НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ПОЛТАВСЬКА ПОЛІТЕХНІКА
ІМЕНІ ЮРІЯ КОНДРАТЮКА

ЗБІРНИК МАТЕРІАЛІВ

77-Ї НАУКОВОЇ КОНФЕРЕНЦІЇ ПРОФЕСОРІВ, ВИКЛАДАЧІВ, НАУКОВИХ ПРАЦІВНИКІВ, АСПІРАНТІВ ТА СТУДЕНТІВ УНІВЕРСИТЕТУ

16 травня – 22 травня 2025 р.

УДК 621.396:004.056

А.М. Капітон, професор
О.С. Дзюбан, аспірант
Р.М. Талибов, аспірант
Національний університет
«Полтавська політехніка імені Юрія Кондратюка»

ПОТЕНЦІАЛ 5G ТЕХНОЛОГІЙ ТА ВИКЛИКИ КІБЕРБЕЗПЕКИ

Технологія п’ятого покоління мобільного зв’язку, відома як 5G, відкриває нові горизонти у сфері телекомунікацій, забезпечуючи надвисокі швидкості передачі даних, мінімальну затримку та можливість підключення величезної кількості пристроїв. Ці інновації створюють безліч перспектив для різних галузей, але водночас породжують нові виклики для забезпечення інформаційної безпеки.5G забезпечує швидкість передачі даних до 20 Гбіт/с, що значно перевищує можливості 4G. Завдяки цьому відкриваються нові перспективи для віртуальної та доповненої реальності, Інтернету речей (IoT), автономного транспорту, розумних міст і хмарних сервісів. Проте повне глобальне розгортання 5G ще не завершено, а деякі країни уже досліджують технології 6G.

Однією з ключових переваг 5G є підтримка масового підключення пристроїв, що сприяє розвитку розумних екосистем, наприклад, у сферах дистанційної медицини, автоматизації промислових процесів і міського планування. Крім того, 5G сприяє розвитку периферійних і хмарних обчислень, що забезпечує гнучкість у обробці великих обсягів даних. Технологічні переваги 5G ускладнюють захист інформації. Велика кількість підключених пристроїв розширює поверхню для потенційних атак, роблячи системи вразливими до кіберзагроз. Зростаюча залежність від хмарних сервісів і периферійних обчислень вимагає посилених заходів для захисту даних у розподілених мережах.

З одного боку, 5G пропонує нові інструменти для підвищення безпеки. Наприклад, технологія сегментації мережі (network slicing) дозволяє створювати ізольовані віртуальні мережі з індивідуальними налаштуваннями безпеки. Покращені протоколи шифрування також сприяють захисту даних. Проте високі швидкості передачі можуть використовуватися для потужних атак типу DDoS, які перевантажують системи та порушують їхню роботу. Крім того, залежність від програмно-визначених мереж створює ризики, якщо в програмному забезпеченні є неусунуті вразливості.

Для реалізації потенціалу 5G і мінімізації ризиків необхідний комплексний підхід. Співпраця між урядами, операторами зв’язку, розробниками технологій і науковцями є критично важливою для створення надійних стандартів безпеки. Постійні дослідження в галузі

шифрування, виявлення кібератак і управління вразливостями допоможуть випереджати нові загрози. Особливістю 5G є широке використання віртуалізації, де ключову роль відіграють програмні рішення, а не лише апаратні інновації. Це дозволяє адаптувати мережу до потреб різних користувачів – від індивідуальних гаджетів до промислових комплексів із високим навантаженням. Такий підхід докорінно змінює концепцію мереж, створюючи нові бізнес-моделі та сприяючи інноваціям у виробництві, сервісах і взаємодії між пристроями.

5G – це технологія, яка відкриває двері до інновацій, але вимагає пильної уваги до питань кібербезпеки. Її можливості для трансформації суспільства величезні, але без належного захисту даних і мереж ці перспективи можуть бути затьмарені ризиками. Спільні зусилля у створенні безпечної інфраструктури дозволять 5G стати основою для процвітаючого цифрового майбутнього.

Література

1. Швачко В. П. Кібербезпека в інформаційних системах: сучасні виклики: монографія. – Львів: Видавництво Львівської політехніки, 2021. – 260 с.

2. Грицик В. В. Захист інформації в телекомунікаційних системах: монографія. – Київ: НТУУ "КПІ", 2019. – 320 с.

3. Сидоренко О. М. Сучасні загрози кібербезпеці в телекомунікаційних мережах: монографія. – Одеса: ОНУ імені І. І. Мечникова, 2023. – 220 с.

УДК 004.9

В.В. Васюта, к.т.н, доцент
В.К. Шевченко, студент групи 401-ТК
Національний університет
«Полтавська політехніка імені Юрія Кондратюка»

РОЗРОБКА ПРОГРАМНО-АПАРАТНОГО ЗАБЕЗПЕЧЕННЯ УПРАВЛІННЯ 3D-ПРИНТЕРОМ НА БАЗІ МІКРОКОНТРОЛЕРА ARDUINO

У сучасних умовах розвитку цифрових технологій та автоматизованих систем особливу увагу привертає галузь адитивного виробництва, зокрема тривимірного друку. 3D-принтери дедалі ширше застосовуються в прототипуванні, промисловості, медицині, освіті та побуті. Навколо цих пристроїв сформувалося велике коло виробників, вони пропонують пристрої для різних потреб і обмежень по бюджету. Постійно розвивається вбудоване програмне забезпечення для принтерів, що забезпечує