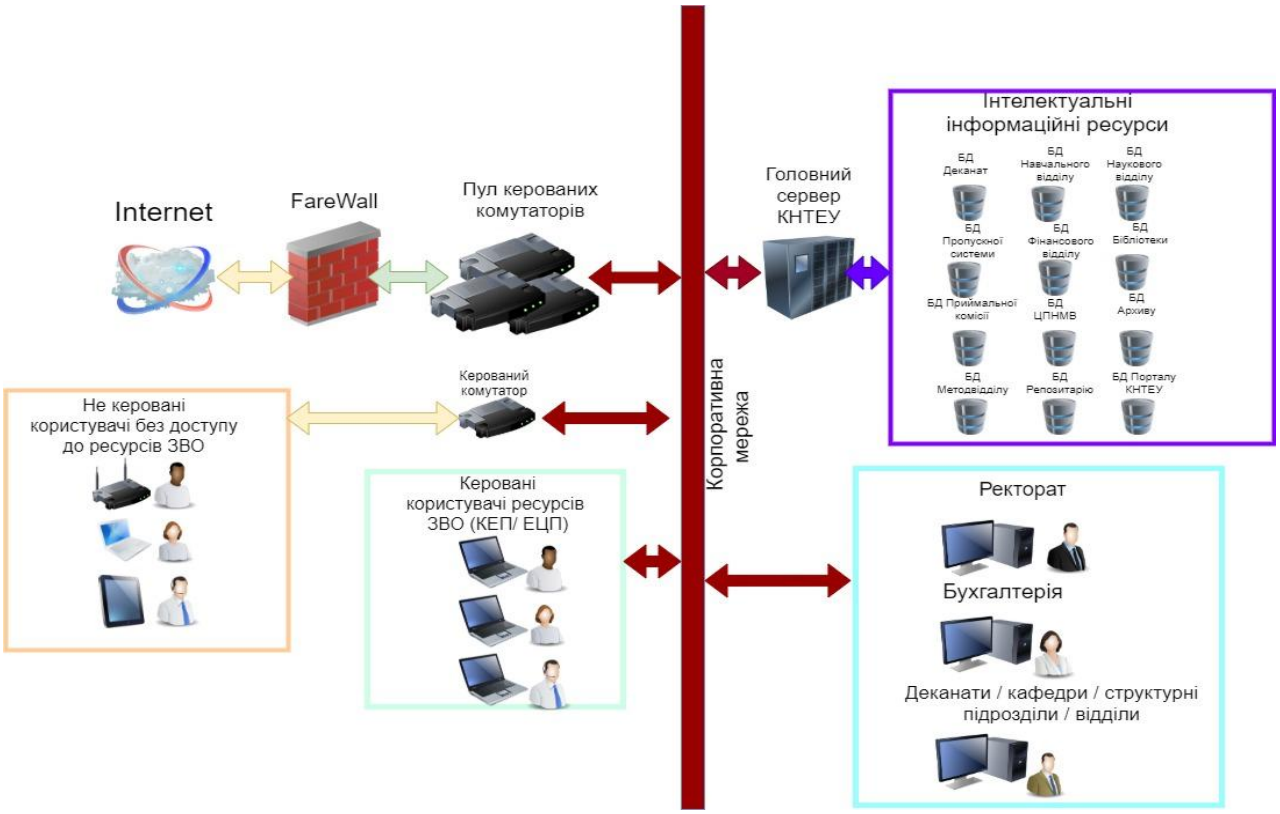

Рисунок 3 – Модель інформаційної інфраструктури ЗВО (фізичні з'єднання та зміни в комутаційній архітектурі ЗВО). Джерело: розроблено авторами

Основна ідея цієї моделі полягає у впровадженні контрольованих процесів керування інформаційними потоками та інтелектуального розподілу ресурсів відповідно до актуальних

DOI:/10.31548/itees.2025.01.058
ISSN 3083-7502

запитів користувачів. Система дозволяє здійснювати аналітичну оцінку потреб у ресурсах, перевіряти їх обґрунтованість і забезпечувати своєчасний доступ у разі необхідності. У межах бездротової мережі ресурси поділяються на сегменти з контрольованим або гостьовим доступом.

На етапі ідентифікації користувача система контролю доступу формує індивідуальний набір ресурсів, необхідних для ефективної діяльності. Якщо користувач потребує підключення до додаткових інформаційних систем, доступ надається автоматично без переривання з'єднання з основним середовищем.

Обмін даними між інформаційними системами здійснюється через електронні запити, які обробляються інтелектуальним центром. Центр структурує отриману інформацію та забезпечує її інтеграцію в інші системи відповідно до змісту запиту. Розподіл ресурсів здійснюється динамічно з урахуванням навантаження та потреб користувачів, що дає змогу ефективно управляти базами даних, прогнозувати пікові навантаження та оптимізовувати їх через перерозподіл або стиснення даних.

Система також підтримує автентифікацію користувачів і надання доступу до локальних або віртуальних мереж із різними рівнями привілеїв. У разі дистанційної роботи передбачене використання електронних цифрових ключів для забезпечення безпечного з'єднання. Такий підхід дозволяє максимально ефективно використовувати інформаційні ресурси навіть за умов змінного навантаження на окремі елементи інфраструктури ЗВО.

На рис. 3 представлено комунікації, фізичні з'єднання та зміни в комутаційній архітектурі, що виникають у результаті впровадження інтелектуального центру, який здійснює повний контроль над розподілом ресурсів, підвищує ефективність їх використання, здійснює аналітичну обробку даних і формує рекомендації для прийняття рішень у межах інформаційної інфраструктури ЗВО.

Порівняльний аналіз моделі на рис. 3 засвідчує якісні зміни в управлінні інформаційними потоками, розподілі ресурсів між різними категоріями користувачів та функціонуванні системи автентифікації.

Інтелектуальний центр виконує низку функцій, зокрема: прогнозування наслідків авторизації користувачів, управління доступом до комп'ютерних ресурсів, баз даних, автоматизованих систем, оптимізацію навантаження на інтернет-ресурси ЗВО, повідомлення про відмови в роботі, а також виявлення спроб несанкціонованого доступу. Такий підхід забезпечує можливість оперативного аналізу інцидентів і реалізації коригувальних заходів з боку адміністраторів інформаційної інфраструктури ЗВО.

Інтеграція інтелектуальної системи до структури інформаційної інфраструктури ЗВО дозволить забезпечити її взаємодію з усіма автоматизованими підсистемами та системою кібербезпеки. До її функцій належить управління адміністративними правами користувачів, що дає змогу, на основі опису параметрів прототипу користувача, призначати типи доступу та регламентувати їх у різних інформаційних автоматизованих системах із можливістю подальшої модифікації.

Крім того, значущим елементом є фіксація фізичної присутності користувача. Зчитування перепустки через систему контролю доступу відображає присутність у загальній системі, що може додатково підтверджуватися засобами відеоспостереження шляхом зіставлення обличчя користувача з фотографією.

Також передбачена можливість застосування альтернативних засобів біометричної ідентифікації – зокрема, за голосом або відбитками пальців. Утім, реалізація таких підходів потребує значних фінансових ресурсів та модернізації контрольно-пропускних пунктів університету, що наразі є обмежуючим фактором.

Після підтвердження фізичної присутності користувача на території кампусу, інтелектуальна система автоматично надає йому доступ до всіх доступних ресурсів відповідно до його ролі та рівня прав. Водночас система здатна адаптуватися до індивідуальних звичок і потреб: вона може враховувати вподобання в харчуванні, щоб оптимізувати приготування їжі,

повідомляти про нові надходження у бібліотеці за тематикою дослідження, зміни в розкладі занять, навантаженні чи анонси наукових подій та зустрічей.

Також запропонована інтелектуальна система може автоматично фіксувати фактичну присутність співробітників на робочому місці, передаючи ці дані у фінансово-економічну систему. Користувачі можуть отримувати нагадування про майбутні зміни у правах доступу, навчання з підвищення кваліфікації та інші внутрішні оновлення.

Для забезпечення повноцінного кібернетичного захисту рекомендуємо налаштувати, адаптувати та використовувати SIEM системи, які постійно проводять збір, обробку та аналіз подій безпеки, виявляти загрози у реальному часі, проводити аналіз та управління безпекою, а також проводити розслідування інцидентів. Цікава така система тим, що конфігурується та налаштовуються для всієї інформаційної інфраструктури ЗВО. За браком фахівців з кіберзахисту рекомендуємо використовувати систему, яку можна використати й ІТ фахівцями з проведеними певними специфічними навчаннями. Така система автоматично оновлюється, використовує автоматизований аудит інформаційної інфраструктури ЗВО. Такі системи дозволяють автоматизувати фільтрацію подій, виявлення порушень безпеки, сповіщення подій, аналіз та управління, отримання сповіщень в результаті виявлення загроз чи прогнозування кібератак на інформаційні ресурси ЗВО.

Інтелектуальна система, провівши автентифікацію, забезпечує безперешкодний доступ до необхідних платформ та сервісів без додаткових дій з боку користувача. За потреби, адміністратори мають змогу індивідуально або колективно змінювати рівень доступу, з обов’язковим підтвердженням змін.

Система кіберзахисту при цьому виконує функцію постійного моніторингу безпеки, оперативно повідомляючи відповідальних осіб про виявлені загрози, спроби несанкціонованого втручання чи атаки, дії адміністратора з їх нейтралізації, а також прогнозує можливі наслідки. Після ліквідації загроз система оцінює терміни відновлення стабільної роботи інформаційної інфраструктури ЗВО, забезпечуючи безперервність освітнього процесу.

Після підтвердження фізичної присутності користувача на території кампусу через системи автентифікації (наприклад, біометричні сканери, RFID-мітки або мобільні додатки), інтелектуальна система автоматично активує персоналізований профіль доступу. Такий механізм дозволяє одразу використовувати інформаційні ресурси ЗВО – навчальні платформи, бази даних, адміністративні сервіси, лабораторії, бібліотеки чи харчоблоки – відповідно до ролі користувача (ЗдВос, викладач, науковець, технічний працівник) та затвердженого рівня прав.

Система виконує контекстний аналіз попередніх дій користувача, історії взаємодії з сервісами, відвідуваності заходів, запитів до бібліотеки чи меню в їдальні, тим самим дозволяючи прогнозувати потреби та підлаштовувати середовище під кожного індивідуально. Наприклад, модуль харчування може проаналізувати звички користувача й оптимізувати обсяг порцій, зменшуючи харчові втрати та витрати. Освітній модуль надсилає повідомлення про нові бібліотечні надходження згідно з науковим профілем користувача, а також повідомляє про зміни в розкладі, перенесення занять, появу вільних слотів для консультацій, наукових подій, гостьових лекцій та стипендіальних можливостей (рис. 4).

Адміністративна частина системи забезпечує автоматичну фіксацію робочого часу співробітників у форматі очної присутності, синхронізуючи ці дані з бухгалтерськими та кадровими модулями. Також система здатна заздалегідь інформувати про планові зміни у правах доступу до ресурсів, проходження обов’язкових атестацій, тренінгів чи заходів із підвищення кваліфікації.

Автоматизоване управління правами доступу забезпечує прозору та гнучку модель регулювання: при зміні статусу користувача (наприклад, переведення ЗдВос на іншу форму навчання або підвищення посади співробітника), адміністратор може швидко оновити профіль доступу як на індивідуальному, так і на груповому рівні з миттєвим підтвердженням змін.

DOI:/10.31548/itees.2025.01.058
ISSN 3083-7502

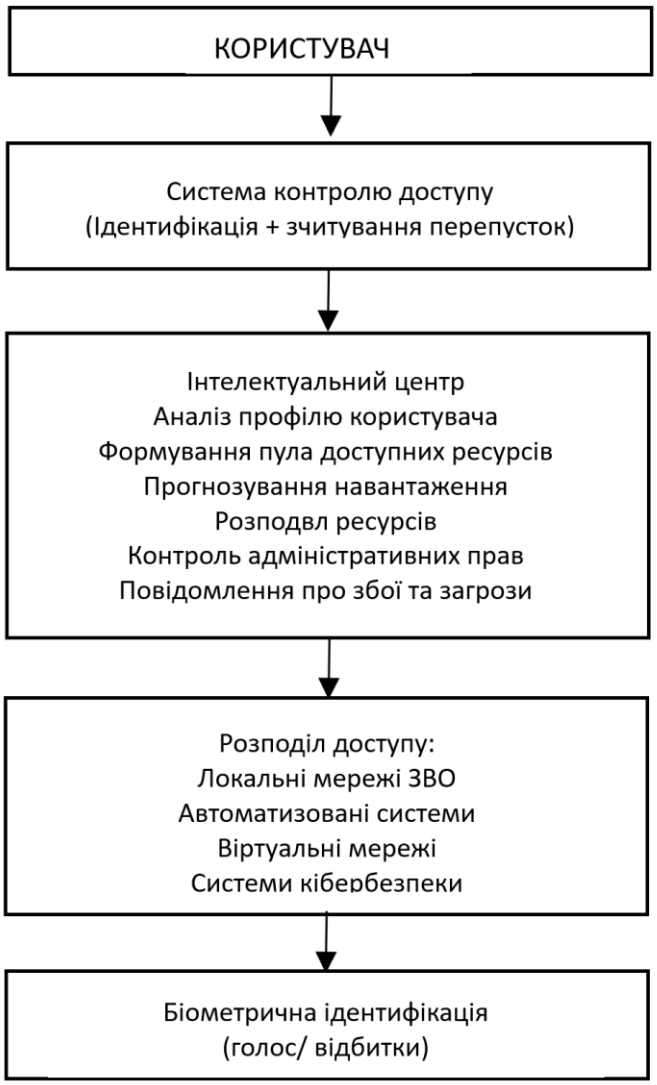

Рисунок 4 – Схема взаємодії інтелектуальної системи в інформаційні інфраструктурі ЗВО. Джерело: розроблено авторами

Визначальну роль у функціонуванні всієї системи відіграє комплекс кіберзахисту, який здійснює цілодобовий моніторинг усіх вузлів цифрової інфраструктури. Він здатен виявляти аномалії, блокувати потенційні вторгнення, реєструвати підозрілі дії, включно з втручанням адміністраторів, та оперативно інформувати відповідальних осіб. Система автоматично формує прогнози щодо шкоди від атак, надає рекомендації щодо нейтралізації загроз, оцінює терміни відновлення стабільного функціонування інформаційної інфраструктури ЗВО (зокрема інформаційної інфраструктури Державного торговельно-економічного університету та Національного університету біоресурсів та природокористування України) і забезпечує сталий перебіг освітнього процесу навіть за умов надзвичайних ситуацій.

Висновки і перспективи. Впровадження інтелектуальних систем у внутрішню інфраструктуру ЗВО відкриває можливості для глибокої трансформації процесів управління ресурсами, організації навчального процесу та обслуговування користувачів. Завдяки застосуванню багаторівневої автентифікації, персоналізованого доступу до сервісів і постійному збору аналітичних даних формується динамічне цифрове середовище, яке здатне адаптуватися до індивідуальних потреб кожного учасника освітнього процесу — ЗдВос, викладача чи адміністративного працівника.

Функціональність такої системи виходить далеко за межі звичайного надання доступу до ресурсів: вона виконує прогнозно-аналітичні завдання, аналізує поведінкові шаблони

користувачів для ефективного розподілу ресурсів (наприклад, у використанні простору кампусу або бібліотечних фондів), автоматизує повсякденні адміністративні процеси — такі як контроль відвідуваності або розрахунок заробітної плати, — і підвищує ефективність управління завдяки централізованій системі прав доступу.

Головним компонентом цієї цифрової екосистеми є система кібербезпеки. Вона не лише забезпечує захист даних, підтримуючи їхню конфіденційність і цілісність, а й створює умови для безперервного функціонування освітнього процесу в умовах кіберзагроз. Завдяки можливості проактивного виявлення загроз, блокування атак та прогнозування їх наслідків, кіберзахисні механізми значно підвищують цифрову стійкість ЗВО. Вважаємо що провідну роль відіграють SIEM-системи, які забезпечують гнучке та комплексне реагування на події безпеки в мережі ЗВО.

Загалом, інтеграція таких інтелектуальних систем у цифрову інфраструктуру університету є не лише відповіддю на виклики цифрової трансформації освіти, а й основою для формування освітнього простору, який поєднує безпеку, гнучкість, ефективність та здатність до адаптації в умовах постійних змін.

Список використаних джерел

1. Прус А. (2023) Математичне моделювання як лінза реального світу. Physical and Mathematical Education. 38(4), 56–61. URL: https://doi.org/10.31110/2413-1571-2023-038-4-008
2. Sophos. (2024). The state of ransomware 2024. https://www.sophos.com/en-us/content/state-of-ransomware.
3. BlueVoyant. Cybersecurity in higher education. Retrieved February 25, 2025, from https://www.bluevoyant.com/resources/cybersecurity-in-higher-education.
4. Zavhorodnya, E., Shestak, Y., & Kryvoruchko, O. (2025). Digital risk management in higher education. In Modern achievements and prospects of socio-economic development (pp. 138–143). Eastern European Center for Scientific Research. https://researcheurope.org/wp-content/uploads/2025/05/re-16.05.25.pdf.
5. Shestak, Y., & Zavhorodnya, E. (2025). Protection principles of HEIs information infrastructure. In Innovations and their impact on the economy and society (pp. 138–143). Eastern 6. European Center for Scientific Research. https://researcheurope.org/wp-content/uploads/2024/11/re-25.10.24.pdf.
6. El Latif, A. A. A., Maleh, Y., El Affendi, M. A., & Ahmad, S. (Eds.). (2023). Cybersecurity management in education technologies: Risks and countermeasures for advancements in E-learning (1st ed.). CRC Press. https://doi.org/10.1201/9781003369042.
7. Peng, L. (2023). Design of smart campus security management and control platform based on Big Data technology. In Proceedings of the 2022 International Conference on Educational Innovation and Multimedia Technology (EIMT 2022) (pp. 586–595). Atlantis Press. https://doi.org/10.2991/978-94-6463-012-1_65
8. Ni, Q., & Zeng, Y. (2025). Research on smart campus system architecture design and data security protection strategy. Frontiers in Computing and Intelligent Systems, 11(3), Article 98. https://doi.org/10.54097/f6sy7t88.
9. Tahsien, S. M., Karimipour, H., & Spachos, P. (2020). Machine learning based solutions for security of Internet of Things (IoT): A survey. Journal of Network and Computer Applications, 161, 102630. https://doi.org/10.1016/j.jnca.2020.102630.
10. Lakhno, V., Malyukov V., Kryvoruchko, O., Desiatko, A., & Shestak Y. (2020). Smart city technology investment solution support system accounting multi-factories. In R. Silhavy, P. Silhavy, Z. Prokopova (Eds.), Software engineering perspectives in intelligent systems (pp. 1–11). Springer. https://doi.org/10.1007/978-3-030-63322-6_1.
11. Domínguez Bolaño, T., Barral, V., Escudero, C. J., & García Naya, J. A. (2024). An IoT system for a smart campus: Challenges and solutions illustrated over several real world use cases. IEEE

DOI:/10.31548/itees.2025.01.058
ISSN 3083-7502

Access, 12, 104592–104606. https://doi.org/10.48550/arXiv.2403.15395. https://doi.org/10.1016/j.iot.2024.101099.
12. Peng, C. F., Peng, L., & Liu, Y. (2023). Application of Big Data technology in campus security management under the background of information age. Journal of Physics: Conference Series, 2458(1), 012012. https://doi.org/10.1088/1742-6596/1881/2/022097.
13. Zhang, Z., Hamadi, H.A., Damiani, E., Yeun, C.Y., & Taher, F. (2022). Explainable Artificial Intelligence Applications in Cyber Security: State-of-the-Art in Research. IEEE Access, 10, 93104-93139. https://doi.org/10.1109/ACCESS.2022.3204051.
14. Lakhno, V., Lakhno, M., Kryvoruchko, O., Kaminskyi, S., & Makaiev, V. (2024). Automation of DDoS attack investigation in industrial control systems using Bayesian networks on Python. In CEUR Workshop Proceedings on Cybersecurity Providing in Information and Telecommunication Systems II (CPITS-II 2024), pp. 282–287. https://ceur-ws.org/Vol-3826/short18.pdf.
15. Литвинов, О., Філіпенко, Н., Лукашевич, С., & Палкова, К. (2024). Кібербезпека як фактор ефективності закладів вищої освіти. Пропілеї права та безпеки, 5, Article Ключові аспекти кіберзахисту ЗВО та підготовка персоналу, 15-23. https://doi.org/10.32620/pls.2024.5.02.
16. Трофименко, О., Логінова, Н., Сергійчук, М., & Дубової, Ю. (2022). Кіберзагрози в освітньому секторі. Кібербезпека: освіта, наука, техніка, 4(16), 76–84. https://doi.org/10.28925/2663-4023.2022.16.7684 (csecurity.kubg.edu.ua)
17. Ільєнко, А., Ільєнко, С., Яковенко, О., Галич, Є., & Павленко, В. (2024). Перспективи інтеграції штучного інтелекту в системи кібербезпеки. Кібербезпека: освіта, наука, техніка, 1(25), 318–329. https://doi.org/10.28925/2663-4023.2024.25.318329 (csecurity.kubg.edu.ua)
18. Скумін, Т. Ф., & Стасишин, Р. М. (2015). Інтелектуальна система кіберзахисту. Тези доповідей IV Міжнар. наук.-техн. конференції «Актуальні задачі сучасних технологій», ТНТУ (Тернопіль), 53–54. https://elartu.tntu.edu.ua/handle/123456789/11060?locale=it.
19. Костікова, М. В. (2022). Сучасний освітній процес і кібербезпека. Матеріали Всеукр. наук.-практ. Internet конф. (м. Харків, 15–16 листоп.), 57–59. (dspace.khadi.kharkov.ua)
20. Доценко, С. О. (2022). Кібербезпека учасників освітнього процесу в умовах дистанційного і змішаного навчання. Нац. ун-т «Одеська юридична академія». (dspace.hnpu.edu.ua)
21. Dets, D., Barduk, A., & Syvolap, O. (2025). Cybersecurity in the field of open access: Principles for protecting educational and scientific resources. Automation of Technological and Business Processes, 17(1), 17–24. https://doi.org/10.15673/atbp.v17i1.3081.
22. Шестак Я.І. (2022). Моделювання єдиного інформаційного простору закладу вищої освіти. Управління розвитком складних систем, 49, 81–89. URL: https://doi.org/10.32347/2412-9933.2022.49.81-89.

Shestack Yaroslav
PhD, Associate Professor, Department of Software Engineering and Cybersecurity,
State University of Trade and Economics, Ukraine
ORCID: https://orcid.org/0000-0002-5102-9642
E-mail: shestack@knute.edu.ua

Tsiutsiura Svitlana
Doctor of Technical Sciences, Professor, Professor of the Department of Software Engineering and Cybersecurity,
State University of Trade and Economics, Ukraine
ORCID: https://orcid.org/0000-0002-4270-7405
E-mail: svtsutsura@dteu.edu.ua

Kryvoruchko Olena
Doctor of Technical Sciences, Professor, Professor of the Department of Computer Systems, Networks and Cybersecurity,

National University of Life and Environmental Sciences of Ukraine
ORCID: https://orcid.org/0000-0002-7661-9227
E-mail: o.kryvoruchko@nubip.edu.ua

Lakhno Valerii
Doctor of Technical Sciences, Professor, Professor of the Department of Computer Systems, Networks and Cybersecurity,
National University of Life and Environmental Sciences of Ukraine
ORCID: http://orcid.org/0000-0001-9695-4543
E-mail: lva964@nubip.edu.ua

Kasatkin Dmytro
PhD of Pedagogical Sciences, Associate Professor, Head of the Department of Computer Systems, Networks and Cybersecurity,
National University of Life and Environmental Sciences of Ukraine
ORCID: https://orcid.org/0000-0002-2642-8908
E-mail: d.kasatkin@nubip.edu.ua

CYBER RESILIENCE OF UKRAINIAN HIGHER EDUCATIONAL INSTITUTIONS IN A WARFARE CONDITION

Abstract. *The article examines the problem of ensuring cyber resilience of higher education institutions (HEIs) by developing and implementing a comprehensive cyber defense architecture. It is shown that the effectiveness of such a system is determined by the ability to integrate educational, administrative, and resource subsystems, taking into account their interdependence and specifics of functioning. The main risks and consequences of cyber attacks are considered. The principles of building a secure information infrastructure and the criteria that a reliable and effective HEI cybersecurity system must meet are outlined. A model for managing HEI information flows and resources using neural network technologies and intelligent decision support systems is proposed. The results of the study demonstrate the feasibility of using modeling tools to predict threats, optimize resource allocation, and increase the resilience of the educational environment to cyber risks.*

Keywords: *cybersecurity, information infrastructure, development trajectories, cybersecurity systems, infrastructure cyber resilience, neural network technologies, communication networks.*