Shestak Yaroslav,

State University of Trade and Economics, Kyiv,

Senior Lecturer at the Department of Software Engineering and Cybersecurity,

Zavhorodnya Elizaveta

State University of Trade and Economics, Kyiv,

Assistant at the Department of Software Engineering and Cybersecurity,

***Abstract.*** *The information systems of higher education institutions are constantly undergoing transformations, and there is a coordination between the information systems of the digital state, including applications and systems: DIIA, EDEBO, education quality assessment systems, NAQA. Given the constant addition of services to electronic information resources, there is a need to build secure communication channels and ensure the protection of local networks and infrastructure in general*

***Keywords:*** *information, protection, HEI, infrastructure, system.*

PROTECTION OF THE INFORMATION INFRASTRUCTURE OF THE HEI

Шестак Ярослав,

Державний торговельно-економічний університет, Київ

аспірант, старший викладач кафедри інженерії програмного забезпечення та кібербезпеки,

ORCID 0000-0002-5102-9642

Завгородня Єлизавета

Державний торговельно-економічний університет, Київ

аспірант, асистент кафедри інженерії програмного забезпечення та кібербезпеки,

ORCID 0000-0003-0549-7020

**ЗАХИСТ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ ЗВО**

***Анотація.*** *В інформаційних системах закладів вищої освіти постійно тривають трансформації, відбуваються узгодження між інформаційними системами цифрової держави, зокрема із застосунками і системами: ДІЯ, ЄДЕБО, системи оцінювання якості освіти, НАЗЯВО. З огляду на постійне додавання сервісів до інформаційних електронних ресурсів, постає необхідність у побудові захищених каналів зв’язку та забезпеченні захисту локальних мереж та інфраструктури в цілому.*

***Ключові слова:*** *інформація, захист, ЗВО, інфраструктура, система.*

В період воєнного стану дуже актуальним є проблема побудови інформаційних систем, розвитку та впливу на інфраструктуру різних зовнішніх систем до яких будуть підключатися зовнішні канали зв’язку для передачі даних. кіберризики, які утворилися вніслідок воєнних дій проти України, впливають на ймовірне використання інформаційних систем та на стійкість інфраструктури ЗВО у кіберпросторі. Впродовж багатьох років інформаційні технології та інформаційні системи входили у повсякденне життя людей, давали багато зручних сервісів, спрощення процедур та отримання позитивних відгуків на всі надані чи отримані послуги. Наша держава постійно розвивається і тому збільшуються сфери надання цифрових послуг у державному секторі, бізнес секторі тощо. Інформаційна інфраструктура ЗВО в процесі цифровізації освіти, бізнесу, державних установ, установ спеціального призначення постійно оновлювалася, модернізувалася, удосконалювалася та трансформувалася відповідно до їх потреб і виконуваних задач. Сьогодні немає жодного процесу, який не був би охоплений інформаційними системами, які розвиваються паралельно з розвитком апаратного забезпечення та інформаційних технологій. Так дедалі більше інформації користувачі можуть отримати не виходячи з дому, ефективно і швидко вирішувати багато питань стосовно отримання освіти, вибору курсів, закладів, отримання підтвердження кваліфікації онлайн тощо.

Інформаційна інфраструктура ЗВО дає можливість підключатися, брати, формувати та надавати інформацію за запитами глобальної інфраструктури Smart-міста, цифрової держави, що полегшує роботу самих систем, зменшує ризики надання не достовірної, не коректної інформації, не актуальної інформації чи не правдивої інформації (фейків).

Споживачами цифрової інформації ЗВО наразі є інформаційні системи Smart-міста та зовнішні інфраструктури: підрозділи міністерств, електронні майданчики для проведення тендерів, системи для звітування, єдина державна електронна база з питань освіти, система для учнів закладів середньої освіти, які обирають напрям та спеціальність для навчання у ЗВО. Здобувачі вищої освіти отримують з інформаційних систем ЗВО всю необхідну інформацію, визначену їм правами доступу, у процесі навчання, підтвердження наукових досягнень, рівню знань, план проведення наукових заходів, участь у заходах та результати їх проведення, отримання відповідної кваліфікації у процесі навчання, можливість працевлаштування та реалізації своїх прав. В свою чергу стейкґолдери отримують права доступу до інформаційних систем інфраструктури ЗВО, зокрема до робочих програм, силабусів, дискутують та беруть участь у погодженні запропонованих набуття компетентностей здобувачів вищої освіти, підготовці майбутніх фахівців відтворення у їх документах підтвердження набутих знань і умінь дипломом, відомствами чи сертифікатами відповідних органів чи іншими документами. Тому, від правильності побудови інформаційної інфраструктури ЗВО, кібернетичного захисту та продуманості каналів зв’язку (API) залежить ефективне функціонування ЗВО, його місце у інформаційному просторі міста, у інформаційному просторі наукового середовища країни та світу.

Для позиціонування ЗВО як наукової світової ланки необхідно розвивати належним чином свою інформаційну інфраструктуру, розвивати інтерфейси відповідно до досягнень власних науковців та залучених ззовні, персоналізувати їх, демонструвати, пропонувати власні розробки, курси, займатися науковими розробками спільно із фахівцями інших ЗВО, наукових інституцій, тим самим піднімаючи власні рейтинги. Додатково, важливим є постійний розвиток і підтримка всіх зовнішніх зв’язків з впливовими інформаційними інфраструктурами регіонального, державного, наукового та світового сектору. Тому інформаційна інфраструктура дуже важлива для всіх ЗВО, навчальних закладів, державних органів і комерційних установ, оскільки має надавати інформацію, з її подальшою верифікацією, без окремого керування фізично окремими особами, що в свою чергу підтвердить прозорість системи та унеможливить вплив корупційних складових на процеси в освітньому середовищі. Таким чином, для забезпечення виконання цих завдань для інформаційної інфрастукутри має бути застосована система збереження конфіденційності інформації та захисту персональної інформації на основі критеріїв прозорості та відкритості. Крім того, має бути організована та застосована система кіберзахисту, що наразі, в період воєнного стану в Україні є актуальною і важливою.

Розвиток Smart-міста та цифрової держави не можливий без цифровізації всіх ділових, державних, цивільних та інших процесів в установах, а саме всіх етапів навчання людини, її соціалізації, розвитку на всіх етапах її становлення. Також розвиток особистості залежить від розвитку інфраструктури міста, регіону та всієї держави, всіх сфер обслуговування. Відповідно, важливим є інформування про можливість у цифровому просторі відобразити, надати доступ до ресурсів всіх відкритих і закритих інформаційних систем інфраструктури. Від розвитку інфраструктури залежить обізнаність людей у недоліках і перевагах систем та іх місце у розвитку регіону держави, важливість вкладу кожного громадянина відповідно до своєї діяльності – реалізації проєктів з розбудови держави. Інформаційна інфраструктура закладів вищої освіти залежить від всіх ланок міської, регіональної та державної інфраструктури, вона не може існувати окремо, не може самостійно розвиватися чи впливати на будь які процеси. Тому інформаційна інфраструктура ЗВО має багатогранну структуру з великою кількістю зав’язків, системою кіберзахисту та зовнішніми інформаційними системами інформаційних структур цифрового міста, держави.

Застосування бази знань у інформаційній інфраструктурі ЗВО дає позитивні зрушення через глибокий аналіз всіх процесів управління освітнім процесом. Так використання інтелектуальних систем у вирішенні задач з керування освітнім процесом, дають можливість охопити всі інформаційні системи, аналізувати та надавати рекомендації чи пропозиції з керування всіма процесами у ЗВО, структурувати інформацію з різних інформаційних систем, накопичувати її, з подальшою обробкою масивів цифрової інформації, надавати пропозиції стосовно побудови кібернетичного захисту інформаційних систем та інформаційної інфраструктури ЗВО, надавати прогнози стосовно траєкторії розвитку ЗВО та напрямів затребуваних спеціальностей, коригувати навчальні плани відповідно до потреб стейкґолдерів тощо. Для цього необхідно сформувати базу знань, яка постійно через нейронні мережі буде навчатися, удосконалюватися та видавати необхідну інформацію залежно від потреб внутрішніх та зовнішніх запитів користувачів системи. База знань дозволить оптимізувати керування освітнім процесом, виявляти недоліки інформаційних систем та інформувати відповідальних фахівців для їх усунення, коригувати параметри, трансформувати бази даних та канали зв’язку, а також виявляти потребу в модифікації системи кібернетичного захисту інформаційної інфраструктури ЗВО. Нейронна мережа з алгоритмами дозволяє у скорочені терміни переформатовувати цифрову інформацію, перетворювати та концентрувати всю важливу для ЗВО інформацію, організувувати архівування та подальше накопичення для аналізу, трансформації та прогнозування. Також є можливість шифрування інформації з постійними і тимчасовими ключами, які система генерує і використовує для захисту. Таким чином інфраструктура закладу вищої освіти потребує детального вивчення, та побудови захисту відповідних інформаційних систем. Суттєвим є і будуть важливі системи кіберзахисту та системи подвійної ідентифікації користувачів для автентифікації у інформаційних системах.

Висновки: Аналізуючи різні інформаційні системи, їх розвиток, стратегічного підходу до формування інформаційної інфраструктури в Україні та за кордоном, було виявлено загальний підхід до опису функціональних характеристик загальної побудови інформаційної інфраструктури ЗВО, каналів зв’язку (API), ідентифікації та передачі даних у зашифрованому вигляді. Для структуровання вхідної та вихідної інформації, ресурсів, процесів вибору каналіз зв’язку підбираються системи кібербезпеки, ключів шифрування, методів ідентифікації тощо. Отже необхідно це питання розглядати, обговорювати та приймати рішення по оптимізації інфраструктури, застосуванні нових методів захисту у кібернетичному просторі та побудови безпечних інтерфейсів зв’язку між загально-державними електроннми системами.

**Список використаних джерел**

1. Шестак Я.І. Моделювання єдиного інформаційного простору закладу вищої освіти. Управління розвитком складних систем. 2022. №. 49. С. 81–89. URL: <https://doi.org/10.32347/2412-9933.2022.49.81-89>

2. Шестак Я., Чубаєвський В. Моделювання інформаційної інфраструктури ЗВО. Кібербезпека: освіта, наука, техніка. 2023. Т. 1, № 21. С. 121–135. URL: <https://doi.org/10.28925/2663-4023.2023.21.121135>

3. Моделювання інформаційної системи підприємства / О. В. Криворучко та ін. Комплексне забезпечення якості технологічних процесів та систем : матеріали тез доп. XІ Міжнар. науково-практ. конф., м. Чернігів, 26–27 трав. 2021 р. Чернігів, 2021. С. 190. URL: <https://drive.google.com/file/d/1NnRKAAoqZQUCurDMuE5TXRfNyPYDyZX4/view>