

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. Ніщук

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

© Навчально-науковий інститут природничо-математичних наук, інформатики та менеджменту Державного закладу «Південноукраїнський національний педагогічний університет імені К. Д. Ушинського», кафедра прикладної математики та інформатики, 2025

© Факультет математики, фізики та інформаційних технологій Одеського національного університету імені І. І. Мечникова, кафедра математичного забезпечення комп'ютерних систем, 2025

АНАЛІЗ НЕЙРОМЕРЕЖЕВИХ МОДЕЛЕЙ ДЛЯ ЗАВДАНЬ ПРОГНОЗУВАННЯ ТРЕНДІВ ТА ФОНДОВИХ РИНКАХ	95
Лобко Г. Ю., Шпінарева І. М., Шведов Д. С.	95
ПРОЕКТ НЕЙРОМЕРЕЖЕВОЇ СИСТЕМИ ПРОГНОЗУВАННЯ ЦІН НА ФОНДОВОМУ РИНКУ	97
Лобко Г. Ю., Шпінарева І. М., Шведов Д. С.	97
АНАЛІЗ ПРОБЛЕМАТИКИ АВТОМАТИЗАЦІЇ ОБЛІКУ ДАНИХ У МОРСЬКИХ ПОРТАХ	99
Мкртичян А. А., Вичужанін В. В.	99
ПРОЕКТ ІНТЕРФЕЙСУ ПРОГРАМНОГО ЗАСТОСУВАННЯ АВТОМАТИЗАЦІЇ ОБЛІКУ ДАНИХ ДИСПЕТЧЕРСЬКОЇ СЛУЖБИ ПОРТУ	101
Мкртичян А. А., Вичужанін В. В.	101
АКТУАЛЬНІСТЬ ТА ОСОБЛИВОСТІ ЗАСТОСУВАННЯ ІНТЕЛЕКТУАЛЬНОЇ АНАЛІТИКИ ДЛЯ ПРИЙНЯТТЯ РІШЕНЬ.....	103
Огородюк Р. В., Рудніченко М. Д., Шведов Д. С.	103
РОЗРОБКА КОНЦЕПЦІЇ ІНТЕЛЕКТУАЛЬНОЇ СИСТЕМИ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ ДЛЯ ВИБОРУ АЛЬТЕРНАТИВ В НАСТІЛЬНО-РОЛЬОВИХ ІГРАХ.....	105
Отращенко А. А., Рудніченко М. Д., Шведов Д. В.	105
МОЖЛИВОСТІ ГЕЙМІФІКАЦІЇ ОБ'ЄКТІВ НА БАЗІ UNREAL ENGINE ДЛЯ ЗАВДАНЬ ТЕСТУВАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ.....	108
Плаксін В. С., Гришин С. І.	108
РОЗРОБКА ПРОТОТИПІВ АКТИВНОСТЕЙ ПРОГРАМНОГО ЗАСТОСУВАННЯ ТЕСТУВАННЯ ГЕЙМІФІКОВАНИХ ОБ'ЄКТІВ.....	110
Плаксін В. С., Гришин С. І.	110
АНАЛІЗ ШЛЯХІВ ТА ТЕХНІЧНИХ ЗАСОБІВ РОЗРОБКИ КОРПОРАТИВНИХ СОЦІАЛЬНИХ МЕРЕЖ	112
Полунєєв К. А., Кунуп Т. В.	112
РОЗРОБКА ДІАГРАМИ ВАРІАНТІВ ВИКОРИСТАННЯ КОРПОРАТИВНОЇ СОЦІАЛЬНОЇ МЕРЕЖІ ДЛЯ КОМУНІКАЦІЇ ТА ОБМІНУ ДАНИМИ СПІВРОБІТНИКІВ	114
Полунєєв К. А., Кунуп Т. В., Потієнко О. С.	114
ОГЛЯД ТЕХНОЛОГІЙ РОЗРОБКИ ВЕБ-ОРІЄНТОВАНИХ РЕКОМЕНДАЦІЙНИХ ПЛАТФОРМ.....	116
Привалов А. Г., Рудніченко М. Д.	116
АКТУАЛЬНІСТЬ ЗАСТОСУВАННЯ ГРАФОВИХ СТРУКТУР ДАНИХ У ЗАДАЧАХ ПОБУДОВИ ПЕРСОНАЛІЗОВАНИХ РЕКОМЕНДАЦІЙ	118
Ропай А. Р., Рудніченко М. Д.	118
АНАЛІЗ АЛГОРИТМІВ ОЦІНКИ РИЗИКІВ ЗДОРОВ'Ю НАСЕЛЕННЯ ВІД АНТРОПОГЕННИХ ФАКТОРІВ.....	120
Рудницький М. І., Шпінарева І. М., Отрадська Т. В.	120

підбирати ресурси, уникати перевантаження інформацією та підтримувати баланс між онлайн-навчанням і традиційними методами викладання.

Література

1. Веселовська Г. В. Комп'ютерна графіка: Навчальний посібник для вузів.— Херсон: ОЛДІ-плюс, 2004. — 582 с
2. Маренкокра Т.В., Зуноваре О.С. Використання Інтернету та електронних освітніх ресурсів у навчальному процесі вищих навчальних закладів. *Вісник Дніпропетровського університету імені Альфреда Нобеля*. 2016. № 1 (11). С.251-255
3. Шаповалова Н.О. Використання комп'ютерних мереж у навчальному процесі [Електронний ресурс] / Н.О. Шаповалова. – Режим доступу: <http://schoolcollection.edu.ru/about/filling/textbook/>

ВИКОРИСТАННЯ АПАРАТНОГО ШИФРУВАННЯ ДЛЯ ЗАХИСТУ ІНФОРМАЦІЇ В СИСТЕМАХ ІОТ

Ісаєв О. М., Ларін Д. Г.

Одеський національний університет імені І.І. Мечникова

У роботі проведено аналіз вразливостей систем IoT та запропоновано підхід до захисту інформації з використанням апаратного шифрування, зокрема через вбудовані або окремі криптографічні модулі, як ефективний спосіб забезпечення безпеки IoT-пристроїв.

Ключові слова: Інтернет речей (IoT), захист інформації, апаратне шифрування, криптографічні модулі, кібербезпека, АТЕСС608А, Secure Elements.

Сучасний світ неможливо уявити без Інтернету речей (IoT), який об'єднує велику кількість пристроїв – від розумних датчиків у будинках до систем моніторингу в розумних містах. За даними Statista, у 2025 році кількість підключених IoT-пристроїв перевищить 30 мільярдів, що підкреслює стрімкий розвиток цієї технології[1]. IoT підвищує ефективність, комфорт і автоматизацію в таких сферах, як медицина, промисловість і транспорт. Проте зростання популярності IoT супроводжується збільшенням кіберзагроз, що робить захист інформації критично важливим завданням.

Предметна область IoT охоплює широкий спектр технологій, включаючи протоколи передачі даних (MQTT, CoAP, LoRaWAN, Zigbee, BLE) та методи забезпечення безпеки. IoT-пристрої вразливі через обмежені обчислювальні ресурси, використання незахищених мереж і слабкі механізми захисту. За даними Symantec, у 2023 році кількість атак на IoT зросла на 35%, включаючи атаки типу "людина посередині" (MITM), DDoS через ботнети та перехоплення даних через дефолтні паролі [2]. Такі атаки можуть призвести до витоку конфіденційних даних,

порушення роботи критичної інфраструктури чи загрози життю, наприклад, у медичних системах.

Одним із наймасштабніших прикладів кібератак на IoT-системи стала атака Mirai у 2016 році, коли зловмисники використали IoT-пристрої, такі як розумні камери та роутери, для створення ботнету. Ключовим фактором вразливості стали стандартні паролі від виробника, наприклад, "admin/admin", які користувачі часто не змінюють, що дозволило зловмисникам легко заразити понад 600 000 пристроїв шкідливим ПЗ. Принцип атаки (див. рис. 1), полягав у тому, що скомпрометовані пристрої об'єднувалися в ботнет і масово надсилали запити до серверів, викликаючи DDoS-атаку (Distributed Denial of Service).

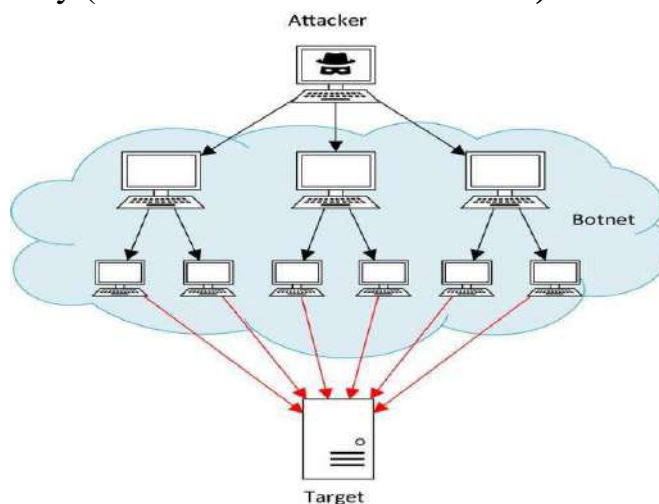


Рисунок 1 – Принцип DDoS атаки з використанням ботнету

Захист інформації в IoT потребує комплексного підходу, який включає шифрування, автентифікацію та ізоляцію ключів. Проте програмні методи, такі як TLS, часто неефективні для слабких пристроїв через високі вимоги до ресурсів. Саме тому апаратне шифрування є перспективним рішенням, оскільки воно забезпечує швидке виконання криптографічних операцій і захист ключів від фізичного доступу.

Найдешевшим варіантом для забезпечення безпеки є вбудовані криптографічні блоки в мікроконтролерах, таких як ESP32, які підтримують AES-128, але не забезпечують ізоляцію ключів. Більш ефективні – окремі модулі, наприклад, АТЕСС608А від Microchip, який підтримує AES-128, ECDSA і ECDH, а також ізоляцію ключів, що ідеально для IoT-пристроїв, таких як розумні замки чи медичні датчики [3].

Таким чином, апаратне шифрування дозволяє ефективно вирішувати проблеми безпеки в IoT, забезпечуючи захист даних і стійкість до атак. Використання модулів, таких як АТЕСС608А, є оптимальним для слабких пристроїв, підвищуючи безпеку без значних витрат ресурсів.

Література

1. Statista. Number of IoT devices worldwide 2015-2025. [Електронний ресурс] – Режим доступу до ресурсу: <https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/>;
2. Symantec. Internet Security Threat Report. [Електронний ресурс] – Режим доступу до ресурсу: <https://www.symantec.com/security-center/threat-report>;
3. Microchip. ATECC608A Datasheet. [Електронний ресурс] – Режим доступу до ресурсу: <https://www.microchip.com/wwwproducts/en/ATECC608A>.

СИНТЕЗ ТРІЙКОВИХ ЛОГІЧНИХ ЕЛЕМЕНТІВ НА КМДН-ТРАНЗИСТОРАХ

Кивиржік В. А., Мартинович Л. Я.

Одеський національний університет імені І. І. Мечникова

Анотація: робота присвячена принципам синтезу трійкових логічних пристроїв на основі комплементарних метал-діелектрик-напівпровідник (КМДН) транзисторів. Розглянуто вимоги до елементної бази та методику синтезу логічних схем.

Ключові слова: трійкова логіка, КМДН-транзистор, порогова напруга, логічний синтез, базовий компонент.

Дослідження трійкової логіки є актуальним напрямком у пошуку альтернатив бінарним обчислювальним системам. Історичний досвід та теоретичні оцінки вказують на потенційне зменшення кількості апаратних засобів та/або підвищення продуктивності при переході до трійкової системи числення для певних задач [1].

Запропоновано реалізацію трьох логічних станів (-1, 0, +1) за допомогою трьох рівнів напруги: негативної ($-U_{ee}$), нульової (GRD) та позитивної ($+U_{dd}$) відносно двополярного джерела живлення. КМДН-транзистори використовуються як керовані ключі для комутації відповідного рівня напруги на вихід логічного елемента, як це схематично показано на Рис. 1. Використання комплементарних пар n- та p-канальних транзисторів дозволяє зберегти ключові переваги КМДН-технології: високу швидкодію перемикавання та практично нульове статичне енергоспоживання [2].

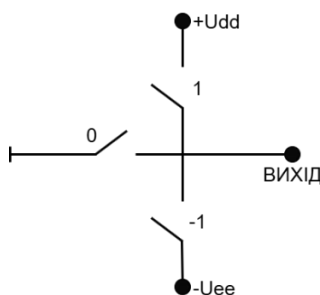


Рис. 1 – Схема вихідної частини трирівневих структур

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