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

вбудований макрос asm!(). Його можна використовувати для вбудовування власного коду асемблера в кінцевий результат компілятора [1, 2].

Для прикладів розглядається операційна система 1981 року розробки – MS-DOS. Для неї не існує стандартної бібліотеки Rust, треба використовувати вставки асемблера для зв'язку з середовищем. Він відбувається через переривання 0x21 (MS-DOS) і через переривання 0x10 (BIOS).

Перед перериванням, в необхідні регістри записується інформація, яку ОС буде використовувати згідно протоколу, наприклад: номер системного виклику, вказівник на рядок та ін.

За допомогою цього, наприклад, можна запустити відомий алгоритм ASCII Donut, що створює динамічну 3D-анімацию (рис.1). Або інший контент, що потребує постійного оновлення.

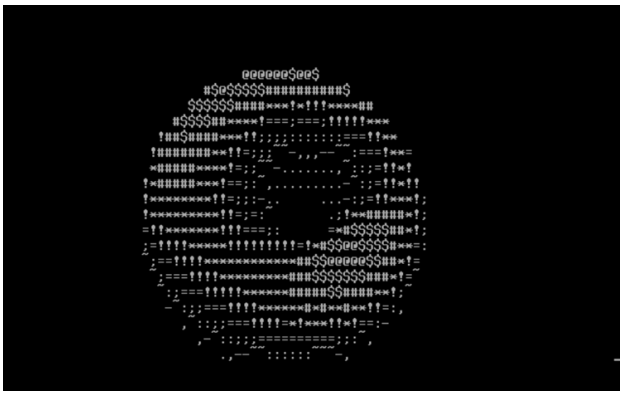

Рис 1.

ВИСНОВКИ. Вибір мови програмування повинен задовольняти багатьом факторам, включаючи цільову платформу, гнучкість мови, підтримку фахівців, попередній досвід із мовою та сучасність мови. Популярність надає можливість використання мов програмування найбільш ймовірними у суспільстві.

Література

1. McNamara Tim. Rust in Action. Shelter Island : Manning Publications, 2021. 456 p.
2. https://doc.rust-lang.org/rust-by-example/unsafe/asm.html (дата звернення 16.04.2025)

СИНТЕЗ ПРОГРАМНО-ТЕХНІЧНОЇ СИСТЕМИ КОНТРОЛЮ ДОСТУПУ ДО ОБЛАДНАННЯ РОЗУМНОГО БУДИНКУ

Шух М. С., Михайленко В. С.
Одеський національний університет імені І. І. Мечникова

Анотація. У роботі розглядається розробка програмно-технічної системи для контролю доступу до обладнання розумного будинку на основі біометричного розпізнавання обличь. Аналізуються сучасні виклики безпеки та необхідність створення гнучких і автономних рішень для розумних будинків.

Ключові слова: розумний будинок, контроль доступу, біометрія, розпізнавання обличь, IoT.

Сучасні розумні будинки стають невід'ємною частиною повсякденного життя, забезпечуючи комфорт, багатофункціональність, енергоефективність і безпеку.[1] Зростання кількості підключених пристроїв і розвиток технологій Інтернету речей (IoT) підвищують вимоги до систем контролю доступу, які мають бути надійними, зручними та адаптивними. Традиційні механічні та електронні замки, хоча й залишаються поширеними, не відповідають сучасним викликам через вразливість до компрометації та обмежену інтеграцію з автоматизованими системами. Біометричні системи, зокрема ті, що базуються на розпізнаванні обличь, відкривають нові можливості для підвищення безпеки, усуваючи потребу в фізичних ключах чи паролях, які легко втрачаються чи передаються [2]. Однак комерційні рішення, таки як Lockly Visage Zeno Series чи August Smart Lock, часто залежать від хмарних сервісів і мають проблеми з масштабуванням у межах одного будинку, що ускладнює їхнє використання в складних побутових сценаріях.

Предметна область розумних будинків охоплює широкий спектр технологій, включаючи IoT, комп'ютерний зір і штучний інтелект. Контроль доступу в такій системі передбачає ідентифікацію користувачів, перевірку їхніх прав і надання доступу до фізичних чи логічних ресурсів. Основними викликами є забезпечення безпеки даних, стійкість до зовнішніх умов (наприклад, зміни освітлення для камер) і гнучкість управління кількома точками доступу. Існуючі рішення, такі як Lockly Visage Zeno Series мають високу ціну та проблемами з масштабуванням, а August Smart Lock, своєю чергою, пропонує інтеграцію з IoT-платформами, просте налаштування але не завжди підтримує біометрію як основний метод. Ці обмеження підкреслюють необхідність розробки автономних систем, які поєднують локальну обробку даних із можливістю масштабування.

Метою даного проєкту є синтез програмно-технічної системи контролю доступу, яка забезпечує біометричне розпізнавання обличь для управління обладнанням розумного будинку. Така мета є необхідною через зростаючу потребу в безпечних і економічних рішеннях, які можуть працювати незалежно від хмарних сервісів і підтримувати кілька точок доступу в одному будинку. Запропонована система вирішує цю проблему, використовуючи локальну обробку даних для підвищення безпеки та централізоване управління для спрощення масштабування. На відміну від комерційних продуктів, вона не потребує постійного підключення до мережі й дозволяє гнучко додавати нові пристрої без значних витрат. Це робить її перспективною альтернативою для побутового використання, де важливі автономність і доступність.

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.

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