Міністерство освіти і науки України
Харківського національного університету імені В.Н. Каразіна
Навчально-наукового інституту комп'ютерних наук та штучного інтелекту
Спеціальність 125 «Кібербезпека та захист інформації»
Освітня програма «Безпека інформаційних і комунікаційних систем»

В.о. зав. кафедрою КІСМТ
Марина ЄСІНА
"Допущено до захисту"

" " _____2024р.

Пояснювальна записка

до кваліфікаційної роботи магістра

на тему: " Дослідження, аналіз та порівняння методів і засобів забезпечення кібербезпеки в закладах вищої освіти України"

оцінка "_____"

Голова ЕК
Лемешко О.В.

Керівник: к.т.н., доцент Єсіна М. В.

Рецензент: к.т.н., доцент Голубничий Д.Ю.

Виконавець: студент групи КБ-61
Дубина В.П.

Харків 2024

РЕФЕРАТ

Пояснювальна записка до проєкту магістра містить 66 сторінок, 5 рисунків, 6 посилань на джерела.

Метою даної роботи є вивчення та аналіз методів та інструментів, що використовуються для забезпечення кібербезпеки у закладах вищої освіти України, з акцентом на оцінку сучасних підходів, виявлення проблем та порівняння ефективності різних заходів кібербезпеки.

Об'єктом дослідження є процес забезпечення кібербезпеки закладівв вищої освіти України.

Предметом дослідження є основні методи та інструменти, що використовуються для забезпечення кібербезпеки, включаючи системи контролю доступу, шифрування, захисту даних, виявлення інцидентів та системи реагування, що використовуються в українських університетах. У дослідженні також розглядаються ключові проблеми, з якими стикаються ці установи при забезпеченні безпеки своїх інформаційних систем, а також стратегії поліпшення їх можливостей в області кіберзахисту.

Основними методами дослідження є аналіз і порівняння існуючих заходів, інструментів і технологій кібербезпеки, що використовуються в українських університетах, а також оцінка ефективності цих методів у боротьбі з поточними загрозами і вразливістю.

У цій дипломній роботі розглядаються: поточний стан кібербезпеки у закладах вищої освіти України, основні методи та інструменти, що використовуються для захисту університетських інформаційних систем, ключові проблеми, з якими стикаються навчальні заклади, та роль нових технологій, таких як інтелектуальні системи моніторингу та двофакторна автентифікація, у підвищенні безпеки. У даній роботі також пропонуються рекомендації щодо зміцнення систем кібербезпеки університетів шляхом впровадження передових систем моніторингу, поліпшення управління доступом користувачів і регулярних перевірок безпеки.

Результати цього дослідження можуть бути використані для поліпшення інфраструктури безпеки українських університетів, розробки майбутньої політики кібербезпеки в секторі вищої освіти та сприяння розробці більш ефективних стратегій і практик кібербезпеки.

Ключові слова: КІБЕРБЕЗПЕКА, ЗАКЛАДИ ВИЩОЇ ОСВІТИ, ІНФОРМАЦІЙНА БЕЗПЕКА, КОНТРОЛЬ ДОСТУПУ, ШИФРУВАННЯ, ДВОФАКТОРНА АВТЕНТИФІКАЦІЯ, ІНТЕЛЕКТУАЛЬНІ СИСТЕМИ МОНІТОРИНГУ, ВИЯВЛЕННЯ ІНЦИДЕНТІВ, АУДИТ БЕЗПЕКИ, ЦИФРОВІ ЗАГРОЗИ, УПРАВЛІННЯ РИЗИКАМИ.

ABSTRACT

The explanatory note to the master's project contains 66 pages, 5 Figures, and 6 links to sources.

The purpose of this paper is to study and analyze the methods and tools used to ensure cybersecurity in higher educational institutions of Ukraine, with an emphasis on evaluating modern approaches, identifying problems and comparing the effectiveness of various cybersecurity measures.

The object of research is the process of ensuring cybersecurity of higher educational institutions in Ukraine.

The subject of the study is the main methods and tools used to ensure cybersecurity, including access control systems, encryption, Data Protection, Incident Detection and response systems used in Ukrainian universities. The study also examines the key challenges these institutions face in ensuring the security of their information systems, as well as strategies to improve their cyber defense capabilities.

The main methods of research are Analysis and comparison of existing cybersecurity measures, tools and technologies used in Ukrainian universities, as well as evaluation of the effectiveness of these methods in combating current threats and vulnerabilities.

This thesis discusses: the current state of cybersecurity in institutions of Higher Education of Ukraine, the main methods and tools used to protect University Information Systems, key problems faced by educational institutions, and the role of new technologies, such as intelligent monitoring systems and two-factor authentication, in improving security. The document also offers recommendations for strengthening University cybersecurity systems by implementing advanced monitoring systems, improving user access control, and regular security checks.

The results of this study can be used to improve the security infrastructure of Ukrainian universities, develop future cybersecurity policies in the higher education sector, and promote the development of more effective cybersecurity strategies and practices.

Keywords: CYBERSECURITY, INSTITUTIONS OF HIGHER EDUCATION, INFORMATION SECURITY, ACCESS CONTROL, ENCRYPTION, TWO-FACTOR AUTHENTICATION, INTELLIGENT MONITORING SYSTEMS, INCIDENT DETECTION, SECURITY AUDIT, DIGITAL THREATS, RISK MANAGEMENT.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ЗВО — Заклад вищої освіти

ІТ — Інформаційні технології

СУОП — Система управління освітнім процесом

ДН — Система дистанційного навчання

LAN — Локальна обчислювальна мережа

TCP/IP — Протокол зв'язку (Transmission Control Protocol/Internet Protocol)

IPv4 — Інтернет-протокол версії 4

DoS — Атаки відмови в обслуговуванні (Denial of Service)

MitM — Атаки "людина посередині" (Man-in-the-Middle)

DDoS — Розподілені атаки відмови в обслуговуванні (Distributed Denial of Service)

CMS — Система управління контентом (Content Management System)

IAM — Управління ідентифікацією та доступом (Identy and Access Managment)

RBAC — управління доступом на основі ролей (Role-Based Access Control)

ВСТУП

Стрімка цифровізація закладів вищої освіти (ЗВО) в Україні та в усьому світі призвела до зростання залежності від інформаційних технологій, що, в свою чергу, підвищило важливість забезпечення надійної системи кібербезпеки. Інтеграція систем електронного навчання, хмарних обчислень, електронних бібліотек і платформ онлайн-комунікації зробила університети вразливими перед цілим рядом кіберзагроз. Ці вразливості не тільки ставлять під загрозу конфіденційні дані студентів та викладачів, але й ставлять під загрозу цілісність дослідницьких та інституційних мереж. Оскільки кібератаки стають все більш витонченими та частими, необхідність впровадження найкращих практик та стратегій забезпечення кібербезпеки у сфері вищої освіти стає більш гострою, ніж будь-коли [2].

Ретельний аналіз поточного стану кібербезпеки у закладах вищої освіти показує динамічний і складний ландшафт. Як у вітчизняній, так і в міжнародній дослідницькій літературі висвітлюються різні методи і підходи, використовувані для захисту цифрового середовища освітніх установ. В Україні багато університетів впровадили базові заходи кібербезпеки, але в комплексних, адаптивних і проактивних стратегіях забезпечення безпеки як і раніше існує значний пробіл [11]. Існуючі структури часто орієнтовані на реактивні механізми забезпечення безпеки, що робить навчальні заклади вразливими перед виникаючими загрозами.

Вітчизняні вчені та фахівці з кібербезпеки внесли свій внесок у розробку фундаментальних моделей кібербезпеки, адаптованих до унікальних потреб українських університетів. Однак залишаються прогалини в розробці масштабованих рішень, які можуть адаптуватися до різноманітної інфраструктури та умов роботи закладів вищої освіти. Науковому співтовариству ще належить розробити повністю інтегровані системи кібербезпеки, що поєднують в собі передові механізми виявлення загроз, реагування та превентивні стратегії для освітнього сектора.

Патентний пошук також вказує на зростаючий обсяг інтелектуальної власності в галузі кібербезпеки для освітніх установ, що свідчить про інновації в системах виявлення вторгнень, захищених комунікаційних протоколах і системах безпеки, заснованих на штучному інтелекті. Незважаючи на ці досягнення, як і раніше існує значний пробіл в спеціалізованих рішеннях з кібербезпеки, які можуть задовольнити конкретні потреби і виклики, з якими стикаються заклади вищої освіти України.

Глобальні тенденції свідчать про перехід до рішень в області кібербезпеки, заснованим на штучному інтелекті, хмарній інфраструктурі безпеки і зростаючої ролі машинного навчання в прогнозуванні загроз. Крім того, акцент на захисті персональних даних та дотриманні міжнародних стандартів, таких як GDPR та інші регіональні нормативні акти, змінює концепцію кібербезпеки в сфері освіти [3].

Актуальність даного дослідження підкреслюється зростаючою залежністю українських закладів вищої освіти від цифрових технологій, що призвело до посилення схильності кіберризикам. З огляду на стратегічну важливість освіти для національного розвитку, захист закладів вищої освіти від кіберзагроз має вирішальне значення для захисту інтелектуальної власності, дослідницьких даних і конфіденційності студентів і викладачів. Крім того, триваючий конфлікт в Україні підвищив вразливість цифрової інфраструктури до кібератак, що робить необхідним вирішення цих проблем шляхом розробки комплексних стратегій кібербезпеки.

Незважаючи на те, що в усьому світі робляться значні зусилля з підвищення кібербезпеки в навчальних закладах, університети України стикаються з унікальними проблемами, пов'язаними з обмеженістю ресурсів, застарілою інфраструктурою і відсутністю досвіду в галузі кібербезпеки. Дане дослідження має велике значення для усунення цих прогалин шляхом аналізу існуючих методів, порівняння кращих міжнародних практик і пропозиції рішень, які можуть бути адаптовані до українських умов.

Основною метою даної дипломної роботи є проведення ретельного аналізу та порівняння методів і засобів забезпечення кібербезпеки у закладах вищої освіти України. У ході дослідження буде вивчено поточний стан практики кібербезпеки в

українських університетах, виявлено існуючі вразливості та оцінено ефективність існуючих заходів безпеки. Порівнюючи ці практики з міжнародними стандартами та інноваціями, дане дослідження спрямоване на те, щоб запропонувати практичні, масштабовані рішення, які можуть бути впроваджені для підвищення кібербезпеки в українських закладах вищої освіти.

У рамках дослідження буде проведено поглиблений огляд вітчизняної та міжнародної літератури з кібербезпеки у сфері вищої освіти, аналіз поточної практики кібербезпеки в українських університетах та оцінка різних моделей та інструментів кібербезпеки. Очікується, що результати цього дослідження дадуть цінну інформацію політикам, університетським адміністраторам і фахівцям в області кібербезпеки, сприяючи розробці більш ефективних стратегій кібербезпеки в сфері вищої освіти.

Висновки цієї дипломної роботи також будуть застосовні до інших навчальних закладів, які стикаються з аналогічними проблемами, як в Україні, так і в інших країнах з порівнянними освітніми та технологічними умовами. Пропонуючи порівняльний аналіз, ця робота покликана сприяти глобальному обговоренню питань підвищення кібербезпеки в секторі освіти.

1. ТЕОРЕТИЧНИЙ АНАЛІЗ ЗАГРОЗ ІНФРАСТРУКТУРИ ЗВО

1.1. Аналіз інфраструктури ЗВО

Інфраструктура університету включає багато компонентів, включаючи інформаційні системи, комп'ютерне обладнання, комунікаційні мережі, системи контролю доступу по всьому кампусу, сервери, мережеві пристрої, Системи управління освітнім процесом, системи дистанційного навчання та інші важливі елементи [7]. Оскільки університет продовжує вдосконалювати свої інформаційні системи, він переживає процес цифрової трансформації, переходячи від "Індустрії 4.0" до повністю інтегрованої "цифрової екосистеми". Цей зсув являє собою комплексну цифровізацію всього освітнього середовища.

Отже, інфраструктура інформаційних систем у закладах вищої освіти, включаючи університети, еволюціонувала для підтримки роботи всіх підрозділів в рамках навчального закладу. Ця еволюція призвела до постійного збільшення навантаження на сервери, кероване мережеве обладнання та мережі зв'язку. Щоб підтримати це розширення, університети впроваджують гібридні мережеві конфігурації, які інтегрують різні типи інфраструктури. Ці мережі полегшують підключення університетського обладнання в різних кампусах і забезпечують високошвидкісне підключення до постачальників інтернет-послуг за допомогою волоконно-оптичних кабелів і оптичних комутаторів [5]. Крім того, ці системи часто поєднуються з традиційними мідними дротовими мережами (кабелями крученої пари) та бездротовими точками зв'язку, такими як маршрутизатори, для створення безшовної інтегрованої мережевої інфраструктури по всьому університету.

Все це обладнання вимагає регулярної високоякісної підтримки, правильного налаштування та постійного технічного обслуговування для забезпечення оптимальної функціональності. Ця інфраструктура об'єднує широке коло користувачів, включаючи співробітників комп'ютерних лабораторій, аудиторій, фінансових відділів, деканатів, академічних кафедр і спеціально відведених зон для відкритого доступу, як показано на рисунку 1.1.

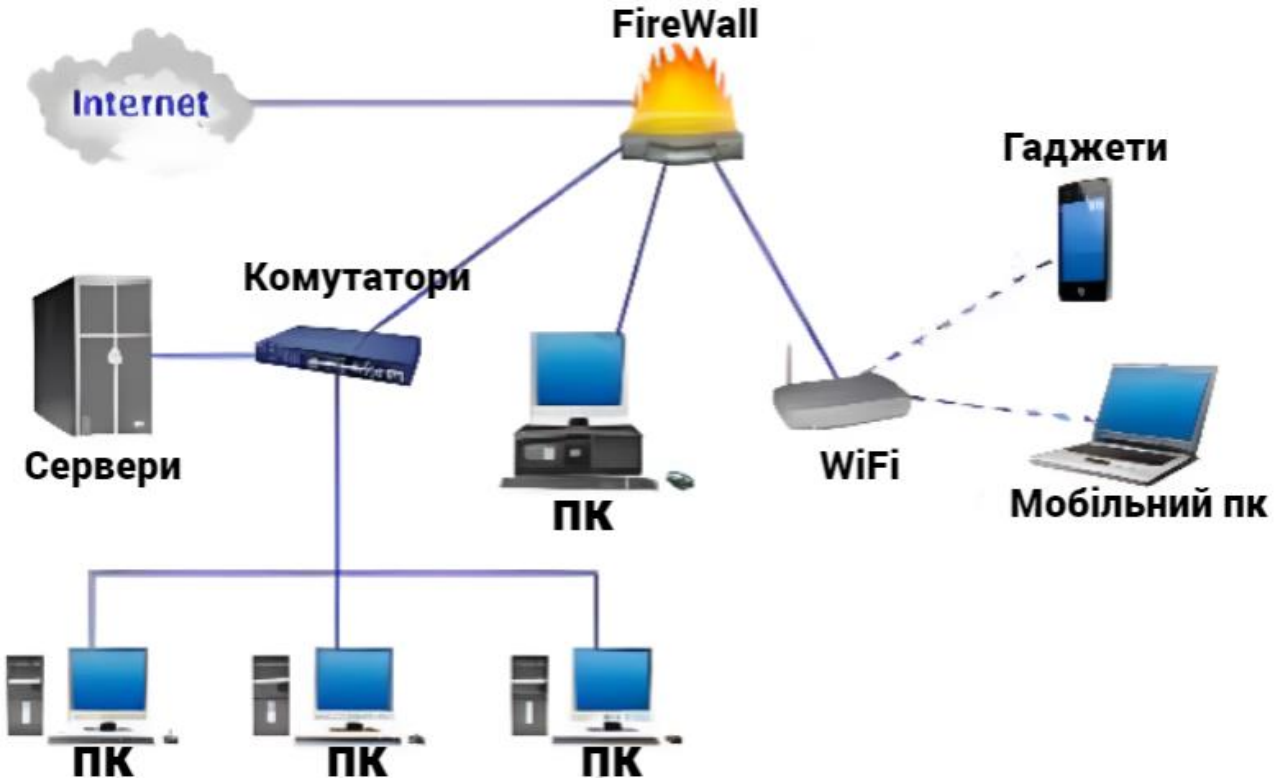

Рисунок 1.1 – Архітектура інфраструктури закладу вищої освіти

Таким чином, постійний моніторинг обладнання та управління ним необхідні поряд з організацією розподілу ресурсів. Розподіл ресурсів здійснюється відповідно до політики використання установи, яка гарантує, що кожен користувач має відповідні рівні доступу. Більшість ресурсів закладу вищої освіти доступні через локальну обчислювальну мережу (LAN), яка складається як з дротових, так і з бездротових компонентів. Цими ресурсами можуть користуватися різні групи, включаючи викладачів, Адміністративний персонал, студентів і навіть керівництво навчального закладу [8]. Мережева інфраструктура забезпечує ефективний доступ до інформації та інструментів, необхідних для прийняття рішень та внесення змін до навчального процесу, забезпечуючи інтегроване середовище для всіх учасників академічної екосистеми.

Для оцінки стабільності інфраструктури інформаційних систем застосовуються стандартні процедури, що забезпечують ретельний аналіз. Всі комп'ютери, що використовуються на кафедрах університету і працюють під управлінням різних операційних систем, підтримують стандартні протоколи зв'язку, зокрема TCP/IP IPv4, з фізичними IP-адресами, присвоєними щоб уникнути конфліктів в мережі. Така конфігурація забезпечує належний розподіл мережевих

компонентів по декількох підмережах, які визначаються мережевими масками, зберігаючи організованість і знижуючи ризик випадкових перешкод.

Для ефективної мережевої взаємодії використовуються як керовані, так і некеровані Комутатори, а також точки бездротового доступу і маршрутизатори, що забезпечують підключення користувачів по всьому кампусу. Ці компоненти працюють спільно, забезпечуючи відповідність інфраструктури вимогам університетського співтовариства.

Незважаючи на наявність великих ресурсів, доступ до багатьох із цих систем залишається нерегульованим або недостатньо керованим, що призводить до потенційної неефективності. Хоча деякі ресурси активно використовуються, інші зарезервовані або недостатньо використовуються, що призводить до нерівності в доступності. Крім того, системи мають різний рівень захисту, а відсутність централізованого контролю за доступом користувачів до інформаційних систем ускладнює управління безпекою.

Для вирішення цих завдань в інформаційних системах університету впроваджені системи ідентифікації особи. Кожна система оснащена унікальними ідентифікаторами, які необхідні для управління доступом. Ці ідентифікатори мають вирішальне значення для забезпечення доступності, цілісності та конфіденційності цифрової інформації, гарантуючи, що конфіденційні дані залишаються захищеними і що тільки авторизовані користувачі можуть отримати доступ до критично важливих ресурсів. Відсутність централізованої системи управління безпекою залишається однією з найбільш серйозних перешкод на шляху забезпечення надійного захисту всієї університетської інфраструктури.

1.2. Огляд вразливостей інфраструктури ЗВО

Інформаційні системи, що входять в інфраструктуру університету, нічим не відрізняються від тих, що використовуються в інших кіберпросторових середовищах [7]. Сьогодні багато систем розгортаються виключно в корпоративних мережах, тоді як інші пов'язані із зовнішніми інфраструктурами, що потенційно робить їх доступними з більш широких середовищ, таких як "розумні міста", цифрові державні мережі або навіть весь кіберпростір. Як результат,

ідентифікація користувача в цих системах надає доступ до інформаційного простору, але цей процес також створює вразливості в ширшому кіберпросторі.

Однією з ключових проблем є використання вразливих паролів великою кількістю користувачів. Ці вразливі паролі можна зламати за допомогою утиліт та генераторів паролів, що робить критично важливі інформаційні ресурси вразливими. Більше того, використання комунікаційних протоколів, у яких відсутні механізми шифрування або безпечної передачі, ще більше збільшує ризик, оскільки відкриті протоколи передачі даних роблять мережу вразливою для прослуховування. Це може призвести до перехоплення та компрометації конфіденційних даних, що загрожує інформаційним ресурсам університету [6].

Неадекватний захист від кібербезпеки також може дозволити зловмисникам проникнути в інфраструктуру, що призведе до таких атак, як атаки "людина посередині" (MitM). Ці атаки особливо небезпечні, оскільки дозволяють зловмиснику видавати себе за легітимні процеси в корпоративній мережі, маніпулювати даними або підміняти інформацію, залишаючись при цьому непоміченим. В результаті зловмисник може отримати несанкціонований доступ до інформаційних систем або декількох взаємопов'язаних систем, порушуючи цілісність всієї інфраструктури.

Атаки відмови в обслуговуванні (DoS) є ще однією серйозною загрозою. Ці атаки зазвичай перевантажують мережеві ресурси надмірними запитами, роблячи їх недоступними для законних користувачів. Це призводить до порушення нормальної роботи і може серйозно ускладнити функціонування критично важливих компонентів інфраструктури. Уразливість мережі ще більше посилюється при використанні слабких механізмів автентифікації, таких як легко вгадувані паролі [1].

Крім того, поширеною проблемою є атаки на системи автентифікації. Ці атаки пов'язані з підбором або крадіжкою шкідливих паролів або інших форм ідентифікаційних даних для отримання несанкціонованого доступу до мережі. Такі атаки можуть призвести до порушення роботи бездротових мереж в інфраструктурі університету, що дозволить зловмисникам маніпулювати мережевими операціями або порушувати їх роботу і отримувати незаконний доступ до конфіденційних

ресурсів. Атаки на бездротові мережі становлять значну загрозу для інфраструктури університету, насамперед через недосконалу конфігурацію бездротових точок доступу та потенційну можливість несанкціонованого доступу до корпоративної мережі Університету. Отримання доступу до фізичних точок в мережевій інфраструктурі може служити шлюзом для подальших дій зловмисників. Як тільки зловмисник отримає доступ до бездротової мережі університету, він може використовувати її для розповсюдження шкідливого програмного забезпечення, здійснення шахрайських дій або запуску додаткових атак. Несанкціонований доступ до корпоративних бездротових мереж також може статися ненавмисно, коли користувачі несвідомо підключаються до незахищених мереж, що ще більше піддає систему ризику.

Відсутність шифрування в протоколах передачі даних робить корпоративну мережу особливо вразливою для перехоплення даних. Це відкриває можливості для підробки та компрометації конфіденційної інформації, що впливає на цілісність як академічних, так і адміністративних ресурсів. Використання безкоштовних веб-ресурсів або платформ, особливо тих, що використовують вразливі шаблони, ще більше збільшує ризик. [12] Ці платформи, які часто не мають належних заходів безпеки, надають зловмисникам можливість використовувати ресурси університету для зловмисних цілей.

Більше того, відсутність ефективних організаційних заходів щодо дотримання правил кібербезпеки, таких як дотримання базових стандартів кібергігієни та "кіберчистоти" серед співробітників університетів, студентів та зацікавлених сторін, створює додаткові вразливості. Без належних рекомендацій користувачі можуть несвідомо сприяти ослабленню захисту мережі.

Оцінюючи ці ризики, важливо ретельно оцінити всі потенційні фактори, які можуть призвести до порушень безпеки, беручи до уваги як внутрішні, так і зовнішні загрози. Необхідно вжити попереджувальних заходів для забезпечення безпеки корпоративної мережі Університету та всіх її взаємопов'язаних компонентів. Це передбачає застосування протоколів шифрування до всієї інформації, що передається через університетську мережу, що допоможе забезпечити цілісність даних та конфіденційність [10].

Також важливо забезпечити використання безпечних протоколів для веб-ресурсів, впровадити стабільні системи управління контентом (CMS) і впровадити надійні методи забезпечення безпеки баз даних. Університети повинні дотримуватися рекомендованих найкращих практик виявлення та усунення загроз безпеці, таких як розподілені атаки відмови в обслуговуванні (DDoS), перехоплення даних та порушення автентифікації, серед інших. Збір та аналіз даних про ці загрози дає цінну інформацію про потенційні вразливості, дозволяючи установам передбачати ризики та вживати профілактичних заходів.

На жаль, багато загроз кібербезпеці непередбачувані, але їх наслідки можуть бути серйозними. Ці атаки можуть завдати серйозної шкоди репутації університету, призвести до поширення неправдивої або шкідливої інформації або порушити цілісність конфіденційних академічних та адміністративних даних. Університетам важливо бути пильними у боротьбі з цими загрозами, щоб забезпечити збереження та репутацію своїх навчальних закладів у все більш цифровому світі. Важливо перевіряти точність і достовірність будь-якої цифрової інформації, перш ніж вона буде опублікована або передана в загальний доступ. Забезпечення коректності даних, їх відсутності помилок або маніпуляцій має життєво важливе значення для підтримки цілісності діяльності університету і його репутації. Враховуючи складність сучасних університетських мереж та інформаційних систем, безперервний моніторинг стає незамінним інструментом для підтримки безпеки та стабільності роботи.

Впровадження безперервного моніторингу по всій інфраструктурі університету дозволяє в режимі реального часу відстежувати стан всіх інформаційних систем і мереж зв'язку. Такий попереджувальний підхід дозволяє виявляти потенційні уразливості або порушення при їх появі. Аналізуючи дані цих систем моніторингу, IT-адміністратори університетів можуть не тільки оцінити поточний стан інфраструктури, але й спрогнозувати потенційні проблеми або зміни, які можуть вплинути на стабільність системи.

Здатність прогнозувати та розпізнавати критичні зміни особливо важлива для мінімізації часу простою та запобігання порушенням безпеки. Завдяки постійному

моніторингу установи можуть швидко виявляти ненормальну поведінку, спроби несанкціонованого доступу або збої в обслуговуванні, які можуть вказувати на кібератаку або збій системи. Оперативно вирішуючи ці проблеми, університети можуть зменшити ризик подальшої шкоди та забезпечити, щоб їхні інформаційні системи залишалися безпечними, надійними та здатними підтримувати академічні та адміністративні потреби закладу [1].

Включення таких систем моніторингу в Стратегію кібербезпеки університету забезпечує динамічний і Проактивний механізм захисту, що гарантує, що всі компоненти інфраструктури працюють в безпечних умовах. Такий підхід також підвищує здатність університету реагувати на виникаючі загрози та підтримувати загальний стан своєї цифрової екосистеми.

1.3. Досвід міжнародних університетів у сфері кібербезпеки

Міжнародні університети вже давно перебувають на передовій у розробці та впровадженні передових заходів кібербезпеки для захисту своїх інформаційних систем та цифрової інфраструктури. Оскільки навчальні заклади все більше покладаються на цифрові інструменти для викладання, досліджень та управління, потреба в надійних методах забезпечення кібербезпеки є більш гострою, ніж будь-коли. Ці університети використовують цілий ряд стратегій, інструментів та фреймворків для захисту своїх систем від постійно розвиваються кіберзагроз. У цьому розділі висвітлюються ключові практики кібербезпеки, прийняті провідними університетами світу, і розглядається, як їх досвід може допомогти в реалізації ініціатив в області кібербезпеки в інших навчальних закладах.

1) Комплексне управління ризиками.

Провідні університети по всьому світу, такі як університети Сполучених Штатів та Європи, розробили комплексні системи управління ризиками, які забезпечують інтеграцію кібербезпеки в загальне інституційне управління. У цих університетах зазвичай створюються спеціальні групи з кібербезпеки, які стежать за впровадженням протоколів безпеки, проводять регулярні оцінки ризиків і забезпечують дотримання національних і міжнародних нормативних актів. Вони застосовують проактивний підхід до управління ризиками, який передбачає

постійний моніторинг систем, виявлення потенційних вразливостей і усунення їх до того, як вони можуть бути використані.

Наприклад, Стенфордський університет (США) використовує ризикований підхід до кібербезпеки, класифікуючи свої інформаційні системи відповідно до їх чутливості та критичності. Це дозволяє університету застосовувати різні рівні контролю безпеки залежно від потенційних наслідків порушення безпеки. Регулярно проводячи оцінку вразливостей і тестування на проникнення, команда Стенфордського університету з кібербезпеки може усувати виникаючі загрози в режимі реального часу.

2) Двофакторна автентифікація та контроль доступу

Ключовою практикою підвищення безпеки в освітніх установах по всьому світу є широке впровадження двофакторної автентифікації (2FA) і механізмів контролю доступу. Такі університети, як Оксфордський університет (Великобританія) та ETH Цюріх (Швейцарія), запровадили обов'язкову 2FA для студентів, викладачів та співробітників, які мають доступ до конфіденційних даних або університетських систем. Це гарантує, що навіть у разі порушення пароля користувача несанкціонований доступ буде запобігати завдяки додатковому рівню безпеки, наданому 2FA.

Оксфордська система кібербезпеки вимагає від користувачів автентифікації, використовуючи як традиційний пароль, так і одноразовий код, створений за допомогою мобільного додатка, який залежить від часу. Аналогічно, Гарвардський університет (США) інтегрує біометричні дані та смарт-картки у свої процеси автентифікації, гарантуючи, що лише авторизований персонал може отримати доступ до зон та систем підвищеної безпеки. Контроль доступу також посилюється за рахунок моніторингу поведінки користувачів, що гарантує надання доступу до ресурсів відповідно до ролей і потреб, що зводить до мінімуму ризик несанкціонованого доступу до даних [9].

3) Шифрування даних і захищені канали зв'язку

Ще одним наріжним каменем практики кібербезпеки в міжнародних університетах є шифрування даних. Захист конфіденційних даних, особливо при передачі та зберіганні, має першорядне значення. Такі університети, як

Массачусетський технологічний інститут (MIT) (США) і Мельбурнський університет (Австралія), використовують наскрізне шифрування для обміну даними між базами даних, серверами і зовнішніми системами, гарантуючи неможливість несанкціонованого перехоплення.

Массачусетський технологічний інститут впровадив протокол безпеки транспортного рівня (TLS) для шифрування даних, якими обмінюються Університетські сервери, студентські портали та дослідницькі бази даних. Подібним чином, Університетський коледж Лондона (UCL) використовує вдосконалені алгоритми шифрування, включаючи AES (Advanced Encryption Standard), для захисту записів студентів, фінансових даних та дослідницьких матеріалів, що зберігаються в його інформаційних системах. Використовуючи ці методи шифрування, ці установи можуть забезпечити конфіденційність та цілісність своїх конфіденційних даних.

4) Програми навчання та підвищення обізнаності в галузі кібербезпеки

Міжнародні університети також визнають, що технології самі по собі не можуть гарантувати кібербезпеку — навчання користувачів не менш важливе. Такі університети, як Каліфорнійський університет, Берклі (США) та Сіднейський університет (Австралія), розробили комплексні навчальні програми з кібербезпеки для всіх студентів, викладачів та співробітників. Ці програми навчають найкращих практик управління паролями, запобігання фішингу та захисту даних, гарантуючи, що вся університетська спільнота буде готова виявляти та реагувати на потенційні загрози [13].

У Берклі для нових студентів та співробітників проводяться обов'язкові заняття з підвищення обізнаності про кібербезпеку, присвячені таким темам, як безпечна поведінка в Інтернеті, розпізнавання фішингових атак та належне поводження з конфіденційними даними. Університет Сіднея також інвестував в онлайн-навчальні модулі та семінари для підвищення обізнаності про ризики кібербезпеки та надання допомоги особам у виявленні загроз, перш ніж вони можуть завдати шкоди.

5) Системи виявлення інцидентів і реагування на них.

Щоб убезпечити себе від потенційних кібератак, багато університетів вклали значні кошти в системи виявлення інцидентів і реагування на них. Такі університети, як Університет Торонто (Канада) та Мюнхенський технічний університет (TUM) (Німеччина), створили спеціалізовані центри безпеки (SoCs), які відстежують мережевий трафік у режимі 24/7 та реагують на інциденти безпеки, коли вони трапляються. Ці SOC оснащені найсучаснішими інструментами для аналізу загроз у режимі реального часу, виявлення вторгнень та реагування на інциденти.

Наприклад, Університет Торонто використовує безліч систем виявлення вторгнень (IDS) для аналізу мережевого трафіку на наявність ознак підозрілої активності. При виявленні потенційної атаки команда SOC негайно отримує повідомлення і вживає заходів щодо усунення загрози. Аналогічно, TUM використовує систему управління інформацією про безпеку та події (SIEM) для збору, зіставлення та аналізу журналів з усієї університетської мережі. Цей проактивний моніторинг дозволяє швидко виявити будь-які порушення, мінімізуючи потенційну шкоду.

6) Безпечна хмарна інтеграція та віртуальні навчальні середовища

У рамках своєї стратегії забезпечення безперервності освіти та наукових досліджень Міжнародні університети все частіше використовують хмарну інфраструктуру для зберігання даних, розміщення додатків та підтримки віртуальних навчальних середовищ. Такі установи, як UCLA (UCLA) та Національний університет Сінгапуру (NUS), використовують захищені хмарні платформи для розміщення свого освітнього контенту, записів учнів та дослідницьких даних, забезпечуючи захист цих систем за допомогою передових заходів безпеки, включаючи шифрування, контроль доступу та регулярне резервне копіювання.

Наприклад, UCLA використовує Amazon Web Services (AWS) для розміщення дослідницьких даних, застосовуючи суворий набір протоколів шифрування для їх захисту під час зберігання та передачі. NUS інтегрував хмарну систему управління навчанням (LMS), яка забезпечує безпечний доступ до навчальних матеріалів, оцінок учнів та інструментів співпраці. Обидві установи

також гарантують, що їхні хмарні провайдери дотримуються суворих стандартів кібербезпеки та дотримуються таких правил, як GDPR (загальні правила захисту даних) та FERPA (Закон про права сім'ї на освіту та конфіденційність).

7) Регулярні аудити та тестування на проникнення

Для забезпечення ефективності та актуальності заходів кібербезпеки університети по всьому світу регулярно проводять аудити безпеки та тестування на проникнення. Ці оцінки допомагають виявити потенційні слабкі місця в інфраструктурі університету до того, як зловмисники зможуть ними скористатися. Такі університети, як Кембриджський університет (Великобританія) та Австралійський національний університет (ANU), проводять періодичні перевірки безпеки, оцінку вразливостей та імітацію кібератак для тестування своїх систем [1].

Наприклад, Кембриджський університет наймає сторонні охоронні фірми для проведення регулярних тестів на проникнення, гарантуючи, що їх захист надійний і стійкий до атак. ANU, з іншого боку, приділяє особливу увагу постійному вдосконаленню шляхом частого аудиту своїх інформаційних систем та мереж, гарантуючи оперативне виявлення та усунення будь-яких прогалин у безпеці.

1.4. Висновки до розділу.

У першому розділі ми провели поглиблений аналіз інфраструктури університету, вивчивши різні інформаційні системи, інтегровані в цифрову екосистему університету. Сюди входять програмні засоби, Інформаційні технології, комп'ютерне обладнання, системи зв'язку, мережеве програмне забезпечення та користувачі інформаційного простору, а саме викладачі, співробітники та абітурієнти закладів вищої освіти. Крім того, ми вивчили нормативну базу, що регулює ці системи, і описали системні ресурси, які підтримують діяльність університету. У розділі також визначено ключові тенденції у розвитку безпеки університетської інфраструктури, а також триваюча трансформація та оновлення інформаційних систем у сфері кібербезпеки.

Крім того, ми проаналізували вразливості в інфраструктурі університету, визнавши важливість прогнозування потенційних ризиків та вжиття заходів безпеки для забезпечення безпечного функціонування інформаційних систем, комп'ютерного обладнання та засобів зв'язку. Оскільки інфраструктура

університету стає все більш взаємопов'язаною з більш широким цифровим світом, включаючи екосистему "розумного міста" та ініціативи "цифрової держави", необхідність надійних заходів кібербезпеки стає першорядною.

Також було досліджено та проаналізовано методи кіберзахисту в університетах інших країн. Методи забезпечення кібербезпеки, прийняті провідними міжнародними університетами, демонструють прихильність захисту конфіденційної інформації та забезпечення безперервності академічної та адміністративної діяльності. Приділяючи особливу увагу комплексному управлінню ризиками, шифруванню даних, автентифікації користувачів та реагуванню на інциденти, ці навчальні заклади розробили надійні системи, що забезпечують високий рівень захисту від кіберзагроз. Завдяки їхньому досвіду університети можуть отримати цінні уроки про важливість постійного вдосконалення, створення проактивних механізмів захисту та формування культури обізнаності про кібербезпеку. Застосовуючи подібні стратегії та інструменти, університети по всьому світу можуть зміцнити власні інфраструктури кібербезпеки та краще захистити свої цифрові активи від зростаючого спектру кіберзагроз.

Основні висновки:

Мінливий ландшафт загроз: загрози кібербезпеки постійно розвиваються і стають все більш витонченими. Оскільки кіберзлочинці вдосконалюють свої методи, необхідність постійного вдосконалення заходів безпеки стає критичною. Користувачі та адміністратори університетських систем повинні залишатися пильними та активно зміцнювати свої системи кібербезпеки.

Багатофакторна автентифікація (MFA): впровадження багатофакторної автентифікації (MFA) стає стандартом безпеки в різних інформаційних системах. MFA додає додатковий рівень захисту, вимагаючи багаторазової перевірки перед наданням доступу до критичних систем, що ускладнює отримання доступу несанкціонованими користувачами.

Конфігурація мережі та протоколи безпеки: усі комп'ютери на факультетах університету працюють під різними операційними системами, але вони підтримують загальні протоколи зв'язку, такі як TCP/IP IPv4, використовуючи

фізичні IP-адреси. Така структура мережі спрямована на запобігання випадкових перешкод. Мережеві компоненти університету організовані в різних підмережах, кожна з яких визначається певною мережевою маскою для підвищення організаційного контролю та безпеки.

Ризики, пов'язані з відкритими протоколами передачі даних: використання відкритих протоколів передачі даних, наприклад, без шифрування, піддає системи університету значним загрозам, включаючи перехоплення даних або підслуховування. Зловмисники можуть перехопити і скомпрометувати конфіденційну інформацію, що передається по мережі. Крім того, слабкий кіберзахист може дозволити зловмисникам проникнути в інфраструктуру та здійснити атаки "людина посередині" (MitM). Ці типи атак особливо небезпечні, оскільки зловмисник може маскуватися під законний процес у корпоративній мережі, потенційно дублюючи або змінюючи мережеві транзакції.

Захист від соціальної інженерії: атаки соціальної інженерії, при яких зловмисники маніпулюють людьми з метою розголошення конфіденційної інформації, стають все більш витонченими. Для боротьби з цим важливо підвищити обізнаність та пильність усього університетського персоналу, запобігаючи маніпуляціям за допомогою оманливих тактик.

Регулювання та законодавство: уряди та регулятори все більше зосереджуються на кібербезпеці, впроваджуючи нові закони та стандарти для посилення захисту цифрової інфраструктури. Університет повинен бути в курсі цих правил і забезпечувати відповідність своєї практики забезпечення кібербезпеки розвивається правовій базі.

Висновок та рекомендації:

Оцінюючи ризики кібербезпеки університету, важливо ретельно оцінити всі потенційні загрози та вразливості. Необхідно вживати активних заходів для захисту корпоративної мережі Університету та всіх підключених компонентів. Однією з ключових рекомендацій є впровадження надійних протоколів шифрування для передачі даних через Університетські інформаційні системи, що забезпечують конфіденційність і цілісність переданих даних. Крім того, впровадження багаторівневого підходу до безпеки, що поєднує технологічні

рішення, навчання користувачів та культуру обізнаності про кібербезпеку, має вирішальне значення для зменшення ризику атак.

Інтеграція багатофакторної автентифікації та безперервного моніторингу університетської інфраструктури ще більше підвищить рівень безпеки, дозволяючи університету виявляти потенційні загрози до того, як вони зможуть заподіяти шкоду. Вживши цих заходів, університет буде краще підготовлений до захисту своїх цифрових ресурсів, захисту конфіденційної інформації та забезпечення безперервності своїх освітніх та адміністративних функцій.

2. ЗАГРОЗИ ТА РИЗИКИ РОБОТИ ІНФОРМАЦІЙНИХ СИСТЕМ У ІНФРАСТРУКТУРІ ЗВО

2.1. Аналіз загроз інформаційних систем

Інформаційні системи у закладах вищої освіти впроваджуються в різних областях, причому у кожного навчального закладу різні тимчасові рамки і різна ступінь автоматизації. Ці системи сприяють постійному обміну інформацією в рамках університетської інфраструктури, що вимагає постійної адаптації та трансформації для задоволення мінливих потреб. Інформаційні ресурси в рамках цих систем розробляються різними постачальниками і використовують різні бази даних з унікальною структурою. Як результат, адміністративні системи в межах кожного набору інформаційних систем також відрізняються, з різним рівнем контролю та управління.

Однією з ключових проблем, з якими стикаються Університетські інформаційні системи, є складність, яка виникає через велику кількість користувачів, кожен з яких використовує різні операційні системи та протоколи безпеки. Це створює неоднорідне середовище, в якому заходи безпеки повинні бути адаптовані для різних систем. Критичною вразливістю в цьому контексті є слабкий захист паролем — багато користувачів покладаються на слабкі або прості паролі, що робить ці системи дуже вразливими до злому паролів. Крім того, користувачі часто керують кількома засобами автентифікації на різних платформах, іноді навіть повторно використовуючи одні й ті ж паролі в різних системах, що ще більше збільшує ризик несанкціонованого доступу [10].

Для забезпечення сумісності цих різних систем використовуються різні драйвери підключення до баз даних, що дозволяють клієнтам адаптивно працювати з базами даних на різних платформах. Така гнучкість забезпечує безперебійний зв'язок між системами, але також створює ризик несумісних заходів безпеки або вразливостей. Тому ці інформаційні системи повинні бути адаптовані до широкого спектру операційних систем і технологій баз даних, що ускладнює управління безпекою.

Мережі зв'язку у закладах вищо освіти створюються поступово, часто з використанням різного комунікаційного обладнання, що забезпечує різні рівні захисту, керованості та архітектуру мережевої безпеки. Мережева інфраструктура може відрізнятися від одного навчального закладу до іншого, що призводить до неузгодженості в механізмах захисту, розгорнутих в системах. Як результат, деякі сегменти мережі можуть бути більш вразливими до кіберзагроз, ніж інші.

На ризики безпеки користувачів цих інформаційних систем впливають політики безпеки, встановлені системними адміністраторами. Ці політики призначені для захисту інформації, баз даних та персональних даних, але їх ефективність залежить від того, наскільки суворо вони застосовуються та адаптовані до мінливого ландшафту загроз. Вжиті заходи безпеки часто відображають ресурси, досвід та толерантність до ризиків установи, а це означає, що методи безпеки в різних установах можуть суттєво відрізнятися. [6] Ця мінливість створює потенційні вразливості, які можуть бути використані зловмисниками.

Таким чином, складність і різноманітність інформаційних систем у закладах вищої освіти створюють серйозні проблеми для забезпечення кібербезпеки. Для вирішення цих проблем навчальні заклади повинні впроваджувати комплексні політики безпеки, що враховують широкий спектр використовуваних користувачів, систем і мережевих компонентів. Це вимагає постійної адаптації та впровадження найкращих практик управління паролями, системної автентифікації, безпеки баз даних та захисту мережі. Більш того, установи повинні зосередитися на створенні єдиної системи безпеки, яка дозволить ефективно управляти різноманітною інфраструктурою і знижувати ризики на всіх рівнях організації. [2]

Загрози, які варто враховувати та систематизувати для їх ідентифікації (дивитися Рисунок 2.1).

Рисунок 2.1 – Загрози інформаційних систем ЗВО

Несанкціонований доступ – це відбувається, коли неавторизовані особи отримують можливість втручатися в роботу інформаційних систем через зловживання привілеями зловмисниками. Якщо цифрові дані не зашифровані або зберігаються в небезпечних місцях, вони можуть бути доступні неавторизованим особам, що може порушити цілісність і роботу системи.

Пощирення зловмисних програм – це розповсюдження шкідливого коду, такого як віруси та шкідливе програмне забезпечення, через інформаційні системи та комунікаційні мережі. Певні програмні засоби можуть ненавмисно сприяти поширенню цих шкідливих програм, що призводить до порушень безпеки.

Втрата даних – несанкціонований доступ створює загрозу цілісності обміну даними, особливо при відсутності захищених протоколів. Це збільшує ймовірність втрати даних, яка може статися внаслідок непередбачених подій, таких як збої пристрою або випадкове видалення.

Витік конфіденційної інформації – ця загроза пов'язана з передачею конфіденційних даних стороннім особам, що може завдати шкоди репутації установи і привести до втрати довіри [1].

Помилки користувачів – ці загрози виникають, коли користувачі ненавмисно отримують доступ до інформаційних систем або певних ресурсів, що призводить до непередбачуваних та потенційно небезпечних наслідків. Ці помилки можуть піддавати систему загрозам безпеки, впливаючи на її загальну цілісність.

Збої синхронізації – загрози виникають при збоях в процесах обміну даними між різними інформаційними ресурсами, пристроями, клієнтами, серверами, локальними системами і хмарними сервісами. Якщо Синхронізація порушена,

інформація може стати неузгодженою у всій інфраструктурі, що особливо важливо під час кризових ситуацій, таких як воєнний стан. Недотримання синхронізації систем може призвести до використання застарілих або невірних даних, що підриває процес прийняття рішень і оперативну ефективність.

Слабкий захист комунікаційних систем-уразливості в безпеці каналів зв'язку можуть призвести до несанкціонованого доступу до критично важливих баз даних, особливо якщо користувачам надані надмірні привілеї або паролі ненадійні. Недостатні механізми захисту також можуть зробити інформаційні системи вразливими до злому, дозволяючи зловмисникам отримати несанкціонований доступ або підробити дані. Слабкий захист систем ще більше підвищує ризик несанкціонованого втручання в інформаційну інфраструктуру університету.

Загальні вразливості системи – всі ці загрози вказують на загальну слабкість захисту системи, підвищуючи ймовірність втручання в інформаційну інфраструктуру університету. Такі порушення можуть зробити істотний вплив на роботу ключових компонентів і окремих систем. До проблемних областей належать потенційні витоки інформації, зміна або втрата даних, а також вплив шкідливого програмного забезпечення, такого як віруси. Ці вразливості ставлять під загрозу конфіденційність та цілісність інформації, що зберігається та передається в мережах університету [3].

Питання кібербезпеки та захисту конфіденційних даних – поглиблений аналіз інформаційної інфраструктури університету виявив кілька слабких місць. Після виявлення цих проблем можна вивчити та вжити заходів для підвищення безпеки системи. Це дослідження має на меті виявити потенційні загрози, що виникають внаслідок неадекватних заходів безпеки обміну даними, які можуть призвести до витоку інформації, маніпулювання даними або впровадження шкідливих вірусів. Виявивши ці вразливості, ми зможемо внести необхідні поліпшення в інформаційні системи, підвищивши їх загальну стійкість і захистивши конфіденційні дані.

Такий проактивний підхід до виявлення та усунення слабких місць має вирішальне значення для захисту цілісності інфраструктури університету та забезпечення безпеки його цифрових активів.

2.2. Аналіз ризиків та вразливостей інформаційних систем

Традиційні методи оцінки ризиків безпеки:

1) Метод статистичного аналізу: цей підхід використовує статистичні дані та історичні інциденти для оцінки ймовірності та впливу різних загроз. Аналізуючи минулі випадки, можна отримати уявлення про ймовірність виникнення певних загроз і потенційні наслідки для організації.

2) Метод аналізу ймовірності та впливу (матриця ризиків): цей метод використовує матрицю ризиків для оцінки ймовірності виникнення конкретних загроз та їх потенційного впливу на організацію. Він обчислює загальний ризик шляхом множення ймовірності події на її потенційний вплив, допомагаючи визначити пріоритети загроз, які потребують негайної уваги.

3) Метод аналізу вразливостей: цей метод спрямований на оцінку вразливостей в окремих компонентах системи. Він виявляє потенційні слабкі місця, якими можуть скористатися зловмисники, і допомагає виявити конкретні вразливі місця в системі, які необхідно захистити.

4) Метод аналізу витрат і вигод: цей метод порівнює витрати на впровадження різних заходів безпеки з потенційним зниженням ризику. Це допомагає визначити, чи виправдані інвестиції в Контроль безпеки з точки зору зменшення ризику, який вони забезпечують, забезпечуючи ефективний розподіл ресурсів.

5) Метод оцінки загроз та вразливостей: цей метод призначений для виявлення потенційних загроз та вразливостей у системах та мережах. Він дозволяє організаціям зрозуміти, які атаки можуть бути націлені на конкретні уразливості, і оцінити рівень ризику, пов'язаного з цими загрозами.

6) Метод діаграм випадків використання: цей метод допомагає визначити різні сценарії використання системи та потенційні загрози, пов'язані з кожним сценарієм. Визначаючи різні способи використання системи, цей підхід визначає потенційні загрози безпеці в конкретних контекстах, допомагаючи активно вирішувати загрози.

7) Злом комунікаційної інфраструктури університету для обміну даними: важливий приклад порушення безпеки стався, коли сервіс LastPass був

скомпрометований в результаті атаки, в результаті якої зловмисники отримали доступ до даних облікових записів користувачів і паролів. Цей інцидент підкреслює ризики, пов'язані зі слабкими паролями, і демонструє, як зловмисники можуть використовувати вразливості в інформаційних системах. Для університету це послужило наочним прикладом важливості політики використання надійних паролів і безпечних методів автентифікації для захисту конфіденційних даних.

8) Злом інформаційної інфраструктури – на сервері виявлено серйозну вразливість, яка може дозволити зловмисникам легко отримати доступ до облікових даних користувачів в інформаційних системах університету. Ця вразливість є серйозною загрозою безпеці, що вимагає негайного виправлення та захисту системи для запобігання несанкціонованому доступу.

9) Недостатнє шифрування інформації – деякі з використовуваних в даний час систем шифрування засновані на ненадійних або застарілих методах, які порушують конфіденційність і доступність даних, що зберігаються в базах даних університету. Посилення протоколів шифрування має важливе значення для захисту конфіденційної інформації від несанкціонованого доступу та забезпечення збереження даних.

10) Помилки користувачів – Користувачі можуть ненавмисно робити помилки під час процесу автентифікації, наприклад, кілька разів вводити неправильні облікові дані для входу. Це може призвести до автоматичного блокування облікових записів у різних інформаційних системах. Хоча цей захід безпеки допомагає запобігти несанкціонованому доступу, Він також може порушити доступ користувачів до критично важливих ресурсів і підкреслює необхідність більш ефективних методів автентифікації користувачів, таких як багатофакторна автентифікація (MFA).

2.3. Використання методів кібербезпеки в оцінці ризиків

Використання методів кібербезпеки при оцінці ризиків є важливим кроком у забезпеченні безпеки інформаційних систем університету, що охоплюють як локальні сервери баз даних, так і хмарні ресурси. Ця оцінка охоплює всі аспекти інфраструктури, включаючи розподіл ресурсів, дротові та бездротові мережі, системи управління, а також автентифікацію та ідентифікацію користувачів.

Застосовуючи методи забезпечення кібербезпеки, університет може виявляти потенційні загрози, оцінювати ймовірність їх виникнення та прогнозувати можливі наслідки для навчального закладу.

Процес оцінки ризиків допомагає зрозуміти вразливості в різних компонентах системи та готує університет до активного зменшення ризиків. Це включає в себе виявлення слабких місць як в апаратному, так і в програмному забезпеченні, а також людського фактора, який може сприяти порушенням безпеки. Завдяки ретельному аналізу університет може передбачити різні сценарії, оцінити їх вплив та відповідно визначити пріоритети зусиль щодо безпеки [2].

1) Аналіз вразливостей та тестування на проникнення:

Тестування на проникнення передбачає спробу злому мережі або системи за допомогою імітаційних атак, що допомагає виявити слабкі місця. Цей процес дозволяє фахівцям з безпеки оцінити потенційні загрози та вразливості в системі. Використовуючи методи аналізу вразливостей, організації можуть точно визначити конкретні слабкі місця в своїх системах або мережах, які можуть бути використані зловмисниками [8]. Ці тести оцінюють ризики, пов'язані з цими вразливими місцями, та їх потенційні наслідки. Тестування на проникнення імітує реальні сценарії атак, дозволяючи отримати цінну інформацію про те, як можна використовувати ці вразливості і який вплив такі порушення можуть мати на цілісність і безпеку системи.

2) Моніторинг та реєстрація інцидентів:

Постійний моніторинг мережевої активності необхідний для виявлення незвичної або підозрілої поведінки, яка може свідчити про загрозу, що насувається. Журнали подій служать важливим джерелом даних для аналізу безпеки, допомагаючи фахівцям з безпеки виявляти потенційні ризики на ранній стадії. Завдяки веденню детальних журналів активності системи стає простіше відстежувати та аналізувати інциденти безпеки, що сприяє швидшому реагуванню та пом'якшенню наслідків. Регулярний моніторинг і ведення журналу забезпечують механізм проактивного захисту, допомагаючи виявляти загрози до того, як вони зможуть завдати значної шкоди.

3) Системи виявлення та запобігання вторгнень (IDS / IPS):

Системи виявлення вторгнень (IDS) та системи запобігання вторгненням (IPS) є важливими інструментами для виявлення та блокування шкідливих дій у мережі. IDS може виявляти підозрілі дії, такі як спроби несанкціонованого доступу або розповсюдження шкідливих програм, тоді як IPS робить це на крок далі, активно блокуючи ці атаки в режимі реального часу. Системи IDS / IPS допомагають захистити інформаційну інфраструктуру університету, запобігаючи поширенню кіберзагроз та забезпечуючи швидке виявлення та нейтралізацію будь-якої шкідливої активності.

4) Багатофакторна автентифікація (MFA):

Впровадження багатофакторної автентифікації (MFA) забезпечує додатковий рівень безпеки, вимагаючи проходження декількох форм перевірки перед наданням доступу до систем або конфіденційних даних. Зазвичай це включає поєднання того, що відомо користувачеві (наприклад, пароль), того, що він має (наприклад, смартфон або маркер безпеки), і Ким є користувач (наприклад, біометричні дані, такі як відбитки пальців або розпізнавання обличчя). MFA значно зменшує ймовірність несанкціонованого доступу, оскільки зловмиснику набагато важче скомпрометувати кілька форм автентифікації, ніж лише одну.

5) Шифрування даних:

Шифрування даних-це найважливіший захід безпеки, який захищає як передані, так і збережені дані від перехоплення та несанкціонованого доступу. Завдяки шифруванню конфіденційних даних, навіть якщо вони перехоплені або до них отримали доступ сторонні особи, вони залишаються нечитабельними і безпечними. Шифрування гарантує, що особиста, фінансова та конфіденційна інформація залишається захищеною від кіберзагроз, таких як порушення даних або атаки "людина посередині". Це особливо важливо для захисту даних при передачі по мережах або при зберіганні в хмарних середовищах.

6) Брандмауери та захист периметра:

Впровадження брандмауерів та інших заходів безпеки на периметрі мережі є ключовим компонентом контролю доступу та блокування небажаного або шкідливого трафіку. Брандмауери служать бар'єром між надійними внутрішніми мережами та ненадійними зовнішніми мережами (наприклад, Інтернетом),

допомагаючи запобігти несанкціонованому доступу та потенційним кібератакам. Додаткові засоби захисту периметра, такі як системи запобігання вторгненням (IPS), можуть ще більше підвищити безпеку мережі, активно виявляючи і блокуючи підозрілі дії.

7) Захист від відмов в обслуговуванні (DoS) / розподілених атак типу "відмова в обслуговуванні" (DDoS):

Атаки типу "DOS" і "DDoS-атаки" спрямовані на перевантаження мережі або сервера трафіком, що робить їх недоступними для законних користувачів. Для захисту від подібних атак потрібні спеціалізовані системи і сервіси, які можуть пом'якшити наслідки таких атак і забезпечити надійність мережі. Рішення можуть включати обмеження швидкості, фільтрацію трафіку та використання хмарних служб захисту від DDoS, які допомагають розподіляти та поглинати надлишковий трафік, забезпечуючи постійний доступ до критичних служб під час атаки.

8) Управління ідентифікацією та доступом (IAM):

Системи IAM необхідні для управління ідентифікаційними даними користувачів і дозволами на доступ в мережі. Ці системи дозволяють університету контролювати, хто і до яких ресурсів має доступ, гарантуючи, що тільки авторизовані користувачі і пристрої зможуть отримати доступ до конфіденційної інформації. Реалізуючи управління доступом на основі ролей (RBAC), яке використовує певні ролі та привілеї для обмеження доступу авторизованим користувачам до системи, надійні методи автентифікації та постійний моніторинг активності користувачів, IAM знижує ризик несанкціонованого доступу, зводячи до мінімуму ймовірність порушень безпеки.

9) Статистичний аналіз даних:

Статистичний аналіз даних включає вивчення історичних даних про інциденти безпеки та мережеву активність для оцінки ймовірності та потенційного впливу конкретних загроз. Використовуючи аналітику на основі даних, організації можуть передбачити ймовірність виникнення певних атак та визначити можливі наслідки для мережі та систем. Цей метод допомагає визначити пріоритетність заходів безпеки на основі найбільш ймовірних і дієвих загроз, оптимізуючи розподіл ресурсів для забезпечення кібербезпеки.

10) Стратегії управління ризиками:

Розробка та застосування стратегій управління ризиками мають вирішальне значення для виявлення, оцінки та зменшення потенційних ризиків для інфраструктури організації. Ці стратегії включають визначення прийнятного рівня ризику (толерантності до ризику) і реалізацію заходів щодо зниження загроз до прийнятних рівнів. Це може включати Налаштування відповідних засобів контролю, таких як шифрування, багатофакторна автентифікація та навчання користувачів, щоб мінімізувати вплив кіберзагроз. Необхідно регулярно проводити оцінку ризиків, щоб забезпечити адаптацію системи безпеки організації до нових та еволюційних ризиків.

Ці методи кібербезпеки необхідні для виявлення потенційних загроз та ризиків для інформаційних систем в університетській інфраструктурі, включаючи системи зв'язку як у дротових, так і в бездротових мережах. Вони допомагають оцінити вплив цих ризиків і дозволяють вжити необхідних заходів для забезпечення ефективного захисту мережі та даних. Ключовим аспектом є використання комплексного і постійно розвивається підходу до оцінки ризиків, оскільки загрози кібербезпеки динамічні і постійно розвиваються. Такі технології, як шифрування, ідентифікація користувача та двофакторна автентифікація в системах контролю доступу, мають вирішальне значення для безпечного управління доступом користувачів [11]. Крім того, безпечний обмін даними між внутрішніми і зовнішніми інформаційними системами, такими як мережі Smart City і digital state, забезпечується за допомогою VPN з шифруванням і персональними ключами. Ці технології не тільки забезпечують конфіденційність і цілісність переданих даних, але і відіграють вирішальну роль у перевірці особистості користувача і контролі доступу до ресурсів, гарантуючи, що тільки авторизовані особи мають відповідний доступ (дивитися Рисунок 2.2)

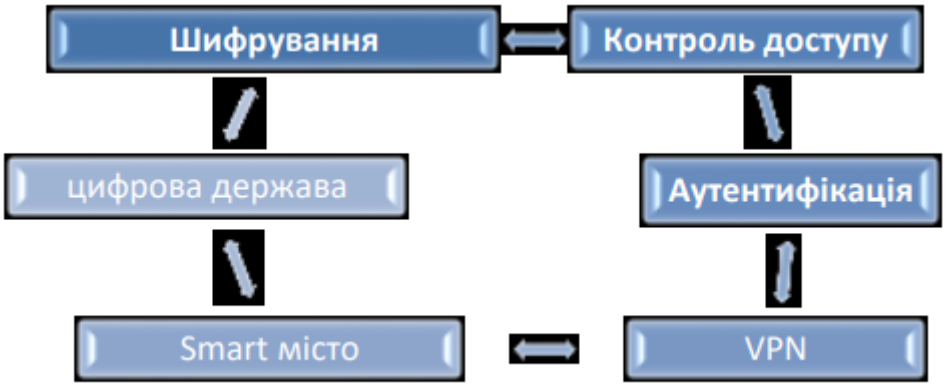

Рисунок 2.2 – Технології шифрування, автентифікації та контролю доступу

Аналіз технологій автентифікації, контролю доступу та шифрування в інформаційних системах університету має вирішальне значення для забезпечення безпеки баз даних та всіх систем у закладах вищої освіти. Належне впровадження цих технологій допомагає захистити конфіденційні дані від несанкціонованого доступу та потенційних кіберзагроз [2]. Нижче наведено ключові сфери, на які слід звернути увагу:

1) Шифрування:

a) Шифрування даних в режимі очікування:

Шифрування даних у режимі очікування-це метод, який використовується для захисту збережених цифрових даних, включаючи структуровану інформацію в базах даних. Це гарантує, що навіть якщо несанкціоновані особи отримають доступ до носія, дані залишаться нечитабельними та неструктурованими. Завдяки шифруванню даних, коли до них не здійснюється Активний доступ, цей метод забезпечує захист конфіденційної інформації в сховищі, запобігаючи її розкриття в разі витоку даних.

b) Шифрування передачі даних:

Для захисту переданих даних використовуються методи шифрування, що забезпечують безпечну передачу по мережах. Такі технології, як протоколи SSL/TLS, зазвичай використовуються для шифрування даних під час передачі, що ускладнює зловмисникам перехоплення та зчитування даних під час їх передачі. Це особливо важливо при передачі конфіденційної інформації через загальнодоступні або незахищені мережі, такі як Інтернет.

c) Шифрування за протоколом веб-ресурсів (HTTPS):

Одним з ключових елементів забезпечення безпеки онлайн-комунікацій є використання протоколу HTTPS, який шифрує зв'язок між користувачами і веб-ресурсами. Цей протокол гарантує, що будь-які дані, якими обмінюється браузер користувача з веб-ресурсами університету (наприклад, порталами, базами даних та іншими онлайн-сервісами), залишаються зашифрованими і безпечними, що значно знижує ризик злому або несанкціонованого доступу. Протокол HTTPS необхідний для захисту облікових даних для входу, особистих даних та іншої конфіденційної інформації, до якої можна отримати доступ через Інтернет.

d) Конфіденційність даних:

Шифрування відіграє найважливішу роль у забезпеченні конфіденційності даних. Завдяки шифруванню даних в режимі очікування і під час передачі система гарантує, що навіть якщо неавторизовані особи отримають доступ до даних, вони не зможуть їх прочитати або використовувати. Це особливо важливо для захисту особистої інформації, академічних записів, фінансових даних та інших конфіденційних університетських даних. Шифрування гарантує, що інформація залишається приватною та конфіденційною, зменшуючи ризик порушення даних.

e) Захист від перехоплення:

Шифрування каналів передачі даних необхідно для захисту інформації від перехоплення під час її передачі по мережах. Воно забезпечує додатковий рівень захисту від зловмисників, які можуть спробувати перехопити або підслухати дані під час їх передачі. Це особливо важливо в середовищах, де здійснюється обмін даними між внутрішніми системами (наприклад, базами даних, серверами) і зовнішніми системами (наприклад, сторонніми сервісами, хмарними провайдерами). Захист конфіденційних даних від перехоплення є життєво важливим для підтримки цілісності каналів зв'язку університету та запобігання кібератакам, таким як атаки "людина посередині" або порушення даних.

2) Автентифікація:

a) Двофакторна автентифікація (2FA):

Двофакторна автентифікація (2FA) вимагає від користувачів надати дві окремі форми підтвердження своєї особи. Як правило, це включає щось відоме

користувачеві (наприклад, пароль) і те, що він має (наприклад, одноразовий код, згенерований мобільним пристроєм або додатком для автентифікації). Цей додатковий рівень безпеки гарантує, що навіть у разі злому одного з факторів (наприклад, пароля) зловмисник не зможе отримати доступ без використання другого фактора, що значно знижує ризик несанкціонованого доступу.

b) Біометрична автентифікація:

Біометрична автентифікація використовує унікальні фізичні характеристики, такі як відбитки пальців, розпізнавання обличчя або сканування сітківки ока, щоб підтвердити особу користувачів. Ця система забезпечує високозахищену форму ідентифікації, оскільки біометричні характеристики надзвичайно складно відтворити. Це гарантує, що лише авторизовані користувачі зможуть отримати доступ до конфіденційних систем та даних. Біометрична автентифікація особливо корисна для внутрішньої перевірки ідентичності всіх користувачів, підвищуючи безпеку та зручність використання.

c) Одноразові паролі (OTP):

Одноразові паролі (OTP) - це тимчасові паролі, створені для одноразової автентифікації. Ці паролі надсилаються користувачам через захищений канал (наприклад, SMS, електронну пошту або застосунок) і дійсні протягом обмеженого періоду часу або лише для одноразового доступу. OTP забезпечує додатковий рівень захисту, гарантуючи, що навіть якщо звичайні облікові дані користувача (наприклад, пароль) будуть скомпрометовані, зловмиснику все одно знадобиться OTP для завершення процесу автентифікації. Цей метод особливо корисний для перевірки особи тимчасових або нечастих користувачів.

d) Перевірка особистості:

Впровадження надійних методів автентифікації, таких як 2FA, має вирішальне значення для забезпечення доступу лише авторизованих користувачів до цифрових інформаційних систем та ресурсів університету. Захищаючи особистість користувача за допомогою цих багаторівневих процесів автентифікації, університет значно знижує ризик несанкціонованого доступу до своєї інфраструктури. Сувора автентифікація відіграє вирішальну роль у захисті конфіденційних даних та запобіганні потенційним витокам.

e) Захист від атак зі зломом паролів:

Двофакторна автентифікація та інші сучасні методи автентифікації (такі як біометрична верифікація або OTP) допомагають захистити від атак зі зломом паролів. Ці методи значно ускладнюють зловмисникам отримання несанкціонованого доступу до систем шляхом компрометації паролів користувачів. Додавання другого рівня безпеки не тільки ускладнює атаки паролів, але й зменшує ймовірність витоку облікових даних, що ще більше захищає інформаційні системи університету від використання зловмисниками.

3) Управління доступом:

a) Управління доступом на основі ролей (RBAC):

Модель управління доступом на основі ролей (RBAC) призначає права доступу користувачам на основі їх ролі в організації, причому різні ролі мають різні обов'язки та привілеї. В інформаційній інфраструктурі університету користувачам присвоюються ролі (наприклад, студент, викладач, адміністратор) та надається доступ до ресурсів, що відповідають їхнім обов'язкам. Такий підхід гарантує, що лише авторизовані користувачі можуть отримати доступ до певних ресурсів, і полегшує управління дозволами користувачів шляхом категоризації прав доступу на основі ролей, а не окремих користувачів.

b) Управління доступом на основі атрибутів (ABAC):

Управління доступом на основі атрибутів (ABAC) визначає права доступу на основі атрибутів користувача, таких як відділ, посада або допуск до секретної інформації. Це дозволяє здійснювати більш детальний контроль доступу, враховуючи різні атрибути при визначенні того, чи слід надавати користувачеві доступ до певних ресурсів. Наприклад, користувачеві з "інженерного відділу" може бути наданий доступ до певних інженерних ресурсів, тоді як користувач з атрибутом "Студент" може мати доступ лише до спільних ресурсів для студентів. ABAC забезпечує динамічне та гнучке управління доступом на основі комбінації атрибутів.

c) Модель з найменшими привілеями:

Модель з найменшими привілеями гарантує, що користувачам надається лише мінімальний доступ, необхідний для виконання їх робочих функцій. Ця

модель зводить до мінімуму ризик неправильного використання або випадкового пошкодження ресурсів університету, обмежуючи права доступу кожного користувача тільки тими ресурсами, які йому необхідні. Наприклад, працівникові може бути наданий доступ до певної бази даних або файлової системи, але він не матиме прав на зміну системних налаштувань або доступ до конфіденційної інформації про викладачів. Принцип найменших привілеїв знижує ймовірність атак з підвищенням привілеїв, коли права доступу користувача використовуються для отримання несанкціонованого доступу до інших ресурсів.

Аналіз цих технологій необхідний для організації безпечних меж ресурсів в інформаційній інфраструктурі університету, забезпечення чіткого визначення прав користувачів, цифрових інформаційних ресурсів і параметрів облікового запису в системах контролю доступу та належного управління ними. Впроваджуючи комбінацію технологій шифрування, автентифікації та контролю доступу, університет може створити надійні заходи безпеки, які захистять його цифрові активи.

Інтеграція безлічі технологій безпеки, таких як різні методи шифрування, багатофакторна автентифікація і управління доступом на основі ролей або атрибутів, допомагає створити комплексний захист від широкого спектру кіберзагроз. Такий багаторівневий підхід гарантує, що ресурси університетської інфраструктури, такі як бази даних, програми та мережі, захищені як індивідуально, так і колективно. Це підвищує загальну кібербезпеку інформаційних систем університету, роблячи їх більш стійкими до потенційних зломів і атак.

Ці технології безпеки відіграють найважливішу роль у:

Запобігання несанкціонованому доступу: використовуючи надійні моделі контролю доступу (наприклад, RBAC, ABAC, Least Privilege) у поєднанні з багатофакторною автентифікацією (2FA), університет гарантує, що тільки авторизовані особи можуть отримати доступ до конфіденційних ресурсів.

Захист конфіденційної інформації: шифрування гарантує, що конфіденційні дані, незалежно від того, зберігаються вони в базах даних або передаються по

мережах, залишаються конфіденційними і захищені від перехоплення або несанкціонованого доступу.

Моніторинг та аудит: ці технології дозволяють здійснювати постійний моніторинг активності користувачів та доступу до системи, допомагаючи виявляти та запобігати потенційним інцидентам безпеки до їх ескалації.

Забезпечення цілісності даних: поєднуючи контроль доступу з шифруванням, університет може захистити цілісність своїх даних, гарантуючи, що вони залишаються точними, незмінними та надійними.

Запобігання витоку даних: безпечний контроль доступу в поєднанні з належними методами шифрування значно знижує ризик випадкового або шкідливого витоку даних.

Ефективно поєднуючи ці технології шифрування, автентифікації та контролю доступу, університет створює систему безпеки, яка запобігає збору, витоку або несанкціонованому доступу до конфіденційної інформації. Це також гарантує безпечне управління обліковими даними користувачів і доступ до ресурсів інфраструктури університету тільки авторизованим користувачам [5]. Такий комплексний підхід до кібербезпеки гарантує безперебійну роботу та захист інформаційних систем університету, знижуючи ймовірність порушень безпеки та підвищуючи загальну довіру до цифрового середовища навчального закладу.

2.4. Висновки до розділу.

У цьому розділі було розглянуто різні загрози та ризики, пов'язані з обміном даними та контролем доступу в контексті кібербезпеки університетських інформаційних систем. На основі аналізу інформаційних систем можна зробити наступні висновки:

Важливість надійного шифрування:

Обмін даними і протоколи передачі цифрових даних, в яких відсутнє належне шифрування, представляють серйозну загрозу конфіденційності переданої інформації. Для запобігання несанкціонованому доступу та витоку даних необхідно шифрувати як дані в стані спокою, так і дані в процесі передачі. Без шифрування існує ризик того, що конфіденційна інформація стане доступною для зловмисників.

Ризик порушення незахищеного пароля:

Обмін цифровою інформацією повинен здійснюватися тільки після повної ідентифікації користувача. Якщо методи захисту паролем є слабкими, це створює вразливості, які можуть бути використані для злому пароля або інших форм несанкціонованого доступу. Витік інформації, зловживання повноваженнями або злом паролів можуть надати зловмисникам доступ до конфіденційних ресурсів і облікових записів користувачів, ставлячи під загрозу безпеку інфраструктури університету.

Важливість систем контролю доступу та автентифікації:

Щоб мінімізувати ризик несанкціонованого доступу, важливо впроваджувати сучасні методи автентифікації, такі як двофакторна автентифікація (2FA), та налаштовувати системи контролю доступу, які обмежують обмін даними лише авторизованими користувачами. Це можна додатково покращити за допомогою одноразових паролів (OTP), які запобігають несанкціонованому доступу, навіть якщо зловмисник отримує доступ до основних облікових даних користувача.

Необхідність постійного моніторингу:

Моніторинг та аудит інфраструктури університету мають вирішальне значення для забезпечення цілісності та безпеки інформаційних систем. Регулярне спостереження допомагає виявити аномалії, такі як незвична активність, які можуть свідчити про порушення безпеки. Раннє виявлення цих проблем є життєво важливим для запобігання злому та зменшення потенційної шкоди, заподіяної кіберзагрозами.

Підвищення обізнаності користувачів:

Важливо інформувати користувачів про ризики та рекомендації щодо забезпечення кібербезпеки. Користувачі з певними ролями, правами та рівнями доступу повинні знати, як створювати надійні паролі, використовувати двофакторну автентифікацію та дотримуватися інших рекомендацій щодо безпеки. Підвищення обізнаності користувачів є ключем до того, щоб вони ненавмисно не сприяли появі вразливостей в системі безпеки.

Необхідність регулярних оновлень і виправлень:

Виправлення безпеки для інформаційних систем, комунікаційних протоколів і систем обміну даними повинні регулярно оновлюватися для усунення відомих вразливостей. Постійний моніторинг та аудит необхідні для забезпечення своєчасного виявлення та усунення потенційних вразливостей. Підтримуючи системи в актуальному стані, університет може зменшити ризик використання їх у кіберзагрозах.

Загальні висновки:

Безпека каналів зв'язку і цифрового обміну даними між інформаційними системами - багатогранна задача, що вимагає інтеграції різних технологій кібербезпеки і передових практик. Використання сучасних методів шифрування, автентифікації та контролю доступу в системах університетської інфраструктури має вирішальне значення для забезпечення захисту конфіденційних даних.

Ризики та загрози, пов'язані з обміном цифровою інформацією у внутрішніх системах університету, підкреслюють важливість захисту інформації та облікових даних користувачів. Захист баз даних та забезпечення цілісності даних є фундаментальним компонентом загальної стратегії кібербезпеки університету. Використовуючи сучасні технології кібербезпеки, такі як шифрування, системи контролю доступу та автентифікації, університет може забезпечити надійний і безпечний обмін інформацією по всій своїй інфраструктурі.

У заключенні, забезпечення безпеки інформаційної інфраструктури університету вимагає постійної пильності, впровадження найкращих практик та застосування передових технологій кібербезпеки для протидії виникаючим загрозам. Регулярні оновлення, всебічний моніторинг та навчання користувачів є важливими кроками у захисті цифрових активів університету та підтримці конфіденційності, цілісності та доступності його інформаційних систем.

3. РОЗРОБКА МЕТОДІВ ЗАХИСТУ ІНФРАСТРУКТУРИ ЗВО

3.1. Розгляд сучасних методів забезпечення безпеки обміну даними в інфраструктурі ЗВО

В даний час існує потреба в перетворенні інфраструктури університету шляхом впровадження нових методів створення захищених цифрових каналів зв'язку, а також для генерації, зберігання та обробки інформації в рамках інформаційних систем університету. Кібербезпека в цьому контексті передбачає розробку надійного захисту цифрових даних, створення захищених мереж зв'язку і забезпечення безпечного обміну даними між користувачами і базами даних, а також систем контролю доступу, що містять конфіденційну інформацію. Ці системи повинні бути захищені від потенційних загроз та кібератак. Тому існує гостра необхідність у впровадженні сучасних методів і засобів забезпечення безпеки для захисту обміну цифровими даними в інформаційних системах університету. Використання сучасних методів і засобів забезпечення безпеки має вирішальне значення для забезпечення стійкості та надійності інфраструктури університету. Шифрування цифрових даних, каналів зв'язку та передачі даних між системами є фундаментальним аспектом забезпечення безпеки інформаційного обміну. Цифрові дані, що зберігаються на університетських ресурсах, повинні бути зашифровані для забезпечення їх захисту. Застосування сучасних криптографічних алгоритмів, таких як Advanced Encryption Standard (aes), забезпечує надійний захист інформації та конфіденційних ресурсів від несанкціонованого доступу [3].

Шифрування переданих даних відіграє важливу роль у забезпеченні безпеки обміну інформацією між базами даних в інфраструктурі університету та зовнішніми системами, будь то через Інтернет або локальну мережу. Використання протоколів SSL / TLS забезпечує шифрування даних під час передачі, запобігаючи несанкціонованому перехопленню конфіденційної інформації. Таке шифрування захищає цілісність даних та конфіденційність протягом усього процесу обміну даними.

На додаток до шифрування, двофакторна автентифікація (2FA) служить важливим заходом безпеки для перевірки ідентичності користувачів, які отримують доступ до інформаційних систем університету. Цей метод вимагає від користувачів надати дві форми ідентифікації: те, що вони знають (наприклад, пароль), і те, що вони мають (наприклад, одноразовий код автентифікації). Така дворівнева перевірка значно підвищує безпеку облікових записів користувачів, особливо при доступі до конфіденційних ресурсів, таких як локальні сервери або хмарні системи [3].

Механізми контролю доступу є ще одним ключовим аспектом забезпечення безпеки університетської інфраструктури. Ці системи визначають права доступу користувачів до інформаційних систем та керують ними. Управління доступом на основі ролей (RBAC) дозволяє адміністраторам призначати певні ролі користувачам, визначаючи їхні права доступу та обов'язки на основі їх ролі в організації. Крім того, управління доступом на основі атрибутів (ABAC) пропонує більш детальний підхід, що обмежує доступ до даних на основі атрибутів користувача (таких як відділ, допуск до секретної інформації або посада) та членство в групах, гарантуючи, що користувачі отримують доступ лише до даних, що стосуються їх функцій.

На додаток до контролю доступу, моніторинг та аудит системи необхідні для виявлення будь-яких порушень або підозрілих дій, які можуть свідчити про порушення безпеки або потенційні кібератаки. Інструменти безперервного моніторингу відстежують діяльність користувачів, продуктивність системи та обмін даними, попереджаючи адміністраторів про будь-які ознаки незвичної поведінки. Відстежуючи стан безпеки системи в режимі реального часу, ці інструменти моніторингу допомагають своєчасно виявляти потенційні загрози і усувати їх до того, як вони зможуть заподіяти значної шкоди [5].

3.2. Вибір методів дослідження та інструментів

Сучасні засоби захисту університетської інфраструктури необхідні для захисту конфіденційної інформації та усунення потенційних загроз безпеці. Ці засоби відіграють життєво важливу роль у підтримці цілісності та конфіденційності інформаційних систем університету. Наступні сучасні рішення

щодо безпеки особливо цінні для покращення інформаційної інфраструктури університету [5]:

Криптографічні бібліотеки та API: сучасні рішення безпеки часто постачаються з інтегрованими криптографічними бібліотеками та програмними інтерфейсами (API), які дозволяють розробникам легко впроваджувати методи шифрування. Ці інструменти дозволяють використовувати надійні криптографічні алгоритми для захисту конфіденційних даних, що зберігаються в базах даних і під час передачі, гарантуючи, що дані залишаються захищеними від несанкціонованого доступу.

SSL / TLS проксі: SSL / TLS проксі забезпечують безпечну передачу даних по мережах за рахунок шифрування з'єднань між користувачами і системами. Ці проксі-сервери забезпечують шифрування будь-яких повідомлень, якими обмінюються клієнти та сервери, запобігаючи перехопленню конфіденційної інформації та захищаючи цілісність даних під час передачі.

Рішення для двофакторної автентифікації (2FA): інструменти для реалізації двофакторної автентифікації (2FA) забезпечують додатковий рівень безпеки при вході користувача в систему. Ці рішення вимагають від користувачів автентифікації своєї особи за допомогою двох різних факторів-того, що вони знають (наприклад, пароль), і того, що вони мають (наприклад, одноразовий код доступу, Створений апаратним маркером, мобільним додатком або хмарною службою). Цей метод подвійної автентифікації значно підвищує безпеку від несанкціонованого доступу.

Інструменти контролю доступу: ефективні інструменти управління контролем доступу дозволяють адміністраторам визначати та застосовувати права доступу користувачів, обмежуючи доступ до певних ресурсів або функціональних можливостей на основі ролей або інших критеріїв. Це гарантує, що лише уповноважений персонал може отримати доступ до конфіденційних даних або виконувати критичні завдання в інформаційній системі.

Інструменти моніторингу та аудиту: інструменти моніторингу та аудиту безпеки відстежують активність користувачів та системи, надаючи цінну інформацію про те, як використовуються інформаційні системи. Реєструючи та

аналізуючи ці дії, адміністратори можуть виявити будь-яку підозрілу поведінку, потенційні порушення або аномалії, які можуть свідчити про постійну загрозу безпеці. Ці інструменти допомагають підтримувати загальну працездатність і безпеку системи, дозволяючи своєчасно виявляти ризики.

Інструменти управління правами користувачів: ці інструменти допомагають адміністраторам налаштовувати та застосовувати права доступу користувачів. Вони дозволяють централізовано управляти дозволами користувачів, забезпечуючи узгоджене застосування політик безпеки і відповідність доступу користувачів їх ролям і обов'язкам. Це також включає управління політикою безпеки та забезпечення внутрішніх правил.

Засоби захисту від витоків: для запобігання несанкціонованому доступу до даних Засоби захисту від витоків застосовують такі політики, як встановлення вимог до надійності пароля, обмеження кількості невдалих спроб входу в систему і обов'язкова регулярна зміна пароля. Ці кошти призначені для мінімізації ризиків витоку даних та забезпечення безпеки паролів та інших облікових даних для доступу.

Інструменти виявлення та реагування на інциденти: ці інструменти мають вирішальне значення для своєчасного виявлення та реагування на інциденти з кібербезпекою, включаючи несанкціонований доступ, порушення даних та потенційні порушення. Засоби виявлення інцидентів і реагування на них, що забезпечують моніторинг в режимі реального часу і автоматичні оповіщення, дозволяють адміністраторам швидко усувати загрози, обмежувати збиток і підтримувати безпеку університетських систем і даних.

Сучасні інструменти, призначені для забезпечення безпеки обміну даними між базами даних в інформаційних системах, створені відповідно до галузевих стандартів, що дозволяє їм відповідати сучасним вимогам кібербезпеки. Ці інструменти відіграють вирішальну роль у захисті баз даних, збереженні конфіденційності конфіденційної інформації та запобіганні загрозам безпеці, які постійно виникають в онлайн-середовищі або кіберпросторі. Нижче наведено деякі найефективніші методи захисту університетської інфраструктури [5]:

Регулярні оновлення та виправлення: одним із ключових компонентів ефективного захисту є послідовне застосування автоматизованих оновлень, виправлень та заходів безпеки до інформаційних систем. Регулярно оновлювані системи необхідні для усунення прогалин у безпеці та вразливостей, які можуть бути використані кіберзлочинцями. Адміністратори повинні переконатися, що всі компоненти інфраструктури інформаційної системи університету підтримуються в актуальному стані, мінімізуючи ризик атак.

Двофакторна автентифікація (2FA): високоефективний метод безпеки, двофакторна автентифікація (2FA) вимагає від користувачів підтвердити свою особу за допомогою двох різних факторів, перш ніж отримати доступ до певних ресурсів. Ці фактори можуть включати поєднання того, що відомо користувачеві (пароль), і того, що він має (одноразовий код, відбиток пальця, карта доступу, PIN-код або SMS-код). Додаючи цей додатковий рівень безпеки, 2FA значно посилює захист, гарантуючи, що навіть якщо зловмисник отримає доступ до пароля, він не зможе отримати доступ до системи без другого фактора автентифікації.

Управління правами доступу: управління правами доступу є найважливішим методом налаштування та управління дозволами в університетських інформаційних системах. Цей підхід визначає детальний контроль доступу для користувачів, гарантуючи, що вони зможуть отримати доступ лише до певних ресурсів, функцій та даних, необхідних для виконання своїх обов'язків. Застосовуючи суворий контроль доступу, цей метод запобігає непотрібному доступу до конфіденційної інформації, такої як приватні бази даних, гарантуючи, що користувачі матимуть доступ лише до даних, необхідних для їх роботи.

Шифрування даних: забезпечення безпеки цифрових даних, особливо баз даних в інформаційних системах університету, вимагає надійних методів шифрування даних. Усі конфіденційні дані повинні бути надійно зашифровані як у стані спокою (збережені дані), так і під час передачі. Сучасні алгоритми шифрування, такі як Advanced Encryption Standard (aes), забезпечують високий рівень захисту від несанкціонованого доступу і витоків даних, гарантуючи, що навіть в разі перехоплення даних вони залишаться нечитабельними для сторонніх осіб.

Моніторинг та аналіз активності: постійний моніторинг та аналіз дій користувачів та системи є життєво важливим для підтримки кібербезпеки університетської інфраструктури. Інструменти моніторингу дозволяють виявляти незвичні або підозрілі дії в мережі, дозволяючи адміністраторам швидко реагувати на потенційні загрози. Ці інструменти автоматично збирають дані, аналізують мережевий трафік і можуть відправляти оповіщення про кіберінциденти в режимі реального часу, що дозволяє оперативно вживати заходів щодо зниження ризиків до їх ескалації.

Захист від впровадження SQL та міжсайтових атак: для захисту від певних типів кібератак, таких як впровадження SQL та міжсайтовий сценарій (XSS), університети повинні впроваджувати заходи безпеки, які захищають їхні інформаційні системи від цих вразливостей. ІН'ЄКЦІЇ SQL та атаки XSS можуть бути використані для використання вразливостей бази даних та витоку конфіденційних даних. Для запобігання цим атакам важливо використовувати безпечні методи кодування, перевірки даних та фільтрації вхідних даних, які блокують шкідливі запити та забезпечують безпечну взаємодію з базою даних.

Захист від витоків: запобігання витокам даних передбачає встановлення чіткої політики та контролю, таких як вимагання створення складних паролів та забезпечення регулярної зміни паролів. Застосовуючи суворі правила щодо використання паролів та контролюючи права доступу, університети можуть значно зменшити ризик випадкового або навмисного порушення даних. Крім того, заходи щодо захисту від витоків допомагають захистити цифрові дані від несанкціонованого доступу, гарантуючи, що конфіденційна інформація залишається в безпеці всередині системи.

Викладені підходи та методи необхідні для забезпечення безпеки інфраструктури університету. Необхідно створити захищені канали для обміну цифровою інформацією між різними інформаційними системами, мережами зв'язку, базами даних по всьому університету та зовнішніми інфраструктурами, такими як Мережі "Розумне місто" та "цифрова держава". Незважаючи на те, що система кіберзахисту університету вже впроваджена і функціонує, важливо розуміти, що її ефективність не може підтримуватися без постійного

вдосконалення та адаптації. Система повинна розвиватися у відповідь на виникаючі загрози кібербезпеки та інциденти, що зачіпають інфраструктуру.

Крім того, постійний моніторинг всієї університетської інфраструктури має вирішальне значення для оцінки рівня її безпеки та виявлення потенційних вразливостей. Для забезпечення довгострокової надійності система повинна постійно впроваджувати нові заходи безпеки, адаптуючись до технологічного прогресу і мінливих загроз. Крім того, надзвичайно важливо поширювати ці інновації серед усіх користувачів університету, щоб вони були обізнані про доступні функції безпеки та могли повною мірою їх використовувати.

Усі аспекти інфраструктури кіберзахисту вимагають регулярної підтримки, оновлення та модернізації, щоб залишатися стійкими. Ці зусилля повинні бути зроблені на всіх рівнях діяльності університету з акцентом на забезпечення безпеки всієї інфраструктури та її оптимального функціонування перед лицем зростаючих кіберзагроз.

3.3. Розробка та імплементація методів та інструментів для забезпечення безпеки інфраструктури ЗВО

Для створення захищеної інформаційної інфраструктури в університеті важливо визначити всі інформаційні системи, які повинні надійно функціонувати, забезпечуючи безпечний обмін інформацією по захищених каналах (як показано на рисунку 3.1).

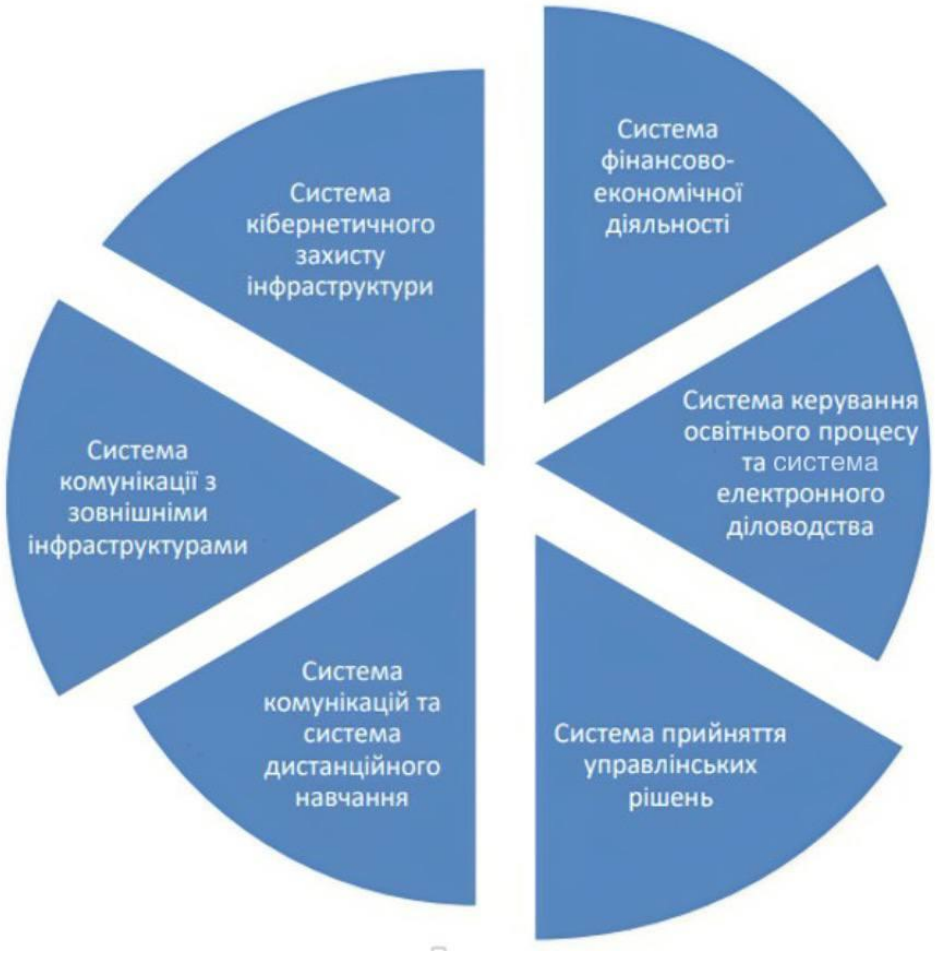

Рисунок 3.1 – Компоненти інформаційної інфраструктури ЗВО.

Система фінансово-економічної діяльності: ця інформаційна система обробляє всі фінансові операції університету, включаючи Облік матеріальних ресурсів, ведення записів співробітників і відстеження вступників до закладів вищої освіти. Він також здійснює нагляд за нарахуванням заробітної плати та стипендій, веде облік соціальної допомоги та контролює витрати навчального закладу, пов'язані з підтриманням необхідних умов для навчання та наданням матеріально-технічної підтримки.

Система керування освітнього процесу та система електронного діловодства: ця система або набір взаємопов'язаних баз даних підтримує повний спектр дій, пов'язаних з управлінням освітнім процесом. Вона включає в себе електронний журнал, розміщення навчальних матеріалів, проведення електронних іспитів і моніторинг успішності. Інформаційна система електронного діловодства також є частиною цієї системи, допомагаючи університетам керувати всіма документами,

контрактами, наказами, інструкціями, листами та іншою документацією, необхідною для повсякденного оперативного управління навчальним закладом.

Система прийняття управлінських рішень: ця інформаційна система надає керівному персоналу інструменти для аналізу різних процесів та отримання точних аналітичних даних на основі отриманих даних. Ці аналітичні дані допомагають прогнозувати розвиток університету та допомагають приймати обґрунтовані рішення.

Система кібербнетичного захисту інфраструктури: це комплексна система, яка включає організаційні, апаратні та програмні заходи безпеки. Вона включає в себе розробку політик безпеки і впровадження різних стратегій захисту дротових і бездротових мереж, систем зв'язку, серверного обладнання, обчислювальних пристроїв і хмарних ресурсів, забезпечуючи загальну безпеку цифрової інфраструктури університету.

Системи комунікацій та система дистанційного навчання: це спеціалізовані інформаційні системи, що використовуються для організації дистанційного навчання та проведення відеоконференцій. Система зв'язку включає керовані комутатори, які допомагають контролювати мережевий трафік, ефективно розподіляти ресурси та підтримувати надійні з'єднання для забезпечення безперебійного зв'язку.

Система комунікацій із зовнішніми інфраструктурами: цей набір інструментів з'єднує системи університету із зовнішніми мережами. Він включає спеціалізоване програмне забезпечення для генерації запитів та отримання інформації із зовнішніх інформаційних центрів відповідно до стандартів інфраструктури, забезпечуючи безперебійний зв'язок із зовнішніми системами.

Для підвищення безпеки інформаційної інфраструктури університету був розроблений ряд заходів і методів, що використовують сучасні засоби захисту інформації. Ці кроки спрямовані на підвищення загальної безпеки та надійності цифрового середовища університету.

Крок 1: Розробка організаційних заходів безпеки

Відповідно до політики безпеки університету, важливо розробити і впровадити заходи кібербезпеки. Це включає створення системи політики,

стандартів та процедур для управління ризиками безпеки та усунення їх наслідків у навчальному закладі.

Крок 2: управління правами доступу

Наступний крок включає розробку та впровадження комплексної системи управління правами доступу. Ця система гарантує, що користувачам надається доступ тільки до певних ресурсів і функціональних можливостей, які необхідні для виконання їх функцій, що допомагає запобігти несанкціонованому доступу до конфіденційної інформації.

Крок 3: двофакторна автентифікація (2FA)

Впровадження двофакторної автентифікації (2FA) для користувачів має вирішальне значення. На додаток до традиційного пароля, користувачам доведеться надати другий фактор автентифікації, такий як одноразовий код, згенерований мобільним додатком, що значно підвищить безпеку від несанкціонованого доступу.

Крок 4: SSL / TLS для безпечного зв'язку

Використання протоколів SSL / TLS забезпечує безпечний зв'язок між базами даних університету та іншими інформаційними системами. Ці протоколи забезпечують шифрування, автентифікацію і гарантують надійність передачі даних, захищаючи їх від потенційного перехоплення і несанкціонованого втручання.

Крок 5: моніторинг активності

Впровадження інструментів моніторингу мережі є ключем до виявлення незвичної активності користувачів. Ці інструменти можуть допомогти виявити потенційні загрози, такі як кібератаки або несанкціонований доступ, і дозволяють аналізувати поведінку системи в режимі реального часу для запобігання порушенням безпеки.

Крок 6: захист від ІН'ЄКЦІЙ SQL та інших атак

Для захисту системи від вразливостей, таких як ІН'ЄКЦІЇ SQL та інші типи атак, важливо впровадити суворі методи перевірки даних та фільтрації вхідних даних. Ці заходи допомагають забезпечити цілісність системи і підтримувати її стабільність і безпеку.

Крок 7: інструменти виявлення та реагування на інциденти

Розробка і впровадження ефективної системи виявлення інцидентів і реагування на них має життєво важливе значення. Ця система дозволить на ранній стадії виявляти потенційні загрози і вживати оперативних заходів для зниження будь-яких ризиків. Своєчасне реагування на інциденти забезпечує постійний захист університетських систем та даних.

Крок 8: Постійне оновлення

Системи кібербезпеки вимагають постійного розвитку. Вся інфраструктура університету повинна регулярно контролюватися і оновлюватися, щоб протистояти виникаючим загрозам. Це включає впровадження нових інструментів, методів та стратегій безпеки відповідно до останніх тенденцій кібербезпеки.

Крок 9: регулярні перевірки безпеки

Необхідно періодично проводити аудити безпеки, щоб оцінити надійність і стійкість інфраструктури університету до зовнішніх загроз. Ці аудити допомагають виявити слабкі місця, дозволяючи адміністраторам усувати уразливості і покращувати загальний стан безпеки системи.

Ці методи та інструменти призначені для підвищення кібербезпеки інформаційних систем університету, сприяючи безпечному обміну даними між базами даних та забезпечуючи безпечну передачу інформації між інфраструктурою університету та зовнішніми користувачами. Вони забезпечують надійний захист від потенційних загроз і кібератак.

Для підвищення безпеки обміну даними між інформаційними системами необхідно впровадження нових заходів безпеки. Це включає розгортання сучасних брандмауерів, систем контролю доступу та комплексних рішень для моніторингу, які контролюють всю інфраструктуру. Ці системи повинні відстежувати активність користувачів, мережевий трафік і навантаження на систему, а також керувати інтерфейсами між локальними серверами і хмарними сервісами. Ці захисні механізми призначені для повного захисту систем і відповідають сучасним стандартам кібербезпеки і передовій практиці [6].

Постійний розвиток, оновлення та впровадження нових інструментів і політик безпеки забезпечать повний захист інфраструктури університету від

кіберзагроз. Цей безперервний процес вдосконалення зміцнить систему кібербезпеки, зберігши цілісність і збереження всієї системи.

3.4. Розробка захищеної системи кіберзахисту інфраструктури ЗВО

Захищена система інформаційної інфраструктури забезпечує надійний і стабільний кіберзахист, ефективне управління цифровими каналами зв'язку і використання шифрування для захисту даних при зберіганні і передачі між користувачами в інформаційних системах. Нижче представлений пропонований алгоритм і ключові етапи побудови такої системи [6]:

Крок 1: створення захищеної системи університетської інфраструктури.

Розробка системи (рисунок 3.2): при проектуванні системи слід враховувати унікальні аспекти кіберзахисту в університетах, особливо в умовах воєнного стану. Це передбачає реструктуризацію функцій та взаємозв'язків між інформаційними системами університету для забезпечення стійкості та безпеки в складних умовах.

Рисунок 3.2 – Компоненти захисту інформаційної інфраструктури ЗВО.

Крок 2: Реєстрація, автентифікація та авторизація користувачів

1) Реєстрація та автентифікація користувачів:

Всі користувачі повинні бути зареєстровані у всіх системах, що забезпечує єдиний реєстр користувачів.

Для автентифікації користувача потрібна двофакторна автентифікація (2FA), що підвищує безпеку шляхом перевірки особи за допомогою двох незалежних факторів.

Авторизація повинна відповідати сучасним стандартам безпеки, включаючи використання криптографічних електронних підписів (Кеп), електронних цифрових підписів (ЕЦП) і механізмів хешування.

2) Авторизація користувачів в інформаційних системах:

Кожному користувачеві надаються певні права з обмеженнями доступу на основі його ролі та статусу в системі.

Для регулювання доступу користувачів до ресурсів, моніторингу дій користувачів і забезпечення дотримання прав доступу слід використовувати різні алгоритми авторизації. Це також передбачає виявлення та усунення потенційних прогалин у безпеці баз даних системи.

3) Управління обліковими даними користувачів:

Система доступу повинна підтримувати додавання, оновлення та видалення облікових даних користувачів.

Для запобігання несанкціонованого доступу слід застосовувати посилений контроль доступу до ресурсів, а для цілей аудиту слід вести докладні журнали всіх дій користувача.

Крок 3: Захист каналів обміну даними між інформаційними системами

1) Шифрування даних:

Для захисту цілісності обміну даними рекомендується використовувати надійні протоколи шифрування (наприклад, TLS/SSL) для захисту каналів зв'язку між базами даних та іншими системами.

2) Автентифікація користувача і призначення прав:

Двофакторна автентифікація (2FA) повинна бути інтегрована з механізмами автентифікації, такими як API-Ключі, токени, CAP (криптографічні процедури

доступу) і ЕЦП (електронні цифрові підписи), щоб забезпечити безпечний доступ до ресурсів на основі прав користувача.

Крок 4: Захист, архівування та відновлення бази даних

1) Шифрування бази даних:

Для шифрування конфіденційного вмісту бази даних слід використовувати надійні методи шифрування, такі як aes. Це допомагає захистити дані від несанкціонованого доступу та забезпечує їх конфіденційність.

2) Контроль цілісності бази даних:

Захищені бази даних повинні контролюватися та управлятися системними утилітами. Після автентифікації користувача повинні бути надані права доступу і встановлені захищені канали зв'язку між інформаційними системами (як внутрішніми, так і зовнішніми) і хмарними сервісами.

Крок 5: моніторинг інфраструктури та реагування на інциденти

1) Моніторинг інфраструктури університету:

Впровадьте інструменти моніторингу активності для відстеження поведінки користувачів в інформаційних системах та проведення аудиту подій для виявлення аномальних дій та потенційних загроз безпеці.

Використовуйте системи моніторингу мережі та комунікацій для відстеження завантаження мережі та баз даних, аудиту дій та виявлення потенційних загроз зв'язку.

2) Виявлення інцидентів і реагування на них:

Повинні бути розроблені процедури реагування на інциденти з призначеними системними адміністраторами, відповідальними за обробку інцидентів кібербезпеки. Ці адміністратори повинні бути навчені швидкій оцінці підозрілої діяльності та прийняттю відповідних контрзаходів.

Крок 6: Регулярне оновлення інфраструктури та навчання персоналу

1) Оновлення системи та внесення виправлень:

Необхідно регулярно оновлювати інфраструктуру інформаційних систем університету для усунення вразливостей і підвищення безпеки.

2) Навчання персоналу:

Співробітники повинні проходити безперервне навчання, щоб бути в курсі новітніх знань і практик в області кібербезпеки, що дозволить їм ефективно захищати інформаційні системи університету від виникаючих загроз.

В інфраструктурі університету створена надійна система кібербезпеки, що дозволяє здійснювати всебічний моніторинг всіх дій користувачів в системі. Це включає механізми контролю доступу та управління каналами зв'язку, що забезпечують безпечний обмін даними між базами даних інформаційної системи університету.

Розробка повнофункціональної і безпечної системи контролю доступу, поряд з управлінням каналами зв'язку між базами даних, повинна бути адаптована до конкретних потреб і викликів безпеки закладів вищої освіти. Це складне завдання, для вирішення якої потрібне застосування різних технічних рішень.

Технічна реалізація цієї системи повинна здійснюватися відповідно до кроків, описаних нижче:

Аналіз інформаційних систем університету:

Проведення комплексного аудиту інформаційних систем університету з метою виявлення вразливостей в операційних системах, клієнтському програмному забезпеченні та потенційних загроз функціональності системи.

Аналіз систем зв'язку та каналів обміну даними:

1) Аудит мережевого обладнання, конфігурацій серверів, мережевих операційних систем, серверного обладнання, віртуальних мереж, віртуальних серверів і каналів зв'язку.

2) Виявлення загроз безпеці, пов'язаних із серверами та комунікаційним обладнанням в інформаційних системах університету.

Компоненти системи:

1) Комп'ютерне обладнання, включаючи гаджети та планшети.

2) Мультимедійне обладнання, таке як телевізори, світлодіодні екрани, проектори.

3) Конференц-системи, як дротові, так і бездротові аудіосистеми, системи розповсюдження відеоконтенту та інфраструктура потокової передачі.

4) Студії звукозапису та відеомонтажу.

5) Спеціалізовані лабораторії, комп'ютерні класи та дослідницькі центри.

6) Системи контролю доступу для управління доступом до ресурсів університету та їх використанням.

7) Фінансові та адміністративні системи, включаючи бухгалтерський облік, планування, Соціальне забезпечення, управління гуртожитками та багато іншого.

8) Системи електронного діловодства для обробки документів.

9) Веб-сайт університету, системи дистанційного навчання та хмарні ресурси.

10) Системи для взаємодії із зовнішніми користувачами через інфраструктуру університету.

11) Гостьові та персоналізовані системи бездротового доступу для забезпечення безпечних з'єднань.

Система кібербезпеки в умовах воєнного стану: система кібербезпеки інформаційних систем університету в умовах воєнного стану включає наступні компоненти:

1) Організаційний захист:

Розробка політики кібербезпеки, яка регулює діяльність університету. Усі користувачі інформаційних систем повинні дотримуватися політики, викладеної в рамках концепції.

2) Двофакторна автентифікація (2FA):

Обов'язкова для всіх користувачів, які отримують доступ до університетських ресурсів. 2FA може включати облікові дані для входу, криптографічні процедури доступу (CAP), ЕЦП (електронні цифрові підписи) або біометричні дані для підвищення безпеки.

3) Доступ та управління ресурсами на основі ролей:

Користувачам призначаються певні ролі з певними правами доступу до ресурсів. Система підтримує керування обліковими записами користувачів, включаючи реєстрацію, визначення прав, зміну доступу та деактивацію облікових записів.

4) Шифрування даних:

Шифрування даних використовується для зберігання конфіденційної інформації в базах даних та забезпечення безпечного доступу до Інтернету. Доступ до зашифрованих даних можуть отримати Тільки авторизовані користувачі.

5) Розробка API для обміну даними:

API розроблені для забезпечення безпечного обміну даними між внутрішніми інформаційними системами та зовнішніми інфраструктурами.

6) Безпечні протоколи зв'язку:

Захищені канали зв'язку, такі як HTTPS, використовуються для забезпечення цілісності та конфіденційності даних під час передачі.

7) Впровадження брандмауера:

Як внутрішні, так і зовнішні брандмауери використовуються для захисту локальних серверів і обмеження несанкціонованого доступу з скомпрометованих клієнтських систем.

8) Захист від відмов в обслуговуванні (DOS) і DDoS-атак:

Створені системи захисту від DoS-атак і DDoS-атак, що забезпечують надійність і стійкість мережі.

9) Системи виявлення та запобігання вторгнень:

Використовуються інструменти для виявлення і блокування шкідливої мережевої активності, що запобігають несанкціоновані вторгнення.

10) Регулярні оновлення системи та внесення виправлень:

Інфраструктура постійно оновлюється та оновлюється за допомогою виправлень для усунення вразливостей та забезпечення постійного захисту.

11) Захист від поширених атак:

Існують механізми захисту від типових кібератак, таких як ІН'ЄКЦІЇ SQL, міжсайтовий сценарій, переповнення буфера та інші шкідливі дії.

12) Виявлення інцидентів і реагування на них:

Для своєчасного виявлення та усунення загроз впроваджена комплексна система реагування на інциденти. Система регулярно оновлюється, щоб відповідати виникаючим ризикам в області кібербезпеки.

13) Навчання спеціалістів з кіберзахисту:

Співробітникам кібербезпеки надаються можливості для постійного навчання та підвищення кваліфікації, включаючи практичні заняття з кібербезпеки для підвищення кваліфікації.

14) Захист інфраструктури:

Застосовуються запобіжні заходи для запобігання несанкціонованому доступу та захисту базової інфраструктури, що підтримує інформаційні системи університету.

Принципи побудови системи кібербезпеки:

1) Початковий аналіз інфраструктури:

Перший крок передбачає ретельний аналіз всієї університетської інфраструктури, включаючи всі інформаційні системи, з метою виявлення вразливостей.

2) Прозорість і керованість:

Система повинна бути прозорою і простою в Управлінні, з чітким контролем за обміном даними між інформаційними системами всередині університету.

3) Резервне копіювання та відновлення даних:

Для захисту від втрати даних впроваджені системи резервного копіювання та процедури відновлення цифрових даних.

4) Регулярні перевірки інфраструктури:

Проводьте регулярні аудити інфраструктури для виявлення слабких місць і забезпечення стійкості системи до потенційних кібератак.

5) Постійне оновлення системи:

Постійний моніторинг та оновлення необхідні для того, щоб випереджати розвиток кіберзагроз.

6) Навчання фахівців в області кібербезпеки:

Постійна освіта фахівців з кібербезпеки дозволяє їм бути в курсі останніх досягнень у галузі безпеки, інструментів та технологій.

Розробка комплексної системи кіберзахисту передбачає ретельну оцінку потреб інфраструктури університету та потенційних загроз, а також інтеграцію передових інструментів, технологій та методологій кібербезпеки. Ключовим компонентом цієї системи є створення надійної та безпечної системи управління

обміном даними, яка передбачає розробку API для захищених каналів зв'язку між різними інформаційними системами.

Ця система повинна бути адаптованою та масштабованою, щоб відповідати майбутньому зростанню та виникаючим загрозам. Процеси реєстрації користувачів у поєднанні з двофакторною автентифікацією через захищені канали зв'язку є невід'ємною частиною системи. Таким чином, рішення повинно також включати додаткові заходи безпеки, такі як управління правами доступу, шифрування даних для обміну інформацією, моніторинг активності та інші захисні механізми.

Базова система безпеки та автентифікації може постійно вдосконалюватися та розширюватися відповідно до конкретних вимог, забезпечуючи її відповідність мінливим вимогам університетської інфраструктури кібербезпеки.

3.5. Розробка та впровадження інтелектуальної системи моніторингу та прогнозування кіберзагроз для захисту інформаційних ресурсів ЗВО

Перед обличчям все більш витончених кіберзагроз українські університети, як і багато навчальних закладів по всьому світу, потребують передових систем захисту своїх інформаційних ресурсів. Розробка та впровадження інтелектуальної системи моніторингу та прогнозування кіберзагроз має вирішальне значення для захисту критично важливих даних, забезпечення безперервності академічних операцій та підтримки цілісності дослідницької діяльності. У цьому розділі описані кроки, необхідні для створення такої системи, включаючи її дизайн, функціональність і переваги, які вона надасть українським університетам в зниженні потенційних кіберризиків.

1) Проектування та архітектура системи.

Інтелектуальна система моніторингу та прогнозування для українських університетів має бути розроблена для активного виявлення, аналізу та прогнозування кіберзагроз у режимі реального часу. Архітектура системи повинна включати багаторівневий моніторинг безпеки, моделі машинного навчання та автоматизовані механізми реагування для забезпечення надійності та оперативності. Ключові компоненти цієї системи включатимуть:

Виявлення загроз у режимі реального часу: Система повинна інтегрувати датчики, системи виявлення вторгнень (IDS) та інструменти управління

інформацією про безпеку та події (SIEM) для моніторингу мережевого трафіку, активності користувачів та потенційних вразливостей в IT-інфраструктурі університету. Аналізуючи величезну кількість даних із серверів, кінцевих точок, мережевих пристроїв та хмарних сервісів, система може виявити аномальну поведінку, яка може свідчити про кіберзагрозу.

Машинне навчання та прогнозна аналітика: використання алгоритмів машинного навчання може підвищити здатність системи прогнозувати виникаючі загрози. Аналізуючи Історичні дані про кібератаки, система може вивчати закономірності і тенденції, що дозволить їй з більшою точністю прогнозувати майбутні загрози. Прогнозована аналітика дозволила б виявити нові вектори та методи атаки на ранній стадії, надаючи команді з кібербезпеки достатньо часу для вжиття запобіжних заходів до того, як атака здійсниться [4].

Автоматизовані механізми реагування: при виявленні потенційної загрози система повинна бути здатна активувати автоматичні контрзаходи, щоб звести до мінімуму ризик злому. Наприклад, автоматизовані системи можуть ізолювати вразливі сервери, блокувати шкідливі IP-адреси або обмежувати доступ користувачів, щоб запобігти поширенню атаки. Ці дії будуть здійснюватися паралельно з контролем з боку персоналу, щоб гарантувати оперативність і адекватність реагування.

2) Інтеграція з існуючою університетською інфраструктурою.

Щоб система була ефективною, вона повинна бути повністю інтегрована з існуючою IT-інфраструктурою університету, включаючи:

Мережі кампусу та центри обробки даних: система моніторингу повинна охоплювати всі канали зв'язку в університеті, включаючи дротові та бездротові мережі, VPN та хмарні сервіси. Це гарантує, що всі внутрішні та зовнішні обміни даними постійно відстежуються на предмет потенційних кіберзагроз.

Системи управління базами даних: слід використовувати безпечні механізми контролю доступу, такі як доступ на основі ролей та двофакторна автентифікація (2FA), щоб гарантувати, що лише уповноважений персонал може взаємодіяти з критичними даними. Аналізуючи журнали доступу та схеми дій, система може

виявити незвичну поведінку, яка може свідчити про спробу зламати конфіденційну інформацію.

Освітні платформи та програми: в умовах зростаючої залежності від систем управління навчанням (LMS), онлайн-порталів та дослідницьких баз даних важливо забезпечити захист цих платформ від кіберзагроз. Інтелектуальна система моніторингу повинна мати можливість відстежувати доступ користувачів та їх взаємодію на цих платформах, виявляючи потенційні вразливості, шкідливі логіни або несанкціоновані зміни Даних.

Інструменти спільної роботи та хмарні ресурси: оскільки українські університети все частіше звертаються до хмарних сховищ та інструментів онлайн-спільної роботи, моніторинг цих сервісів на предмет потенційних витоків даних, несанкціонованого доступу або підозрілого обміну файлами має вирішальне значення. Інтеграція з хмарними платформами, такими як Google Cloud, Microsoft Azure або Amazon Web Services (AWS), дозволить системі відстежувати передачу файлів, спроби доступу та інші потенційні ризики, пов'язані з хмарними ресурсами.

3) Аналіз загроз та зовнішніх джерел даних.

Використання інформаційних джерел про зовнішні загрози може значно розширити можливості системи для прогнозування. Аналітичні дані про загрози можуть надати цінну інформацію про новітні методи атаки, вразливості та тактику, що використовуються кіберзлочинцями. Об'єднуючи глобальні та регіональні джерела інформації про загрози, українські університети можуть бути в курсі виникаючих загроз, які можуть бути спрямовані проти їх інфраструктури.

Глобальні мережі збору інформації про загрози: до них відносяться такі джерела, як ISACs (центри обміну інформацією та аналізу), CERTs (групи реагування на комп'ютерні надзвичайні ситуації) і галузеві джерела інформації про загрози, які надають актуальну інформацію про поточні уразливості і активних експлойтів.

Місцеві джерела інформації про загрози: враховуючи геополітичний контекст України, місцеві джерела інформації про загрози, включаючи урядові установи, організації з кібербезпеки та національні сертифікати, можуть допомогти виявити загрози, характерні для конкретного регіону. Ця інформація має

вирішальне значення для розуміння кібератак, які можуть бути спрямовані проти українських установ, особливо в разі геополітичної напруженості або військових конфліктів.

4) Прогнозна аналітика та моделі машинного навчання.

В основі інтелектуальної системи моніторингу лежить її здатність прогнозувати кіберзагрози. Прогнозні моделі, засновані на алгоритмах машинного навчання, можуть аналізувати закономірності в даних попередніх кіберінцидентів для прогнозування майбутніх атак. До числа ключових областей, в яких може застосовуватися прогнозна аналітика, відносяться:

Поведінкова аналітика: вивчаючи моделі поведінки користувачів (наприклад, час входу в систему, частоту доступу, зміни файлів), система може виявляти відхилення, які вказують на потенційну внутрішню загрозу або скомпрометований обліковий запис.

Аналіз мережевого трафіку: моделі машинного навчання можуть аналізувати мережевий трафік на предмет аномальних моделей, що вказують на атаки, такі як розподілена відмова в обслуговуванні (DDoS), активність ботнету або спроби порушення даних. Ці прогнозні моделі можуть попередити охорону про підозрілі дії, перш ніж вони переростуть у повноцінні атаки.

Фішинг та атаки з використанням соціальної інженерії: аналізуючи трафік електронної пошти, активність в Інтернеті та схеми спілкування, система може виявити потенційні спроби фішингу або соціальної інженерії, спрямовані проти співробітників Університету або студентів. Прогнозні моделі можуть виявляти поширені тактики фішингу, такі як підозрілі посилання, вкладення або адреси електронної пошти.

5) Інформаційні панелі та звітність у режимі реального часу.

Для ефективного прийняття рішень інтелектуальна система повинна включати інформаційну панель у режимі реального часу, яка надає командам з кібербезпеки всебічну інформацію про стан мережі Університету, поточні загрози та потенційні ризики. Ключові функції інформаційної панелі повинні включати:

Візуальні карти загроз: відображають поточний стан мережі, виділяють зони, що знаходяться під загрозою, і точно визначають поточні атаки.

Сповіщення та сповіщення про загрози: автоматичне сповіщення про виявлені загрози з повідомленнями, що надсилаються співробітникам Служби безпеки в режимі реального часу, що допомагає їм оперативно реагувати.

Відстеження інцидентів: дозволяє відстежувати інциденти з часом, аналізувати закономірності та створювати звіти про попередні загрози та про те, як вони були усунені.

Ці інформаційні панелі також повинні підтримувати можливості детальної звітності з метою дотримання вимог, що дозволить університету продемонструвати свою прихильність національним правилам та стандартам кібербезпеки.

6) Реагування на інциденти та судово-медична експертиза.

У разі виявлення загрози система повинна розробити надійний план реагування на інциденти, що гарантує прийняття всіх необхідних заходів для стримування, пом'якшення наслідків і відновлення після атаки. Це включає в себе:

Ізоляцію інцидентів: автоматичну ізоляцію скомпрометованих пристроїв або сегментів мережі для запобігання подальшого поширення атаки.

Криміналістичний аналіз: надання інструментів для криміналістичного розслідування після нападу, що дозволяє фахівцям з безпеки відстежувати джерело та масштаби нападу, розуміти використовувані методи та виявляти потенційні слабкі місця в інфраструктурі.

Відновлення та резервне копіювання: забезпечення регулярного резервного копіювання університетських даних та можливості їх відновлення у разі кібератаки. Система повинна забезпечувати швидке відновлення з резервних копій і відновлення нормальної роботи якомога швидше.

7) Постійне вдосконалення та навчання.

У міру розвитку кіберзагроз необхідно вдосконалювати системи моніторингу та прогнозування. Регулярні оновлення систем, навчання моделям машинного навчання та перепідготовка персоналу є важливими компонентами ефективної стратегії кібербезпеки. Українські університети повинні інвестувати в постійне вдосконалення, використовуючи відгуки про інциденти безпеки, нові аналітичні дані про загрози і уроки, витягнуті з минулих атак, для вдосконалення своїх моделей виявлення і прогнозування загроз.

Крім того, слід впроваджувати програми поінформованості про кібербезпеку для навчання персоналу, студентів та викладачів розпізнаванню та реагуванню на кіберзагрози, що ще більше зменшує ймовірність людських помилок, що призводять до порушень безпеки.

3.6. Висновки до розділу.

У цьому розділі розглядаються сучасні підходи до побудови безпечної університетської інфраструктури з акцентом на створення захищених каналів зв'язку, забезпечення безпечного обміну даними між базами даних та впровадження систем контролю доступу, які захищають конфіденційні облікові дані та конфіденційну інформацію. Ці системи повинні бути достатньо надійними для захисту від потенційних загроз та кібератак. Принципи архітектури системи кібербезпеки, включаючи виявлення загроз, механізми реагування та протоколи контролю доступу, мають вирішальне значення для забезпечення стабільності та надійності інформаційних систем університету.

Шифрування переданих даних має важливе значення при обміні інформацією між університетськими базами даних та зовнішніми системами через різні канали передачі, такі як Інтернет або локальні мережі. Використання протоколів SSL / TLS при передачі даних гарантує шифрування, яке ефективно запобігає несанкціонованому перехопленню конфіденційної інформації.

Двофакторна автентифікація (2FA) відіграє важливу роль у ідентифікації та авторизації користувачів в університетських інформаційних системах. Вона забезпечує безпечний доступ як до локальних, так і до хмарних ресурсів, вимагаючи від користувачів підтвердження своєї особи двома різними способами, такими як пароль в поєднанні з одноразовим кодом. Цей додатковий рівень безпеки гарантує, що навіть у разі порушення пароля несанкціонований доступ все одно буде запобігати без використання другого фактора автентифікації.

Сучасні інструменти та методи забезпечення безпеки університетської інфраструктури незамінні для захисту конфіденційних даних та запобігання потенційним кіберзагрозам. Використання 2FA особливо важливо, оскільки воно підвищує безпеку інформаційних систем, вимагаючи двох окремих форм автентифікації, будь то пароль і одноразовий код, відбиток пальця і код-шифр, PIN-

код за допомогою карти або інші методи. Такий підхід значно підвищує безпеку, гарантуючи, що зловмисник не зможе отримати доступ, просто скомпрометувавши один з факторів автентифікації.

Шифрування даних-ще один важливий метод захисту всієї цифрової інформації в інформаційних системах університету. Сучасні алгоритми шифрування, такі як AES, забезпечують надійний захист від несанкціонованого доступу до конфіденційних даних, що зберігаються в базах даних.

Завдяки впровадженню цих найкращих практик безпеки інформаційні системи університету будуть краще оснащені для забезпечення безпечного обміну даними та захисту від потенційних загроз та атак. Застосування брандмауерів, систем контролю доступу і комплексних інструментів моніторингу, таких як відстеження активності користувачів, аналіз мережевого навантаження і безпечні з'єднання між локальними і хмарними сервісами, підвищить загальну безпеку.

Постійні оновлення та розробка нових заходів безпеки забезпечать повний захист інфраструктури, адаптуючись до мінливих загроз та стандартів кібербезпеки. Це забезпечить довгостроковий кіберзахист інфраструктури університету, захищаючи як внутрішні системи, так і обмін даними із зовнішніми організаціями.

Розробка та впровадження інтелектуальної системи моніторингу та прогнозування кіберзагроз в українських університетах є важливим кроком на шляху до забезпечення безпеки та відмовостійкості їх інформаційних ресурсів. Використовуючи моніторинг у режимі реального часу, Машинне навчання, прогнозну аналітику та проактивний аналіз загроз, ці системи можуть значно підвищити здатність університету виявляти потенційні кібератаки, реагувати на них та пом'якшувати їх наслідки. Цей найкращий підхід до кібербезпеки не тільки захистить конфіденційні дані, але й забезпечить безперебійну роботу академічних та адміністративних служб, незважаючи на зростаючі складності та ризики, пов'язані з кіберзагрозами. Завдяки інтеграції цих інноваційних систем українські університети будуть краще оснащені для захисту своєї цифрової інфраструктури та підтримки безпечного середовища для викладання, досліджень та адміністрування.

ВИСНОВКИ

Розробка та впровадження системи кіберзахисту для українських університетів є важливим кроком на шляху до забезпечення цілісності, доступності та конфіденційності їх інформаційних систем. Ця дипломна робота детально описує основні компоненти, необхідні для створення захищеної інформаційної інфраструктури, з акцентом на ключові механізми, такі як двофакторна автентифікація (2FA), шифрування даних та захищені протоколи зв'язку. Ці заходи не тільки захищають від несанкціонованого доступу, але й забезпечують безпечний обмін даними між різними університетськими системами та зовнішніми інфраструктурами.

В умовах воєнного стану необхідність у надійній кібербезпеці стає ще більш нагальною. Організаційні заходи безпеки набувають вирішального значення, і всі користувачі університетських інформаційних систем повинні бути належним чином поінформовані про їх роль у забезпеченні безпеки. Для захисту конфіденційних даних потрібні методи безпечного доступу, включаючи використання захищених електронних підписів (SES), зашифрованих систем зберігання та біометричної автентифікації. Використання сучасних брандмауерів — як зовнішніх, так і внутрішніх — також допомагає контролювати доступ до університетських систем і запобігати несанкціонованим вторгненням, а системи виявлення інцидентів і реагування на них дозволяють швидко реагувати на потенційні загрози.

Для забезпечення постійної безпеки інформаційної інфраструктури університету в даній дипломній роботі пропонується кілька рекомендацій. До них відносяться проведення всебічного аналізу інфраструктури, впровадження прозорої системи управління обміном даними та використання регулярних аудитів для виявлення вразливостей системи. Крім того, впровадження двофакторної автентифікації (2FA) у всіх інформаційних системах має важливе значення для підвищення безпеки обміну даними, в той час як управління обліковими записами користувачів забезпечує належне визначення і дотримання прав доступу.

Важливою рекомендацією є розробка інтелектуальної системи моніторингу для виявлення та прогнозування кіберзагроз. Ця система використовуватиме Машинне навчання та інтелектуальну аналітику для моніторингу мережевого трафіку університету, виявлення незвичних закономірностей та прогнозування потенційних атак до того, як вони відбудуться. Завдяки інтеграції аналізу даних у режимі реального часу та аналізу загроз система дозволить університетам активно виявляти вразливості та своєчасно реагувати на кіберінциденти.

Використовуючи передові технології, університет може не тільки захистити свої інформаційні системи від відомих загроз, але й передбачити нові види кіберризиків, підвищуючи загальну стійкість. Використання такої інтелектуальної системи моніторингу стане ключовим фактором у мінімізації наслідків кібератак, скороченні часу реагування та забезпеченні постійної адаптації до виникаючих загроз.

Використовуючи ці методи та інструменти, університет може значно зміцнити свою позицію в галузі кібербезпеки, забезпечивши безпечний обмін даними, захист від потенційних загроз та зберігаючи цілісність своїх інформаційних систем. Поєднання організаційних заходів безпеки, технологічних рішень та можливостей прогнозного моніторингу допоможе українським університетам захистити свої цифрові ресурси та продовжити свою академічну, дослідницьку та адміністративну діяльність без збоїв.

Таким чином, інтеграція інтелектуальної системи моніторингу в існуючу систему кібербезпеки поряд з впровадженням надійних організаційних і технічних заходів безпеки забезпечить комплексний адаптивний захист від мінливого ландшафту кіберзагроз, забезпечуючи довгострокову стійкість і безпеку університетської інформаційної інфраструктури.

ПЕРЕЛІК ПОСИЛАНЬ

1. Данюк Ю.Г. основи кібербезпеки та кібероборони: підручник/ ОНАЗ ім. О.С. Попова, Одеса 2019 – 320с.

2. Домарєв В.В, Система ситуаційного управління/ Знання України, Київ 2017 – 348с.

3. Остапов С. Е. технологія захисту інформації : навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с

4. Дубина В.П. Розробка та впровадження інтелектуальної системи моніторингу та прогнозування кіберзагроз для захисту інформаційних ресурсів ВНЗ/Дубина В,П. // Інформаційні технології і автоматизація – 2024: Матеріали XVII Міжнародної науково-практичної конференції, [Одеса], 31 жовтня – 1 листопада 2024 р. – Одеса, Видавництво ОНТУ, 2024 р. – С. 190.

5. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби : посібник / [В. Л. Бурячок, С. В. Толюпа, В. В. Семко та ін.]. – К. : ДУТ-КНУ, 2016. – 178 с.

6. Захарченко М.В. Інформаційна безпека інформаційно-комунікаційних систем. Захист інформації від НСД у каналах зв'язку: навч. посіб. / М.В. Захарченко, В.В. Топалов, М.С. Русляченко // За ред. чл.-кор. МАЗ В.Г. Кононовича. – Одеса: ОНАЗ ім. О.С. Попова, 2014. – 228 с.

7. Про основні засади забезпечення кібербезпеки України [Закон України]: № 2163-VIII від 5 жовтня 2017 року. [Електронний ресурс]. — Режим доступу: https://zakon.rada.gov.ua/laws/show/2163-19#Text. (дата звернення: 11.11.2024).

8. Державна служба спеціального захисту зв'язку та захисту 1нформаці [державні сайти України]. [Електронний ресурс]. — Режим доступу: https://cip.gov.ua/ua. (дата звернення: 11.11.2024).

9. К. Бєляков, Інформатизація в Україні: проблеми організаційного, правового та наукового забезпечення/ Київ, Україна: КВІЦ, 2008. – 576 с.

10. Закон України «Про захист персональних даних», від 01.06.2010 № 2297-VI. [Електронний ресурс]. — Режим доступу:

https://www.kadrovik01.com.ua/article/3659-qqq-17-m4-normativna-baza-tatermnologya-u-sfer-zahistu-personalnih-danih

11. EU General Data Protection Regulation, EU GDPR. [Електронний ресурс]. — Режим доступу: https://www.kingston.com/ru/ solutions/data-security/eu-gdpr (дата звернення: 17.11.2024).

12. В. Бурячок, В. Богуш, Ю. Борсуковський, П. Складанний, та В. Борсуковська, "Модель підготовки фахівців у сфері інформаційної та кібернетичної безпеки в закладах вищої освіти України", Інформаційні технології та засоби навчання, т. 67, № 5, с. 277-291, 2018. [Електронний ресурс]. — Режим доступу: http://nbuv.gov.ua/UJRN/ITZN_2018_67_5_24 (дата звернення: 22.11.2024).

13. В. Чекурін, та О. Будік, "Модель інформаційної системи ВНЗ та підхід до оцінювання її ризиків"/ Вісник Національного університету "Львівська політехніка", 2010. № 665. с. 83-90,