Вісник ЛДУБЖД
Bulletin of Lviv State University of Life Safety
https://journal.ldubgd.edu.ua/index.php/Visnuk
ISSN 2078-4643 (print), ISSN 2708-1389 (online)

UDC 004.056.5:004.415.2
DOI: 10.32447/20784643.31.2025.11

А. І. Івануса, Р. Л. Ткачук, Н. О. Маслова, В. І. Ящук, А. М. Ткаченко
Львівський державний університет безпеки життєдіяльності, м. Львів, Україна
ORCID: https://orcid.org/0000-0001-9141-8039 – А. І. Івануса
https://orcid.org/0000-0001-9137-1891 – Р. Л. Ткачук
https://orcid.org/0000-0002-9078-0973 – Н. О. Маслова
https://orcid.org/0000-0003-2651-4918 – В. І. Ящук
https://orcid.org/0009-0009-6830-4741 – А. М. Ткаченко
ivaaanusa@gmail.com

УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ТА КІБЕРЗАХИСТОМ У ЗАКЛАДАХ ВИЩОЇ ОСВІТИ

Постановка проблеми. У сучасних умовах стрімкої цифровізації освіти питання забезпечення інформаційної безпеки та кіберзахисту в закладах вищої освіти набувають виняткової актуальності. Навчальні заклади зберігають значний обсяг конфіденційних даних, включаючи персональну інформацію студентів, працівників, результати досліджень та інтелектуальну власність. Несанкціонований доступ до таких даних може спричинити серйозні репутаційні та фінансові збитки. З огляду на це, реалізація ефективної політики інформаційної безпеки є ключовим елементом стратегії управління ризиками. Вона дозволяє регламентувати порядок обробки, зберігання та передачі інформації, запобігаючи витокам і зловживанням. Кіберзагрози, що постійно еволюціонують, потребують системного підходу до формування захисних механізмів. Політика кіберзахисту сприяє впроваджнню процедур виявлення, реагування та усунення інцидентів безпеки. Вона також забезпечує дотримання законодавчих та нормативних вимог, зокрема щодо захисту персональних даних. Реалізація зазначеної політики підвищує рівень обізнаності учасників освітнього процесу щодо інформаційної безпеки. Таким чином, формування і впровадження політики інформаційної безпеки та кіберзахисту в закладах вищої освіти є необхідною умовою стабільного та безпечного функціонування освітнього середовища.

Мета. Метою роботи є вдосконалення робочого інструментарію управління інформаційною безпекою та кіберзахистом у закладах вищої освіти шляхом ідентифікації загроз, аналізу вразливостей мережевої інфраструктури та розробки політики інформаційної безпеки на основі оцінювання ризиків, відповідно до сучасних міжнародних і національних стандартів у сфері захисту інформації.

Методи досліджень. У роботі використаний системний аналіз, спостереження, моделювання, порівняння, експертне оцінювання, ранжування, нормування, теорії ймовірностей, теорії прийняття рішень, теорії захисту інформації.

Результати. У дослідженні розглянуто процес управління інформаційною безпекою та його зв’язок із безперервністю операційних процесів. Виявлено, що відсутність ефективних заходів та політики інформаційної безпеки може поставити під загрозу безперервність повсякденної діяльності ЗВО. Особливу увагу приділено дискретності в управлінні процесами інформаційної безпеки, яка є ключовим аспектом захисту інформаційних активів. На прикладі Львівського державного університету безпеки життєдіяльності проведено аналіз засобів захисту інформації та мережевої інфраструктури, виявлено недоліки та запропоновано організаційні, програмно-технічні заходи для підвищення рівня інформаційної безпеки. Запропонована адаптивна методика аналізу технічного програмного забезпечення підходить для використання суб’єктами господарювання незалежно від їх фінансових можливостей.

Ключові слова: політика інформаційної безпеки, управління ризиками, експертне оцінювання ризиків, мережева інфраструктура, заклад вищої освіти, кібератаки та загрози.

A. I. Ivanusa, R. L. Tkachuk, N. O. Maslova, V. I. Yashchuk, A. M. Tkachenko
Lviv State University of Life Safety, Lviv, Ukraine

INFORMATION SECURITY AND CYBERSECURITY MANAGEMENT IN HIGHER EDUCATION INSTITUTIONS

Research problem. In the current conditions of rapid digitalization of education, the issues of information security and cybersecurity in higher education institutions are becoming extremely relevant. Educational institutions store a significant amount of confidential data, including personal information of students, employees, research results or intellectual property. Unauthorized access to such data can cause significant reputational and financial damage. In this context, the implementation of an effective information security policy is a key element of the risk management strategy. It allows you to regulate the procedure for processing, storing, and transmitting information, preventing leaks and misuse. Constantly evolving cyber threats demand a systematic approach to the formation of protective mechanisms. A cybersecurity policy promotes the implementation of procedures for detecting, responding to, and eliminating security incidents. It also ensures compliance with legal and regulatory requirements, particularly with regard to personal data protection. Implementation of this policy raises awareness of information security among participants in the educational process. Thus, the development and implementation of information security and cybersecurity policies in higher education institutions is a prerequisite for the stable and secure functioning of the educational environment.

Aim. The aim of the work is to improve the working tools for managing information security and cybersecurity in higher education institutions by identifying threats, analyzing network infrastructure vulnerabilities, and developing information security policies based on risk assessment, according to modern international and national standards in the field of information security.

Research methods. The study uses system analysis, observation, modeling, comparison, expert evaluation, ranking, normalization, probability theory, decision-making theory, and information security theory.

Results. The study examines the process of information security management and its relationship with the continuity of operational processes. It has been found that the lack of effective information security measures and policies can jeopardize the continuity of the daily activities of the higher education institution. Particular attention is paid to discretion in managing information security processes, which is a key aspect of protecting information assets. Using the example of Lviv State University of Life Safety, the author analyzes the means of information protection and network infrastructure, identifies shortcomings, and proposes organizational, software, and technical measures to improve the level of information security. The proposed adaptive methodology for analyzing technical software is suitable for use by business entities regardless of their financial capabilities.

Keywords: information security policy, risk management, expert risk assessment, network infrastructure, higher education institution, cyberattacks and threats.

Вступ. У сучасних умовах цифрової трансформації освіти питання забезпечення інформаційної безпеки та кіберзахисту набувають особливої актуальності для закладів вищої освіти (ЗВО). Освітнє середовище все більше залежить від інформаційно-комунікаційних технологій, що забезпечують збереження, обробку та передавання великої кількості чутливої інформації: персональні дані здобувачів освіти й працівників, результати наукових досліджень тощо. У зв'язку з цим загрози інформаційній безпеці стають не лише технічно складнішими, але й потенційно більш руйнівними для функціонування освітніх інституцій. Ефективне управління інформаційною безпекою та кіберзахистом у закладах вищої освіти передбачає впровадження комплексного підходу, який охоплює нормативне регулювання, технічне забезпечення, організаційні механізми та кадрову підготовку. Особливе значення має розроблення і реалізація внутрішньої політики інформаційної безпеки (ПІБ), здатної адаптуватися до швидкоплинних змін у цифровому середовищі та відповідати міжнародним стандартам у сфері захисту інформації.

Для здійснення захисту інформації на підприємствах має бути сформовано політику інформаційної безпеки – певний звід правил і нормативних документів підприємства, що регламентують дії співробітників стосовно забезпечення інформаційної безпеки, а також описують програмні засоби які необхідно використовувати для захисту інформації. Кінцева мета розроблення політики інформаційної безпеки – це забезпечити цілісність, доступність і конфіденційність для кожного інформаційного ресурсу в процесі управління інформаційною безпекою. За допомогою політики інформаційної безпеки заходи будуть спрямовані на мінімізацію ризиків витоку інформації про організацію, а також на стале функціонування інформаційної структури підприємства і грамотні управлінські рішення. Порушення ПІБ і відсутність сучасної, правильно вибудованої системи гарантування безпеки в організації може призвести до фінансових, інформаційних та значних матеріальних витрат, а також завдати шкоди іміджеві підприємства, тому необхідно приділяти увагу питанням інформаційної безпеки.

Мета роботи полягає у вдосконаленні робочого інструментарію управління інформаційною безпекою та кіберзахистом у закладах вищої освіти шляхом ідентифікації загроз, аналізу вразливостей мережевої інфраструктури та розробки політики інформаційної безпеки на основі оцінювання ризиків, відповідно до сучасних міжнародних і національних стандартів у сфері захисту інформації. Для досягнення поставленої мети у роботі необхідно було сформулювати та послідовно вирішити такі взаємопов'язані задачі:

− визначити загрози інформаційної безпеки закладу вищої освіти;

− провести аналіз організаційно-штатної структури ЗВО;

− провести стан мережевої інфраструктури та системи захисту інформаційних активів ЗВО;

− ідентифікувати та оцінити ризики, що становлять загрозу інформаційній безпеці (ІБ) ЗВО та розробити систему заходів протидії цим ризикам;

− розробити проєкт політики інформаційної безпеки, врахувавши організаційно-технічні заходи з метою мінімізації ризиків ІБ ЗВО;

Об'єктом дослідження є система захисту інформації у закладах вищої освіти. Предметом дослідження – методи та способи управління процесами інформаційної безпеки ЗВО для забезпечення захисту інформаційних активів. Припущення дослідження полягає в тому, що запропоновані заходи підвищать рівень інформаційної безпеки ЗВО. Теоретична значущість дослідження полягає в реалізації цілісного підходу до розробки політики інформаційної безпеки підприємства.

Для виконання роботи було використано такі **методи дослідження**, як системний аналіз, спостереження, моделювання, порівняння, експертне оцінювання, ранжування, нормування, теорія ймовірностей, теорія прийняття рішень, теорія захисту інформації.

Наукова новизна роботи полягає в тому, що шляхом експертного оцінювання визначено ризики, які становлять загрозу ІБ для ЗВО, що дозволяють розробити оптимальну систему організаційно-технічних засобів захисту інформаційних активів організації. Ця система заходів практично імплементується через політику інформаційної безпеки ЗВО.

Інформаційний аналіз предметної області.

У статті [1] досліджено проблеми управління інформаційною безпекою в дистанційних лабораторіях закладів вищої освіти. Автори пропонують модель інтеграції безпеки на основі стандартів та правових засад для оптимізації адміністративних ресурсів. Застосовано дедуктивний метод та експериментальне дослідження з використанням семи визначених фаз. Результати включають симуляцію оцінки безпеки, архітектуру дистанційної лабораторії та модель інтеграції безпеки. Висновки підкреслюють важливість аналізу безпеки для забезпечення конфіденційності, цілісності та доступності інформації.

Стаття [2] надає критичний огляд останніх досліджень з управління інформаційною безпекою в університетах. Автор аналізує ключові тенденції, методологічні підходи та прогалини в дослідженнях, опублікованих за останнє десятиліття. Виявлено, що, незважаючи на критичну важливість управління безпекою, ця сфера все ще потребує глибшого вивчення. Особлива увага приділяється зростаючим загрозам для персональних та дослідницьких даних в академічних установах. Автор статті наголошує на необхідності подальших досліджень та розробки стратегій для зміцнення інформаційної безпеки в університетах.

У дослідженні [3] розглядаються наслідки цифрової трансформації для кібербезпеки в закладах вищої освіти. Автор проводить систематичний огляд літератури, використовуючи PRISMA-фреймворк, для оцінки поточних кіберзагроз. Виявлено, що цифровізація освіти приносить як переваги, так і численні виклики, пов'язані з кібербезпекою. Стаття підкреслює необхідність підвищення обізнаності та впровадження стратегій захисту систем вищої освіти. Результати дослідження мають на меті сприяти розробці ефективних заходів кіберзахисту в академічному середовищі.

У звіті EDUCAUSE представлено десять основних IT-питань, що стосуються вищої освіти, з особливим акцентом на інформаційну безпеку [4]. Розглядаються виклики, пов'язані з конфіденційністю, ризиками та впровадженням технологій. Звіт дає рекомендації щодо стратегій управління безпекою та підвищення обізнаності в академічних установах. Також обговорюються тенденції та технології, що впливають на IT-ландшафт вищої освіти. Звіт слугує ресурсом для освітніх лідерів у плануванні та прийнятті рішень щодо IT.

У роботі [5] розглядаються аспекти інформаційної безпеки в закладах вищої освіти. Автори підкреслюють важливість постійної освіти та обізнаності про кіберзагрози серед студентів і персоналу. Пропонуються стратегії, включаючи обов'язкові курси та регулярні повідомлення про нові загрози. Також обговорюється необхідність ретельного вибору партнерів та постачальників для забезпечення безпеки даних. Посібник дає практичні поради для зміцнення кібербезпеки в академічному середовищі.

У статті [6] аналізується стан кібербезпеки у вищій освіті, зосереджуючись на основних проблемах та тенденціях. Автори зазначають, що

освітні установи стали основними цілями для кіберзлочинців, зокрема через відкритий характер академічного середовища. Розглядаються наслідки атак, включаючи витоки даних та порушення роботи установ. Стаття також обговорює стратегії захисту та відновлення після кіберінцидентів. Надаються рекомендації для зміцнення кібербезпеки в університетах та коледжах.

У звіті [7] розглянуто три основні проблеми кібербезпеки, з якими стикаються університети та коледжі. Автори вказують на надмірно великі поверхні атак, недостатню обізнаність про кіберзагрози та обмежені ресурси для захисту. Аналізуються дані про зростання кібератак на освітній сектор та їх наслідки. Звіт також пропонує стратегії для зменшення ризиків та підвищення рівня безпеки. Рекомендації спрямовані на покращення кіберзахисту в академічних установах.

У документі [8] обговорюються способи зміцнення кібербезпеки у вищій освіті для юридичних відділів та керівників. Розглядаються основні кіберзагрози, що стоять перед коледжами та університетами, включаючи витоки даних та атаки на інфраструктуру. Автори підкреслюють важливість співпраці між юридичними та IT-відділами для забезпечення безпеки. Пропонуються стратегії управління ризиками та реагування на інциденти. Документ слугує керівництвом для юридичних департаментів у сфері кібербезпеки.

Стаття [9] містить огляд заходів з підвищення кібербезпеки у вищій освіті; акцентовано увагу на ролі постійного навчання та обізнаності у боротьбі з кіберзагрозами. Розглядаються методи підвищення обізнаності серед студентів та персоналу. Також обговорюється впровадження політик безпеки та технічних заходів захисту; надаються рекомендації для покращення кібербезпеки в академічному середовищі.

Агентство CISA надає ресурси та програми для підвищення безпеки в освітніх установах [10]. Розглядаються цифрові та фізичні загрози, з якими стикаються заклади освіти. CISA співпрацює з освітніми установами для розробки планів безпеки та створення безпечного навчального середовища. Пропонуються інструменти для запобігання, реагування та відновлення після надзвичайних ситуацій. Агентство також сприяє розвитку кар'єри в галузі кібербезпеки серед студентів.

У роботах [11-15] обговорюються проблеми кібербезпеки, які виникли у школах під час пандемії COVID-19. Автори зазначають, що перехід до дистанційного навчання посилив існуючі вразливості в цифрових системах. Розглядаються випадки атак на освітні установи та їх наслідки. Стаття підкреслює необхідність інвестування в кібербезпеку та підвищення обізнаності. Наводяться приклади виявлення вразливостей та рекомендації для покращення безпеки.

Результати досліджень. Під час виконання дослідження було проаналізовано матеріали відомих інформаційних джерел і встановлено, що на сьогодні існує велика кількість мережевих атак, які здійснюються з метою порушення конфіденційності, цілісності та доступності інформаційних ресурсів. Залежно від рівня навиків, мотивації та можливостей зловмисників отримати доступ до ресурсів локальних комп'ютерних мереж та їхнього обладнання, вони можуть завдати різного ступеня шкоду, тому ці чинники потрібно враховувати при формуванні системи кіберзахисту в організації. Згідно з дослідженням, яке провели у 2024 році експертно-аналітичні центри США, Identity Theft Resource Center (ITRC) та ЄС, Агентство Європейського Союзу з кібербезпеки (ENISA), встановлено, що керівників організацій в останні кілька років хвилюють загрози, які виходять від дій власних співробітників (рис. 1).

Рисунок 1 – Співвідношення небезпеки внутрішніх і зовнішніх загроз

Для виявлення загроз інформаційній безпеці необхідно визначити можливості порушення основних властивостей інформації в процесі роботи.

Ідентифікація та визначення загроз інформаційній безпеці має бути систематичними і періодичними, причому не лише на етапі створення системи захисту інформації, а й на етапі її функціонування. Необхідно встановити порядок оперативного виявлення та усунення загроз інформаційній безпеці, щоб запобігти можливим збиткам.

Оцінка потенційних загроз безпеці відбувається через формування експертної групи, яка проводить аналіз вразливостей. Завдяки якісному формуванню експертної групи ступінь суб'єктивності в оцінці загроз можна звести до

мінімуму. Склад експертної групи встановлюється відповідно до вимог інформаційної безпеки і не може містити менше трьох осіб. Крім того, цей метод дослідження не містить високих матеріальних витрат, оскільки для його реалізації можна залучити фахівців із власної організації. Проте не слід забувати, що цей метод включає людський фактор, який вносить певний ступінь суб'єктивності і тому може призвести до переоцінки експертами прогнозів і припущень, зроблених у процесі ідентифікації загроз інформаційній безпеці.

Слід мати на увазі, що до складу експертної групи не можна включати тих працівників, які підпадають безпосередньо під той самий управлінський контроль, оскільки це посилить можливість залежної оцінки. Крім того, експерти не повинні мати особистих, комерційних чи інших інтересів у прийнятті рішення, що також досить важко визначити.

Загрози інформаційній безпеці визначаються систематично шляхом здійснення безперервного процесу виявлення та визначення загроз, подальшого визначення джерела загрози та оцінки можливої шкоди у разі її реалізації. Загрози інформаційній безпеці постійно переглядаються та переоцінюються. Автоматизований моніторинг може бути реалізований як керівництвом підприємства, так і адміністратором безпеки. Спостереження та регулювання дій персоналу є частиною системної методології виявлення загроз. Спроба неправомірного доступу працівника того чи іншого рівня до конфіденційної інформації буде зареєстрована в системі інформаційного ресурсу, після чого буде розпочато процедуру виявлення відповідного порушення.

Під час роботи інформаційної системи її відповідний співробітник може налаштувати її основну конфігурацію для надання пріоритетів інформаційної значущості відповідно до появи нових загроз або нових законодавчих вимог.

Необхідність переоцінки загроз інформаційній безпеці також виникає, коли відбуваються зміни в основних компонентах інформаційної системи, оскільки це може призвести до появи нових вразливостей разом із свіжою інформацією про можливих порушників та виявлення вразливостей.

Інформаційний аналізі існуючого стану мережевої інфраструктури. Для проведення наукового дослідження було обрано ЗВО Львівський державний університет безпеки життєдіяльності (ЛДУБЖД). Базова структура мережі ЗВО Львівського державного університету безпеки життєдіяльності представлена на рисунку 2.

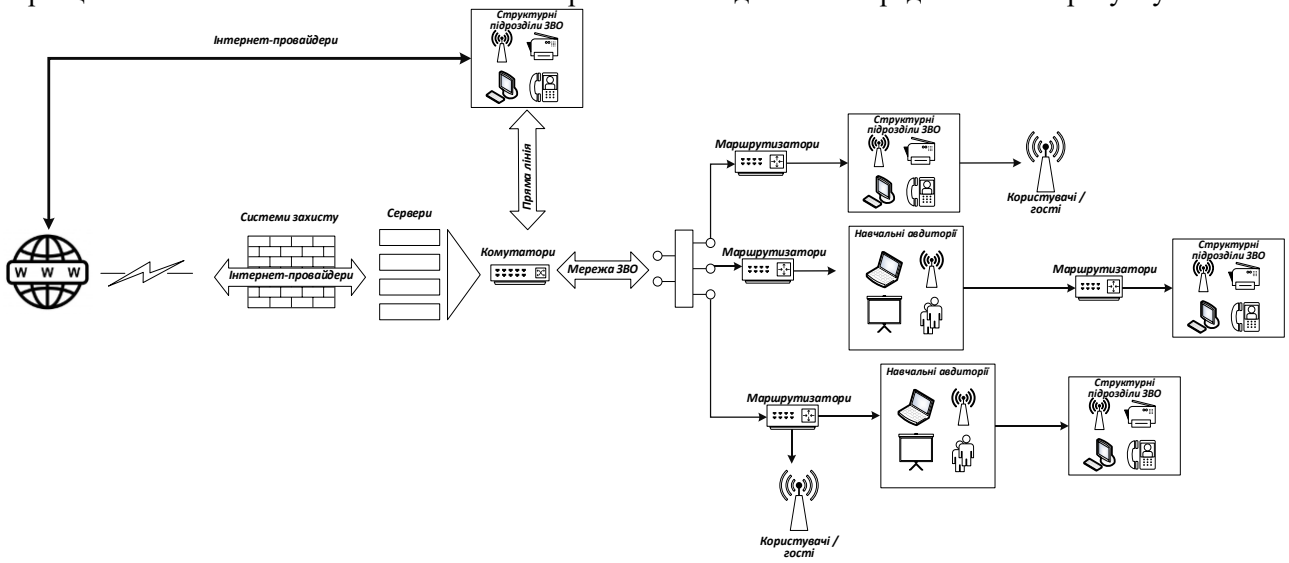

Рисунок 2 – Узагальнена структура мережі ЛДУБЖД

Інформаційна інфраструктура складається з угруповань комп'ютерів. Основними елементами інфраструктури є: мережевий шлюз; сервери; комутаційне обладнання. Повсякденна робота підрозділів неможлива без використання серверів, оскільки інформаційно-комунікаційна мережа організації включає їх у свою структуру побудови. Для 192 мережі доступ до Інтернету надається через мережевий шлюз, який функціонуватиме як брандмауер. Система виявлення вторгнень (англ. Intrusion Detection System, IDS), яка вбудована у брандмауер включає ведення чорного списку IP-адрес, виявлення вторгнень у протоколі Simple Mail Transfer Protocol (SMTP), захист від атак Denial of Service (DOS) та Distributed Denial of Service (DDOS) і їх журналювання. Керування додатками включає їх блокування (виявлення дій понад 1000 додатків), планування та контроль пропускної здатності для вибраних. Веб-інтерфейс брандмауера DFL-870 зображено на рисунку 3.

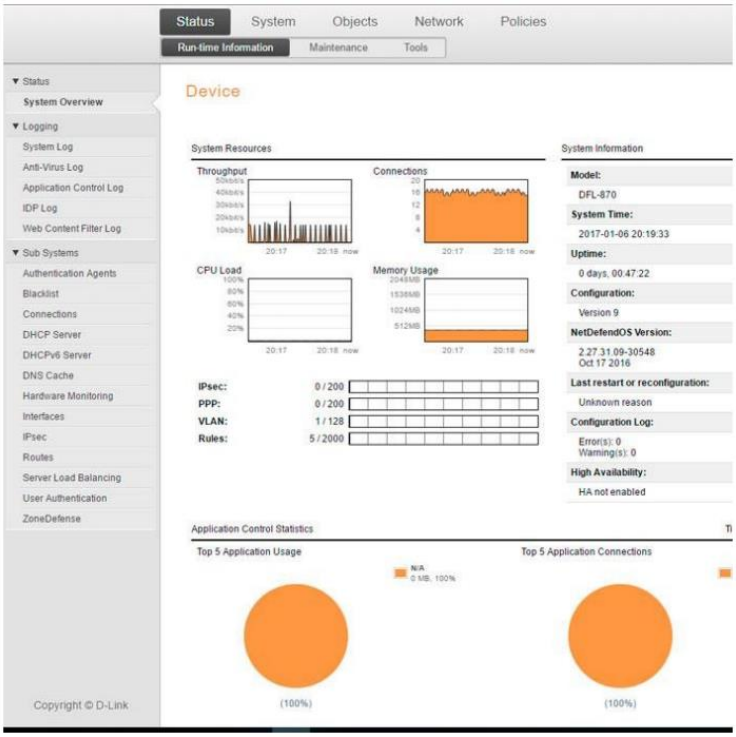

Рисунок 3 – Веб-інтерфейс мережевого шлюзу D-Link

Некеровані комутатори представляють активні мережеві пристрої. Це ефективні інструменти, які дозволяють швидко розгорнути локальну мережу всередині ЗВО. Комутатори, які мають багато версій, більшість із яких у ЗВО призначені для підтримки передачі інформації за допомогою інших стандартів і протоколів. Структурована кабельна мережа сформована за топологією «Зірка». Через обмежену кількість доступних портів у більшості приміщень кожен має власний комутатор. Усі комп'ютери підключені до однієї мережі та мають доступ до Інтернету за статичною або змінною IP. Облікові записи користувачів і облікові записи адміністратора для налаштування системи існують на кожному комп'ютері.

Окремо слід відзначити підключення великої кількості мережевих принтерів, в кожному структурному підрозділі, що дозволяє управляти друком, здійснювати його резервування, планування. Інше обладнання, підключене до автоматизованих робочих станцій співробітників, не має прямого доступу до мережі підприємства; або підключається самостійно (платіжні термінали), або не потребує використання мережі.

Оскільки організація в своїй роботі використовує інформаційні системи, захист інформації базується на використанні засобів криптографічного захисту. Електронні підписи використовуються разом із системою АСКОД для перевірки користувачів і даних.

Модель загроз, для її побудови, потребує деталізації розгляду, оскільки вона визначає рівень захисту. Це необхідно здійснити з метою визначення рівня та вимог до забезпечення безпеки цінних інформаційних ресурсів, а також з метою визначення обґрунтованості впровадження заходів захисту цінної інформації. Слід зазначити, що створена в рамках дослідження модель загроз передбачає методичний процес їх ідентифікації інформаційній безпеці. Під час ідентифікації загроз інформаційній безпеці визначено як розташування обладнання, так і межі системи. Інформаційна система розгорнута в конструкції будівлі, межа якої є контрольованою зоною. Інформаційна система має локальну мережу, яка обробляє інформацію різного рівня конфіденційності; мережа фізично з'єднується з комутатором і логічно відокремлена брандмауером, який пропонує фільтрацію пакетів.

Результати визначення походження загрози наведені в таблиці 1. Ці загрози призводять до порушення властивостей інформації: конфіденційності, цілісності та доступності. Дана таблиця сфомована на основі аналізу таких документів [16-18] :

– ДСТУ 13335-1:2001 (Інформаційна технологія. Настанови щодо управління безпекою інформації. Частина 1. Концепції та моделі безпеки інформації);

– ISO/IEC 27005:2022 (Information technology — Security techniques — Information security risk management);

– Методика моделювання загроз та порушників, затверджена наказом Адміністрації Держспецзв'язку України № 801 від 08.12.2005 (зі змінами).

Таблиця 1

Джерела загроз інформаційній безпеці ЗВО

Джерело загроз	**Тип джерела загроз**	**Використовувані вразливості**	**Способи реалізації загроз**	**Об'єкт інформаційної системи**	**Результат реалізації загроз інформаційної безпеки**
Внутрішній порушник	Людський (антропогенний)	Вразливості в системах захисту інформації від несанкціонованого доступу, відсутність організаційних та технічних заходів	Знищення інформації, викрадення конфіденційної інформації	Комп'ютерна мережа	Порушення конфіденційності, цілісності та доступності інформації
Зовнішній порушник	Людський (антропогенний)	Недостатній рівень організаційно-технічного захисту інформації	Витік інформації через побічні електромагнітні випромінювання та наводки	Комп'ютерна мережа	Порушення конфіденційності інформації
Збій апаратного або програмного забезпечення	Техногенне джерело	Низька якість програмних або технічних засобів, перебої в охолодженні, електропостачанні, помилки обслуговуючого персоналу	Витік інформації, відмова обладнання, порушення роботи технічних засобів	Комп'ютерна мережа	Порушення конфіденційності, цілісності та доступності інформації
Стихійне лихо	Природне джерело	—	Пожежа у приміщенні, де розміщена інформаційна інфраструктура	—	Порушення конфіденційності, цілісності та доступності інформації

Рівень інформаційної загрози встановлюється через належний рівень умінь правопорушників здійснювати кібератаку. Рисунок 4 ілюструє модель порушника та результати його можливостей.

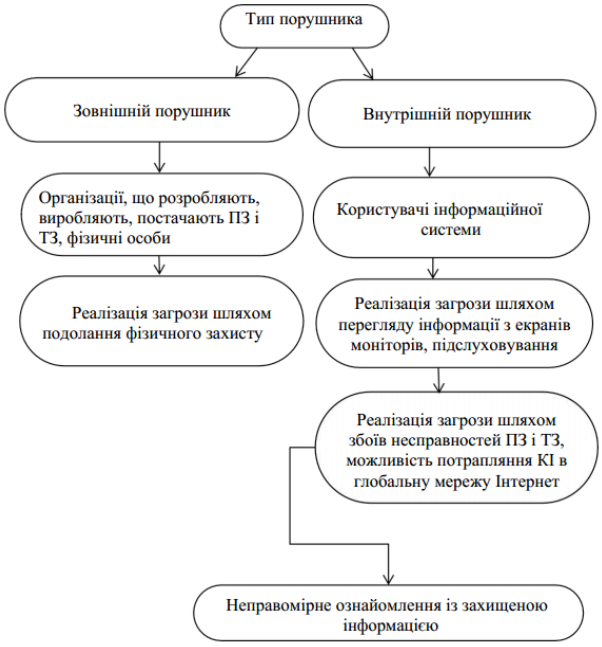

Рисунок 4 – Модель порушника для ЗВО на прикладі ЛДУБЖД

Провівши аналіз стану інформаційно-комунікаційної мережі ЗВО було визначено, що більшість індикаторів безпеки мають низький рівень захисту, тому доцільно розглядати покращення інформаційної безпеки та кіберзахисту через оновлення ПІБ закладу вищої освіти.

У ЛДУБЖД використовується окрема службова кімната з обмеженим доступом для зберігання серверного обладнання (металеві двері, грати на вікнах). Всі технічні приміщення закриваються на ключ, доступ до цих приміщень. обмежений часом роботи в організації (електрощитова, склад мийних засобів, кімната для зберігання мийного обладнання). Інженерно-технічний комплекс представлений системою відеоспостереження, екрануванням вікон, захистом персоналу (металеві двері, грати на вікна). Захист конфіденційної інформації та бухгалтерської документації представлений великим металевим сейфом, який розміщено у фінансовому відділі.

Для вирішення проблем і роботи над поставленими завданнями всі потоки центруються за допомогою централізованої консолі. Прикладом цього в управлінні інформаційними потоками може бути міжмережевий екран D-Link, оскільки він дозволяє контролювати трафік і керувати ним відповідно до потреб. Звіти повинні постійно переглядатися адміністратором безпеки. Такий підхід до забезпечення централізованого управління інформаційною безпекою може сприяти підвищенню ефективності та результативності разом з оптимізацією роботи з інформаційної безпеки ЗВО.

Аналіз та оцінка ризиків для забезпечення управління інформаційною безпекою. Оцінка загроз даних є ключовим способом захисту освітньої організації від небезпек. Завдяки цьому ви можете побачити, наскільки все безпечно. Слід пам'ятати про те, що багато способів підтримувати безпеку інформаційних цінностей ЗВО, представлених в деяких посібниках та правилах, розглядають більшість технічних частин, які зараз є найвідомішими (рис. 5). Але часто залишаються поза увагою деякі інші моменти: контроль роботи всієї системи та системи захисту інформаційних активів за участю співробітників організації та оцінка ступеня надійності співробітників у роботі, пов'язаній з цінними інформаційними ресурсами. Таким чином, розробка сучасного робочого інструментарію у сфері оцінки захищеності цінних інформаційних ресурсів є необхідною задачею з огляду на підвищення рівня управління захистом інформації. Відповідно до поставлених завдань буде проведено аналіз та розроблено методику розрахунку ризиків, які можуть бути.

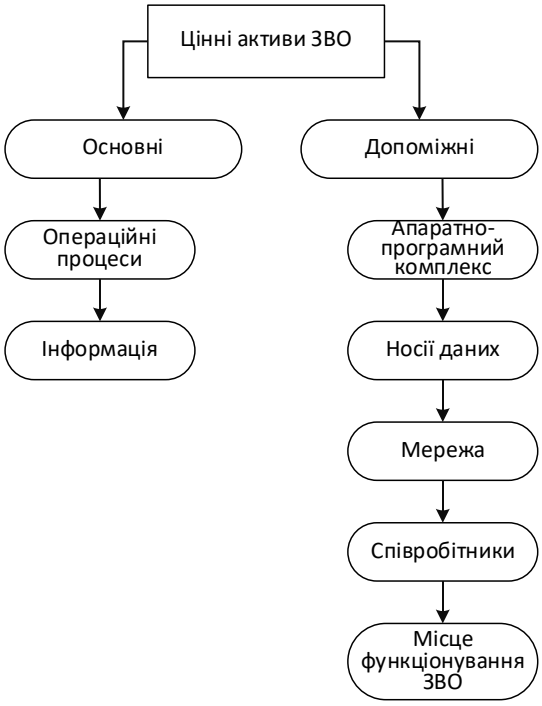

Рисунок 5 – Схема основних і допоміжних активів ЗВО

Розрахунок згідно з методикою оцінювання рівня ризику порушення безпеки інформації в ІТС (Наказ Держспецзв'язку України № 801 від 08.12.2005 р.) повинен починатися з виконання заходів, звідки можна отримати звіт із сумарними результатами всіх заходів для оцінки ступеня ризиків на організації. У нашому випадку ми розглядаємо корпоративну інформаційну систему, яка має доступ до глобальної мережі Інтернет. Також беремо до уваги, що активи, які мають цінність для освітньої організації, необхідно розділити на основні та допоміжні.

Впровадження ризику, спрямованого на цілісність, доступність або конфіденційність, не матиме наслідків, загалом для ЗВО та його повсякденних операційних процесів зокрема. Розглянемо детальніше:

– реалізація ризику, спрямованого на цілісність, доступність або конфіденційність, призведе до незначних збитків для ЗВО, коли відновлення до вихідного стану можливе без зупинки операційних процесів;

– реалізація ризику, спрямованого на цілісність, доступність або конфіденційність, призведе до значних фінансових втрат або негативного матеріального впливу на репутацію організації за обставин, коли відновлення до початкового стану можливе, але потребує значних фінансових витрат або витрат часу;

– прояв ризику, спрямованого на цілісність, доступність або конфіденційність, призведе до повної зупинки операційних процесів, чинитиме

великий негативний вплив на значні фінансові втрати та на репутацію організації.

Представлена таблиця 2 є результатом ідентифікації критичних інформаційних активів організації та їх якісної оцінки за трьома базовими характеристиками інформаційної безпеки: конфіденційністю, цілісністю та доступністю. Такий підхід дозволяє здійснити ранжування активів за ступенем важливості та подальше коректне моделювання ризиків, відповідно до методичних рекомендацій міжнародного стандарту ISO/IEC 27005:2022 або національних нормативів у сфері технічного захисту інформації. Категоризацію можна здійснити на основі цієї таблиці. Основною характеристикою є те, що найбільшу шкоду повсякденним операційним процесам ЗВО можуть завдати загрози доступності комутаторів, маршрутизаторів, програмного та апаратного забезпечення, а не загрози, спрямовані на порушення конфіденційності щодо цінної інформації.

Таблиця 2

Таблиця цінності активів ЗВО

Ідентифікатор	**Актив підприємства**	**Конфіденційність**	**Цілісність**	**Доступність**	**Цінність активу**
A	Відомості, які необхідні для функціонування закладу вищої освіти	3	4	4	3
B	Відомості особистого (конфіденційного) характеру	4	2	2	3
C	Стратегічні відомості, які необхідні для досягнення цілей ЗВО	3	2	3	3
D	Відомості, на опрацювання яких потрібен тривалий час та великі затрати	2	2	3	2
E	Апаратно-програмний комплекс	–	4	3	3
F	Носії інформації	–	3	2	2
G	Мережа	–	3	4	3
H	Співробітники	–	2	1	2
I	Місце функціонування ЗВО	–	2	1	2

Далі було оцінено ризики інформаційної безпеки ЗВО. Аналіз ризику можна розглядати як процес, який є ітераційним і дозволяє збільшити деталізацію в оцінці ризиків у наступних ітераціях. Модель алгоритму аналізу та оцінки ризиків ЗВО наведено на рисунку 6. Контекст ризику передбачає встановлення критеріїв для управління ризиками та призначення відповідальних співробітників, які займаються питаннями, пов’язаними із забезпе-ченням безпеки, у нашому випадку – це постійна група.

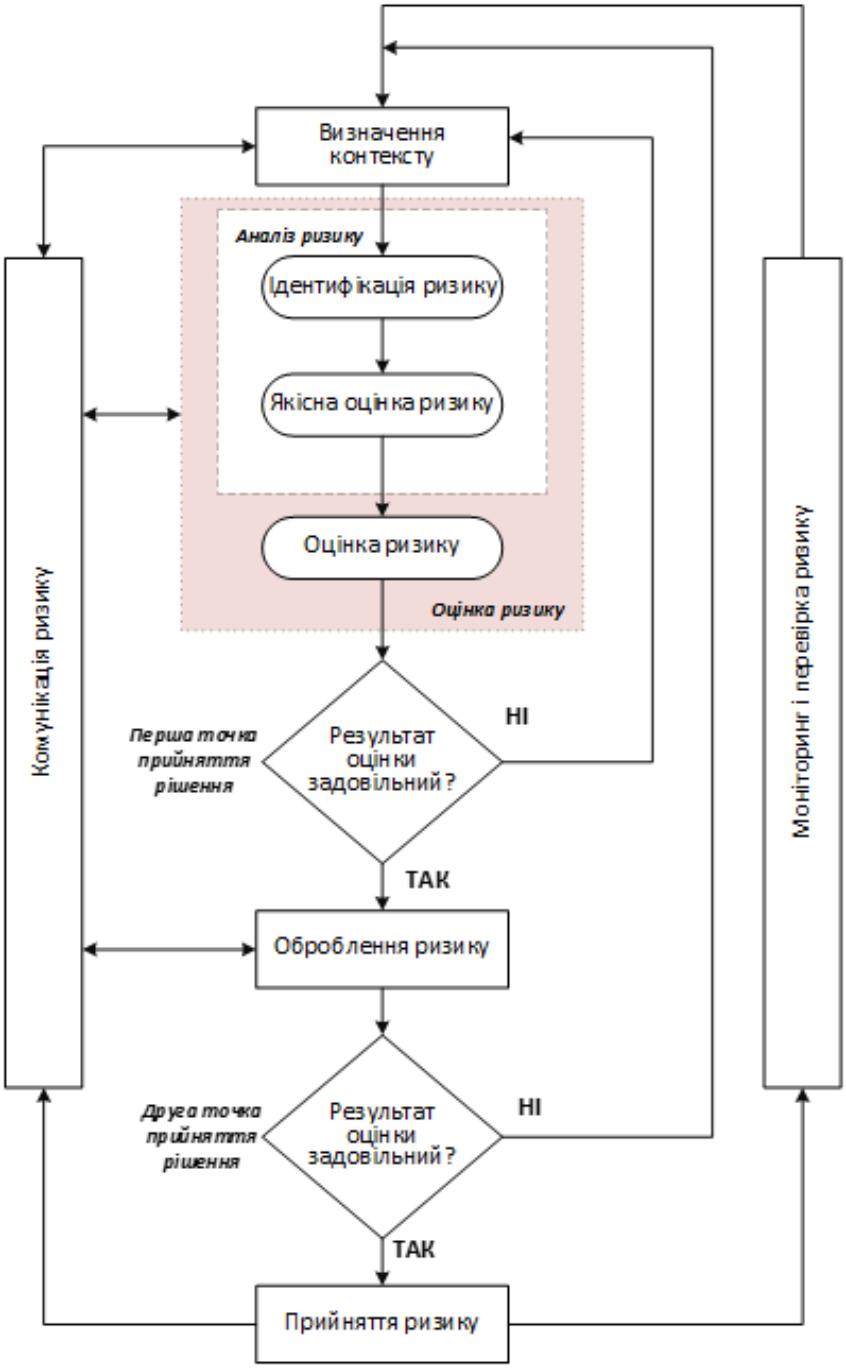

Рисунок 6 – Алгоритм аналізу та оцінки ризиків інформаційної безпеки ЗВО

Ідентифікація ризиків включає діяльність з виявлення та опису ризиків. Оцінка ризику – це оцінка наслідків реалізації ризику та ймовірності його реалізації. Прийняття ризику – це втрата від матеріалізації цього ризику, яка вважається оптимальною, тоді як ймовірність його матеріалізації є низькою, що полегшує процедури обробки ризику, які не виконуються. Комунікація ризиків передбачає обмін повідомленнями щодо реальних ризиків між усіма залученими сторонами. Управління ризиками означає діяльність, спрямовану або на зменшення ймовірності реалізації ризику, або на зменшення впливу ризиків, коли вони матеріалізуються. На рисунку 7 наведено функціональну модель оброблення ризиків ІБ ЗВО.

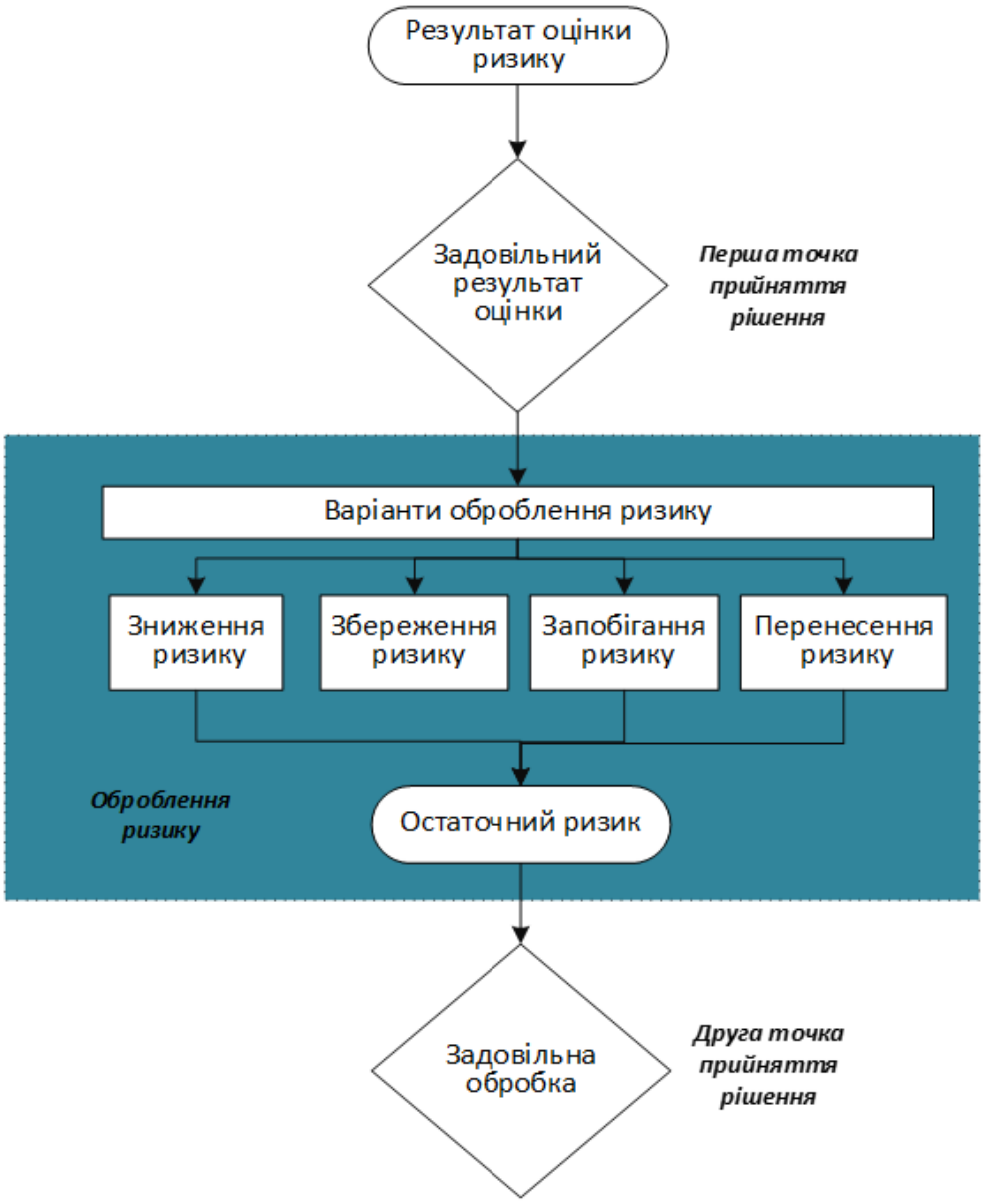

Рисунок 7 – Функціональна модель оброблення ризиків інформаційної безпеки ЗВО

Наступним кроком є визначення ступеня вразливості кожного з цінних активів ЗВО. Ідентифікацію загроз та формування ризиків ІБ було проведено методом мозкового штурму. За результатами роботи було сформовано перелік загроз ІБ для ЗВО, які наведені у таблиці 3.

Таблиця 3

Перелік загроз ІБ для ЗВО та їхні шифри

Назва загрози	Шифр загрози
Надлишкове виділення оперативної пам’яті для користувача на сервері	$З_{01}$
Завантаження адміністратором не штатної операційної системи (піратської, не ліцензованої або іншої)	$З_{02}$
Змінення компонентів інформаційної системи	$З_{03}$
Тривалої затримки обчислювальних потужностей користувача	$З_{04}$

Продовження таблиці 3

Назва загрози	Шифр загрози
Втрати обчислювальних потужностей загальної інформаційно-комунікаційної системи	$З_{05}$
Використання слабких місць протоколів мережевого/локального обміну інформації	$З_{06}$
Втрати носіїв інформації	$З_{07}$
Дослідження зловмисником механізмів роботи програми	$З_{08}$
Маскування дій шкідливого коду	$З_{09}$
Несанкціонованого видалення інформації, яка захищається	$З_{10}$
Впровадження шкідливого коду через рекламу, сервіси, контент	$З_{11}$
Перезавантаження апаратних і програмних засобів обчислювальних потужностей інформаційно-комунікаційної мережі	$З_{12}$
Фізичного старіння апаратних компонентів системи інформаційно-комунікаційної мережі	$З_{13}$
Пошкодження системного реєстру (при його наявності)	$З_{14}$
Поширення вірусу через електронну пошту	$З_{15}$
Підвищеного привілею окремим користувачам	$З_{16}$
Неправомірне шифрування інформації	$З_{17}$
Подолання фізичного захисту (доступ в приміщення, сейф, серверну, тощо)	$З_{18}$
Викрадення засобів зберігання, оброблення, вводу/виводу/передачі інформації	$З_{19}$
Програмного виведення із роботи засобів зберігання, оброблення, вводу/виводу/передачі інформації	$З_{20}$
Фізичного виведення із роботи засобів зберігання, оброблення, вводу/виводу/передачі інформації	$З_{21}$
Блокування інформаційно-комунікаційної мережі (а також відмовлення в обслуговуванні користувача)	$З_{22}$
Форматування носіїв інформації	$З_{23}$

Проведення оцінки, оброблення ризиків до прийнятного рівня проводилось методом експертного оцінювання. Такий вид оцінювання проводився шляхом заповнення анкети експертами за допомогою спеціальної форми (рис. 8.).

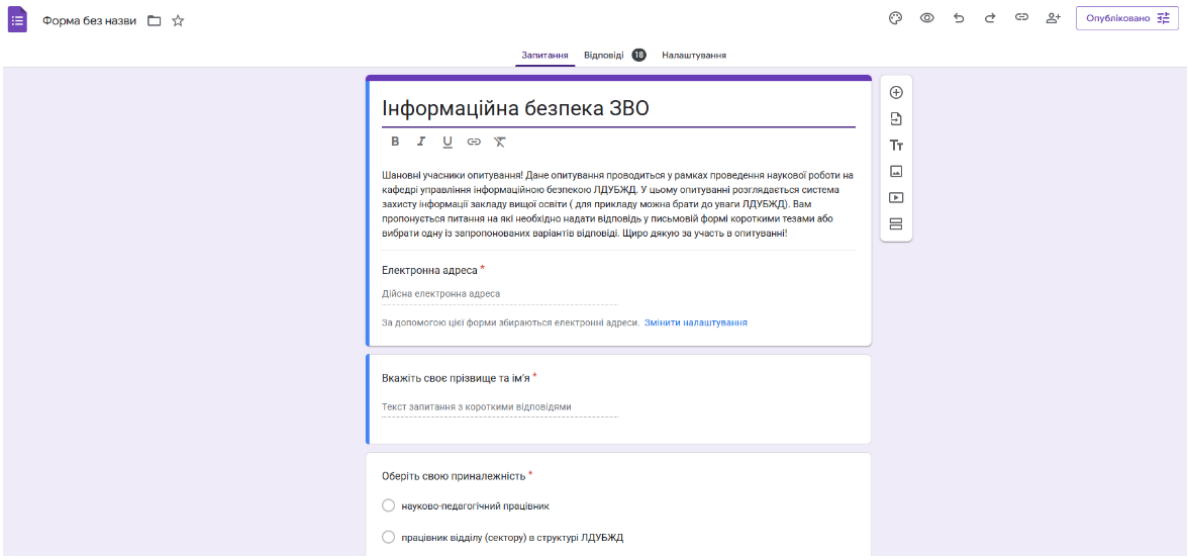

Рисунок 8 – Зразок форми для експертного оцінювання ризиків ЗВО

Результатами експертного оцінювання наведено в табл. 2.4. Загалом в експертному оцінюванні прийняли 17 осіб.

Таблиця 4

Результати експертного оцінювання ризиків ІБ ЗВО

Шифр загрози	E1	E2	E3	E4	E5	E6	E7	E8	E9	E10	E11	E12	E13	E14	E15	E16	E17	E норм.
301	3	3	2	6	2	6	8	3	2	5	4	1	6	1	5	7	5	4,1
302	3	5	2	5	2	10	8	6	7	6	9	2	10	3	5	9	8	5,9
303	4	6	5	7	3	4	9	5	3	4	7	9	7	5	5	5	7	5,6
304	5	5	9	6	3	6	7	5	7	3	5	8	6	8	5	7	6	5,9
305	4	5	10	7	3	7	9	8	7	8	8	8	6	10	5	7	5	6,9
306	7	7	10	8	10	10	9	9	2	7	9	8	10	10	5	9	7	8,1
307	9	6	10	7	5	9	8	9	5	8	10	10	10	10	5	10	10	8,3
308	7	7	8	8	9	10	8	8	5	9	9	6	10	10	5	7	9	7,9
309	7	8	10	8	10	10	9	9	3	8	10	9	10	10	5	8	9	8,4
310	8	7	10	7	9	10	9	9	3	8	9	10	10	10	5	7	8	8,2
311	9	7	5	9	10	10	9	8	5	8	8	7	10	10	5	10	8	8,1
312	8	6	2	7	5	8	8	7	5	8	6	9	7	10	5	8	7	6,8
313	5	9	3	8	7	7	7	5	5	7	6	5	10	8	5	7	6	6,5
314	6	5	3	7	9	7	8	5	5	6	6	10	10	9	5	7	8	6,8
315	9	8	4	9	9	9	8	8	5	5	8	0	10	8	5	10	7	7,2
316	3	7	2	6	8	9	8	8	5	6	7	3	10	10	5	4	8	6,4
317	6	7	2	6	8	9	8	5	5	7	7	3	8	10	5	4	7	6,3
318	4	5	8	5	4	10	9	8	5	9	8	10	10	1	5	9	6	6,8
319	7	6	6	7	4	10	9	8	5	9	8	10	10	10	5	8	3	7,4
320	7	7	6	8	6	10	9	7	5	3	8	10	10	5	5	6	3	6,8
321	7	5	7	7	4	9	9	7	5	8	8	10	7	5	5	7	2	6,6
322	7	8	9	8	6	7	9	7	5	8	7	10	6	6	5	8	5	7,1
323	6	6	10	7	3	8	9	7	5	8	6	10	6	2	5	8	4	6,5

Для дослідження адекватності отриманих результатів було використано штучний інтелект. Для цього було обрано «Чат GPT». Порівняльний аналіз його роботи із нормалізованими оцінками експерті представлено у таблиці 5.

Таблиця 5

Порівняльний аналіз оцінювання експертів із результатами оцінювання ризиків за допомогою моделі штучного інтелекту

Шифр загрози	E норм.	E ші	$\Delta\delta$
301	4,1	4	0,1
302	5,9	6	0,1
303	5,6	7	1,3
304	5,9	5	0,9
305	6,9	8	1,1
306	8,1	9	0,9
307	8,3	8	0,3
308	7,9	7	0,9
309	8,4	9	0,6
310	8,2	9	0,8
311	8,1	8	0,1
312	6,8	6	0,8
313	6,5	6	0,5
314	6,8	5	1,8
315	7,2	8	0,8
316	6,4	9	2,6
317	6,3	9	2,7
318	6,8	8	1,2
319	7,4	8	0,6
320	6,8	8	2,2
321	6,6	8	1,4
322	7,1	9	1,9
323	6,5	9	2,5

Увагу необхідно приділити ризикам, які мають відхилення показників більше ніж на дві позиції. У нашому випадку це такі: загроза підвищеного привілею окремим користувачам ($З_{16}$), загроза неправомірного шифрування інформації ($З_{17}$), загроза програмного виведення із роботи засобів зберігання, оброблення, вводу/виводу/передачі інформації ($З_{20}$) та загроза блокування інформаційно-комунікаційної мережі, а також відмова в обслуговуванні користувача ($З_{22}$).

Загальний рівень ризику інформаційної безпеки ЗВО засвідчив те, що показники ризику є високими, а загрози можуть бути критичними. Ризики, які мають значення понад 6, необхідно мінімізувати. На підтримку методики програмного аналізу технічних засобів планується реалізація організаційних заходів, які забезпечать зменшення рівня можливих загроз для процесів інформаційної безпеки та кіберзахисту при успішній їх реалізації. Ці заходи повинні мати вплив на апаратно-програмний комплекс і мережеву інфраструктуру, в якій обробляється та передається цінна інформація. Після обробки ризиків прийнятним для кожної поточної загрози інформаційній безпеці став залишковий ризик. Залишковий ризик став чисельно прийнятним у значенні до 6.

Досвід практичної діяльності показує, що впровадження ПІБ в організації є ефективним інструментом підвищення рівня інформаційної діяльності та кіберзахисту. Заходи безпеки, які

прописані в політиці, спрямовані на зменшення рівня ризику. Часто такий підхід не потребує значних фінансових витрат, оскільки ці заходи мають організаційний характер, а у організації уже є робочі інструменти для їх впровадження.

Розробка інженерно-технічних заходів щодо забезпечення інформаційної безпеки ЗВО. Відповідно до проведеного аналізу захисту інформаційно-комунікаційної мережі ЗВО ЛДУБЖД, описаного вище, пропонуються такі заходи:

− комутаційне обладнання має бути встановлене в спеціалізованих стійках або металевих шафах із замками, які можна закрити на ключ.

− виконати належну перевірку структурної установки кабелю, щоб дізнатися, чи можна прокласти мережевий кабель таємно, подалі від прямого зору персоналу та користувачів (під стелею, у технічних приміщеннях, на технічних магістралях).

− для зберігання машинних носіїв має бути виділене спеціальне місце (металева шафа, що замикається, або сейф). Скласти інструкції для працівників, які мають право користування машинними носіями, вести облік видачі машинних носіїв, скласти графік доступу та список осіб, які мають доступ до спеціалізованого місця зберігання машинних носіїв.

− адміністратору інформаційної безпеки ЗВО розробити план перевірки інженерно-технічних засобів захисту інформації, у якому відображаються: а) періодичність перевірки; б) перевірка відповідності автоматизованого робочого місця (АРМ) відомостям атестаційного листа; в) перевірка відповідності приміщення відомостям атестаційного листа; г) перевірка обладнання відеоспостереження; д) перевіряти технічний стан і справність металевих дверей, стелажів з обладнанням і шаф, в яких зберігаються машинні носії інформації, сертифікати та парольна інформація на паперових носіях, документація, що містить персональні дані та конфіденційну інформацію;

− перевірити технічний стан активного та пасивного комутаційного обладнання мережевої інфраструктури підприємства;

− здійснити комплекс заходів щодо пошуку місць для встановлення засобів запису аудіо- та візуальної інформації;

− перевірка журналу на мережевому шлюзі для перевірки будь-яких можливих вторгнень ззовні;

− здійснити комплекс заходів щодо контролю систем доступу до приміщень, де проведено атестацію робочих місць та встановлено інформаційні системи обробки персональних даних (перевірка документації, списків осіб, які мають доступ, опитування про місцезнаходження ключів та магнітних карток тощо).

− розглянути комплекс заходів із запровадження систем апаратного та програмного копіювання інформації інформаційних систем обробки персональних даних (де є така можливість).

Ці заходи мають бути включені до ПІБ ЗВО, зважаючи на те, що інженерно-технічний захист є одним із основних напрямів забезпечення інформаційної безпеки.

Висновки. В результаті дослідження було обґрунтовано, що ефективне управління інформаційною безпекою в закладах вищої освіти безпосередньо впливає на стабільність функціонування освітнього процесу, безперервність операційної діяльності та захист критичних інформаційних активів. На прикладі Львівського державного університету безпеки життєдіяльності проведено повномасштабний аналіз чинних засобів захисту, який виявив наявність низького рівня безпеки в більшості підсистем інформаційної інфраструктури.

Під час дослідження ідентифіковано 23 типи загроз інформаційній безпеці, серед яких 4 були відзначені як такі, що мають відхилення у нормалізованій експертній оцінці ризику понад 2 бали між думкою експертів та моделлю штучного інтелекту. Загальний ризик для кожної загрози був визначений методом експертного оцінювання за участі 17 фахівців, а також верифікований за допомогою алгоритму ChatGPT. Загалом 16 загроз мали показник ризику понад 6 балів за 10-бальною шкалою, що підтверджує високий рівень вразливості інформаційного середовища.

На основі аналізу цінності активів було визначено, що найвищий пріоритет захисту мають мережеві компоненти та апаратно-програмні комплекси, адже саме доступність і цілісність цих елементів забезпечують безперервність функціонування ЗВО. У результаті розрахунку цінності активів, 4 об'єкти (ідентифікатори A, C, E, G) отримали оцінку важливості 3 з 5, що підтверджує їхню критичність у загальній структурі ризик-менеджменту.

Розроблена адаптивна методика аналізу технічного стану захисту інформації, що враховує організаційні та технічні параметри, дозволяє знизити рівень залишкового ризику до менше ніж 6 балів, що відповідає прийнятному рівню згідно з методикою Держспецзв'язку України (Наказ №801, 2005 р.). Крім того, запропоновані заходи, зокрема використання IDS-систем, оновлення ПІБ, фізичний захист серверних приміщень, можуть бути впроваджені без значних фінансових витрат завдяки наявній інфраструктурі.

Таким чином, усі поставлені цілі дослідження досягнуто. Отримані результати можуть бути інтегровані в реальні освітні політики з інформаційної безпеки, слугуючи прикладом ефективного управління ризиками для інших закладів вищої освіти.

Список літератури:

1. Andrade, D. A., Toapanta, M. T., Del Pozo Durango, R., & Vanegas, O. (2024). Information Security Management in a Higher Education Institution Based on Standards, Legal Basis for the Optimization of Administrative Resources. *Journal of Ecohumanism*. Retrieved from ecohumanism.co.uk/joe/ecohumanism/article/view/5039:contentReference[oaicite:5]{index=5}

2. Jiang, Y. (2025). Information Security Management at the University: A Critical Review. *ACE Proceedings*. Retrieved from ewadirect.com/proceedings/ace/article/view/17910:contentReference[oaicite:8]{index=8}

3. Siphambili, N. (2024). Exploring Cybersecurity Implications in Higher Education. *European Conference on Cyber Warfare and Security*, 23(1), 526–531. Retrieved from papers.academic-conferences.org/i ndex.php/eccws/article/view/2306:contentReference[oaicite:11]{index=11}

4. EDUCAUSE. (2020). 2020 Top 10 IT Issues. Retrieved from https://www.educause.edu/research-and-publications/research/top-10-it-issues-technologies-and-trends/2020

5. Ellucian. (2021). Information Security for Higher Education. Retrieved from .ellucian.com/assets/en/ebook/information-security-higher-education.pdf

6. BitLyft. (2023). The State of Higher Education Cybersecurity: Top Insights and Trends. Retrieved from bitlyft.com/resources/the-state-of-higher-education-cybersecurity-insights-trends

7. UpGuard. (2025). Why is the Education Sector a Target for Cyber Attacks? Retrieved from https://www.upguard.com/blog/education-sector-cyber-attacks

8. NetDocuments. (2024). Strengthening Cybersecurity in Higher Ed for GCs and Legal Departments. Retrieved from netdocuments.com/resource/strengthening-cybersecurity-in-higher-ed-for-gcs-and-legal-departments: contentReference [oaicite:30] {index=30}

9. Expert Journals. (2024). A Narrative Review on Enhancing Cybersecurity in Higher Education. *Expert Journal of Business and Management*, 12(6), 67–73. Retrieved from business.expertjournals.com/23446781-1206/:contentReference[oaicite:33] {index=33}

10. Cybersecurity and Infrastructure Security Agency (CISA). (2024). Educational Institutions. Retrieved from www.cisa.gov/audiences/educational-institutions:contentReference [oaicite:36]{index=36}

11. Newman, L. H. (2020). Schools Already Struggled With Cybersecurity. Then Came Covid-19. *WIRED*. Retrieved from wired.com/story/schools-already-struggled-cybersecurity-then-came-covid-19/:contentReference[oaicite:39]{index=39}

12. Newman, L. H. (2025). Meet the Hired Guns Who Make Sure School Cyberattacks Stay Hidden. *WIRED*. Retrieved from wired.com/story/meet-the-hired-guns-who-make-sure-school-cyberattacks-stay-hidden/:contentReference[oaicite:42]{index=42}

13. CISA. (2024). Cybersecurity Education & Training Resources. Retrieved from cisa.gov/sites/default/files/2024-02/Resources%20Collection_02062024_508c.pdf:contentReference[oaicite:45]{index=45}

14. NetDocuments. (2024). Strengthening Cybersecurity in Higher Ed for GCs & Legal Departments. Retrieved from pages.netdocuments.com/rs/549-CKV-717/images/strengthening-cybersecurity-in-higher-ed-for-gcs-and-legal-departments.pdf:contentReference[oaicite:48]{index=48}

15. BitLyft. (2023). Managed Detection and Response for Higher Education. Retrieved from https://www.bitlyft.com/managed-detection-and-response-for-higher-education:contentReference [oaicite:51]{index=51}

16. International Organization for Standardization. (2022). ISO/IEC 27005:2022 Information technology — Security techniques — Information security risk management. Geneva, Switzerland: ISO.

17. Державний комітет стандартизації, метрології та сертифікації України. (2001). ДСТУ 13335-1:2001. Інформаційна технологія. Настанови щодо управління безпекою інформації. Частина 1. Концепції та моделі безпеки інформації. Київ: Держстандарт України.

18. Адміністрація Держспецзв'язку України. (2005). Методика моделювання загроз та порушників (Наказ № 801 від 08.12.2005 із змінами). Отримано з https://cip.gov.ua

References:

1. Andrade, D. A., Toapanta, M. T., Del Pozo Durango, R., & Vanegas, O. (2024). Information Security Management in a Higher Education Institution Based on Standards, Legal Basis for the Optimization of Administrative Resources. *Journal of Ecohumanism*. Retrieved from https://ecohumanism.co.uk/joe/ecohumanism/article/view/5039:contentReference[oaicite:5]{index=5}

2. Jiang, Y. (2025). Information Security Management at the University: A Critical Review.

ACE Proceedings. Retrieved from ewadirect.com/proceedings/ace/article/view/17910:contentReference[oaicite:8]{index=8}

3. Siphambili, N. (2024). Exploring Cybersecurity Implications in Higher Education. *European Conference on Cyber Warfare and Security*, 23(1), 526–531. Retrieved from papers.academic-conferences.org/index.php/eccws/article/view/2306:contentReference[oaicite:11]{index=11}

4. EDUCAUSE. (2020). 2020 Top 10 IT Issues. Retrieved from https://www.educause.edu/research-and-publications/research/top-10-it-issues-technologies-and-trends/2020

5. Ellucian. (2021). Information Security for Higher Education. Retrieved from ellucian.com/assets/en/ebook/information-security-higher-education.pdf

6. BitLyft. (2023). The State of Higher Education Cybersecurity: Top Insights and Trends. Retrieved from bitlyft.com/resources/the-state-of-higher-education-cybersecurity-insights-trends

7. UpGuard. (2025). Why is the Education Sector a Target for Cyber Attacks? Retrieved from www.upguard.com/blog/education-sector-cyber-attacks

8. NetDocuments. (2024). Strengthening Cybersecurity in Higher Ed for GCs and Legal Departments. Retrieved from netdocuments.com/resource/strengthening-cybersecurity-in-higher-ed-for-gcs-and-legal-departments:contentReference[oaicite:30]{index=30}

9. Expert Journals. (2024). A Narrative Review on Enhancing Cybersecurity in Higher Education. *Expert Journal of Business and Management*, 12(6), 67–73. Retrieved from business.expertjournals.com/23446781-1206/:contentReference[oaicite:33]{index=33}

10. Cybersecurity and Infrastructure Security Agency (CISA). (2024). Educational Institutions. Retrieved from cisa.gov/audiences/educational-institutions:contentReference[oaicite:36]{index=36}

11. Newman, L. H. (2020). Schools Already Struggled With Cybersecurity. Then Came Covid-19. *WIRED*. Retrieved from wired.com/story/schools-already-struggled-cybersecurity-then-came-covid-19/:contentReference[oaicite:39]{index=39}

12. Newman, L. H. (2025). Meet the Hired Guns Who Make Sure School Cyberattacks Stay Hidden. *WIRED*. Retrieved from wired.com/story/meet-the-hired-guns-who-make-sure-school-cyberattacks-stay-hidden/:contentReference[oaicite:42]{index=42}

13. CISA. (2024). Cybersecurity Education & Training Resources. Retrieved from cisa.gov/sites/default/files/2024-02/Resources%20Collection_02062024_508c.pdf:contentReference[oaicite:45]{index=45}

14. NetDocuments. (2024). Strengthening Cybersecurity in Higher Ed for GCs & Legal Departments. Retrieved from pages.netdocuments.com/rs/549-CKV-717/images/strengthening-cybersecurity-in-higher-ed-for-gcs-and-legal-departments.pdf:contentReference[oaicite:48]{index=48}

15. BitLyft. (2023). Managed Detection and Response for Higher Education. Retrieved from bitlyft.com/managed-detection-and-response-for-higher-education:contentReference[oaicite:51]{index=51}

16. International Organization for Standardization. (2022). ISO/IEC 27005:2022 Information technology — Security techniques — Information security risk management. Geneva, Switzerland: ISO.

17. State Committee for Standardization, Metrology and Certification of Ukraine. (2001). DSTU 13335-1:2001. Information technology. Guidelines for information security management. Part 1. Concepts and models of information security. Kyiv: Derzhstandart of Ukraine.

18. Administration of the State Service of Special Communications and Information Protection of Ukraine. (2005). Methodology for modeling threats and violators (Order No. 801 of 08.12.2005 with amendments). Retrieved from https://cip.gov.ua

Науково-методична стаття.
Надійшла до редакції 07.05.25.
Прийнято до публікації 04.06.2025.