**ОРАНІЗАЦІЯ ЗАХИСТУ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОЇ СИСТЕМИ ЗВО**

**Шестак Ярослав Іванович,**

доктор філософії (комп’ютерні науки), старший викладач

**Завгородня Єлизавета Олександрівна,**

аспірант, асистент

Державний торговельно-економічний університет

м. Київ, Україна

shestack@knute.edu.ua

**Вступ.** Сьогодення в епоху розвитку штучного інтелекту вимагає більш критичного підходу до інформаційно-комунікаційної системи ЗВО у кіберпосторі, та змушує змінювати архітектуру мережі, підвищує вимоги до якості її обслуговування, модернізації та коригування. Багато нових інструментів моніторингу ІКС вимагає певних знань і умінь та використання для управління ресурсами інформаційної інфраструктури ЗВО.

Захист ІКС є важливим і вагомим для забезпечення освітнього процесу ЗВО, його інформаційного забезпечення та фінансово-економічної діяльності, проведення досліджень та розвитку науки, як всередині закладу так і агрегуючись з іншими науковцями.

Відповідно, предметом нашого дослідження є інструменти для захисту ІКС, а саме апаратне та програмне забезпечення, мережеві компоненти, комунікаційне обладнання, технології збору та обробки інформації, мережі, які використовуються в освітньому середовищі.

**Метою дослідження** є аналіз інструментів та процесу забезпечення ефективного захисту ІКС ЗВО, запобігання кіберзагрозам, побудови стабільних захищених інформаційних систем.

**Результати дослідження**. Інфраструктура ЗВО перебуває у постійних трансформаціях, яке викликано постійними змінами вимог до надання освітніх послуг здобувачам вищої освіти. ІКС ЗВО потребує нових підходів до реструктуризації через набуття нових умов використання у кіберпросторі, постійно зростають загрози щодо вільного використання персональних даних та іншої конфіденційної інформації. Відповідно до стандартів безпеки ІКС ЗВО, фахівці з кіберзахисту визначають вимоги та рекомендації щодо захисту даних, кібербезпеки та управління ризиками. Профільні стандарти допомагають створювати надійні системи захисту інформації: ISO/IEC 27001 – стандарт управління інформаційною безпекою, що визначає вимоги до системи управління безпекою інформації; ISO/IEC 27002 – набір практичних правил для впровадження заходів безпеки; NIST Cybersecurity Framework – набір рекомендацій для управління кібербезпекою. Наведені стандарти надають можливість правильно обрати стратегію, інструментарій та побудувати захист ІКС.

Інструменти кіберзахисту допомагають захищати інформаційні системи від загроз, таких як хакерські атаки, шкідливе програмне забезпечення та витоки даних. Прикладами є: брандмауери (firewall) – перший рівень захисту, що фільтрує вхідний та вихідний мережевий трафік інтернету; VPN та менеджери паролів – забезпечують безпечне з’єднання та управління обліковими даними; IDS та IPS – системи виявлення та запобігання вторгненням, які аналізують мережевий трафік та блокують підозрілу активність; Darktrace – платформа на основі штучного інтелекту, яка використовує алгоритми самонавчання для виявлення загроз та реагування на них у реальному часі; CrowdStrike Falcon – хмарне рішення, що застосовує машинне навчання для захисту від складних атак. Щодня всі ІКС державних установ, комерційних організацій, ЗВО та всіх інших користувачів інтернету потребують захисту через постійну активність кіберзлочинців, які намагаються реалізувати навмисні або ненавмисні напади чи інші кіберінциденти, які призводять до порушення цілісності систем, баз даних чи розкриття, знищення персональної чи конфіденційної інформації. Із перерахованих вище інструментів необхідно обрати ті, які забезпечать максимальний захист при застосуванні фахівцями з кібербезпеки. Інформація має бути захищена різними способами залежно від її типу та рівня конфіденційності, та мають бути застосовані відповідні інструменти. Адже втративши важливу інформацію чи розкриття конфіденційної інформації призведе і до фінансових втрат ЗВО. Тому важливими є конфіденційність, цілісність та доступність всіх необхідних інформаційних ресурсів засобами ІКС у кіберпросторі ЗВО. Для застосування комплексних заходів захисту інфраструктури ЗВО можна використати SIEM систему управління інформаційною безпекою, яка включає використання всіх інструментів захисту, моніторинг та своєчасне реагування на кіберінциденти, та прогнозування можливих атак. Застосування сучасних заходів безпеки дозволить побудувати, модернізувати чи реорганізувати ІКС ЗВО таким чином, що повністю забезпечить захист інформації, інфраструктури та безпечного освітнього процесу, надання повного спектру інформаційних освітніх послуг засобами ІКС здобувачам вищої освіти, стимулювання наукових розробок та просування ЗВО за міжнародними рейтингами.

**Список використаних джерел**

1. Шестак Я., Завгородня Є. Захист інформаційної інфраструктури ЗВО. Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення (випуск 92) : матеріали Міжнар. наук. інтернет-конф., м. Тернопіль, 8–9 жовт. 2024 р. Тернопіль, 2024. С. 37–41. URL: <http://www.konferenciaonline.org.ua/ua/article/id-1928/>
2. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements. URL: <https://www.iso.org/standard/27001>
3. Zavhorodnya E., Melnyk T. Factors affecting international competitiveness of ICT sector of the national economy. International scientific journal «Internauka». Series: «Economic Sciences». 2024. № 8. P. 51–66. URL: <https://doi.org/10.25313/2520-2294-2024-8-10179>