© Kostiuk Y., Bebeshko B., Hulak H., Skladannyi P., Rzaeva S., Khorolska K. Ensuring cyber security and high data transmission speed in wireless networks // Ukrainian Scientific Journal of Information Security, 2024, vol. 30, issue 3, pp. 365-375. ©

DOI: 10.18372/2225-5036.30.20357

ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ТА ШВИДКОДІЇ ПЕРЕДАЧІ ДАНИХ У БЕЗПРОВІДНИХ МЕРЕЖАХ

Юлія Костюк, Богдан Бебешко, Геннадій Гулак, Павло Складанний, Світлана Рзаєва, Карина Хорольська

Київський столичний університет імені Бориса Грінченка

КОСТЮК Юлія Володимирівна, Phd in Computer Science
Рік та місце народження: 1980 рік, м. Київ, Україна
Освіта: Державний торговельно-економічний університет.
Посада: доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Наукові інтереси: захист інформації, комп'ютерні мережі, інформаційно-комунікаційні системи, інформаційно-інтелектуальні системи, нейронні мережі.
Публікації: більше 30 наукових публікацій, серед яких монографія, посібник, наукові статті та тези, матеріали доповідей на конференціях.
E-mail: y.kostiuk@kubg.edu.ua
Orcid ID: 0000-0001-5423-0985.

БЕБЕШКО Богдан Тарасович, Phd in Computer Science
Рік та місце народження: 1992 рік, м. Київ, Україна
Освіта: Київський національний торговельно-економічний університет.
Посада: доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка.
Наукові інтереси: game development, front-end development, back-end development, нейронні мережі, цифрові валюти.
Публікації: більше 25 наукових публікацій, серед яких наукові статті та тези, матеріали доповідей на конференціях.
E-mail: b.bebeshko@kubg.edu.ua
Orcid ID: 0000-0001-6599-0808.

ГУЛАК Геннадій Миколайович, доктор технічних наук, професор
Рік та місце народження: 1955 рік, м. Київ, Україна
Освіта: ВШ КДБ.
Посада: професор кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Наукові інтереси: комп'ютерні мережі, інформаційно-інтелектуальні системи, хмарні технології, кібербезпека.
Публікації: більше 100 наукових публікацій, серед яких монографії, підручники, посібники, наукові статті та тези, матеріали доповідей на конференціях.
E-mail: hulak@kubg.edu.ua
Orcid ID: 0000-0001-9131-9233.

СКЛАДАННИЙ Павло Миколайович, кандидат технічних наук, доцент,
Рік та місце народження: 1992 рік, м. Київ, Україна
Освіта: Державний університет телекомунікацій.
Посада: завідувач кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Наукові інтереси: кібербезпека, криптографія, криптоаналіз, математичне моделювання.
Публікації: більше 100 наукових публікацій, серед яких монографії, підручники, посібники, наукові статті та тези, матеріали доповідей на конференціях.
E-mail: p.skladannyi@kubg.edu.ua
Orcid ID: 0000-0002-7775-6039.

РЗАЄВА Світлана Леонідівна, кандидат технічних наук, доцент
Освіта: Севастопольський приладобудівний інститут.
Рік та місце народження: 1968 рік, м. Київ, Україна
Посада: доцент кафедри кафедри комп'ютерних наук
Наукові інтереси: адміністрування і захист баз даних та сховищ даних, моделювання програмного забезпечення та його аналіз, інформаційні технології та системи
Публікації: більше 100 наукових публікацій, серед яких монографії, підручники, посібники, наукові статті та тези, матеріали доповідей на конференціях.
E-mail: s.rzaieva@kubg.edu.ua
Orcid ID: 0000-0002-7589-2045.

ХОРОЛЬСЬКА Карина Вікторівна, Phd in Computer Science
Рік та місце народження: 1996 рік м. Світловодськ, Україна
Освіта: Державний торговельно-економічний університет.
Посада: доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка.
Наукові інтереси: інформаційні технології, front-end development, back-end development, нейронні мережі, 3D моделювання.
Публікації: більше 30 наукових публікацій, серед яких наукові статті та тези, матеріали доповідей на конференціях.
E-mail: karynakhorolska@gmail.com
Orcid ID: 0000-0003-3270-4494.

© Kostiuk Y., Bebeshko B., Hulak H., Skladannyi P., Rzaeva S., Khorolska K. Ensuring cyber security and high data transmission speed in wireless networks // Ukrainian Scientific Journal of Information Security, 2024, vol. 30, issue 3, pp. 365-375. ©

Анотація. *У роботі досліджується проблема забезпечення балансу між безпекою та швидкодією передачі даних у безпровідних комунікаціях, зокрема в контексті технології Bluetooth. Актуальність теми зумовлена зростаючими вимогами до швидкості та надійності передачі відеопотоків, що стає критично важливим в умовах розвитку сучасних інформаційно-комунікаційних систем. Аналізуються технічні особливості Bluetooth, зокрема стандарт IEEE 802.15.1, який забезпечує енергоефективну передачу даних на короткі відстані. Актуальність теми зумовлена зростаючими вимогами до швидкості та надійності передачі відеопотоків, що стає критично важливим в умовах розвитку сучасних інформаційно-комунікаційних систем. Аналізуються технічні особливості Bluetooth, зокрема стандарт IEEE 802.15.1, який забезпечує енергоефективну передачу даних на короткі відстані. Розглядаються основні характеристики Bluetooth, включаючи зіркову мережеву топологію, діапазон частот, методи модуляції та потужність сигналу, що впливають на продуктивність передачі даних. Особливу увагу приділено адаптивній модуляції та методам буферизації, які дозволяють покращити якість передачі в умовах радіочастотних завад та перешкод. Також аналізуються механізми захисту даних, які можуть бути інтегровані в безпровідні мережі, з метою запобігання загрозам безпеки, таких як несанкціонований доступ та перехоплення інформації. Запропоновані рішення враховують особливості Bluetooth Low Energy (BLE), що робить їх особливо ефективними для IoT-аплікацій. Висновки роботи підкреслюють важливість комплексного підходу до управління ресурсами в безпровідних комунікаціях, який дозволяє забезпечити стабільну, безпечну та продуктивну роботу інформаційних систем, зокрема в умовах постійно змінюваного середовища загроз.*

Ключові слова: *захист, ефективність, адаптивна модуляція, буферизація, відеопотік, безпровідна передача даних, однопотоковий відеоконтент, безпровідні мережі, Bluetooth, безпека, швидкодія, оптимізація, продуктивність, взаємозв'язок.*

Постановка проблеми

Сучасний розвиток кібербезпеки та інформаційного захисту набуває значного значення через зростання загроз і вразливостей, які виникають внаслідок швидкого технологічного прогресу. Для забезпечення надійного захисту інформації організації застосовують широкий спектр заходів, зокрема сучасні методи шифрування, системи виявлення вторгнень та навчання персоналу, а також впроваджують політику кібербезпеки. Важливим елементом стратегії захисту є постійний моніторинг нових загроз і регулярне оновлення засобів в умовах захисту сучасного цифрового середовища.

У сучасних умовах забезпечення безпеки передачі відеопотоку через Bluetooth вимагає всебічного підходу, що охоплює не тільки питання конфіденційності, але й підтримку цілісності та доступності даних. При цьому під доступністю мати можливість безперешкодного та ненавмисного доступу до відеоінформації. Наразі для підтримки доступності застосовуються різні фізичні методи, такі як дублювання й резервне копіювання даних і обладнання, однак криптографічні методи захисту часто спрямовані на забезпечення цілісності, не гарантуючи при цьому доступність інформації. Таким чином, розробка методів забезпечення доступності відеоінформації під час її передачі в мережах, зокрема на основі візуальної криптографії та мультиплексування трафіку, є актуальною проблемою безпеки.

Технологія Bluetooth, стандартизована як IEEE 802.15.1, залишається інструментом для радіочастотного зв'язку на короткій відстані. обмеження щодо передачі трафіку через головний вузол, використання Bluetooth за допомогою низьких широких вимог до енергоспоживання та обладнання, відповідно до Wi-Fi. Bluetooth підтримує різні рівні шкоди модуляції захисту й даних, забезпечуючи стійкість до передачі, що особливо важливо в системах із застосуванням OFDM (Orthogonal Frequency Division Multiplexing). Тому при розробці буферної політики пріоритету для захисту інформації та користувачів у відеопотоці через Bluetooth, слід враховувати технічні характеристики та специфіку. Використання адаптивної модуляції разом із тризонним буфером сприяє оптимізації передачі даних, забезпечуючи швидкість, надійність зв'язку та захист від несанкціонованого доступу до відеоданих.

Зростаюча потреба в швидкій та надійній передачі даних у безпровідних комунікаціях, зокрема через технології, такі як Bluetooth, ставить перед розробниками та дослідниками низку викликів. По-перше, необхідно досягти балансу між безпекою та продуктивністю передачі даних, оскільки зростання швидкості передачі часто супроводжується збільшенням ризиків несанкціонованого доступу та втрати даних. По-друге, на якість передачі впливають численні зовнішні фактори, такі як радіочастотний шум, перешкоди та обмеження потужності сигналу, що потребує розробки нових методів буферизації та адаптивної модуляції для покращення продуктивності. По-третє, існує необхідність інтеграції ефективних механізмів захисту, які зможуть протистояти сучасним загрозам безпеки, зокрема у контексті IoT-аплікацій, де бездротові пристрої часто є вразливими до атак.

Таким чином, проблема полягає у пошуку оптимальних рішень, які б забезпечували одночасно високий рівень безпеки та ефективність передачі

інформації в умовах зростаючих вимог до безпровідних комунікацій. Забезпечення безпеки в бездротових комунікаціях є критично важливим, особливо з урахуванням поширення радіочастотних технологій, таких як Bluetooth. Ускладнення комунікаційних систем та збільшення обсягів даних створюють нові виклики щодо підтримки конфіденційності та цілісності інформації.

Розширення кількості «розумних» пристроїв, які широко використовують бездротові технології, підвищує потребу в ефективних заходах захисту. Особливо це стосується пристроїв, які використовують Bluetooth для передачі відеопотоків, що підвищує ризики перехоплення та несанкціонованого доступу до даних. Сучасні дослідження підтверджують, що нові загрози безпеці, включаючи атаки на Bluetooth, можуть використовувати вразливості протоколів для перехоплення або маніпуляцій із даними [1-6, 9-10, 12-16, 20-23].

Для захисту відеопотоків через Bluetooth необхідно впроваджувати ефективні методи шифрування та автентифікації [1, 7-9]. Зі зростанням кількості бездротових пристроїв та ускладненням систем, постійне вдосконалення методів захисту є необхідним. Встановлення тризонного буфера для управління передачею даних може покращити ефективність і безпеку передачі великих обсягів інформації через бездротові мережі. Разом із новими технологіями атак на безпеку важливо розробляти вдосконалені заходи захисту [6-10].

Додатково, зростаюча роль штучного інтелекту та машинного навчання в аналізі загроз та аномалій в мережевому трафіку може стати ключовим фактором у підвищенні рівня безпеки. Використання цих технологій може допомогти в розпізнаванні нових загроз у реальному часі та автоматизації процесів реагування на інциденти. Однак, інтеграція таких рішень також потребує врахування питань конфіденційності, оскільки обробка великої кількості даних може відкривати нові вектори атак.

Загалом, дослідження в цій сфері повинні зосередитися на комплексному підході до забезпечення безпеки, включаючи як технологічні, так і організаційні аспекти, для успішного протистояння сучасним загрозам безпеці в бездротових комунікаціях.

Аналіз останніх досліджень і публікацій

Останні дослідження в галузі безпровідних комунікацій демонструють зростаючу увагу до балансу між безпекою та продуктивністю передачі даних, особливо в контексті технології Bluetooth. Швидкість та надійність передачі відеопотоків стає критично важливою з розвитком IoT-аплікацій. При збільшенні швидкості передачі даних ризики, пов’язані з несанкціонованим доступом та перехопленням інформації, також зростають. Це підкреслюється в численних статтях [1-6, 9-10], які зазначають нові методи атаки, зокрема зловживання вразливостями протоколів Bluetooth. У публікаціях, присвячених адаптивній модуляції та буферизації, акцентується на необхідності розробки нових алгоритмів, що покращують якість передачі в умовах радіочастотних завад [7-9]. Важливим аспектом є також впровадження ефективних механізмів шифрування та автентифікації для захисту відеопотоків, як зазначено в [1, 18, 20-23]. Деякі дослідження фокусуються на інтеграції методів захисту, що враховують специфіку Bluetooth Low Energy (BLE), що є критично важливим для забезпечення безпеки в контексті IoT [10-16, 18-23].

Це підкреслює необхідність комплексного підходу до управління ресурсами в безпровідних мережах, включаючи технічні рішення та управлінські стратегії. Серед науковців, які займалися цими питаннями, можна відзначити Alireza Khosravi, який досліджує вразливості в протоколах Bluetooth, Yun Zhang, який фокусується на адаптивних методах модуляції, а також Alfredo Garcia, що вивчає механізми захисту в IoT-аплікаціях. Також варто згадати Mohammad Ali Hamade, який розробляє нові алгоритми для покращення якості передачі даних, та Hesham ElSayed, який досліджує інтеграцію технологій BLE в системи IoT. Jens Zander аналізує питання управління ресурсами в безпровідних мережах.

Таким чином, аналіз сучасних публікацій демонструє, що забезпечення балансу між безпекою та продуктивністю передачі даних у безпровідних комунікаціях є актуальною та складною задачею, що потребує подальших досліджень і розробок.

Мета та постановка завдання

Метою дослідження є систематичний аналіз та оптимізація механізмів, що забезпечують баланс між безпекою та продуктивністю передачі даних у безпровідних комунікаціях. У сучасних умовах, коли стрімко зростають вимоги до швидкості та надійності передачі даних, особливо в контексті технологій Інтернету речей (IoT), важливо враховувати множину факторів, що впливають на якість зв'язку. Це включає радіочастотний шум, перешкоди в середовищі передачі та варіації потужності сигналу. Дослідження також передбачає розробку та впровадження ефективних методів буферизації та адаптивної модуляції, які можуть суттєво покращити продуктивність безпровідних мереж. Особливу увагу приділено інтеграції сучасних механізмів захисту даних, здатних протидіяти актуальним загрозам безпеки, таким як зловмисне прослуховування та атаки на конфіденційність даних.

Зокрема, розглядаються технології, що базуються на протоколах Bluetooth Low Energy (BLE), які забезпечують енергоефективність та надійність у передачі даних між мобільними пристроями. У ході дослідження формуються рекомендації щодо управління ресурсами в безпровідних комунікаціях, що сприяють досягненню стабільної та безпечної

роботи інформаційних систем. Таким чином, результати дослідження мають на меті не лише підвищення продуктивності передачі даних, але й забезпечення високого рівня безпеки, що є критично важливим в умовах сучасної цифрової економіки.

Виклад основного матеріалу дослідження

Багаторівнева Сучасні версії Bluetooth, такі як 5.2 і 5.3, пропонують підвищену швидкість передачі даних та покращену стабільність, що робить Bluetooth більш привабливим для передачі великих обсягів даних, включаючи відео. Проте це створює нові виклики в галузі кібербезпеки, оскільки швидкісна передача даних може використовуватися для атак зловмисників. Тому дослідники активно працюють над покращенням захисту пристроїв, що використовують Bluetooth, від можливих кіберзагроз [5-9, 17-19].

Політика пріоритету для тризонного буфера забезпечує гнучке керування передачею пакетів, знижуючи ризики переповнення буфера. Зміна швидкості передачі залежно від заповнення буфера дозволяє зберегти стабільність передачі даних та забезпечити їхній захист. Межі буферної зони визначаються на основі частоти появи I-, P- та B-кадрів у відеопотоці та динамічно змінюються залежно від співвідношення розмірів пакетів цих типів кадрів. Іншими словами, розподіл даних для кожного типу кадру у вхідному відеопотоці визначає розміри зон, а сам тип кадру впливає на політику захисту в межах кожної зони. Першою зону займають пакети, що надходять. У зоні 1 не всі пакети B-кадрів отримують захист, а в зонах 2 і 3 пакети B-кадрів залишаються незахищеними. Оскільки лише в зоні 1 B-кадри мають певний захист, розмір цієї зони має відповідати кількості даних у пакетах B-кадрів. Інакше це призведе до невідповідності розміру зони потребам кадрів B. Концепція GOP (Group of Pictures), яка використовується в стандартах відеокодування, таких як MPEG та H.264, служить для організації послідовності кадрів у відеопотоці та визначає структуру відео за допомогою різних типів кадрів: I-кадри (Intra-coded frames) — повністю незалежні кадри, що містять усю інформацію про зображення і не залежать від інших кадрів; P-кадри (Predicted frames) — використовують попередні I- або P-кадри для зменшення обсягу даних шляхом предиктивного кодування; і B-кадри (Bidirectional predicted frames) — кодуються на основі як попередніх, так і наступних кадрів, що дозволяє досягти ще більшого стиснення. Структура GOP визначає частоту використання I-, P- та B-кадрів у потоці, що впливає на якість, стиснення та ефективність обробки відео. Варто зазначити, що через структуру GOP (Group of Pictures) B-кадри зустрічаються частіше за інші типи кадрів. У зоні 2 не всі пакети P-кадрів мають захист, і в зоні 3 захист для них також не передбачений. Розмір зони 2 визначає, з якою швидкістю пакети P-кадрів втрачають захист після зони 1. Це регулюється кількістю P-кадрів у потоці, щоб уникнути невідповідності розміру зони для цих кадрів. У зоні 3, у разі її заповнення, буфер переповнюється, що призводить до втрати захисту пакетів I-кадрів.

Для моніторингу заповнення буфера передавача використовується адаптивна схема підвищення рівня сигналу через інтерфейс контролера хост-контролера Bluetooth. Заповненість буфера є показником перевантаження в Bluetooth-піконеті, оскільки реагує на перевантаження не лише відеопотоку, але й при збільшенні часу обробки в умовах перехресного трафіку. Заповненість буфера дозволяє регулювати схему UP (User Priority), яка визначає пріоритети відеопотоків для забезпечення належної якості обслуговування та запобігання загрозам безпеці.

У сучасних безпровідних комунікаційних системах, таких як Bluetooth, важливо враховувати стан каналу, що можна оцінити за допомогою індикатора рівня сигналу (RSSI) або повідомлень про стан каналу. RSSI (Received Signal Strength Indicator) — це індикатор рівня прийнятого сигналу, що використовується для визначення сили сигналу, який надходить на пристрій. Значення RSSI зазвичай вимірюється в децибелах міліват (dBm) і дозволяє оцінити, наскільки сильним є сигнал у конкретний момент часу. RSSI виконує кілька важливих функцій у процесі оцінки стану каналу. По-перше, він є корисним інструментом для оцінки якості з'єднання: високі значення RSSI свідчать про сильний сигнал і можуть вказувати на хорошу якість з'єднання, тоді як низькі значення можуть сигналізувати про потенційні проблеми, такі як перешкоди або зниження дальності зв'язку. По-друге, RSSI може використовуватися для автоматичного налаштування параметрів зв'язку, таких як модуляція або швидкість передачі даних, що дозволяє системі адаптуватися до змін у якості каналу — особливо важливо в умовах непередбачуваних змін.

Крім того, RSSI відіграє ключову роль у забезпеченні безпеки бездротових систем зв'язку. Моніторинг значень RSSI допомагає виявляти аномалії в поведінці каналу, що можуть свідчити про спроби атак, такі як "відкриття" (eavesdropping) або "відмова в обслуговуванні" (DoS). Наприклад, різке зниження RSSI може вказувати на зловмисні дії, які намагаються перешкодити з'єднанню. Знання про рівень сигналу також може бути використане для реалізації політик контролю доступу, заснованих на потужності сигналу, що дозволяє системі надавати з'єднання лише тим пристроям, які знаходяться в межах певної відстані, таким чином зменшуючи ризик несанкціонованого доступу. Окрім цього, коли RSSI вказує на низьку якість каналу, система може активувати додаткові заходи безпеки, наприклад, підвищити рівень шифрування для захисту даних під час передачі. Таким чином, RSSI не лише є важливим інструментом для оцінки стану каналу, а й виконує

важливу роль у забезпеченні безпеки бездротових комунікаційних систем, сприяючи виявленню загроз і адаптації до змінних умов зв'язку.

Схема поділу даних CQDDR (Code-Quantity Divided Data Rate), яка базується на кількості кодів, дозволяє оптимізувати швидкість передачі даних у цифрових системах зв'язку та передбачає використання різних кодів для розподілу інформаційного потоку, що сприяє підвищенню ефективності передачі та забезпеченню більшої пропускної здатності. Схема CQDDR застосовується для балансування між швидкістю передачі та кількістю кодів, що дозволяє адаптуватися до різних умов роботи мережі, забезпечуючи гнучкість і стабільність зв'язку. Bluetooth має кілька типів пакетів залежно від кількості часових інтервалів (1, 3 або 5) і модуляції. Схема CQDDR класичного Bluetooth регулює вибір типу пакету залежно від якості каналу, використовуючи таблиці пошуку (LUT), що визначають порогові значення SNR для різних пакетів. SNR (Signal-to-Noise Ratio) — це співвідношення сигналу до шуму, яке використовується для оцінки якості передавання сигналу. Воно визначає, наскільки сильний корисний сигнал порівняно з рівнем шуму, що заважає передачі. SNR вимірюється в децибелах (dB), і чим вище значення, тим краща якість сигналу. У контексті порогових значень SNR для різних пакетів мається на увазі, що для кожного типу передаваних даних (пакетів) встановлюються мінімальні значення SNR, при яких передача може здійснюватися з прийнятною якістю. Порогові значення SNR залежать від вимог до надійності передачі та типу модуляції сигналу. Для більш складних або швидкісних пакетів можуть бути потрібні вищі порогові значення SNR, оскільки вони більш чутливі до шуму й перешкод. При погіршенні умов каналу або збільшенні трафіку в піконеті застосовується політика тризонної передачі, що узгоджується із CQDDR.

Модель CQDDR передбачає ретрансляцію пакетів після ARQ до безпомилкової доставки. ARQ (Automatic Repeat reQuest) — це метод контролю помилок у цифрових системах передачі даних, при якому приймач запитує повторну передачу пакету, якщо виявляє в ньому помилку. Коли приймач отримує пакет і перевіряє його за допомогою контрольної суми або іншого механізму, він надсилає підтвердження (ACK, acknowledgment) про успішну передачу. Якщо ж пакет пошкоджений, приймач відправляє запит на повторну передачу (NACK, negative acknowledgment), і відправник повторює передачу до тих пір, поки пакет не буде доставлений правильно.

Отже, у моделі CQDDR, коли відбувається ретрансляція пакетів після ARQ, це означає, що система передбачає повторну передачу пакетів у разі виникнення помилок, доки дані не будуть доставлені безпомилково. Проте "flush таймаут" може бути налаштований для відключення ARQ, що важливо для дотримання часових меж відображення відео. Відправник повідомляє одержувача про зміни в таймауті через протокол L2CAP, без потреби в модифікації заголовків Bluetooth-пакетів. Це дозволяє вибирати тип пакетів залежно від вмісту та якості каналу, що є основою схеми адаптивної модуляції UP.

Запропонована схема не змінює стандарт Bluetooth EDR (Enhanced Data Rate), але вимагає оптимального маркування пакетів на рівні HCI (Host Controller Interface) з можливістю внесення змін на канальному рівні прошивки для підтримки адаптивної модуляції. Bluetooth EDR є розширенням стандарту Bluetooth, що дозволяє передавати дані зі швидкістю до 3 Мбіт/с, що в три рази більше, ніж у базовому режимі (BR, Basic Rate). Основною особливістю EDR є використання більш ефективної модуляції, зокрема π/4-DQPSK або 8DPSK, що забезпечує підвищену пропускну здатність без збільшення смуги пропускання. HCI виконує роль інтерфейсу, який забезпечує зв'язок між стеком протоколів Bluetooth (host) і контролером (hardware), і відповідає за управління основними функціями, такими як обробка команд, подій та передача даних між програмною та апаратною частинами. У контексті запропонованої схеми пріоритетне маркування пакетів на рівні HCI означає, що при обробці команд і передачі даних через HCI деяким пакетам надається пріоритет, що дозволяє оптимізувати процеси передачі даних, підвищуючи загальну ефективність системи Bluetooth EDR.

Аналіз ймовірнісних характеристик моделей та буферизація потокового відео через бездротову мережу Bluetooth є ключовим аспектом забезпечення безпеки відеотрансляцій через цей канал. Вивчення ймовірнісних характеристик дає змогу оцінити ймовірність виникнення подій, що впливають на якість і безпеку передавання відеосигналу [1-3, 8-9]. Буферизація потокових відеоданих через Bluetooth спрямована на забезпечення стабільності передачі та мінімізацію втрат пакетів у разі перешкод або розривів зв'язку. Для гарантування надійної та безпечної передачі відео з підвищеною швидкістю, використовуючи адаптивну модуляцію з тризонним буфером, необхідно детально аналізувати ймовірнісні характеристики та рівні буферизації [9-12]. Важливим є врахування ймовірності втрати пакетів залежно від рівня шуму і перешкод, а також коливань швидкості передачі в бездротових мережах.

Аналіз ймовірнісних характеристик передачі даних сприятиме розробці ефективних алгоритмів буферизації, що забезпечать безперебійну передачу відео через Bluetooth. Застосування адаптивної модуляції з тризонним буфером оптимізує роботу системи з урахуванням змін сигналу і швидкості передачі [6]. Цей підхід дозволить підвищити якість і безпеку відеопотоку, оптимізуючи роботу мережі Bluetooth.

Одним із важливих аспектів впровадження технології Bluetooth та переходу до мереж 5G є підтримка високих навантажень на міжмашинні з'єднання (M2M) та пристрої Інтернету речей (IoT). У контексті зростаючої кількості IoT-пристроїв, які конкурують за доступ до мережі, ефективне управління ресурсами є критично важливим для забезпечення надійності та продуктивності зв'язку. У мережах 5G та LTE, механізм випадкового доступу (Random Access Channel, RACH) відіграє ключову роль у вирішенні проблем масштабованості та перевантажень радіоканалу під час пікових навантажень. RACH забезпечує спосіб для пристроїв ініціювати з'єднання з мережею, зокрема в умовах, коли велика кількість пристроїв намагається підключитися одночасно. Цей механізм дозволяє пристроям відправляти запити на доступ до каналу без попереднього призначення ресурсів, що суттєво знижує затримки та підвищує загальну ефективність мережі. У контексті безпеки, RACH і механізми управління навантаженням мають важливе значення. Висока щільність підключених пристроїв у IoT-середовищі збільшує ризик атаки на мережу, зокрема таких, як DoS (Denial of Service), коли зловмисник намагається перевантажити мережу фальшивими запитами. Використання RACH допомагає зменшити ймовірність таких атак, оскільки дозволяє мережі краще управляти запитами на доступ, запобігаючи ситуаціям, коли зловмисні пристрої можуть створити надмірне навантаження.

Крім того, RACH забезпечує вищий рівень анонімності для пристроїв, що підключаються, що також грає роль у безпеці. Завдяки використанню механізмів випадкового доступу, зловмисникам складніше відстежувати чи ідентифікувати конкретні пристрої, що робить систему менш вразливою для атак. Отже, впровадження технології Bluetooth і перехід до 5G, зокрема механізм RACH, забезпечують не лише підвищення продуктивності та ефективності з'єднань M2M і IoT, а й зміцнення безпеки мережі, що є критично важливим у світі зростаючої кількості підключених пристроїв. У контексті захисту відеопотоку через Bluetooth ці питання вказують на необхідність надійних методів захисту [2, 5-7, 9, 17-23].

Використання багатоантенних технологій (MIMO, Multiple Input Multiple Output) на точках доступу відіграє ключову роль у підвищенні пропускної здатності мережі та швидкості передачі даних. Ця технологія базується на одночасному використанні декількох антен для передачі та прийому сигналів, що дозволяє значно підвищити ефективність використання доступного спектра. Завдяки MIMO, дані можуть передаватися паралельно через кілька каналів, що сприяє зменшенню інтерференції та поліпшенню загальної продуктивності зв'язку. У контексті зростаючого обсягу даних, які передаються в сучасних мережах, зокрема в умовах широкого використання Інтернету речей (IoT) та мобільних пристроїв, важливість MIMO зростає. Збільшення пропускної здатності мережі дозволяє обробляти більше запитів одночасно, що є критично важливим для забезпечення стабільного з'єднання та задоволення вимог користувачів до швидкості передачі даних. З точки зору безпеки, впровадження технології MIMO також має ряд переваг. Перш за все, завдяки здатності зменшувати інтерференцію, MIMO може допомогти покращити якість сигналу, що зменшує ймовірність успішних атак, таких як "відкриття" (eavesdropping). Коли сигнал є більш стабільним і чітким, шанси зловмисників перехопити його інформацію зменшуються. Крім того, MIMO може бути використано в контексті технологій бездротового захисту, таких як різноманітні алгоритми шифрування, які можуть адаптуватися до поліпшеної пропускної здатності. Це дозволяє системі передавати дані з більш високим рівнем шифрування, підвищуючи рівень безпеки передачі.

Отже, інтеграція багатоантенних технологій MIMO в сучасні бездротові мережі не лише підвищує швидкість передачі даних і пропускну здатність, але й робить внесок у безпеку системи, зменшуючи ризики атаки та забезпечуючи надійність зв'язку в умовах зростаючого навантаження на мережу [9, 13-15, 20]. Актуальність цього питання підтверджується численними дослідженнями, які зосереджені на плануванні обслуговування пристроїв з використанням MIMO.

Зростання обсягу потокового мультимедійного трафіку, яке, за даними компанії CISCO, досягло 92% загального трафіку в Інтернеті у 2023 році, підкреслює важливість забезпечення надійної передачі потокового відео. Таке зростання зобов'язує операторів мереж і розробників технологій звертати особливу увагу на ефективність та безпеку потокових систем. У цьому контексті мережі рівних можливостей (P2P, Peer-to-Peer) стали основою для розподілу ресурсів без необхідності в центральному сервері, що надає численні переваги, зокрема зниження затримок і підвищення швидкості доставки контенту. Однак разом із цими перевагами виникає потреба в адекватному захисті відеопотоку, особливо через Bluetooth, від різноманітних загроз безпеки. У мережах P2P користувачі обмінюються даними безпосередньо, що може створити вразливі місця для атак, таких як "відкриття" (eavesdropping), перехоплення даних і несанкціонований доступ до контенту. З огляду на це, питання захисту відеопотоку через Bluetooth стає критично важливим, оскільки технології Bluetooth все частіше використовуються для бездротової передачі мультимедійних даних між пристроями.

Забезпечення безпеки потокового відео в P2P мережах через Bluetooth може включати в себе різноманітні заходи, такі як використання шифрування даних, автентифікації пристроїв та контролю доступу.

Шифрування відео забезпечує, що навіть якщо дані будуть перехоплені, зловмисник не зможе їх розшифрувати без відповідного ключа. Автентифікація пристроїв гарантує, що лише авторизовані користувачі можуть отримати доступ до контенту, знижуючи ризик несанкціонованого доступу.

Отже, збільшення потокового мультимедійного трафіку та популярність P2P мереж вимагають високого рівня безпеки для захисту відеопотоків через Bluetooth. Підходи, які враховують ці фактори, можуть суттєво знизити ризики, пов'язані із загрозами безпеки, забезпечуючи при цьому надійність і якість передачі потокового відео [1-9, 14, 16-21]. Розробка надійних алгоритмів для передачі потокового відео в P2P-мережах, які мають обмеження на швидкість передачі, є необхідною для забезпечення безперервного відтворення відео. Захист відеопотоку через адаптивну модуляцію з тризонним буфером у Bluetooth має включати як безперервність передачі, так і захист від можливих атак та перешкод. Ймовірнісні моделі міжмашинних з'єднань можуть бути використані для контролю якості обслуговування в IoT-мережах, а методи оцінки багатоантенних систем – для управління ресурсами. Такі підходи забезпечать надійну і безпечну передачу відео через Bluetooth з підвищеною швидкістю [1-3, 7-11, 13, 16, 20-23].

Аналіз системних зв'язків процесу передачі відео (рис. 1) дозволяє виявити три фактори, які впливають на кінцеву якість відеозображення: фактор обладнання, фактор мережі та фактор сприйняття [4-10]. Багато дослідників, серед яких Z. Wang, M.H. Pinson, S. Wolf, A.B. Watson працювали над методами оцінки якості відеоізображення (фактор сприйняття). M. Claypool, P. Calyam досліджували вплив характеристик мережі передачі даних на якість відео на приймальному пристрої (тобто зв'язок мережевого фактора і фактора сприйняття). W. Tan, A. Zakhor, G. De Los Reyes, J. Robinson та інші на початку століття вносили свої пропозиції у сфері підвищення якості передаваного відео за допомогою зайвості та особливих методів поширення відеотрафіку по мережі (вплив мережевого фактора на фактор сприйняття). Багато з цих методів на сьогоднішній день вже є стандартами [1-12, 14, 16, 18-20].

На рис. 1 показані основні змінні, що впливають на якість зв'язку: W − розмір пакету RTP (Real-time Transport Protocol, протокол реального часу передачі) в байтах; I - міжпакетний інтервал в секундах; p − відсоток втрат пакетів під час передачі по мережі, %; j − мережевий джиттер в секундах; D − затримка пакетів під час передачі по мережі в секундах; B − пропускна здатність каналу у мегабітах на секунду; Q_{MOS} − якість відео на приймальному пристрої з точки зору людського сприйняття, в балах від нуля до п'яти; Q_{ideal} – максимальна кількість відео для кодека, в балах від нуля до п'яти. Процес передачі відеопотоку через безпровідну мережу досліджується з урахуванням трьох основних чинників: обладнання, мережі та сприйняття. Це дозволяє визначити, яка безпровідна мережа краще чи гірше підходить для передачі потокового відео.

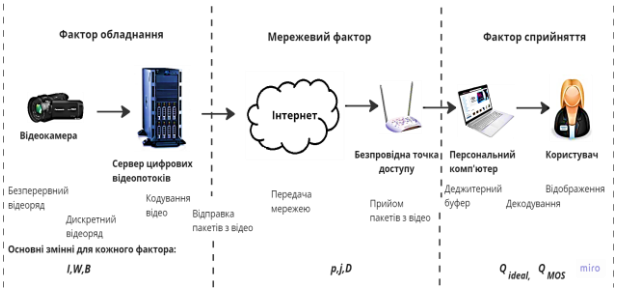

Рис. 1. Системні зв'язки, що впливають на якість передачі відеопотоку
Джерело: агреговано на основі [1-12, 14, 16, 18-23]

Аналіз ймовірнісних характеристик моделей та буферизація потокових даних є ключовими аспектами в захисті відеопотоку за допомогою адаптивної модуляції з тризонним буфером через безпровідну мережу Bluetooth з підвищеною швидкістю передачі даних [14, 19-20, 22-23]. Визначення ймовірнісних характеристик дозволяє прогнозувати ефективність передачі даних і вчасно реагувати на можливі загрози або перешкоди в мережі. Буферизація потокових даних допомагає зберегти інформацію та забезпечити безперервність відтворення відеопотоку навіть при тимчасових втратах зв'язку або зниженні швидкості передачі даних [1-5, 13, 16-21]. Інтеграція цих методів в систему захисту відеопотоку робить її більш надійною та ефективною, забезпечуючи стабільність та якість передачі даних у бездротовому середовищі.

Аналіз показників ефективності мережі пропонується проводити за допомогою наступної моделі, яка враховує основні аспекти функціонування мережі:

$$\mathcal{N} = \langle N, M, a, \beta, lag, d, u, \delta \rangle, \quad (1)$$

де N − кількість користувачів; M − розмір буфера кожного терміналу користувача; $a = (a(n))_{n=\overline{1,N}}$ − вектор ймовірностей підключення користувачів до мережі; $\beta = (\beta(n))_{n=\overline{1,N}}$ − вектор ймовірностей відключення користувачів від мережі; $log = (log(n))_{n=\overline{1,N}}$ − вектор затримок передачі інформації від сервера-джерела потокових мультимедійних даних; $d = (d(n))_{n=\overline{1,N}}$ і $u = (u(n))_{n=\overline{1,N}}$ − вектори швидкостей завантаження і роздачі користувачів відповідно, δ − застосовується в мережі стратегія завантаження даних. Розглядаються стратегії Latest First (LF) і Greedy (Gr). Основними характеристиками ефективності функціонування мережі є ймовірність безперервного відтворення відеопотоку і середній час очікування початку перегляду.

Стан системи можна представити у вигляді:

$$Z = \big(z(n)\big) = (a, X) = (a(n), x(n))_{n=\overline{1,N}}, \quad (2)$$

де матриця $X = x(n))_{n=\overline{1,N}}$ − описує стан буферів усіх користувачів, а $a = (a(n))_{n=\overline{1,N}}$ − вектор індикатор присутності користувача в мережі.

Простір станів системи має розмірність $\mathcal{F} = 2^{N(M+2)}$:

$$\mathcal{F} = \{0,1\}^N \cdot \{0,1\}^{N(M+1)}, \quad (3)$$

Позначимо $\mathrm{M}^0\big(Z, x(n)\big)$ і $\mathrm{M}^{(1)}\big(Z, x(n)\big)$ множини номерів порожніх і заповнених даними місць у буфері n-го користувача відповідно. Для мережі з урахуванням затримок передачі інформації від сервера-джерела даних номер $m_\delta(Z, x(n), x(h), log(n), log(h))$ місця буфера для завантаження даних визначається відповідно до стратегії завантаження $\delta \in \{LF, Gr\}$ за формулою:

$$m_\delta\big(Z, x(n), x(h), lag(n), lag(h)\big) = \begin{cases} minM_\delta\big(Z, x(n), x(h), log(n), log(h)\big), \text{якщо } \delta = LF; \\ maxM_\delta\big(Z, x(n), x(h), log(n), log(h)\big), \text{якщо } \delta = Gr, \end{cases} \quad (4)$$

де:

$$M_\delta\big(Z, x(n), x(h), log(n), log(h)\big) = M^0\big(Z, x(n)\big) \cap M^{(log(n), log(h))}) \cap \cap \{m: m = r - log(n) + log(h),\ r \in M^1\big(Z, x(h)\big) \cap M^{(log(h), log(n))})\}, \quad (5)$$

а множина $M^{(log(i), log(j))}$ визначається за формулою:

$$M^{(log(i), log(j))} = \begin{cases} \{0,1, \dots, M - log(i) + log(j), \text{якщо } log(i) \geq log(j); \\ \{\log(i) - log(j), \dots, M\},\ \text{якщо } log(i) < log(j) \end{cases}, \quad (6)$$

Модель побудовано у вигляді дискретного ланцюга Маркова $\{Z^l\}: \{Z^l, l \geq 0\}$ над простором станів $\mathcal{F}$, де $Z^l = (a^l, X^l)$ − стан мережі на кроці l. Ймовірності $\pi^l(Z) = P\{Z^l = Z\}$ ланцюга Маркова $\{Z^l\}_{l \geq 0}$ на кроці l перебувають в стані Z і задовольняють рівнянням Колмогорова-Чепмена:

$$\pi^{l+1}(Y) = \sum_{Z \in X} \pi^l(Z) \prod^{l\,j+1}(Z, Y), Y \in \mathcal{F}, l \geq 0, \quad (7)$$

причому перехідні ймовірності $\prod^{l\,j+1}(Z, Y)$на кроці l залежать від номера $M_\delta\big(Z, x(n), x(h)\big)$ та від ймовірностей a появи і β відходу користувача.

Ймовірність безперервного відтворення на кроці l визначається за формулою:

$$V^l(n) = \sum_{Y \in X:\ y(n),\ x(n,M)=1,\ a(n)} \pi^l(Y), \quad (8)$$

Аналітичний метод для розрахунку матриці перехідних ймовірностей ланцюга Маркова дає змогу точно розв'язувати задачу для випадку мережі малої розмірності. Якщо $X^l = X$, а $X^{l+1} = Y$, тоді:

$$\Pi^{l,j+1}(X, Y) = 0, \text{якщо } X = Y,$$
$$\Pi^{l,j+1}(X, Y) = 0, \text{якщо } (X, Y) \in \mathcal{X}_{-1} \cup \mathcal{X}_{>1}$$
$$\Pi^{l,j+1}(X, Y) = \prod_{n \in N}(I(A(n,0) = 1) \cdot P^s_{XY}(n) + I(\sum_{m \in M} A(n,m) = 0) \cdot P^-_{XY}(n) + I \sum_{m \in M} A(n,m) = 0) \cdot P^+_{XY}(n)), \text{якщо } (X, Y) \in \mathcal{X}\{\mathcal{X}_{-1} \cup \mathcal{X}_{>1}\} \quad (9)$$

де $P^s_{XY}(n)$ − ймовірність того, що при переході системи зі стану X в стан Y n-й користувач отримав порцію даних від сервера; P^-_{XY} − n-й користувач не отримав даних ні від сервера, ні від інших користувачів; $P^+_{XY}(n)$− n-й користувач успішно завантажив порцію даних від іншого користувача. Множина $\mathcal{X}_{-1}$ пар станів $(X, Y) \subset \mathcal{X} \cdot \mathcal{X}$, що описують переходи зі стану X в стан Y, у яких порції даних зникли з буфера хоча б одного користувача, і множина $\mathcal{X}_{>1}$, що описує переходи, при яких хоча б один користувач завантажив за крок більше однієї порції даних, мають наступний вигляд:

$$\mathcal{X}_{-1} = \{(X, Y): \exists\, n \in \mathcal{N}, \exists\, m \in M, Y(n,m) - SX(n,m) = -1\};$$
$$\mathcal{X}_{>1} = \{(X, Y): \exists\, n \in \mathcal{N}, \sum_{m \in M}(Y(n,m) - SX(n,m)) \geq 2\}. \quad (10)$$

Для стратегії LF:

$$P^s_{XY}(n) = \frac{1}{N},$$
$$P^-_{XY}(n) = \frac{1}{N-1} \times \sum_{h \in N\{n\}} I(\sum_{m \in M}(1 - SX(n,m))\, SX(h,m) = 0),$$
$$P^+_{XY}(n) = \frac{1}{N-1} \cdot \sum_{m \in M \setminus \{0\}} [Y(n,m) - SX(n,m) \times \times \sum_{h \in N\{n\}} SX(h,m) \cdot I\big(\sum_{i=1}^{m-1}(1 - SX(n,i)\big) \cdot SX(n,i) = 0)]. \quad (11)$$

Числовий аналіз, за допомогою якого була визначена оптимальна за ймовірністю неперервного відтворення та часом очікування початку перегляду стратегія завантаження відеоданих. Оптимальною змішаною стратегією є $LF|Gr$, де спочатку для місць $m \in \{0, \cdots, \tilde{m}\}$ буфера застосовується стратегія LF, а потім для інших місць $m \in \{\tilde{m} + 1, \cdots, M\}$ використовується стратегія Gr. Змішана стратегія гарантує високу ймовірність неперервного відтворення при невеликому часі очікування початку перегляду.

Багатопотокове відео, що передається в сучасних системах передачі даних, постає як значний виклик для забезпечення кібербезпеки та захисту інформації. Зростання обсягу відеоданих, яке супроводжується розвитком цифрових технологій, вимагає ефективних заходів для запобігання несанкціонованому доступу, модифікації або знищенню цих даних [4-6, 13, 15-17, 20-23]. Використання багатопотокового відео у системах передачі даних створює ризики, пов'язані з потенційним зловживанням конфіденційною інформацією, а також загрози, що виникають у процесі реального часу зміни контенту. Для забезпечення кібербезпеки багатопотокового відео важливо впроваджувати комплексні заходи захисту, що включають шифрування даних, контроль доступу, автентифікацію користувачів та моніторинг системи на предмет потенційних загроз. Шифрування відеопотоку сприяє захисту вмісту від несанкціонованого доступу шляхом трансформації його в зашифровану форму, що гарантує конфіденційність під час передачі через мережу.

Крім того, важливим є впровадження механізмів автентифікації користувачів та контролю доступу до відеоданих для запобігання несанкціонованому доступу до системи та можливим загрозам безпеці інформації. Моніторинг системи для виявлення аномальної активності та своєчасна реакція на потенційні загрози є критичними

компонентами забезпечення безпеки багатопотокового відео [2, 15-18]. Таким чином, забезпечення кібербезпеки та захисту інформації в сучасних системах передачі даних, зокрема в контексті багатопотокового відео, вимагає комплексного підходу та впровадження передових технологій і стратегій для ефективного управління ризиками, а також для збереження конфіденційності, цілісності та доступності відеоданих [5, 18-20, 23].

У наукових дослідженнях з кібербезпеки та захисту інформації активно застосовується простий поділ на пріоритети користувача (UP) для аналізу як багатопотокового, так і однопотокового відео. У цьому контексті безпека стає ключовим аспектом будь-якої мережі передачі відеоданих, а пріоритезація спрямована на оптимізацію якості обслуговування та забезпечення найвищого рівня безпеки. Аналізуючи різноманіття технологій бездротового зв'язку та їх характеристики, такі як різні форми модуляції, що використовуються в Bluetooth і IEEE 802.11a, стає очевидним, що будь-яка схема захисту повинна враховувати специфіку та можливості технологій бездротового зв'язку.

У дослідженнях [7, 13-15, 17, 19-23] відеопотік поділяється за допомогою багатопозиційного кодування з надлишковістю, в якому кожен підпотік адаптивно модулюється і передається через антенну решітку в системі з множинним входом і множинним виходом (MIMO). Однак, запропоноване рішення [17] може не підходити для Bluetooth через передумови, пов'язані з MIMO. Адаптивна модуляція також може бути застосована [18] через багатошаровість, проте, як зазначалося в Розділі 1, це супроводжується певною гнучкістю. Системи OFDM, такі як IEEE 802.11a, зазнають впливу комбінації FEC та адаптивної модуляції [15, 19, 28]. У [5-6, 9, 15] розшарування реалізується за рахунок дрібнозернистої масштабованості, використовуючи прогресивний внутрішньокодовий рівень посилення. Вертикальна інтеграція заходів захисту, включаючи адаптивний ARQ та FEC, також є важливим аспектом. Проте метод (N, K) кодування Ріда-Соломона (RS) [11-15] не є особливо непридатним для Bluetooth, оскільки RS-коди мають складність $(N-K)log_2N$. Адаптивний ARQ для Bluetooth [20] є перспективною альтернативою адаптивній модуляції. Аналогічно, в роботі [11-16, 19-20] одним із співавторів, вектори руху та інші заголовки даних пріоритезуються за допомогою ієрархічної квадратурної амплітудної модуляції (QAM) для OFDM, призначеної для системи цифрового відеомовлення (DVB). У [9, 11-15] застосовано горизонтальне кодування FEC між пакетами, що забезпечує кращий захист початкових даних у кожному пакеті в порівнянні з пізніми даними, хоча ця схема здебільшого використовувалася для фіксованого Інтернету.

Однопотоковий відеоконтент, що реалізується в сучасних системах передачі даних, є предметом активного наукового дослідження через свою значущість та потенційні виклики в сфері кібербезпеки та захисту інформації [3, 7-9, 16, 20-23]. Однопотокове відео може включати монохромний або кольоровий контент, що передається в режимі реального часу або через зберігання для подальшого відтворення.

Однопотоковий відеоконтент зазвичай передається через різні канали зв'язку, такі як кабельні мережі, бездротовий зв'язок, інтернет-протокол телебачення (IPTV), супутникове телебачення тощо. Цей контент може використовуватися для різноманітних цілей, включаючи трансляцію телевізійних передач, відеоконференції, відеоспостереження, потокове відео на веб-сайтах тощо. Однак використання однопотокового відеоконтенту створює певні виклики з точки зору кібербезпеки та захисту інформації. Оскільки ці дані передаються через відкриті мережі, існує ризик несанкціонованого доступу, перехоплення або модифікації вмісту відеопотоку. Крім того, інформація, що міститься в однопотоковому відеоконтенті, може бути конфіденційною або чутливою, що підкреслює потребу в ефективних заходах захисту даних.

Для забезпечення кібербезпеки однопотокового відеоконтенту важливо використовувати різноманітні заходи захисту, такі як шифрування даних, автентифікація користувачів, контроль доступу та моніторинг системи на предмет потенційних загроз. Шифрування даних дозволяє захистити вміст відеопотоку від несанкціонованого доступу, перетворюючи його в зашифровану форму під час передачі через мережу [7-11, 19-23]. Автентифікація користувачів та контроль доступу сприяють запобіганню несанкціонованому доступу до системи та можливим загрозам інформаційній безпеці. Моніторинг системи на предмет аномальної активності та своєчасне реагування на потенційні загрози є також важливими аспектами забезпечення безпеки однопотокового відеоконтенту.

Таким чином, однопотоковий відеоконтент у сучасних системах передачі даних викликає значний інтерес і потребує системного підходу до забезпечення кібербезпеки та захисту інформації з метою забезпечення конфіденційності, цілісності та доступності даних. Розробка та впровадження нових технологій і стратегій у цій сфері є критично важливими для збереження безпеки відеоданих і довіри користувачів до системи.

Висновки. У сучасному цифровому середовищі, де зростає обсяг потокового мультимедійного контенту, безпека передачі відео через різноманітні технології, зокрема Bluetooth, набуває особливої актуальності. Нові версії Bluetooth, такі як 5.2 і 5.3, пропонують підвищену швидкість передачі даних та стабільність, що робить їх привабливими для передачі великих обсягів інформації, включаючи відео. Однак зростання

швидкості створює нові виклики в галузі кібербезпеки, оскільки зловмисники можуть використовувати ці можливості для атак. Тому дослідники активно працюють над покращенням захисту пристроїв Bluetooth від потенційних загроз. З метою зниження ризиків переповнення буфера та покращення управління передачею пакетів політика пріоритету для тризонного буфера дозволяє адаптувати швидкість передачі в залежності від заповнення буфера. Це забезпечує стабільність передачі даних та їх захист, при цьому межі буферної зони визначаються на основі частоти появи I-, P- та B-кадрів у відеопотоці. Адаптивна схема підвищення рівня сигналу через контролер Bluetooth слугує для моніторингу заповнення буфера, що, у свою чергу, допомагає регулювати пріоритети відеопотоків і забезпечувати належну якість обслуговування.

Крім того, багатоантенні технології (MIMO) підвищують пропускну здатність мережі та покращують якість відео, що є критично важливим у контексті стрімкого зростання потокового відео, яке становить 92% загального трафіку в Інтернеті. Тому забезпечення безпеки відеопотоку через Bluetooth вимагає комплексного підходу, що включає адаптивні механізми, ефективні алгоритми буферизації та моніторинг стану каналу.

Багатопотокове та однопотокове відео стають важливими компонентами сучасних комунікаційних систем, але водночас виявляють численні виклики в сфері кібербезпеки. Розширення обсягу відеоданих вимагає реалізації комплексних заходів для запобігання несанкціонованому доступу, модифікації та знищенню даних. Основні аспекти забезпечення кібербезпеки багатопотокового відео включають шифрування даних, автентифікацію та контроль доступу, що дозволяє уникати несанкціонованого проникнення в систему.

Моніторинг аномальної активності та оперативне реагування на загрози також є критично важливими елементами кібербезпеки. Адаптивні механізми, такі як адаптивне повторне надсилання (ARQ) та кодування виправлення помилок (FEC), оптимізують передачу даних, зменшуючи ризик втрати інформації.

Таким чином, забезпечення захисту інформації в системах передачі даних вимагає інтегрованого підходу, що включає впровадження нових стандартів та технологій. Це стане важливим кроком у напрямку забезпечення безпеки та стабільності передачі потокового відео в сучасних комунікаційних системах, підтримуючи довіру користувачів та безперервність бізнес-процесів у цифровому середовищі.

Список літератури

[1]. Wang We long, Zang Chunhua, Chen Zilong and Liu Shuai (2021) Mobile Node Design of Indoor Positioning System Based on Bluetooth and Loera Network. Journal of Physics: Conference Series, Volume 1738 (1): 4.

[2]. R. Razavi, M. Fleury, and M. Ghanbari (2007) "Low-delay video control in a personal area network for augmented reality," in Proceedings of the 4th Visual Information Engineering, pp. 1245–1300.

[3]. Wilkowska, Wiktoria, Offermann Julia, Spinsante Susanna, Poli Angelica and Ziefle Martina (2022) Analyzing technology acceptance and perception of privacy in ambient assisted living for using sensor-based technologies. PLoS ONE, Volume 17 (7).

[4]. Kostiuk Y.V., Yegor Konstantinov (2024) "Improved security methods in 4G networks to provide effective protection against data transmission attacks" (Series "Pedagogy", Series "Law", Series "Economics", Series "Physical and Mathematical Sciences", Series "Technology"): Journal, № 6(34).

[5]. S. Ye, R. S. Blum, and L. J. Cimini Jr. (2002) Adaptive modulation for variable-rate OFDM systems with imperfect channel information, in Proceedings of the 55th IEEE Vehicular Technology Conference (VTC '02), vol. 2, pp. 767–771.

[6]. Haenssgen, Marco J. (2017) After Access: Inclusion, Development, and a More Mobile Internet. Journal of Human Development and Capabilities, Volume 18 (1).

[7]. Campbell, Scott (2019) From Frontier to Field: Old and New Theoretical Directions in Mobile Communication Studies Communication Theory, Volume 29 (1).

[8]. Core specification of the Bluetooth system, version 2.1 +EDR, July 2007, http://www.Bluetooth.com.

[9]. Svitlana Rzaieva, Dmytro Rzaiev, Yuliia Kostiuk, Hennadii Hulak and Oleksandr Shcheblanin (2024) Methods of Modeling Database System Security CPITS-2024: Cybersecurity Providing in Information and Telecommunication Systems.

[10]. Kryvoruchko O., Kostiuk Y., Desiatko A. (2024) Systematization of signs of unauthorized access to corporate information based on application of cryptographic protection methods// Ukrainian Scientific Journal of Information Security, 2024, vol. 30, issue 1, pp. 140-149.

[11]. Q. Li and M. van der Schaar (2004) Providing adaptive QoS to layered video over wireless local area networks through realtime retry limit adaptation, IEEE Transactions on Multimedia, vol. 6, no. 2, pp. 278–290.

[12]. Iyer and U. B. Desai (2003) A comparative study of video transfer over Bluetooth and 802.11 wireless MAC," in Proceedings of IEEE Wireless Communications and Networking Conference (WCNC '03), vol. 3, pp. 2053–2057.

[13]. Prasad, Revati (2017) Book review: After access: Inclusion, development and a more mobile internet. Communication and the Public, Volume 2 (1): 3.

[14]. C. H. Chia and M. S. Beg (2003) Realizing MPEG-4 video transmission over wireless Bluetooth link via HCI," IEEE Transactions on Consumer Electronics, vol. 49, no. 4, pp. 1028–1034.

[15]. Pearce Katy E. and Rice Ronald (2013) Digital Divides. From Access to Activities: Comparing Mobile and Personal Computer Internet Users. Journal of Communication, Volume 63 (4).

[16]. Ramana Reddy G., Bhatnagar Shalabh, Rakesh V. and Chaturvedi Vijay (2009) An efficient algorithm for scheduling in BLuetooth piconets and scatternets. Wireless Networks, Volume 16 (7).

[17]. Dave Tejal and Pandya Utpal (2018) Simultaneous monitoring of motion ECG of two subjects using Bluetooth Piconet and baseline drift. Biomedical Engineering Letters, Volume 8 (4).

[18]. Rouzbeh, Razavi, Martin, Fleury and Mohammed, Ghanbari (2008) Power-Constrained Fuzzy Logic Control of Video Streaming over a Wireless Interconnect. EURASIP Journal on Advances in Signal Processing, Volume 2008.

[19]. C. Scheiter, R. Steffen, M. Zeller, R. Knorr, B. Stabernack, and K.-W. Wels, (2003) A system for QOS-enabled MPEG-4 video transmission over Bluetooth for mobile applications," in Proceedings of International Conference on Multimedia and Expo (ICME '03), vol. 1, pp. 789–792.

[20]. Tahir Sabeen, Aldabbagh Ghadah Abdullah, Bakhsh Sheikh Tahir and Said Abass Md. Hybrid (2021) Congestion Sharing and Route Repairing Protocol for Bluetooth Networks. WSEAS TRANSACTIONS ON COMPUTERS.

[21]. Chen, Zhi-kui (2006) An adaptive FEC to protect RoHC and UDP-Lite H.264 video critical data. Journal of Zhejiang University - Science A, Volume 7 (5).

[22]. Yang Chorng-Horng and Lee Sian-Jie (2022) Virtual Scatternet Formation for Supporting Multicast in Bluetooth Networks. International Journal of New Technology and Research.

[23]. L.-J. Chen, R. Kapoor, M. Y. Sanadidi, R. Lee, and M. Gerla (2004) Audio streaming over Bluetooth: an adaptive ARQ timeout approach," in Proceedings of the 24th International Conference on Distributed Computing Systems, vol. 24, pp. 196–201.

УДК 621.396.62:004.42

Kostiuk Y., Bebeshko B., Hulak H., Skladannyi P., Rzaeva S., Khorolska K. Ensuring cyber security and high data transmission speed in wireless networks.

Abstract. *The paper investigates the problem of ensuring a balance between information security and data transmission performance in wireless communications, in particular in the context of Bluetooth technology. The relevance of the topic is due to the growing demands on the speed and reliability of video stream transmission, which is becoming critically important in the context of the development of modern information and communication systems. The article analyzes the technical features of Bluetooth, in particular the IEEE 802.15.1 standard, which provides energy-efficient data transmission over short distances. The relevance of the topic is due to the growing demands on the speed and reliability of video streaming, which is becoming critical in the development of modern information and communication systems. The article analyzes the technical features of Bluetooth, in particular the IEEE 802.15.1 standard, which provides energy-efficient data transmission over short distances. The main characteristics of Bluetooth are considered, including the star network topology, frequency range, modulation methods and signal power that affect data transmission performance. Particular attention is paid to adaptive modulation and buffering methods that improve transmission quality in conditions of radio frequency interference and obstacles. Data protection mechanisms that can be integrated into wireless networks are also analyzed to prevent security threats such as unauthorized access and data interception. The proposed solutions take into account the features of Bluetooth Low Energy (BLE), which makes them particularly effective for IoT applications. The conclusions of the paper emphasize the importance of an integrated approach to resource management in wireless communications, which allows for stable, secure, and productive operation of information systems, in particular in an ever-changing threat environment.*

Keywords: *protection, efficiency, adaptive modulation, buffering, video stream, wireless data transmission, single-stream video content, wireless networks, Bluetooth, security, performance, optimization, productivity, interrelation.*

Костюк Юлія Володимирівна, PhD, доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Київського столичного університету імені Бориса Грінченка.
Yuliia Kostiuk, PhD, Associate Professor of the Department of Information and Cyber Security named after Professor Volodymyr Buriachok Borys Grinchenko Kyiv Metropolitan University.

Бебешко Богдан Тарасович, PhD, доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Київського столичного університету імені Бориса Грінченка.
Bohdan Bebeshko, PhD, Associate Professor of the Department of Information and Cyber Security named after Professor Volodymyr Buriachok Borys Grinchenko Kyiv Metropolitan University.

Гулак Геннадій Миколайович, доктор технічних наук, професор, професор кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Київського столичного університету імені Бориса Грінченка.
Hennadii Hulak, Doctor of Technical Sciences, Associate Professor, Professor of the Department of Information and Cyber Security named after Professor Volodymyr Buriachok Borys Grinchenko Kyiv Metropolitan University.

Складанний Павло Миколайович, кандидат технічних наук, доцент, завідувач кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Київського столичного університету імені Бориса Грінченка.
Pavlo Skladannyi, PhD, Associate Professor, Head of the Department of Information and Cyber Security named after Professor Volodymyr Buryachok Borys Grinchenko Kyiv Metropolitan University.

Рзаєва Світлана Леонідівна, кандидат технічних наук, доцент, доцент кафедри комп'ютерних наук Київського столичного університету імені Бориса Грінченка.
Rzaeva Svitlana, Candidate of Technical Sciences, Associate Professor, Associate Professor of the Department of Computer Science Borys Grinchenko Kyiv Metropolitan University.

Хорольська Карина Вікторівна, PhD in Computer Science, доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Київського столичного університету імені Бориса Грінченка.
Karyna Khorolska, PhD in Computer Science " Associate Professor of the Department of Information and Cyber Security named after Professor Volodymyr Buriachok Borys Grinchenko Kyiv Metropolitan University.