Державний заклад
«ПІВДЕННОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ ПЕДАГОГІЧНИЙ УНІВЕРСИТЕТ імені К. Д. УШИНСЬКОГО»

ОДЕСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ імені І. І. МЕЧНИКОВА

ДВАДЦЯТЬ ДРУГА ВСЕУКРАЇНСЬКА КОНФЕРЕНЦІЯ СТУДЕНТІВ І МОЛОДИХ НАУКОВЦІВ

ІНФОРМАТИКА, ІНФОРМАЦІЙНІ СИСТЕМИ ТА ТЕХНОЛОГІЇ

25 квітня 2025 р.

Одеса – 2025

Інформатика, інформаційні системи та технології: тези доповідей двадцять другої всеукраїнської конференції студентів і молодих науковців. Одеса, 25 квітня 2025 р. - Одеса, 2025. – 315 с.

Друкується за рішенням Вченої Ради
Університету Ушинського
(протокол № 16 від 29.05.2025 р.)

Організатори конференції продовжують традицію обміну досвідом у сфері освіти та використання інформаційних технологій. У конференції приймають участь студенти, аспіранти та молоді науковці вищих навчальних закладів України.

Тематика конференції охоплює наступне коло питань: сучасні інформаційні технології; інтелектуальні системи; методика викладання інформатики; інформаційні технології в освіті; психолого-педагогічне забезпечення інформатизації навчальної діяльності; дистанційна освіта і глобальні телекомунікаційні мережі; математичне моделювання й інформаційні технології; інформатизація системи керування освітою; інформаційні технології в менеджменті.

Наукові керівники:

завідувачка кафедри прикладної математики та інформатики
фізико-математичного факультету Університету Ушинського, д. т. н., проф. Т. Л. Мазурок,
завідувач кафедри математичного забезпечення комп'ютерних систем факультету математики, фізики та інформаційних технологій ОНУ імені І. І. Мечникова, д. т. н., проф. Є. В. Малахов

Оргкомітет:

Голова:

Ректор Університету Ушинського,
д. і. наук, доц. А. В. Красножон

Заступники голови:

Проректор з наукової роботи Університету Ушинського, д. політ. н., проф. Г.В. Музиченко
Декан факультету математики, фізики та інформаційних технологій ОНУ імені І. І. Мечникова, д. ф-м. н., проф. Ю. А. Ніцук

Члени оргкомітету:

д. т. н., проф.	Є. В. Малахов	д. т. н., проф.	Т. Л. Мазурок
д. т. н., проф.	Ю. О. Гунченко	к. п. н., доц.	А. О. Яновський
ст. викладач	І. М. Лісіцина	викладач	О. Я. Рубанська
ст. викладач	Н. Ф. Трубіна	к. ф.-м. н.	О. П. Бойко
ст. викладач	В. А. Корабльов	PhD, associated prof. (Poland)	A. Rychlik

Розробка подібної системи є важливим кроком у розвитку розумних будинків, адже вона відповідає сучасним викликам безпеки та автоматизації. Біометричне розпізнавання обличь, як основа системи, забезпечує високий рівень захисту, а локальний підхід усуває залежність від зовнішніх сервісів, що є критичним у контексті захисту особистих даних. Подальші дослідження можуть бути спрямовані на вдосконалення алгоритмів розпізнавання для роботи в складних умовах і розширення інтеграції з іншими IoT-пристроями, що підвищить універсальність системи.

Література

1. Денис Соловей, Що таке розумний будинок і для чого він потрібен [Електронний ресурс] / Березень 15, 2023 – Режим доступу: https://alterair.ua/stati/chto-takoe-umnyy-dom/
2. Cathy Gaphty, Physical or Biometrical Security Keys – Which should you choose? [Electronic resource] / February 27, 2023 – Access mode: https://www.criticalpathsecurity.com/physical-or-biometric-security-keys-which-should-you-choose/

ДОСЛІДЖЕННЯ ІНТЕЛЕКТУАЛЬНОГО ЗАХИСТУ ВІД DDOS АТАК КОМП'ЮТЕРНОЇ СИСТЕМИ УПРАВЛІННЯ СЕРВЕРАМИ БАНКУ

Осіпова О. С., Михайленко В. С.

Одеський національний університет імені І. І. Мечникова

Анотація. Об’єктом дослідження виступає захист інтелектуальних даних від DDoS атак комп’ютерної системи управління серверами банку. Аналізуються існуючі методи запобігання DDoS атакам.

Ключові слова: DDoS-атака, інформаційна безпека, комп’ютерна система управління, банківські сервери, інтелектуальні системи захисту, IDS/IPS-системах.

У сучасних умовах цифровізації банківська сфера активно використовує мережеві комп’ютерні системи для управління транзакціями, базами даних та комунікаціями. Однією з ключових загроз для таких систем залишаються DDoS-атаки (Distributed Denial of Service), які можуть паралізувати роботу серверів, створюючи серйозні фінансові та репутаційні втрати. Ефективний захист від цих атак потребує інтелектуальних рішень, здатних виявляти загрози в реальному часі та адаптуватися до нових методів зловмисників [1].

Зусилля компанії Akamai щодо пом’якшення наслідків були висвітлені у звіті, демонструючи їхній успішний захист від найбільших DDoS-атак на своїх клієнтів у Сполучених Штатах, Європі та Азіатсько-Тихоокеанському регіоні, включаючи рекордну атаку без спричинення будь-яких супутніх збитків.

Звіт цієї компанії також проливає світло на те, як DDoS-атаки застосовуються національними державами, зловмисниками, злочинними угрупованнями та хакерами, які часто використовують доступні DDoS-сервіси за наймом, які можна знайти в темній мережі. Він підкреслює важливість надійної політики кібергігієни для організацій для пом'якшення впливу цих атак [2].

Предметна область кібербезпеки в банківських системах охоплює складні механізми захисту інфраструктури, зокрема протидію розподіленим атакам на відмову в обслуговуванні (DDoS). Такі атаки спрямовані на перевантаження серверів великою кількістю запитів з різних джерел, що призводить до збоїв у роботі систем і втрати доступності критично важливих сервісів. Особливу загрозу це становить для банківських комп'ютерних систем управління, де навіть короткочасна недоступність може спричинити суттєві фінансові втрати та підірвати довіру клієнтів.

Сучасні методи захисту від DDoS-атак базуються на традиційних фільтрах, міжмережевих екранах і IDS/IPS-системах, які не завжди здатні ефективно виявляти нові, динамічні типи атак. Крім того, централізовані рішення часто мають обмеження у масштабуванні та реагуванні в реальному часі. Наприклад, деякі хмарні анти-DDoS сервіси надають широкий функціонал, але вимагають передачі даних третім сторонам, що може суперечити вимогам банківської конфіденційності. Інші локальні рішення забезпечують автономність, проте не мають достатньої адаптивності до змінних сценаріїв атак.

Метою даного проєкту є розробка інтелектуальної системи захисту від DDoS-атак для серверів банківської комп'ютерної системи управління, яка поєднує локальну обробку трафіку з використанням методів машинного навчання. Така система дозволяє адаптивно виявляти аномальний трафік, відрізняти легітимну активність від шкідливої, а також забезпечує масштабування без залежності від зовнішніх провайдерів. Локальний підхід знижує ризики витоку конфіденційної інформації, зберігаючи при цьому високу швидкодію та надійність.

Запропоноване рішення передбачає використання класифікаційних моделей, здатних виявляти патерни атак, а також централізоване управління конфігураціями безпеки у межах банківської інфраструктури.

Розробка такої системи є важливим кроком у підвищенні кіберстійкості банківського сектору, оскільки вона не лише враховує сучасні вимоги до безпеки, а й відповідає викликам, пов'язаним з масштабуванням, автономністю та захистом критичних даних. Подальші дослідження можуть бути спрямовані на вдосконалення точності моделей виявлення загроз та розширення функціоналу для роботи з різними типами мережевих інтерфейсів і серверних конфігурацій.

Література

1. The Effects Of DDoS Attacks On Global Infrastructure And How To Respond - Boston Institute Of Analytics. Boston Institute of Analytics. – Access mode: https://bostoninstituteofanalytics.org/blog/the-effects-of-ddos-attacks-on-global-infrastructure-and-how-to-respond/ .
2. DDoS Attacks Against Financial Industry Up By 154% - FinanceFeeds. FinanceFeeds. – Access mode: https://financefeeds.com/ddos-attacks-against-financial-industry-up-by-154/ .

РОЗРОБКА СИСТЕМИ МОНІТОРИНГУ АУДИТОРІЇ

Грекова В. Ф., Камєнєва А. В.

Одеський національний університет імені І. І. Мечникова

У роботі розглядається проєктування та впровадження Smart Classroom Monitoring System — інноваційної цифрової системи моніторингу навчального процесу. Описано її функціональні модулі, такі як керування курсами, адміністрування користувачів, модулі аналітики та звітності. Обґрунтовано важливість використання штучного інтелекту для персоналізації навчання та адаптації освітнього контенту до потреб студентів. Розглянуто переваги системи в контексті дистанційного та змішаного навчання. Підкреслено роль Smart Classroom Monitoring System у підвищенні ефективності, прозорості та якості сучасної освіти.

Ключові слова: Smart Classroom Monitoring System, цифрові технології в освіті, дистанційне навчання, аналітика та звіти, штучний інтелект, персоналізоване навчання, адаптивне навчання, моніторинг активності студентів.

Цифрові технології змінюють усі сфери нашого життя, і освіта не є винятком. В умовах сучасного світу важливість ефективного моніторингу навчального процесу та адаптації освіти до індивідуальних потреб студентів стає дедалі очевиднішою. Зокрема, системи моніторингу в навчальних закладах дозволяють не лише спостерігати за прогресом студентів, а й забезпечувати персоналізований підхід до навчання. Однією з таких інноваційних систем є Smart Classroom Monitoring System (SCMS), що поєднує в собі новітні технології для ефективного управління освітнім процесом, включаючи аналіз даних про активність студентів, автоматизацію звітності та адаптацію контенту під потреби кожного учня. В даній роботі розглядається проектування та впровадження SCMS як інструменту для підвищення ефективності, прозорості та якості сучасної освіти.

Ця система забезпечує постійний моніторинг аудиторної та позаурочної активності студентів, дозволяючи викладачам оперативно реагувати на зниження активності або проблеми в засвоєнні матеріалу. Особливо актуальним є впровадження таких систем у вищих навчальних закладах, де використання

Державний заклад
«ПІВДЕННОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ ПЕДАГОГІЧНИЙ УНІВЕРСИТЕТ імені К. Д. УШИНСЬКОГО»

ОДЕСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ імені І. І. МЕЧНИКОВА

ДВАДЦЯТЬ ДРУГА ВСЕУКРАЇНСЬКА КОНФЕРЕНЦІЯ СТУДЕНТІВ І МОЛОДИХ НАУКОВЦІВ

ІНФОРМАТИКА, ІНФОРМАЦІЙНІ СИСТЕМИ ТА ТЕХНОЛОГІЇ

Збірник робіт

Збірник робіт надрукований в авторській редакції
без внесення суттєвих змін оргкомітетом

Підписано до друку 25.04.2025
Здано у виробництво 25.04.2025
Формат 60x84/16. Папір офсетний. Друк офсетний.
Тираж 50 примірників

Надруковано з готового оригінал-макета