MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE

KHARKIV NATIONAL
UNIVERSITY OF RADIO ELECTRONICS

RADIOTEKHNIKA

All-Ukrainian
interdepartmental scientific and technical collection

ISSN 0485-8972
eISSN 2786-5525

Founded in 1965

I S S U E 2 2 0

Kharkiv
Kharkiv National
University of Radio Electronics
2025

UDC 621.3

The collection is included in the List of scientific professional publications of Ukraine, category «Б», technical and physical-mathematical sciences (approved by orders of the Ministry of Education and Science from 17.03.2020 № 409; from 02.07.2020 № 886; from 24.09.2020 № 1188) by specialties: 105 – Applied Physics and Nanomaterials; 125 – Cybersecurity and information protection; 163 – Biomedical Engineering; 171 – Electronics; 172 – Electronic communications and Radio Engineering; 173 – Avionics; 174 –Automation and Computer-Integrated Technologies and Robotics; 175 – Metrology and information-measuring technique; 176 – Micro- and Nanosystem Technology.

Website: rt.nure.ua

Registration certificate KV № 12098-969 PR dated 14. 12. 2006.

The authors are responsible for the content of the article.

Editorial Team

Members of the editorial board of foreign scientific institutions and educational institutions

Responsible for the issue: *S.O. Sheiko, PhD, Assoc. prof., I.D. Gorbenko, Dr. Sc. (Tech.), prof.*
Technical Secretary: *O.S. Polyakova.*

Recommended by the Scientific and Technical Council of Kharkiv National University of Radio Electronics, protocol № 3 dated 10.04.2025.

Address of the editorial board: Kharkiv National University of Radio Electronics (NURE), ave. Nauky, 14, Kharkiv, 61166, tel. (0572) 7021-397.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ
УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ

РАДІОТЕХНІКА

Всеукраїнський
міжвідомчий науково-технічний збірник

ISSN 0485-8972
eISSN 2786-5525

Засновано в 1965 р.

В И П У С К 2 2 0

Харків
Харківський національний
університет радіоелектроніки
2025

УДК 621.3

Збірник включено до Переліку наукових фахових видань України, категорія "Б", технічні та фізико-математичні науки (затверджено наказами МОНУ від 17.03.2020 № 409; від 02.07.2020 № 886; від 24.09.2020 № 1188) за спеціальностями: 105 – Прикладна фізика та наноматеріали; 125 – Кібербезпека та захист інформації; 163 – Біомедична інженерія; 171 – Електроніка; 172 – Електронні комунікації та радіотехніка; 173 – Авіоніка; 174 – Автоматизація, комп'ютерно-інтегровані технології та робототехніка; 175 – Метрологія та інформаційно-вимірювальні технології; 176 – Мікро- та наносистемна техніка.

Сайт: rt.nure.ua

Реєстраційне свідоцтво КВ № 12098-969 ПР від 14. 12. 2006.

За зміст статті відповідальні автори.

Відповідальні за випуск: *С.О. Шейко, канд. техн. наук, доц., І.Д. Горбенко, д-р техн. наук, проф.*
Технічний секретар: *О.С. Полякова.*

Рекомендовано Науково-технічною радою Харківського національного університету радіоелектроніки, протокол № 3 від 10.04.2025.

Адреса редакційної колегії: Харківський національний університет радіоелектроніки (ХНУРЕ), просп. Науки, 14, Харків, 61166, тел. (0572) 7021-397.

CONTENT

SYSTEMS AND METHODS OF INFORMATION PROTECTION

AUTOMATION AND ROBOTICS

RADIO ELECTRONIC SYSTEMS

PHYSICS OF DEVICES, ELEMENTS AND SYSTEMS

ELECTRONIC COMMUNICATIONS

ЗМІСТ

СИСТЕМИ І МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ

АВТОМАТИЗАЦІЯ ТА РОБОТОТЕХНІКА

РАДІОЕЛЕКТРОННІ СИСТЕМИ

ФІЗИКА ПРИЛАДІВ, ЕЛЕМЕНТІВ І СИСТЕМ

ЕЛЕКТРОННІ КОМУНІКАЦІЇ

УДК 004.056.55 **DOI:10.30837/rt.2025.1.220.01**

О.Г. КАЧКО, канд. техн. наук, І.Д. ГОРБЕНКО, д-р техн. наук, С.О. КАНДІЙ

ЗАСТОСУВАННЯ ФІКСОВАНОЇ ТОЧКИ ЗАМІСТЬ ПЛАВАЮЧОЇ ДЛЯ РЕАЛІЗАЦІЇ ЕЛЕКТРОННОГО ПІДПИСУ FALCON

Вступ

Перемога схеми електронного підпису (ЕП) FALCON на конкурсі NIST PQC і розробка стандарту на основі цього алгоритму пов'язана з найкращими показниками по розміру відкритого ключа та електронного підпису [1]. Особливості реалізації алгоритму FALCON з детальним описом засобів оптимізації наведено в роботі [2]. Для ефективного виконання операцій множення та ділення для поліномів застосовують швидке перетворення Фур'є, яке потребує представлення даних в форматі з плаваючою точкою. Для забезпечення можливості застосування алгоритмів на обчислювальних засобах, які не підтримують роботу з плаваючою точкою застосовують емуляцію.

Необхідність застосування плаваючої точки або її емуляції приводить до проблеми залежності точності обчислень від порядку, що може привести до додаткових атак [3]. В роботі [4] наведено застосування фіксованої точки для генерації ключів, що, з одного боку, не потребує від обчислювального пристрою роботи з плаваючою точкою, а по друге, практично не поступається за ефективністю алгоритму генерації з застосуванням плаваючої точки. Але, на жаль, масштаб для фіксованої точки, запропонований в роботі [4], не можна застосовувати для формування електронного підпису згідно з алгоритмом [2]. В роботі [5] запропоновано інший масштаб для завдання даних з фіксованою точкою, який дозволяє застосовувати цей формат для генерації ЕП, але застосування різного формату представлення даних для генерації та обчислення ЕП незручно.

Мета роботи – модифікація алгоритму генерації ключів, запропонованого в роботі [4] для формату даних з роботи [5], що забезпечує застосування загального масштабу для операцій генерації ключів та формування ЕП. Операція перевірки ЕП не потребує застосування даних з плаваючою точкою і, відповідно, операцій з фіксованою точкою. Виконано порівняння продуктивності для основних операцій в разі застосування плаваючої точки, її емуляції (авторська реалізація [2]) та фіксованої точки з різними масштабами [4, 5].

1. Представлення даних

Розглянемо представлення значень з фіксованою точкою. Для зберігання значення відводиться 8 байтів, як і для чисел з плаваючою точкою. Будемо називати масштабом числа (SCALE) кількість бітів, які відводяться для нецілої частини числа.

Формат числа показано на рис. 1.

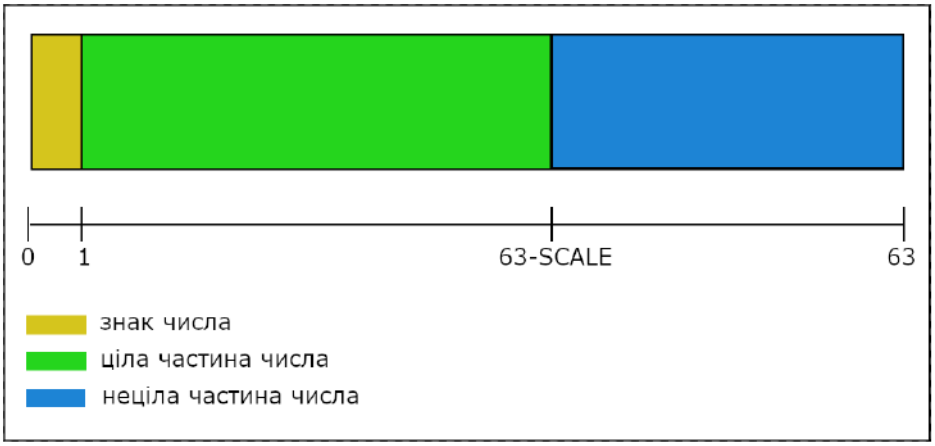


Рис. 1. Формат чисел з фіксованою точкою

Неціла частина має SCALE бітів, де параметр SCALE може приймати значення від 1 до 32. Ціла частина числа має 63 SCALE бітів і знак числа 1 біт (0 для невід'ємного, 1 для від'ємного). Число задається в додатковому коді.

В роботі [4] в якості масштабу застосовують SCALE = 32 біта, тоді для цілої частини залишається 31 біт, що обмежує значення числа. В роботі [5] обчислено масштаб SCALE = 26 біт, який розширює діапазон представлення даних до значень, які дозволяють генерувати ЕП, але, на жаль, зменшує точність даних та потребує суттєво переробити бібліотеку функцій для роботи з фіксованою точкою. У даній роботі була розроблена універсальна бібліотека для довільного масштабу SCALE < 32. Детальний опис функцій наведено у розд. 2.

Для зручності застосування, для функцій, які потрібні при генерації, збережено імена з роботи [4], префікс для імен функцій для реальних даних fxr і для комплексних – fxc. Для обчислення експоненти (під час обчислення ЕП), усі значення менше одиниці, для збільшення точності замість SCALE = 26 застосовують подвійний масштаб SCALE = 2 * 26, і відповідна функція має префікс fxr2.

2. Бібліотека

В табл. 1 представлено набір функцій бібліотеки для роботи з даними з фіксованою точкою, які не залежать від SCALE в умовах загальної довжини числа 64 біта. В якості цих функцій застосовують функції авторів [4]. В табл. 2 представлено набір функцій бібліотеки для роботи з фіксованою точкою, які залежать від SCALE. Туди ж додано функції. які для генерації ключів не застосовуються.

Таблиця 1

Функції, які не залежать від масштабу SCALE

Ім'я функції	Призначення
fxr_add	Додавання даних
fxr_sub	Віднімання даних
fxr_double	Множення на 2
fxr_neg	Для даного x обчислення значення – x
fxr_abs	Обчислення абсолютного значення
fxr_div2e	Ділення числа на 2^n (зсув числа вправо на n біт)
fxr_mul2e	Множення числа на 2^n (зсув числа вліво на n біт)
fxr_lt	Порівняння двох чисел x, y. Якщо x менше y, функція повертає TRUE, інакше FALSE

Таблиця 2

Функції, які залежать від масштабу SCALE

Ім'я функції	Призначення
fxr_of	Перетворення цілого в число з фіксованою точкою
fxr_mul	Множення даних
fxr_sqr	Обчислення квадрату числа
fxr_div	Ділення даних
fxr_inv	Інверсія. Для даного x обчислення 1/x
fxr_sqrt	Корінь квадратний (застосовують для розгортання секретного ключа)
fxr_round fxr_rint	Округлення до найближчого цілого
fxr_trunc	Відсічення нецілої частини
fxr_floor	Ціле значення, яке не перевищує задане
fxr2_exp	Обчислення exp(x), де 0 <=x < 1 (застосовують для обчислення ЕП)

Операції для комплексних чисел (+, -, *, /) застосовують функції для роботи з фіксованою точкою.

Для усіх операцій бібліотеки передбачається, що вхідними даними та результатом виконання є дані з фіксованою точкою, а також відсутність переповнень, тобто ціла частина не перевищує по модулю значення $2^{63\text{-SCALE}}$.

Найбільш ресурсоємними є операції множення, ділення, обчислення кореня та експоненти. Операції множення та ділення застосовують як для реальних так і для комплексних даних. Ці операції застосовують для роботи з секретними ключами, тому для них умова незалежності від часу є обов'язковою.

2.1. Множення даних з фіксованою точкою

Операція множення виконується для невід'ємних чисел. В разі завдання від'ємних чисел, обчислюється їх абсолютне значення. Для кінцевого результату коригується знак.

При множенні даних $x*2^{SCALE}$, $y*2^{SCALE}$ треба отримати результат $x*y*2^{SCALE}$. В результаті множення 64-бітних невід'ємних значень отримаємо 126 бітне дане, яке дорівнює $x*y*2^{2*SCALE}$. Для отримання вірного значення необхідно отриманий результат поділити на 2^{SCALE} з урахуванням округлення. В разі відсутності переповнення отримане значення гарантовано містить не більше ніж 63 біта. Як показує експеримент з генерацією 10000 ключів, формування відповідних ЕП та їх перевірки переповнення не виникають.

При реалізації функції множення не передбачалася підтримка застосування 128 бітних даних, для отримання добутку завдовжки більше ніж 64 біта застосовувалася програмна реалізація за допомогою алгоритму Карацуби (3 множення замість чотирьох).

Спочатку для вхідних даних обчислювалося абсолютне значення. Після множення 64 бітних беззнакових даних отримували добуток завдовжки 126 біт. для якого застосовувався зсув на SCALE бітів вправо та виконувалося округлення. В кінці коригувався знак для результату. Обчислення абсолютного значення та зворотне коригування знаку виконувалося без застосування команд переходу. Квадрат обчислювався множенням однакових значень (функція fxr_sqr). Нижче наведено код функції множення з коментарями основних операцій.

Функція множення чисел у форматі фіксованою точкою.

```
static inline fxr fxr_mul(fxr fx, fxr fy) {
   // Константи множення
   const uint64_t SCALE_MASK = (1ULL << SCALE) - 1;
   const uint64_t ROUND_THRESHOLD = 1ULL << (SCALE - 1);
   // Зчитування значень
   uint64_t x = fx.v;
   uint64_t y = fy.v;
   // Виділення знаків чисел
   uint64_t sign_x = x >> 63;
   uint64_t sign_y = y >> 63;
   uint64_t final_sign = sign_x ^ sign_y;
   // Отримання абсолютних значень
   x = (x ^ -sign_x) + sign_x;
   y = (y ^ -sign_y) + sign_y;
   // Віділення цілої частини
   uint64_t x_high = x >> SCALE;
   uint64_t y_high = y >> SCALE;
   uint64_t x_low = x & SCALE_MASK;
   uint64_t y_low = y & SCALE_MASK;
   // Множення Карацуби
   uint64_t high_product = x_high * y_high;
   uint64_t low_product = x_low * y_low;
```

```
    uint64_t cross_sum = (x_high + x_low) * (y_high + y_low);
    uint64_t middle_term = cross_sum - low_product - high_product;
    // Обчислення результату
    uint64_t result = (low_product >> SCALE) +
        (low_product & SCALE_MASK > ROUND_THRESHOLD) +
        middle_term + (high_product << SCALE);
    // Врахування знаку
    result = (result ^ -final_sign) + final_sign;
    return (fxr){.v = result};
}
```

2.2. Операція ділення

Як і для операції множення для x, y застосовують абсолютне значення, знак результату коригується після обчислень.

При діленні даних $x*2^{SCALE}$, $y*2^{SCALE}$ треба отримати результат $(x/y)*2^{SCALE}$.

Для забезпечення відсутності переповнення x/y повинно не перевищувати $2^{63\ -\ SCALE}$, тобто вхідні дані повинні задовольняти вимозі $x < y * 2^{63\ -\ SCALE}$, або $x/2^{63\ -\ SCALE} < y$. Для x, y застосовують масштабоване значення, тобто для цих значень нерівність залишається.

Фактично застосовують побітовий алгоритм ділення в стовпчик. Починаємо зі старших бітів x, відповідне значення яких не перевищує 2*y, тобто результат ділення x на $2^{62\ -\ SCALE}$, а далі поступово дописуємо по одному біту до тих пір, поки біти x не будуть вичерпані (всього таких бітів 62 – SCALE), які були відкинуті при діленні x на $2^{63\ -\ SCALE}$. В результаті виконання циклу 63 – SCALE разів отримаємо старші 63 – SCALE бітів масштабованого числа. Для отримання решти бітів (нецілу частину) виконуємо цикл SCALE разів число доповнюємо нулями.

Для прикладу роботи алгоритму розглянемо число x з загальною довжиною 8 бітів, масштаб SCALE дорівнює 3 біта. Нехай x = 1011011 і дільник y = 1100.

Згідно з умовою для x, y маємо $x/28 - 3 < y$, тобто значення x можна зсувати на 4 біта і отримаємо значення, яке може перевищувати значення y менше ніж в два рази. На кожному наступному кроці будемо додавати один біт з решти бітів.

Формуємо біти для доповнення, на які ми виконали зсув, доповнюємо нулями до 7 бітів, отримаємо 10110000

Виконуємо 8 кроків для кожного біту результату для ілюстрації роботи алгоритму.

Що порівнюємо	Біт результату	Біти для доповнення
101 < 1100	0	1011000
1011 < 1100	0	011000
10110>1100	1	11000
10101>1100	1	1000
10011>1100	1	000
01110>1100	1	00
00100>1100	0	0
01000>1100	0	
Результат	00111100	

П е р е в і р к а :

X дорівнює 11.2625, y дорівнює 1.5. Результат ділення ≈7.508 і з урахуванням масштабу дорівнює 60. $001111002 = 6010$. Нижче наведено реалізацію функції ділення з коментарями основних операцій.

Функція ділення чисел у форматі фіксованою точкою.

```
static inline fxr fxr_div(fxr fx, fxr fy) {
    const uint64_t MAX_POSITIVE = 0x7FFFFFFFFFFFFFFFULL;
    const int TOTAL_BITS = 64;
    const int SHIFT_BITS = TOTAL_BITS - 2;
    // Зчитування значень та виділення знаку
    uint64_t x = fx.v;
    uint64_t y = fy.v;
    uint64_t final_sign = (x >> 63) ^ (y >> 63);
    // Виділення абсолютних значень
    x = (x ^ -(x >> 63)) + (x >> 63);
    y = (y ^ -(y >> 63)) + (y >> 63);
    // Ініціалізація змінних
    uint64_t quotient = 0;
    uint64_t numerator = x >> (SHIFT_BITS - SCALE);
    uint64_t temp = x << (SCALE + 2);
    // Алгоритм ділення
    #pragma unroll
    for (int i = SHIFT_BITS; i >= 0; i--) {
        uint64_t diff = numerator - y;
        uint64_t bit = 1 - (diff >> 63);

        quotient = (quotient << 1) | bit;
        numerator = ((numerator - (y & -bit)) << 1) | (temp >> 63);
        temp <<= 1;
    }
    // Обчислення результату
    uint64_t final_bit = 1 - ((numerator - y) >> 63);
    quotient = (quotient + final_bit) & MAX_POSITIVE;
    // Врахування знаку
    fx.v = (quotient ^ -final_sign) + final_sign;
    return fx;
}
```

2.3. Операція обчислення кореня квадратного

Застосовують побітовий алгоритм [6], який перетворений для забезпечення незалежності часу виконання операції від конкретних даних. Псевдокод наведено нижче.

Функція обчислення квадратного кореня у форматі фіксованою точкою.

```
static inline fxr fxr_sqrt(fxr fn) {
    const int MAX_STEP = 62;
    const uint64_t INITIAL_D = 1ULL << MAX_STEP;
    const int RESULT_SHIFT = SCALE / 2;
    // Ініціалізація змінних
    uint64_t x = fn.v;
    uint64_t n = x;
    uint64_t c = 0;
    uint64_t d = INITIAL_D;
```

```
    #pragma unroll 4
    for (int step = MAX_STEP; step >= 0; step -= 2) {
        // Ми можемо відняти поточне значення?
        int64_t can_subtract = ~((int64_t)(n - d) >> 63);
        // Обчислення потенційно нового значення
        uint64_t potential = c + d;
        uint64_t trial = can_subtract & potential;
        // Перевірка чи пробне значення в квадраті менше або дорівнює x
        int64_t is_valid = can_subtract & (~((int64_t)(x - trial) >> 63));
        // Оновлення значень
        x -= is_valid & trial;
        c = (can_subtract & (c >> 1)) + (is_valid & d);
        d >>= 2;
    }
    // Врахування масштабу
    fn.v = c << RESULT_SHIFT;
    return fn;
}
```

3. Порівняння продуктивності операцій бібліотеки

Для визначення продуктивності кожної операції виконувався експеримент для 1024 випадкових наборів даних, для яких виключалося переповнення. Для виключення випадкового збільшення часу виконання за рахунок переключення потоків для кожного набору даних виконувалось 256 тестів, з яких обиралося мінімальне значення. Для визначення впливу даних на продуктивність з усіх мінімальних значень обиралося максимальне значення. Продуктивність вимірялася в тактах процесору (12th Gen Intel(R) Core(TM) i5-1240P).

В табл. 3 представлено обчислювальну складність операцій множення та ділення для варіантів: застосування плаваючої точки та її емуляції [1], масштабу SCALE = 32 [3] та масштабу SCALE = 26 [4] відповідно. Для операції обчислення квадратного кореня та експоненти для варіантів застосування плаваючої точки та її емуляції [1] та масштабу SCALE = 26 [4].

Таблиця 3

Продуктивність базових операцій

Операція	Варіант			
	double		SCALE = 32	SCALE = 26
	апаратна	емуляція		
Mul	10 14	10 14	10 14	10 14
Div	10 14	10 14	10 14	10 14
Sqrt	10 14	10 14	-	23 63
Exp	10 14	10 14	-	10 14

Перше число в таблиці визначає мінімальне значення для випадкових 1024 чисел, друге – максимальне. Операція Sqrt виконується при розгортанні секретного ключа і не реалізована для SCALE = 32. Операція exp виконується при генерації ЕП і не реалізована для SCALE = 32. Отримані результати свідчать, що продуктивность окремих операцій практично не залежить від формату.

4. Функції для алгоритму Falcon

4.1. Генерація ключів

Для генерації ключів застосовано авторський алгоритм генерації [4] з деякими змінами.

Для генерації випадкового seed застосовують SHAKE256, функція генерації ключів keygen має інтерфейс, як у авторів falcon [2], наповнення – авторів [4] з масштабом з [5].

Додано генерацію відкритого ключа та видалено перевірку наявності інверсії для поліному f. Наявність інверсії фактично перевіряється при генерації відкритого ключа.

При генерації ключів можливі помилки, пов'язані з невідповідністю згенерованих даних вимогам алгоритму, а саме:

- перевищені максимальні значення для коефіцієнтів або норма для поліномів f, g (fg_error);
- норма ортогонального вектору перевищує максимальну (fg_inv_error);
- помилка при обчисленні відкритого ключа (public_error) або при перевірці наявності інверсії для поліномів f, g (для SCALE = 32);
- NTRU рівняння не має рішення (найбільший спільний дільник не дорівнює 1), gcd_error;
- помилка при редукції поліномів (reduce_error); виникає, якщо в разі редукції для поліномів порядку 2, 4, … n отримаємо значення F, G, які не задовольняють NTRU рівнянню для заданих f, g;
- компоненти поліному F перевищують встановлену границю (limit_error_f);
- компоненти поліному G перевищують встановлену границю (limit_error_g).

В разі наявності будь-якої помилки генерація починається спочатку.

Розглянуто наступні варіанти:

В а р і а н т 1 . Генерація ключів по [2] з застосуванням даних з плаваючою точкою, або емуляції;

В а р і а н т 2 . Генерація ключів по [4] з застосуванням даних з фіксованою точкою, SCALE = 32;

В а р і а н т 3 . Генерація ключів по [5] з застосуванням даних з фіксованою точкою, SCALE = 26;

Варіант 2 не передбачає генерації відкритого ключа, але перевіряє, що вектори f, g мають інверсії, що фактично еквівалентно перевірці наявності відкритого ключа, тому ці дані будуть записані в рядку для public_error.

Для формування випадкових ключів стан генератору встановлюється однаковим для усіх трьох варіантів і задається функціями:

```
inner_shake256_init(&rng);
inner_shake256_inject(&rng, (uint8_t*)buf, strlen(buf));
inner_shake256_flip(&rng);
```

де buf – рядок завдовжки 8 символів, який містить символи:

для n = 512: 0x6b, 0x65, 0x79, 0x67, 0x65, 0x6e, 0x20, 0x39, 0.

Для n = 1024 замість передостаннього символу 0x39 застосовують символ 0x3a.

На рис. 2 представлено дані про кількість помилок при генерації 10000 успішних ключів для Falcon512. На рис. 3 представлено аналогічні дані для Falcon1024.

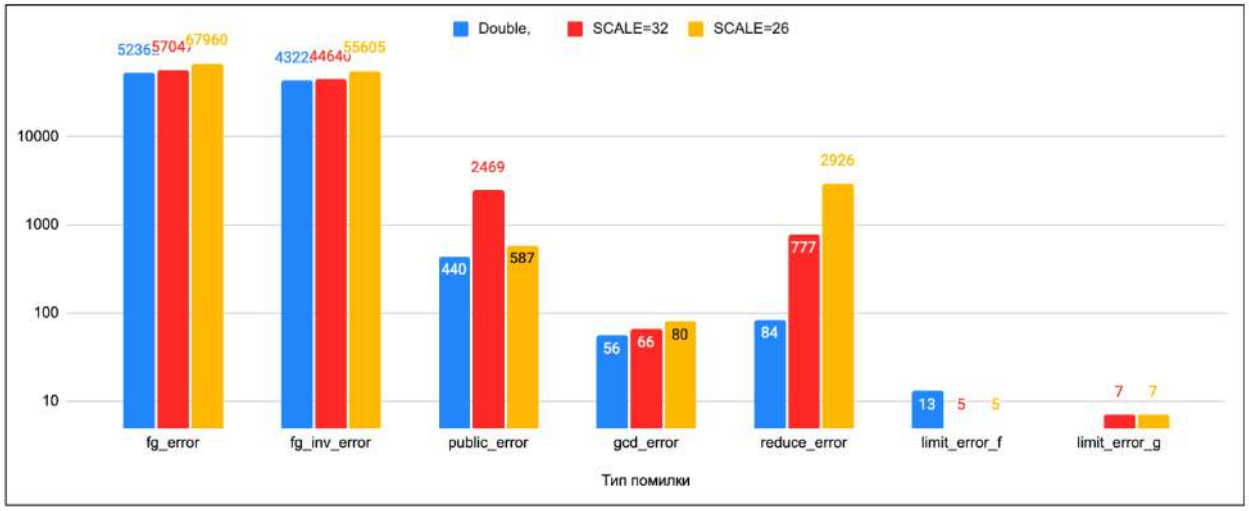


Рис. 2. Дані по помилкам при генерації ключів для Falcon512

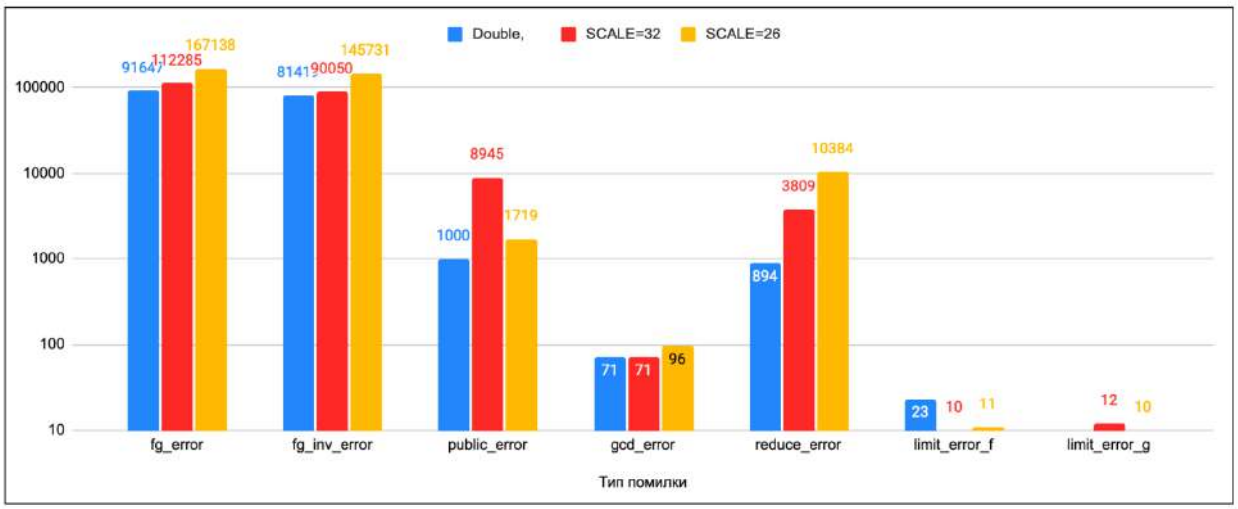


Рис. 3. Дані по помилкам при генерації ключів для Falcon1024

Як показав експеримент, кількість помилок суттєво відрізняється для помилки типу reduce_error. Це пов'язано з суттєвим зменшенням точності в разі застосування фіксованої точки, особливо у варіанті зі SCALE = 26. Збільшення reduce_error впливає на продуктивність операції генерації ключів, тому що ця помилка визначається практично в кінці операції генерації, що потребує починати цю операцію спочатку.

Найбільш "жадібною" серед функцій бібліотеки, які застосовують фіксовану точку, є функція комплексного множення fxc_mul, яка обчислює модуль знаменника (три операції fxr_mul), виконує ділення чисельника на модуль знаменника (дві операції fxr_div) та виконує операцію комплексного множення.

4.2. Розгортання секретного ключа

Розгортання секретного ключа може виконуватись безпосередньо паралельно з генерацією ЕП, а також як окрема функція, яка в якості вхідних даних застосовує тільки набір поліномів для секретного ключа (f, g, F, G).

Варіант з паралельним розгортанням і генерацією ЕП застосовують, якщо обмеження на розмір пам'яті є критичним. В цьому випадку ключи розгортаються кожного разу при створенні ЕП, що збільшує час, необхідний для її генерації. Варіант з окремим розгортанням застосовують, якщо критичним є параметр часу, для одного набору секретних ключів генерують декілька ЕП.

Автори [1, 2] запропонували обидва варіанти, наявність яких може призвести до атаки, за допомогою якої можна обчислити секретні ключі [3]. В [5] визначено умови, при яких дана атака неможлива

Розгортання секретного ключа (побудова дерева Falcon tree) виконується згідно з алгоритмом, представленим в [2] (функція expand_privkey). На основі FFT формату для поліномів f, g, F, G формується дерево, при обчисленні якого застосовують операції з фіксованою точкою. Після обчислення елементів дерева виконується його нормалізація, тобто кожне значення елементу дерева value заміняється значенням $\overline{\overline{\text{value}}}$.

4.3. Електронний підпис

Електронний підпис виробляється згідно з алгоритмом [1, 2] (функція sign_tree), але для роботи з даними з плаваючою точкою застосовується фіксована точка [5]. В якості вхідних даних застосовують повідомлення для підпису, розгорнутий секретний ключ та ініціалізований генератор псевдовипадкових чисел.

Генерація ЕП передбачає генерацію біта, значення якого дорівнює 1 з імовірністю e^x, що потребує обчислення експоненти для аргументу в діапазоні [0.. ln2). Додаткова функція fxr_expm обчислює це значення для аргументів, заданих з фіксованою точкою.

5. Продуктивність функцій алгоритму FALCON

У межах дослідження було виконано порівняння продуктивності функцій генерації ключів, розгортання секретного ключа та вироблення ЕП для варіантів застосування плаваючої точки, емуляції плаваючої точки та фіксованої точки для SCALE = 26.

Як і в попередньому випадку продуктивність визначається в тактах процесору.

Продуктивність визначається для 100 різних ключів.

Для генерації кожного ключа виконується 16 експериментів і визначається мінімальний час (для виключення випадкових переключень потоків). Для 100 різних ключів визначається мінімальна кількість тактів (min), максимальна кількість тактів з мінімальних (max) та середнє значення продуктивності (avg).

Операції розгортання ключів та вироблення ЕП виконується для кожного зі 100 ключів (знову експеримент повторюється для кожного ключа 16 разів, обчислюється мінімальне, максимальне та середнє значення).

Для порівняння застосовується Reference_Implementation без застосування AVX команд авторів (папка falcon-round3, [1]) та відповідна реалізація в разі застосування фіксованої точки з масштабом SCALE = 26.

На рис. 4 наведено результати вимірювання продуктивності функцій алгоритму Falcon для Faclon512. На рис. 5 наведено відповідні дані для Falcon1024.

Для кожного випадку задаються три значення. Перше значення – мінімальне, друге – максимальне з мінімальних, третє – середнє. Для усіх варіантів мінімальне значення для фіксованої точки виграє в порівнянні з мінімальним значенням для режиму емуляції плаваючої точки.

Для усіх варіантів за виключенням генерації ключів для n = 1024 максимальне та середнє значення для фіксованої точки поступається відповідним значенням для режиму емуляції плаваючої точки. Треба зазначити, що застосування фіксованої точки замість плаваючої не вирішує проблему залежності результату від порядку виконання операцій.

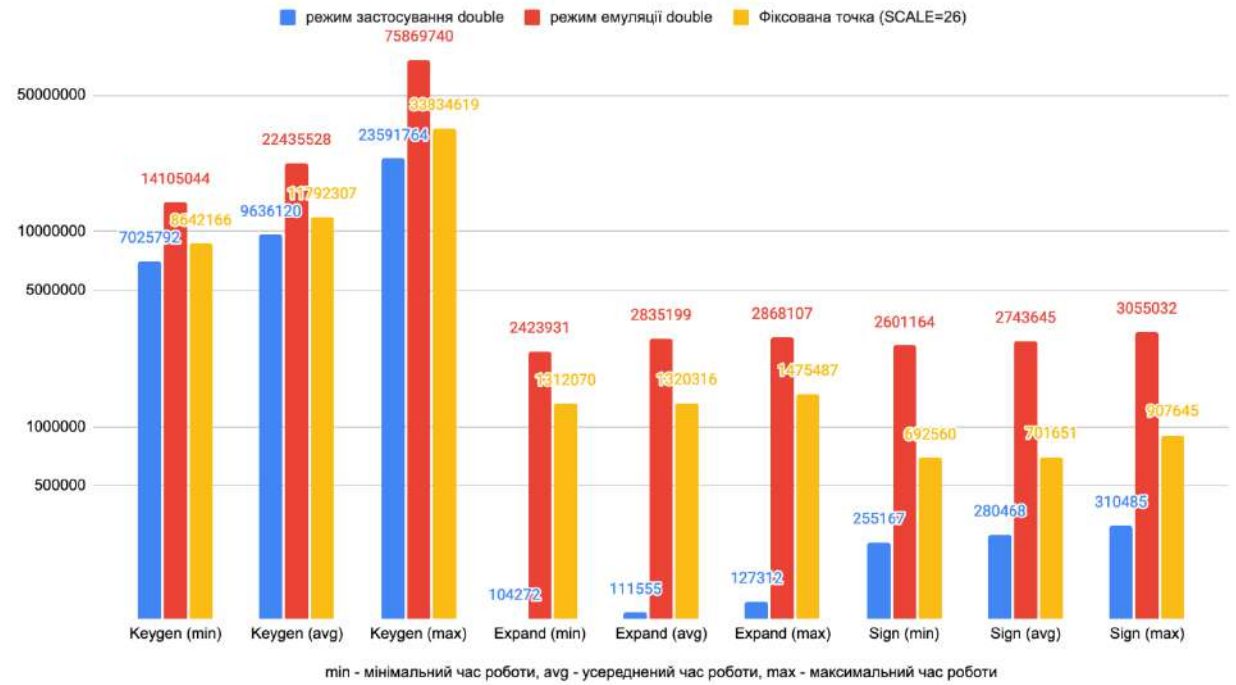


Рис. 4. Оцінка часу роботи функцій Keygen, Expand, Sign для Falcon512

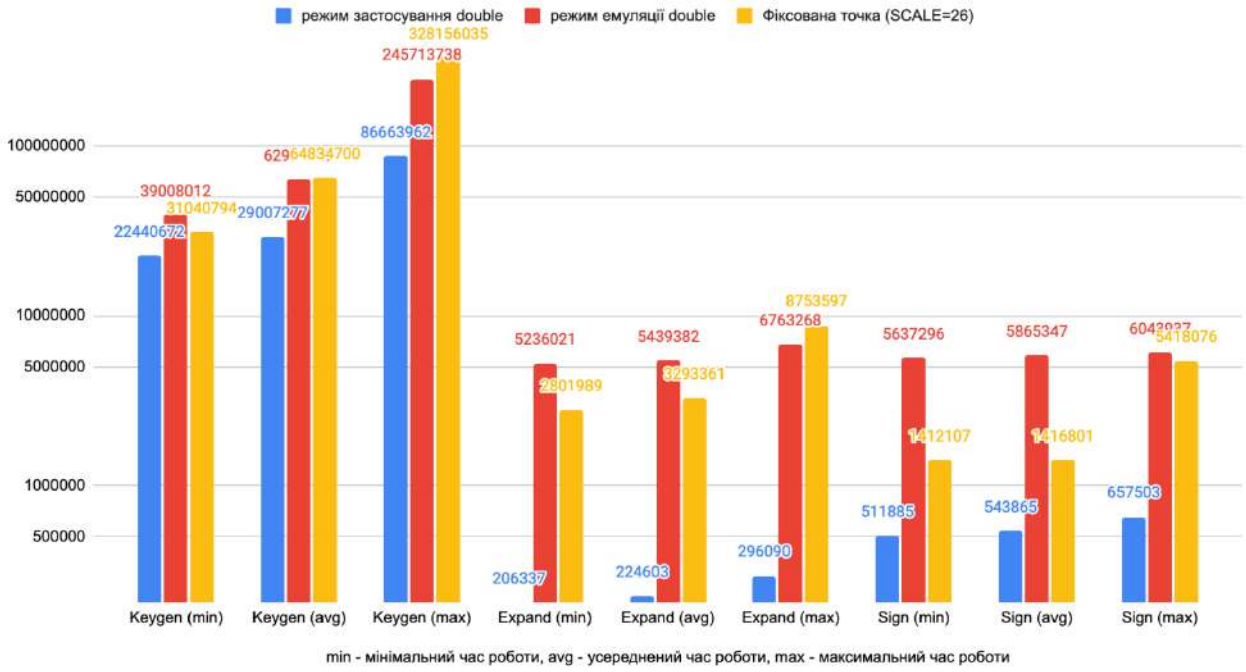


Рис. 5. Оцінка часу роботи функцій Keygen, Expand, Sign для Falcon1024

Висновки

Модифіковано алгоритм генерації ключів та формування електронного підпису з урахуванням формату даних з фіксованою точкою, запропонованого в роботі [5], що дозволило забезпечити єдиний масштаб для усіх операцій генерації ключів та формування електронного підпису. Такий підхід значно спрощує реалізацію криптографічних алгоритмів, зберігаючи при цьому високу продуктивність. Універсальна бібліотека, розроблена в межах дослідження, підтримує масштаб SCALE < 32 та містить реалізації ключових операцій, що враховують специфіку обчислень з фіксованою точкою.

Результати експериментального дослідження показали, що кількість помилок суттєво відрізняється для помилки типу reduce_error. Це пов'язано з суттєвим зменшенням точності в разі застосування фіксованої точки, особливо в варіанті зі SCALE = 26. Збільшення reduce_error впливає на продуктивність операції генерації ключів, тому що ця помилка визначається практично в кінці операції генерації, що потребує починати цю операцію спочатку.

Серед усіх реалізованих функцій найбільш ресурсоємними є операції множення, ділення та комплексного множення. Функція комплексного множення fxc_mul продемонструвала найбільші вимоги до ресурсів через необхідність виконання кількох ключових операцій, таких як обчислення модуля знаменника та ділення. Незважаючи на це, застосування фіксованої точки забезпечує обчислювальну незалежність від часу для операцій із секретними ключами, що є важливою вимогою для забезпечення криптографічної стійкості.

Таким чином, запропоновані модифікації та аналіз продуктивності демонструють, що формат з фіксованою точкою може бути ефективно застосований у криптографічних алгоритмах за умови оптимізації масштабу та врахування впливу на точність. Отримані результати можуть бути використані для подальшого вдосконалення криптографічних протоколів та їх реалізації в обмежених середовищах, де використання плаваючої точки є небажаним або неможливим.

Список літератури:

1. Round 3 submissions – post-quantum cryptography: CSRC, CSRC. Available at: https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-3-submissions (Accessed: 10 November 2024).

2. Pornin T. New efficient, constant-time implementations of Falcon // IACR Cryptology ePrint Archive. Available at: https://eprint.iacr.org/2019/893 (Accessed: 10 November 2024).

3. Potii O. et al. Determining the effect of a floating point on the Falcon Digital Signature Algorithm Security // Eastern-European Journal of Enterprise Technologies. 2024. No 1(9 (127)). P. 52–59. doi:10.15587/1729-4061.2024.295160.

4. Pornin T. Improved key pair generation for Falcon, Bat and hawk // IACR Cryptology ePrint Archive. 2023. Available at: https://eprint.iacr.org/2023/290 (Accessed: 10 November 2024).

5. Kachko O. et al. Improving protection of falcon electronic signature software implementations against attacks based on Floating Point Noise // Eastern-European Journal of Enterprise Technologie. 2024. No4(9 (130)). P. 6–17. doi:10.15587/1729-4061.2024.310521.

6. Woo C. Square root by abacus algorithm, Index of /Martin/Tape/Gos/MISC/personal/MSC/SQRT. Available at: http://freaknet.org/martin/tape/gos/misc/personal/msc/sqrt/ (Accessed: 10 November 2024).

7. Goldwasser S., Micali S. and Rivest R.L. A digital signature scheme secure against adaptive chosen-message attacks // SIAM Journal on Computing. 1988. No17(2). Pp. 281–308. doi:10.1137/0217017.

8. Hövelmanns K., Hülsing A. and Majenz C. Decryption failures and the Fujisaki-Okamoto Transform // Cryptology ePrint Archive. Available at: https://eprint.iacr.org/2022/365.pdf (Accessed: 13 October 2024).

Надійшла до редколегії 06.01.2025

Відомості про авторів:

Качко Олена Григорівна – канд. техн. наук, Харківський національний університет радіоелектроніки, професор кафедри програмної інженерії, факультет комп'ютерних наук; АТ «Інститут інформаційних технологій», начальник відділу програмування; Україна; e-mail: iit@iit.kharkov.ua, ORCID: https://orcid.org/0000-0001-9249-0497

Горбенко Іван Дмитрович – д-р техн. наук, професор, Харківський національний університет ім.В.Н. Каразіна, професор кафедри кібербезпеки інформаційних систем, мереж і технологій, навчально-науковий інститут комп'ютерних наук та штучного інтелекту, АТ «Інститут інформаційних технологій», головний конструктор; Україна; e-mail: i.d.gorbenko@karazin.ua; ORCID: https://orcid.org/0000-0003-4616-3449

Кандій Сергій Олегович – Харківський національний університет ім. В. Н. Каразіна, аспірант кафедри кібербезпеки інформаційних систем, мереж і технологій, навчально-науковий інститут комп'ютерних наук та штучного інтелекту, АТ «Інститут Інформаційних технологій», науковий консультант; Україна; e-mail: sergeykandy@gmail.com; ORCID: https://orcid.org/0000-0003-0552-8341

УДК 004.05 **DOI:10.30837/rt.2025.1.220.02**

В.В. БОРОДАВКА, В.І. ЄСІН, д-р техн. наук

ДОЦІЛЬНІСТЬ ВИКОРИСТАННЯ МОЖЛИВОСТЕЙ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ПІДПРИЄМСТВА, ЯКА ҐРУНТУЄТЬСЯ НА КОНЦЕПЦІЇ НУЛЬОВОЇ ДОВІРИ

Вступ

Швидкість розвитку та зміни кіберпростору в останні три-п’ять років вражають не тільки недосвідчених користувачів, а й спеціалістів у галузі інформаційних технологій та інформаційної безпеки. Відбувається стрімкий розвиток не лише обсягу оброблюваних даних, кількості пристроїв, підключених до Інтернету або чисельності застосунків та сервісів, а й самих концепцій і технологій. Всеосяжна цифровізація та перехід бізнесу в онлайн, прискорені пандемією та війною, багато в чому сприяли розвитку цієї тенденції.

Широке використання мов програмування, фреймворків і середовищ розробки, розвиток хмарної інфраструктури та технологій віртуалізації й контейнеризації дають змогу збирати нові застосунки у безпрецедентно короткий термін, в тому числі за допомогою штучного інтелекту (ШІ). З іншого боку, з такою ж швидкістю множаться і кіберзагрози, оскільки зловмисники використовують аналогічні високоефективні інструменти розробки, але у своїх протиправних цілях. Це виводить рівень кіберпротидії на новий рівень: якщо раніше протистояння зі зловмисниками можна було описати як боротьбу розумів і налаштованих засобів захисту інформації, то тепер це вже можна назвати своєрідним поєдинком технологій, у якому задіяний ШІ. Звіт компанії (лідера у сегменті автоматизованої перевірки безпеки) Pentera [1] про стан тестування на проникнення за 2024 р. проливає світло на нагальні проблеми та зміну парадигм кібербезпеки в глобальних організаціях.

Розмови про практичне використання ШІ у сфері кібербезпеки ведуться вже тривалий час, але лише нещодавно ці інструменти стали доступними на ринку. Сьогоднішній рівень зрілості таких рішень дозволив забезпечити впровадження їх у корпоративні середовища для прийняття важливих рішень, причому цілком з виправданими витратами на їх реалізацію, в тому числі враховуючи можливості для зловмисників, що знову відкрилися. А саме, ефективна та своєчасна протидія атакам стає можливою лише із застосуванням технологій ШІ.

Згідно зі звітом «The macroeconomic impact of artificial intelligence» від міжнародної аудит-консалтингової корпорації PwC [2] прогнозується, що до 2030 р. завдяки прискореному розвитку систем ШІ глобальний ВВП може зрости на 14 % (це близько 15,7 трлн доларів США). У сфері комп’ютерних наук ШІ означає здатність машин виконувати завдання, для яких, зазвичай, вимагається наявність людського інтелекту. При цьому ШІ включає багато суміжних областей та технологій, таких як машинне навчання, глибоке навчання, нейронні мережі, обробка природних мов та інші.

На тлі швидкого розвитку інноваційних технологій ШІ набуває широкого застосування для виявлення кіберзагроз і забезпечення посиленого захисту від кібератак, а також сприяє прийняттю обґрунтованих та скоординованих управлінських рішень. Розширюючи інструментарій для виявлення й запобігання кіберзагрозам, автоматизуючи рутинні завдання та скорочуючи час реагування на кіберінциденти, технологія ШІ може значно зміцнити захист від кібератак, що дозволить мінімізувати загрозливі тенденції у цій сфері. За даними компанії IBM [3], збитки від порушення даних у всьому світі можуть бути знижені, якщо організації застосовуватимуть автоматизовані рішення безпеки. Організації, які не застосовували автоматизацію в безпеці, зазнали витрат у зв’язку з порушеннями, які були на 95 % вищими, ніж порушення в організаціях з повністю розгорнутою автоматизацією.

Поряд з цим, щоб захистити сучасне цифрове підприємство, необхідна комплексна стратегія для безпечного доступу у будь-який час і в будь-якому місці до корпоративних ресурсів підприємства (застосунків, застарілих / успадкованих систем, даних, пристроїв тощо) неза-

лежно від того, де вони розташовані [4, 5]. Дійсно, розвиток хмарних обчислень, Інтернету речей, бізнес-партнерів та зростаючої кількості віддалених співробітників підвищує складність захисту цифрових активів підприємства, оскільки точок входу, виходу та доступу до даних істотно збільшилося, а існуючі рішення не завжди здатні реагувати на динамічні зміни, через те, що часто ґрунтуються на статичних наборах правил, брандмауерах, віртуальних приватних мережах (Virtual Private Network – VPN). Тому підприємства стали переосмислювати традиційний підхід до захисту, що базується на забезпеченні безпеки периметра мережі, схиляючись до нової концепції та архітектури захисту. Такою концепцією зараз стала парадигма безпеки, відома як «нульова довіра» (Zero Trust – ZT). Її особливістю можна вважати жорсткіший принцип «ніколи не довіряти, завжди перевіряти». Тобто згідно з її основною ідеєю – не існує областей, які заслуговують на довіру. Нульова довіра – це не єдина архітектура, а набір керівних принципів для робочого процесу, проектування системи та операцій, які можна використовувати для покращення стану безпеки будь-якої класифікації або рівня чутливості [6].

Виходячи з сказаного, спираючись на принципи цієї концепції і задіявши можливості ШІ (технології ШІ можуть ефективно використовуватися для своєчасного виявлення вразливостей у різних інформаційних системах та мережах), можна спробувати побудувати відповідну сучасним вимогам адаптивну і стійку систему безпеки, яка постійно буде перевіряти кожну взаємодію та швидко реагувати на загрози, що знову з’являються.

У рамках вирішення зазначеної задачі розглянемо деякий підхід, що спирається на принципи концепції нульової довіри та потенціал ШІ, а саме – можливість вирішення актуального завдання, яке полягає у подальшому удосконаленні моделей і методів захисту від кібератак та зловживань шляхом інтегрування концептуальних принципів нульової довіри та ШІ. Такий підхід може дозволити забезпечити більш динамічний та адаптивний захист за рахунок постійної перевірки автентичності користувачів і процесів, незалежно від їх попереднього статусу довіри, та більш ефективно ідентифікувати потенційні загрози в режимі реального часу й реагувати на них раніше, ніж вони можуть завдати шкоди.

1. Огляд концепції нульової довіри

Як відомо [7], традиційна мережева безпека ґрунтується на концепції периметра безпеки, згідно з якою мережа поділяється на дві частини: внутрішню довірену мережу та зовнішню недовірену мережу. Відповідно до цього підходу добре структурована архітектура безпеки розглядає безпеку мережі як багаторівневу систему, де кожен периметр захищає область, яку він покриває. За даними дослідників із компанії Akamai [8], периметр – укріплена ділянка мережі, яка може включати граничні маршрутизатори, міжмережеві екрани (брандмауери, файрволи), системи виявлення вторгнень (Intrusion Detection System – IDS), системи запобігання вторгненням (Intrusion Prevention System – IPS), VPN, програмну архітектуру, демілітаризовану зону (Demilitarized Zone – DMZ) та віртуальні локальні мережі (Virtual Local Area Network – VLAN).

Міжмережеві екрани або фаєрволи захищають активи, ізолюючи приватні мережі від публічних шляхом фільтрації трафіку та блокування доступу до недовірених джерел або IP-адрес. Однак, якщо зловмиснику вдається прорвати захисний периметр, фаєрвол не може зупинити його в подальших діях у внутрішній мережі. VPN часто використовується для доступу до віддалених мереж, створюючи захищене з’єднання між локальною та віддаленою мережею за допомогою шифрування даних. Хоча цей метод ефективний для захисту комунікацій, він становить загрозу для корпоративних активів, оскільки VPN використовує статичну автентифікацію та не може безперервно перевіряти особу користувача та надійність кінцевого пристрою під час сесії. Також VPN не здатен визначати та обмежувати рівень доступу користувачів, що дозволяє їм необмежено користуватися внутрішніми ресурсами після підключення. Мережа DMZ додає ще один рівень безпеки для внутрішньої мережі. Однак, як і у випадку з іншими методами, надмірна залежність від фаєрволів може призвести до виник-

нення певних проблем. Якщо зловмисник зможе обійти фаєрвол, наприклад, через фішингові електронні листи, що дозволить отримати доступ до внутрішньої мережі, то DMZ не зможе протидіяти такій загрозі. Крім того, DMZ не здатен виявляти атаки довірених пристроїв на інші довірені пристрої.

Архітектура безпеки периметра забезпечувала ефективний захист від типових загроз, таких як шкідливе програмне забезпечення, фішингові атаки, атаки на відмову в обслуговуванні та атаки нульового дня. Однак зі зростанням обсягу даних, що переміщуються у хмарні сервіси, та з розширенням кількості користувачів, включно з пристроями Інтернету речей (Internet of Things – IoT), традиційне розуміння мережевого периметра змінилося, що зробило зовнішні атаки більш складними та динамічними. Поверхня атак збільшилася, багато загроз походять зсередини, і захист на основі периметра більше не може ефективно протидіяти внутрішнім загрозам, оскільки являє собою одно-направлений захист і безсилий проти атак зсередини мережі.

Концепція нульової довіри, «ніколи не довіряй, завжди перевіряй», була вперше запропонована у 2010 р. [9] для розв'язання проблем, спричинених внутрішніми загрозами для організацій. Нульова довіра відноситься до двох основних областей: автентифікації та авторизації [6]. В її основі лежить ідея обмеження неявної довіри як визнання обмеженості використання одиничних статичних засобів захисту у великій мережі.

Порівнюючи традиційну модель безпеки та модель нульової довіри можна побачити (табл. 1 [5, 10]), що традиційний підхід на основі захисту згідно з периметром ефективно захищає від зовнішніх атак, але ігнорує внутрішні атаки.

Таблиця 1

Порівняння традиційної моделі безпеки та моделі нульової довіри

Характеристика	**Традиційна модель безпеки**	**Модель нульової довіри**
Підхід	Довіряй але перевіряй.	Нікому не довіряй і все перевіряй.
Межа довіри	Зовнішня (немає довіри). Внутрішня (довірена).	Мікросегментація (мережі поділяються на дрібніші сегменти або безпечні зони, щоб обмежити бічне переміщення загроз; кожен сегмент має свої засоби керування доступом користувачів та політики безпеки).
Мережева архітектура	Модель «замок та рів» з підвищеним акцентом на захист периметра.	Децентралізована та мікросегментована, з детальним контролем доступу.
Контроль доступу	Контроль доступу на основі IP.	Керування доступом, орієнтоване на дані (з урахуванням ідентифікаційних та контекстно-залежних даних).
Автентифікація	Однократна після перевірки при початковому доступі та статична.	Перед доступом та постійна (мультимодальна та динамічна) перевірка.
Керування безпекою	Індивідуальний моніторинг та видимість.	Видимість, автоматизація та оркестрування поведінки, пристроїв, сервісів та безпеки.
Політика безпеки	Заздалегідь встановлені правила та загальна політика.	Деталізовані правила та адаптивні політики (оцінка рівня безпеки).
Шифрування зв'язку	Зовнішня мережа (шифрування). Внутрішня (без шифрування).	Повне шифрування трафіку.
Реагування на порушення	Після того, як периметр порушено, зловмисники отримують можливість діяти вільно.	Навіть якщо порушення сталося, переміщення зловмисників ретельно відстежуються.

Традиційна архітектура захисту не спроможна ефективно протистояти сучасним кібератакам, привілейовані шляхи доступу стають більш ризикованими й ускладнюють захист згідно з периметром від несанкціонованих атак з боку легітимних внутрішніх користувачів. У той час як використання, наприклад, принципу найменших привілеїв та мікросегментація архітектури нульової довіри (Zero Trust Architecture – ZTA) ефективно обмежує привілеї внутрішніх користувачів і дозволяє уникати ризиків необмеженого бічного переміщення (lateral movement) користувачів у мережі.

Принципи нульової довіри не є новими, але їх унікальність полягає в комплексному застосуванні для захисту корпоративних ресурсів. На відміну від традиційних систем, де права доступу визначаються статично відповідно до посадових обов'язків, підхід концепції нульової довіри передбачає динамічне прийняття рішень через центр політики на основі внутрішніх правил і зовнішніх даних. Хоча автоматизація є ключовим елементом таких систем, вони також забезпечують можливість ручного втручання на окремих етапах перед запуском автоматичних процесів реагування [5].

У спеціальній публікації NIST 800-207 [6] нульова довіра описується як парадигма кібербезпеки, яка зміщує акцент захисту. Нульова довіра зосереджена на захисті ресурсів (активів, служб, робочих процесів, мережевих облікових записів тощо), а не на сегментах мережі, оскільки мережеве розташування більше не вважається основним компонентом безпеки ресурсу. Згідно з концепцією нульової довіри активам або обліковим записам користувачів не надається ніякої неявної довіри на основі їхнього фізичного або мережевого розташування. Натомість автентифікація та авторизація передбачають певні кроки перед тим, як отримати доступ до корпоративного ресурсу [6]. На рис. 1 представлено основні логічні компоненти архітектури нульової довіри, а також взаємозв'язок між ними.

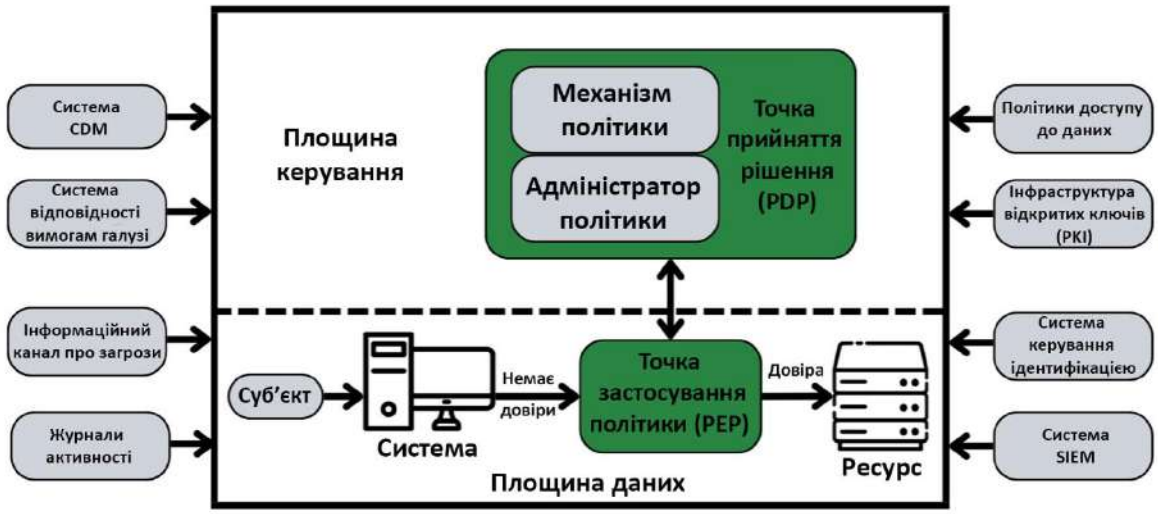


Рис. 1. Основні логічні компоненти ZTA

В даній схемі існує поняття суб'єкта, яке визначається NIST [6] як користувач, сервіс, застосунок або пристрій, що працює в комп'ютерній системі (або разом з нею) і має доступ до корпоративного ресурсу (Enterprise Resource). Цей ресурс може бути застосунком, даними, документом або робочим навантаженням, які знаходяться під контролем організації та захищені системою нульової довіри. Вважається, що суб'єкт працює в ненадійному середовищі в ненадійній мережі, і йому дозволено отримати доступ до ресурсу лише через точку застосування політики (Policy Enforcement Point – PEP). PEP контролює доступ суб'єкта до ресурсу через те, що NIST [6] називає неявною зоною довіри (implicit trust zone). PEP не зберігає і не визначає політику – цю роботу виконує точка прийняття рішення (Policy Decision Point – PDP). Варто звернути увагу, що суб'єкт взаємодіє з корпоративним ресурсом через так звану площину даних, яка відрізняється від площини керування – як зазначає NIST [7], PDP і PEP «взаємодіють у мережі, яка є логічно відокремленою і не є безпосередньо доступною для активів і ресурсів організації. Площина даних використовується для трафіку даних застосунків».

Крім цих основних компонентів на підприємстві, що реалізує ZTA, є ряд зовнішніх компонентів, які сприяють реалізації безпеки з нульовою довірою. А саме – існує кілька локальних та зовнішніх джерел даних, що надають вхідні дані та правила політик, які використовуються механізмом політик при прийнятті рішень про доступ. Серед них: система керування ідентифікацією (ID management system), інфраструктура відкритих ключів (Public Key

Infrastructure – PKI), система аналізу загроз (інформаційні канали про загрози), підсистема реєстрації подій і моніторингу, підсистема безперервної діагностики та усунення наслідків, система управління інформацією та подіями безпеки (Security Information and Event Management – SIEM), система безперервної діагностики та пом'якшення наслідків – Continuous Diagnostics and Mitigation (CDM). Ці елементи є важливими вхідними даними (контекстом) для системи нульової довіри і, безумовно, впливають на її практичні рішення.

У свою чергу, компанія Forrester запропонувала [11] розширену архітектуру нульової довіри (Zero Trust Extended – ZTX), що охоплює ширше коло потоків даних, зокрема тих, що проходять через локальні мережі, хмарні сервіси, зовнішні застосунки, сайти та різні види кінцевих пристроїв, зокрема датчики IoT тощо. Компанія Gartner, ґрунтуючись на принципі безперервного адаптивного оцінювання ризику та довіри, також висунула ідею [12] про ZTX. Покращена модель нульової довіри розширює архітектуру, запропоновану NIST, забезпечуючи більш повну обізнаність про ситуацію і враховує практичні особливості введення в експлуатацію. Згідно з такою моделлю у процесі вибору рішень беруть до уваги і суб'єкт, і кінцеву точку, включно зі ступенем їхньої відповідності вимогам безпеки. Приблизно в той самий час Google розпочала розробку своєї реалізації концепції безпеки з нульовою довірою BeyondCorp [13], яка перенесла контроль доступу з периметру мережі на окремі пристрої та користувачів. BeyondCorp, базуючись на політиках автентифікації, авторизації та контролю доступу, гарантує доступ до корпоративних ресурсів лише авторизованим користувачам і пристроям. Додатковий імпульс розвитку концепції надали публікації NIST [6] та NCCoE (National Cybersecurity Center of Excellence) [15], які акцентували увагу на ZTA для захисту корпоративних даних [5].

Деякі спеціалісти з безпеки компанії Oracle пов'язують, наприклад, дії щодо забезпечення безпеки на основі принципів концепції нульової довіри з використанням чотирьох ключових напрямків (рис. 2), зокрема [14]: запобігання атакам (Attack Prevention), виявлення інцидентів (Incident Detection), усунення інцидентів (Incident Response) та аналіз подій (Event Analysis). Такий підхід підкреслює безперервний цикл захисту даних, інтегруючи системи керування ідентифікацією та доступом (Identity and Access Management – IAM), автоматизоване виявлення загроз, безпеку застосунків та моніторинг мережі.

Рис. 2. Ключові напрями підходу до захисту

У 2023 р. компанія Fortinet провела дослідження серед компаній-лідерів у сфері безпеки з 31 країни, що охоплювало різні галузі, включно з державним сектором. Результати показали, що лише 28 % організацій впровадили повноцінне рішення нульової довіри для мінімізації кіберризиків [16]. Це свідчить про те, що значна частина компаній ще не реалізувала комплексні заходи ZTA, що залишає їх вразливими до сучасних кіберзагроз. Проте впроваджен-

ня подібних рішень не лише дозволить підвищити рівень безпеки, а й забезпечить значні операційні та економічні переваги для підприємства, що робить ZTA ключовим елементом ефективного управління кіберризиками. Однією з головних переваг концепції нульової довіри є оптимізація витрат на забезпечення кібербезпеки, скорочення обсягу робіт із дотримання нормативної відповідності та ефективне використання ресурсів. Крім аспектів безпеки, ZTA відіграє ключову роль у підтримці цифрової трансформації бізнесу, а організації отримують додаткові конкурентні переваги, такі як підвищення операційної гнучкості, ефективне управління ресурсами та здатність швидко адаптуватися до змін у динамічному цифровому середовищі [17].

В цілому ж можна констатувати, що реалізація концепції нульової довіри передбачає впровадження комплексних заходів безпеки, спрямованих на мінімізацію ризиків і забезпечення захисту ресурсів організації в умовах сучасного цифрового середовища. І одним із ключових компонентів у цьому аспекті є безперервний моніторинг та аудит, які дозволяють виявляти підозрілу активність та аномалії шляхом аналізу даних із мережевого трафіку, журналів активності користувачів та систем захисту кінцевих точок. Це забезпечує реальний час для оцінки загроз, реагування на інциденти (Incident Response – IR), проведення цифрової криміналістики (digital forensics) та аналізу кіберзагроз. Поряд із цим важливим є IAM, яка визначає правила доступу до ресурсів і передбачає перевірку кожного запиту на основі багатофакторної автентифікації та динамічної оцінки ризиків. Ця система забезпечує високу точність контролю доступу за рахунок інтеграції параметрів, таких як ідентифікатор та пароль користувача, пристрій, час поточного місцезнаходження, права доступу тощо. Іншим критично важливим елементом ZTA є аналіз поведінки користувачів та сутностей (пристроїв, застосунків та інших об’єктів в інформаційній системі; User and Entity Behavior Analysis – UEBA), який дозволяє виявляти аномальні дії, наприклад спроби несанкціонованого доступу або передачі даних. Це допомагає ідентифікувати загрози, включаючи розподілені атаки на відмову в обслуговуванні, атаки грубої сили, витоки даних та інсайдерські загрози, забезпечуючи пріоритетність реагування на найбільш серйозні ризики. Водночас важливим є і реагування на інциденти (IR), що передбачає швидке виявлення атак, визначення їх масштабів, нейтралізацію наслідків та запобігання повторенню. Організації можуть мінімізувати вплив кіберінцидентів, скоротити час простою і захистити свою репутацію, впроваджуючи відповідний план IR. З іншого боку, система аналізу загроз сприяє збору та аналізу інформації про дії зловмисників і використовувані ними вразливості. Сюди входить інформація про те, що роблять зловмисники, як вони це роблять і які вразливості вони використовують. Ця інформація допомагає організаціям проактивно захищати свої активи, підвищуючи стійкість до сучасних кіберзагроз. На думку експертів з інформаційної безпеки [18], вище вказані компоненти безпеки зазвичай вважаються ключовими та важливими і мають бути дотримані при будь-якій реалізації концепції нульової довіри. У свою чергу, компанія ManageEngine для впровадження ZTA та підвищення ефективності безпеки в організаціях запропонувала комплексний підхід [19]. Одним із ключових компонентів комплексного підходу ManageEngine вважає багатофакторну автентифікацію (Multi-Factor Authentication – MFA), що надає додатковий рівень перевірки ідентифікації. Це значно ускладнює несанкціонований доступ навіть у разі компрометації облікових даних, наприклад, через фішингові атаки. MFA має застосовуватися для різних операційних систем (Windows, macOS, Linux), VPN-сервісів (Fortinet, Cisco AnyConnect, Pulse, OpenVPN) та кінцевих точок із підтримкою RADIUS (Citrix Gateway, VMware Horizon, Microsoft RDP). Як додаткові фактори при автентифікації можна використовувати відбитки пальців, розпізнавання обличчя, а також застосунки на кшталт Microsoft Authenticator, Google Authenticator, Duo Security або YubiKey Authenticator. Однак, з огляду на зростаючі вимоги до безпеки та зручності, сучасні підходи до автентифікації спрямовані на мінімізацію залежності від традиційних паролів. У цьому контексті безпарольна автентифікація, що реалізована через відкриті стандарти (OAuth, OpenID Connect, SAML), дозволяє значно знизити ризики, пов’язані з крадіжкою паролів, а механізм єдиного входу

(Single Sign-On – SSO) забезпечує централізований доступ до множини ресурсів без необхідності повторного введення облікових даних. Іншим важливим елементом ZTA в рамках комплексного рішення від ManageEngine є реалізація широко відомого принципу найменших привілеїв, який полягає у наданні користувачам доступу лише до тих ресурсів, які необхідні для виконання їхніх завдань. Це зменшує ризик витоку інформації у разі компрометації облікового запису. Реалізація цього принципу передбачає автоматизоване керування дозволами, створення шаблонів для нових співробітників на основі їхніх посадових обов'язків і тимчасове надання доступу до певних ресурсів. У рішеннях UEBA, запропонованих тією ж компанією ManageEngine, аномальна поведінка користувача виявляється шляхом аналізу шаблонів та відхилень від нормальної поведінки (наприклад, спроби несанкціонованого доступу чи передачі даних). При цьому інтеграція UEBA з уніфікованим рішенням SIEM (Security Information and Event Management – система керування інформацією та подіями безпеки) дозволяє автоматизувати аналіз загроз, систематизувати події за ступенем ризику та забезпечувати реагування в режимі реального часу шляхом надсилання сповіщень командам безпеки.

Таким чином, концепція нульової довіри є сучасним підходом до кібербезпеки, який забезпечує комплексний захист даних через постійний моніторинг, керування доступом та швидке реагування на загрози. При цьому слід зазначити, що дана концепція продовжує еволюціонувати, оскільки постачальники та організації зі стандартизації постійно оновлюють і вдосконалюють її специфікації та реалізації, визнаючи її кардинальною зміною в підході до кібербезпеки [5, 18]. Тому, з огляду на зростаючу складність атак, природно, як окремі традиційні методи кібербезпеки, так і комплексний захист, заснований на концепції нульової довіри, повинні доповнюватися інноваційними технологіями, зокрема ШІ, які здатні допомогти організаціям забезпечити постійний моніторинг систем і швидке реагування на нові загрози. Таким чином, концепція нульової довіри в поєднанні з можливостями ШІ, може стати не лише технологічним рішенням, але й стратегічним підходом, що дозволить організаціям ефективно протистояти сучасним кіберзагрозам, забезпечуючи безпеку даних на всіх етапах їх обробки, передачі та зберігання.

2. Напрями застосування штучного інтелекту в рамках концепції нульової довіри

З розвитком ШІ еволюціонують і ризики. Широка доступність таких інструментів, як ChatGPT, Google Gemini та інших, надала зловмисникам можливість швидко підвищувати складність кібератак. Тому фахівці з безпеки повинні активно та оперативно впроваджувати сучасні підходи та стратегії для захисту ресурсів підприємств від подібних загроз. Для боротьби зі зловмисниками та програмами генеративного ШІ дуже важливо, щоб розробка, вдосконалення та впровадження надійних засобів захисту здійснювалися постійно.

Найпоширенішою сферою застосування технологій ШІ з метою захисту інформації є автоматизовані та інформаційні системи, включно з комп'ютерними мережами різної архітектури. До основних завдань захисту інформації з використанням ШІ можна віднести:

- виявлення та запобігання витокам конфіденційних даних;
- виявлення кібератак та шкідливих програм;
- виявлення модифікованих даних або повідомлень;
- підвищення надійності та кіберстійкості систем, сервісів і мереж;
- оцінка ризиків кібербезпеки.

Недоліки традиційних систем безпеки багато в чому пов'язані з тим, що вони засновані на статичних правилах. Тобто, використовуються заздалегідь визначені методи виявлення загроз і реагування на них. Це тягне за собою обмеження, зокрема нездатність реагувати на нові загрози, оскільки з появою нових загроз правила повинні оновлюватися вручну. Іншим обмеженням є обсяг даних. Наявні системи безпеки можуть генерувати великі обсяги даних, які складно аналізувати в реальному часі. Крім того, системи, засновані на статичних правилах, можуть виявитися неефективними під час виявлення складніших атак, наприклад тих, що використовують ШІ для імітації звичайної поведінки користувача.

Можливість швидкої обробки великих масивів даних для завчасного реагування – це одна з ключових переваг ШІ. За допомогою ШІ можна в режимі реального часу аналізувати великі обсяги інформації, насамперед мережевого трафіку, виявляти аномалії та незвичні активності. ШІ може аналізувати дані з декількох джерел, включно з мережевим трафіком та системними журналами, для виявлення подій, що виходять за рамки норми. При виявленні кібератак або шкідливих програм основним сценарієм застосування технології ШІ може бути визначення аномалій у поведінкових моделях користувачів інформаційних систем. Наприклад, ШІ може виявити незвичні моделі поведінки або аномалії, які можуть вказувати на кібератаку, зокрема, передачу великих обсягів даних у зовнішню мережу, нестандартні спроби входу в систему, дії пов'язані з внутрішніми загрозами (доступ співробітників до даних у неробочий час або отримання доступ до даних, до яких зазвичай немає дозволу).

Застосування ШІ в рамках ZTA є перспективним напрямком у галузі кібербезпеки, що дозволить підвищити рівень захисту корпоративних систем від сучасних загроз. Модель нульової довіри виходить з того, що жоден користувач або пристрій не повинні отримувати автоматичну довіру – навіть якщо вони знаходяться всередині корпоративної мережі. В такому середовищі ШІ може відіграти ключову роль, допомагаючи автоматизувати процеси моніторингу, виявлення загроз і своєчасного реагування. Наприклад, якщо система ШІ виявляє спробу кібератаки, вона може автоматично заблокувати доступ до скомпрометованої системи, запобігаючи подальшим ризикам, а також надсилати сповіщення адміністраторам безпеки, надаючи їм інформацію про інцидент.

На рис. 3 показано основні логічні компоненти ZTA, які можуть загалом використовувати алгоритми ШІ, зокрема: механізм політики, точка застосування політики (PEP) та деякі зовнішні компоненти.

Рис. 3. Логічні компоненти ZTA, які можуть використовувати алгоритми ШІ

2.1. Механізм політики

Механізм політики є ключовим компонентом ZTA, оскільки відповідає за остаточне ухвалення рішень щодо надання або обмеження доступу до ресурсів. Він використовує політики підприємства, а також інформацію із зовнішніх джерел (наприклад, системи CDM, служби аналізу загроз тощо) як вхідні дані для алгоритму довіри для надання, заборони або скасовування доступу до ресурсу. Для прийняття рішень механізм політики використовує алгоритм довіри, який враховує різні джерела даних, такі як роль користувача, інформацію про поведінку, дані про ресурс (наприклад, тип операційної системи, рівень виправлень/оновлень), а також контекстні атрибути (час, місцезнаходження тощо). На основі цих даних алгоритм обчислює рівень довіри до суб'єкта та визначає, чи можна надати доступ до ресурсу, обмежити його або повністю заборонити [17].

Алгоритм довіри може бути реалізований у різний спосіб. Наприклад, у підході, заснованому на критеріях, доступ надається лише у випадку, якщо всі встановлені умови виконані. Ці умови можуть включати вимоги до автентифікації, параметри безпеки ресурсу тощо. Інший підхід, заснований на оцінках, передбачає розрахунок рівня довіри шляхом аналізу

значень різних атрибутів з урахуванням їх вагових коефіцієнтів. Якщо отримана оцінка перевищує порогове значення, доступ надається; у протилежному випадку запит відхиляється або рівень доступу обмежується. Крім того, алгоритми довіри можуть бути сингулярними або контекстними. Сингулярний підхід не враховує історичну інформацію про користувача, що дозволяє пришвидшити процес прийняття рішень, але може знизити ефективність виявлення аномалій або зловмисних дій. Навпаки, контекстний підхід аналізує історичні моделі поведінки користувача, що дозволяє виявляти нетипові дії та потенційні загрози. Наприклад, якщо користувач раптово намагається отримати доступ до ресурсу з нового місцезнаходження або в незвичний час, система може ініціювати додаткові перевірки або повністю заблокувати доступ.

Таким чином, механізм політики та алгоритм довіри в ZTA забезпечує гнучкий та адаптивний підхід до контролю доступу, що дозволяє ефективно реагувати на зміни в поведінці користувачів та наявні загрози. Автоматизація цього процесу є складним завданням, проте її реалізація, насамперед із використанням можливостей ШІ, значно підвищує ефективність політик безпеки та забезпечує надійний захист критичних ресурсів. ШІ здатен здійснювати постійний аналіз та оцінку рівня довіри до користувачів і пристроїв у корпоративному середовищі. В свою чергу, використання передових методів машинного навчання, таких як алгоритми кластеризації, дозволяє більш ефективно оцінювати рівень довіри та адаптивно регулювати доступ до ресурсів. Дослідники [20] проаналізували умови, за яких алгоритми оцінки довіри на основі машинного навчання можуть підвищити надійність пристроїв у розподіленій системі. У цій роботі вони виконали комплексний аналіз сучасних підходів до оцінки довіри, виділили ключові вимоги, яким повинні відповідати такі методи, та розробили критерії оцінки їх ефективності. Вони також класифікували існуючі підходи за сценаріями застосування, розглянувши широкий спектр методів машинного навчання, що використовуються для оцінки довіри у різних галузях, включно з багатокомпонентними системами, сервісами та мережами. Як результат, автоматизація процесів та інтеграція механізмів ШІ та машинного навчання в алгоритми оцінки довіри, незважаючи на свою складність, стає ключовим фактором підвищення ефективності механізму політики в рамках ZTA та відкриває нові можливості для створення більш надійних та адаптивних систем контролю доступу.

2.2. Точка застосування політики

PEP є ключовим компонентом ZTA, відповідальним за підключення, моніторинг та завершення з'єднань між суб'єктом та корпоративним ресурсом [17]. Усі комунікації, що проходять через PEP, контролюються відповідно до встановлених політик безпеки, що забезпечує динамічне управління доступом. Одним із ключових аспектів роботи PEP є контроль доступу, що є одним з основних механізмів захисту в рамках ZTA. Традиційні механізми контролю доступу обмежують дії користувача або застосунку всередині мережі, однак з появою, наприклад, технології 5G та IoT, кількість інтелектуальних пристроїв, що під'єднуються до мережі, зростає, що призводить до розширення поняття контролю доступу. Зараз контроль доступу більше не обмежується лише регулюванням доступу до даних для користувачів і застосунків. В архітектурі ZTA контроль доступу переосмислюється таким чином, що лише автентифіковані та авторизовані суб'єкти можуть отримати доступ до системи (можливе динамічне надання або відкликання доступу). Суб'єктами виступають як користувачі, так і застосунки (або сервіси) або їх комбінації з пристроїв, серверів, сервісів, застосунків тощо. Тоді як система може являти собою пристрій, такий як ноутбук, мобільний телефон, віртуальна машина, контейнер тощо [17].

Основними моделями контролю доступу, які використовуються в ZTA, вважаються моделі контролю доступу на основі ролей (Role-based Access Control – RBAC) та атрибутів (Attribute-based Access Control – ABAC) [18]. Їх використання дає змогу автоматично призначати ролі та дозволи користувачам на основі їх статичних і динамічних атрибутів для більш детального та гнучкого контролю доступу. Статичні атрибути можуть містити ідентифікато-

ри користувача або пристрою, тоді як динамічні атрибути охоплюють такі фактори, як час та місце запиту на доступ.

Однак, слід зауважити, що концепція нульової довіри не визначає RBAC як кращу методологію керування доступом [9]. Моделі контролю доступу на основі ролей вимагають постійного ручного втручання при створенні, видаленні та керуванні ролями, що створює труднощі в масштабованості та адаптації системи до змін в організаційній структурі. Статичні ролі, в свою чергу, можуть не відповідати поточним потребам користувачів, що призводить до надмірного або недостатнього доступу. Крім того, традиційні RBAC-рішення часто не враховують контекстні атрибути, що знижує ефективність управління доступом в динамічних середовищах. Тому необхідно застосовувати підходи, що забезпечують автоматизоване коригування ролей та дозволів відповідно до актуальних умов використання ресурсів. Одним із таких підходів є інтелектуальне призначення ролей на базі ШІ [21], що передбачає динамічний розподіл ролей користувачам на основі контекстних факторів, що покращує управління доступом і підвищує рівень безпеки. ШІ здатний аналізувати поведінку та історичну інформацію користувачів, щоб пропонувати відповідні призначення ролей, а також визначати ролі з високим рівнем ризику та небезпечні комбінації ролей. Подібна адаптивна система на основі ШІ може виявляти закономірності між користувачами зі схожими посадовими обов'язками, що сприяє більш точному та обґрунтованому призначенню ролей, також автоматично оцінювати сценарії використання ролей, виявляти надмірні або конфліктні права доступу та пропонувати оптимальні зміни для їх коригування. Це дозволяє організаціям зменшити ризики, пов'язані з надмірними дозволами, що можуть спричинити витік даних або несанкціонований доступ, а також забезпечити не лише підвищення рівня безпеки, але й зменшити адміністративне навантаження на систему контролю доступом.

З іншого боку, формально, роль можна розглядати як особливий вид атрибута, і тому ABAC можна трактувати як підмножину RBAC. Насправді, як стверджують фахівці [18], архітектури нульової довіри – це найбільш ефективний спосіб керування доступом на основі атрибутів.

Застосування ШІ також є перспективним напрямом і в системі керування привілейованим доступом (Privileged Access Management – PAM). Алгоритми ШІ здатні аналізувати та навчатися на основі шаблонів входу привілейованих користувачів [22], встановлюючи базовий рівень стандартної поведінки та виявляючи аномалії, що може свідчити про потенційні загрози безпеці. Однією з ключових переваг використання ШІ в PAM є можливість прогнозування, тобто аналізуючи історичні дані та виявляючи закономірності, він може передбачати ймовірні загрози ще до їх реалізації, що дозволяє організаціям завчасно вживати заходи для усунення потенційних загроз. У межах системи PAM, ШІ може удосконалювати механізми надання та відкликання привілейованого доступу, забезпечуючи обґрунтованість, відповідність політикам безпеки та мінімізуючи ризики несанкціонованого використання. Додатково ефективні рішення системи PAM повинні містити оцінку ризиків на основі поведінкових факторів та історичної інформації кожного користувача, а інтеграція ШІ з механізмами моніторингу користувачів може своєчасно виявляти аномальні шаблони поведінки та потенційні загрози безпеці, підвищуючи ефективність управління привілейованим доступом.

Підходи, що базуються на алгоритмах ШІ, можуть значно скоротити час і підвищити точність призначення прав доступу порівняно з традиційними ручними методами, що є важливим кроком у забезпеченні більш ефективної та адаптивної безпеки в рамках ZTA.

2.3. Зовнішні компоненти

Окрім основних компонентів на підприємстві, важливу роль у реалізації ZTA відіграють зовнішні компоненти, які забезпечують організацію додатковою інформацією для ухвалення рішень щодо безпеки. Використання можливостей ШІ у цих системах дозволяє автоматизувати аналіз великих обсягів даних, виявляти аномалії, прогнозувати потенційні загрози та

адаптивно коригувати політики доступу, що підвищує ефективність контролю та забезпечує проактивний підхід до кібербезпеки.

2.3.1. Керування ідентифікацією

Керування ідентифікацією є ключовою компонентою ZTA, забезпечуючи точну автентифікацію та авторизацію користувачів і пристроїв для доступу до ресурсів організації. Тому, враховуючи важливість точної автентифікації ZTA, доцільним є впровадження MFA, через те, що вона додає додаткові рівні перевірки. Окрім базового методу автентифікації (наприклад, пароля), MFA передбачає використання одноразового пароля (One Time Password – OTP), що генерується на основі часу в мобільному пристрої користувача або надсилається на електронну пошту чи в SMS повідомленні [23]. Крім того, MFA включає різні додаткові принципи автентифікації, які застосовуються до процесу входу в систему, дозволяючи перевірити користувача через кілька незалежних каналів і підтвердити його особу за допомогою додаткових атрибутів. У зв'язку з цим, у межах ZTA реалізується багаторівневий підхід до керування ідентифікацією, що включає як біометричну автентифікацію, так і автентифікацію на фізичному рівні.

Біометричні характеристики людини, такі як голос, райдужна оболонка ока чи відбитки пальців, є унікальними для кожної особи [24]. Застосування же технологій ШІ при автентифікації за допомогою голосу дозволяє підвищити її точність, зокрема шляхом навчання системи розрізняти голоси окремих осіб і мінімізувати ризики при спробах його підробки. При цьому машинне навчання забезпечує обробку великих обсягів даних та здатність адаптуватися до змін навколишнього середовища, що включає виявлення специфічних мовних особливостей, таких як акцент або емоційні варіації в голосі [25]. Аналогічно, при автентифікації за допомогою розпізнавання обличчя або райдужної оболонки ока технології ШІ порівнюють зібрані біометричні дані з базами даних для визначення відповідності. Відмінності в структурі обличчя чи райдужної оболонки є унікальними для кожної особи, що робить ці методи високоточними для ідентифікації. Завдяки можливостям ШІ, подібні системи можуть точно визначати відмінності в цих характеристиках навіть за умов поганої освітленості чи змін у зовнішньому вигляді користувача. Це дозволяє ефективно використовувати такі методи в системах безпеки, де вони можуть замінювати традиційні способи доступу, такі як пропуски чи паролі, знижуючи ймовірність несанкціонованого доступу та підвищуючи рівень захисту [26].

Однак традиційні методи біометричної автентифікації, що базуються на поверхневих ознаках, поступово втрачають ефективність. Це пояснюється тим, що такі характеристики, як відбитки пальців, можуть бути легко викрадені або підроблені. У зв'язку з цим увага дослідників усе більше зосереджується на використанні біометричних даних, що відображають внутрішні характеристики організму, які важче підробити або скопіювати. Такі дані можуть бути зібрані за допомогою сучасних носимих смарт-пристроїв, однак ключовим викликом залишається ефективна класифікація та ідентифікація цих даних. Методи ШІ є перспективним рішенням цієї проблеми. Вони дозволяють автоматично обробляти дані, отримані від носимих пристроїв, і використовувати їх для ідентифікації особи. Зокрема, у роботі [27] проаналізовано застосування алгоритмів машинного навчання для забезпечення постійної (безперервної) багатофакторної автентифікації, що включає кілька біометричних ознак. Для автоматизованої ідентифікації користувачів зібрані біометричні характеристики спочатку перетворюються у числовий формат і класифікуються за допомогою алгоритмів машинного навчання під наглядом, таких як алгоритм KNN або дерева рішень. Ці методи надалі використовуються для побудови моделей автентифікації. Разом з тим, глибокі нейронні мережі, такі як згорткові нейронні мережі (Convolutional Neural Networks – CNN), дозволяють автоматично виділяти та навчатися на біометричних характеристиках користувача, які отримуються від біометричних пристроїв моніторингу, що значно підвищує точність та надійність ідентифікації. Крім того, для вирішення проблем, пов'язаних із недостатнім обсягом біометричних даних, застосовуються підходи глибокого передавального навчання (Deep Transfer Learning –

DTL). Такі методи дозволяють використовувати попередньо навчені моделі для адаптації до нових даних, забезпечуючи високу продуктивність навіть у разі обмежених ресурсів для навчання.

Інший підхід, пов'язаний з безперервною автентифікацією, спрямований на забезпечення постійного підтвердження ідентичності кінцевих точок протягом усього сеансу зв'язку. Для його реалізації перспективним вважається метод використання автентифікації на рівні пристроїв на основі фізичного рівня (Physical Layer Authentication – PLA), де алгоритми ШІ дозволяють ефективно виділяти характеристики пристроїв із комунікаційних каналів і безперервно перевіряти ідентичність як користувачів, так і пристроїв [28]. Дослідження [29] містить детальний огляд сучасних технологій на основі PLA. Автори підкреслюють, що традиційні криптографічні методи автентифікації мають низку суттєвих обмежень, таких як низька сумісність, ненадійність і висока складність впровадження. Тому у цьому контексті вони вважають, що PLA на основі пристроїв виступає перспективним доповненням, оскільки такий метод дозволяє використовувати унікальні фізичні властивості середовища та пристроїв.

Однак порівняно з властивостями пристроїв, характеристики каналу зв'язку є значно складнішими для копіювання або імітації, що забезпечує вищий рівень безпеки при автентифікації пристроїв. Виділення характеристик каналу здійснюється на основі комунікаційного потоку між пристроями, і їх ручна класифікація є практично неможливою через значний обсяг і складність даних. Для вирішення цієї проблеми у межах ZTA перспективним рішенням було б застосування технологій ШІ та машинного навчання, які можуть автоматично аналізувати характеристики каналів зв'язку, ідентифікувати пристрої та значно підвищувати ефективність і точність їх автентифікації.

2.3.2. Журнали активності

ZTA потребує постійного моніторингу всіх дій користувачів, пристроїв та сервісів. Навіть після успішної автентифікації користувачів або пристроїв необхідно відстежувати їхню поведінку для виявлення аномалій та потенційних загроз. Це дозволяє ідентифікувати підозрілі дії легітимних користувачів або скомпрометованих пристроїв. У цьому контексті журнали активностей відіграють ключову роль у забезпеченні безпеки, оскільки дозволяють аналізувати поведінку (маючи зворотний зв'язок про роботу системних компонентів та користувачів), вчасно ідентифікувати аномальну активність при отриманні доступу до сервісу та оперативно реагувати на загрози. Журнали зазвичай реєструють роботу системи у вигляді часових послідовностей. І в цьому зв'язку методи аналізу журналів активності, засновані на контрольованому навчанні (supervised learning) можуть дуже допомогти в автоматизації при визначенні аномальних ознак в подібних часових рядах. Наприклад, модель Deeplog [30] фокусується на аналізі виявлених аномалій в файлах журналів. Проте Wang Y. M. та Ji Z. X. [31] зазначили, що продуктивність Deeplog є незадовільною, тому вони провели її оптимізацію та, використовуючи алгоритм виявлення відхилень, запропонували напівконтрольовану модель для виявлення аномалій. Однак методи машинного навчання, що покладаються на мітки, не задовольняють вимогам систем виявлення аномалій у реальному часі, оскільки процес маркування даних є трудомістким. Для вирішення цієї проблеми доцільно застосовувати неконтрольовані методи аналізу журналів [32], які можуть ефективно виявляти аномалії без необхідності визначати явні ознаки, скорочувати час навчання та підвищувати ефективність обробки даних. На рис. 4 представлено схему моделі неконтрольованого аналізу журналів.

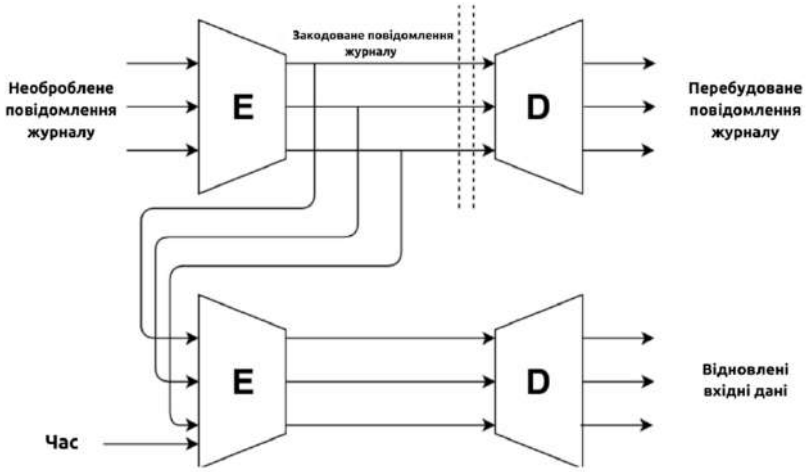


Рис. 4. Схема моделі неконтрольованого аналізу журналів

Дана модель визначає початковий автокодувальник **E**, що вставляє повідомлення журналу, тренується на тексті журналу (без позначки часу), щоб навчитися додавати повідомлення журналу фіксованої розмірності. Після навчання дешифратор **D** відкидається, після чого автокодувальник **E** для виявлення аномалій навчається на основі вкладених повідомлень та числової часової мітки повідомлення. Далі обчислюється міра відстані між входами та виходами, і вхід вважається аномальним, якщо його міра відстані перевищує відповідним чином вибраний поріг. Головна інновація цієї роботи полягає в тому, що модель не накладає вимог на структуру повідомлень журналу і не вимагає попередньої обробки повідомлень журналу, що забезпечує гнучкість до будь-якого типу журналів.

В цілому ж, застосування неконтрольованих методів при аналізі журналів активності дозволяє ефективно виявляти аномалії без потреби в маркуванні даних, що є суттєвою перевагою для систем, які працюють в режимі реального часу. Проте ці методи не завжди здатні забезпечити повну оцінку потенційних загроз, що виникають у результаті аномальної активності. З огляду на це, для підвищення точності оцінки загроз доцільно поєднувати методи аналізу журналів активності з механізмом постійного моніторингу, який дозволяє відстежувати доступ до ресурсів, виявляти потенційні загрози з боку вже авторизованих суб'єктів і тим самим запобігати їхнім протиправним діям. У цьому сенсі ШІ може сприяти підвищенню ефективності цього процесу. А саме, ШІ забезпечує можливість безперервного моніторингу, що дозволяє адаптивно контролювати доступ на основі поведінки користувачів та пристроїв. Це сприяє створенню більш динамічного та безпечного середовища контролю доступом. Завдяки аналізу активності, системи на базі ШІ спроможні виявляти аномальну або потенційно небезпечну поведінку, що може свідчити про несанкціонований доступ чи компрометацію облікових записів. При цьому слід мати на увазі, що поведінка користувачів, яка, в тому числі, може бути об'єднана в деякі групи, може змінюватись в залежності від конкретних умов, що створює нові виклики у виявленні аномалій. Тому для вирішення цієї проблеми у свій час був запропонований раніше згаданий метод кластеризації [33], заснований на аналізі траєкторій поведінки користувачів у програмному середовищі, в якому дані про доступ та операції користувачів у матриці траєкторій підлягають відповідній трансформації, в результаті якої визначається подібність поведінки. З метою покращення точності виявлення аномалій у поведінці користувачів та пристроїв в системах, що здійснюють моніторинг, можуть ефективно використовуватись алгоритми глибокого навчання (Deep Learning – DL). Наприклад, алгоритми DL, такі як мережі на основі довгої короткочасної пам'яті (Long short-term memory – LSTM) [34], що дозволяють ефективно виокремлювати часові ознаки в поведінці користувачів і пристроїв, запропонований авторами роботи [35] метод виявлення аномалій у мережевій поведінці користувачів, який базується на гібридному алгоритмі машинного навчання, або модель виявлення аномальної поведінки користувачів, яка використовує

LSTM для моделювання шаблонів поведінки в рамках активності користувачів, зокрема під час їх комунікації з сервісами та ресурсами [36]. Також може бути використана вдосконалена модель виявлення загроз, яка базується на використанні двонаправленої мережі LSTM (Bi-LSTM) для більш ефективного вибору ознак, а також метод опорних векторів (Support Vector Machine – SVM) для класифікації поведінки користувачів на звичайну (normal) або зловмисну (malicious) [37].

Однак навіть за умов високої точності в аналізі поведінки користувачів та пристроїв, самостійне функціонування таких систем не гарантує комплексного керування загрозами без належної класифікації та централізованого керування виявленими інцидентами. Більше того, у разі ідентифікації аномалій вони не завжди автоматично корелюються з іншими подіями безпеки, що ускладнює формування загальної картини загроз. Відсутність своєчасного сповіщення адміністраторів безпеки або невчасне застосування контрзаходів може призвести до негативних наслідків для інформаційної інфраструктури організації. Для вирішення цих проблем важливим є інтеграція систем моніторингу користувачів та пристроїв із зовнішніми компонентами архітектури нульової довіри, зокрема з SIEM.

2.3.3. SIEM

Автоматизована SIEM (*SIEM* – це область комп'ютерної безпеки, в якій програмні продукти та послуги поєднують у собі управління інформацією про безпеку (*SIM – security information management*) та управління подіями безпеки (*SEM – security event management*)) є ефективним рішенням проблеми автоматичного виявлення аномалій або загроз у поведінці не тільки користувачів, а й пристроїв. Дане рішення може забезпечити ефективну класифікацію та управління цими подіями безпеки. Більше того, при виявленні подій безпеки відбувається автоматичне попередження адміністратора з безпеки для вживання контрзаходів.

Однак існуючі системи SIEM мають недоліки через обмеженість в аналізі великих обсягів даних [38]. Тому до таких систем доцільно впроваджувати технології машинного навчання.

Наприклад, автори роботи [39] впровадили технології машинного навчання в SIEM і довели можливість ефективного аналізу великих об'ємів даних у цій системі. В інший роботі [40] автори зосередилися на поєднанні даних з різних джерел для вдосконалення SIEM та застосували моделі виявлення вторгнень на основі нейронних мереж (рис. 5).

Рис. 5. Система розпізнавання на основі SVM-нейромережі

Запропонована система використовувала набір даних NSL-KDD (Network Security Layer-Knowledge Discovery Database) як вхідний набір даних, де перший шар моделі використовував нейронні мережі для класифікації системних подій на зловмисні та звичайні, а другий шар використовував метод SVM для підвищення продуктивності класифікації. У рамках даного дослідження визначено низку параметрів, які мають суттєвий вплив на продуктивність нейронних мереж у завданнях виявлення вторгнень. До таких параметрів належить кількість обраних ознак або атрибутів, які визначають обсяг вхідних даних і можуть значно впливати на точність класифікації. Важливим фактором є нормалізація даних, яка забезпечує уніфікацію масштабу вхідних параметрів, сприяючи кращій збіжності алгоритму, а також характеристики архітектури нейронної мережі, зокрема кількість вузлів у прихованому шарі, що визначає складність і здатність моделі до узагальнення. Крім того, важливо враховувати вибір функції активації, яка впливає на нелінійність мережі, а також параметри швидкості

навчання та моменту часу, що оптимізують процес збіжності. Ці аспекти визначають ефективність роботи моделі та її здатність до адаптації в умовах варіативності вхідних даних. Для перевірки цих припущень у роботі [40] було реалізовано 37 нейронних мереж прямого поширення (Feed-Forward Neural Networks – FFNN) з використанням різних алгоритмів навчання та функцій вартості, а отримані результати підтвердили критичну важливість цих параметрів для досягнення високої точності. Зокрема, встановлено, що вибір відповідної функції вартості дозволяє підвищити точність алгоритму *traingd* (алгоритм оберненого градієнтного спуску для навчання нейронної мережі) на 17,74 %. Аналіз набору даних NSL-KDD показав, що алгоритм *trainrp* (алгоритм стійкого оберненого поширення для навчання нейронної мережі) демонструє швидшу збіжність та вищу точність класифікації порівняно з іншими методами навчання. Крім того, точність *trainrp* виявилася співставною, а подекуди й вищою, ніж у більш складних моделей на основі нейронних мереж, що підкреслює його потенціал для покращення ефективності та швидкості класифікації вторгнень.

У роботі [41] був розроблений набір інструментів для автоматичної класифікації подій на основі машинного навчання, за допомогою якого проводилися експерименти з різними алгоритмами машинного навчання на декількох наборах даних, з метою – знайти найбільш ефективну модель класифікації даних. Результати проведених тестів показали, що метод опорних векторів (SVM) досяг найкращого показнику ефективності на наборі даних *TippingPoint* (набір IP-адрес та DNS-імен, які представляють потенційні ризики для мережевої безпеки) і становив 95,08 %.

Певні автоматизовані рішення SIEM активно застосовуються у різних практичних сценаріях, зокрема, в критичній інфраструктурі. Наприклад, Hindy H. та інші [42] розробили SIEM для виявлення аномальних подій у системі водопостачання, що контролюється системою SCADA (Supervisory Control And Data Acquisition). Використовуючи машинне навчання, дослідники класифікували дані про атаки на 14 різних сценаріях, які автоматично повідомлялися операторам служби безпеки. Представлені експериментальні сценарії охоплювали широкий спектр подій, від відмов обладнання до саботажу, й містили три дослідження із застосуванням шести методів машинного навчання. У першому експерименті оператору повідомлялася лише наявність аномалії у вигляді двійкового результату, без деталізації її типу. Другий експеримент уточнював пошкоджений компонент, надаючи інформацію про дані одного або кількох датчиків. Третій експеримент, що забезпечив найвищу ефективність, деталізував аномалію до рівня конкретного сценарію, дозволяючи операторам вживати коригувальних заходів. Загальна точність досягала 94 % для двійкової класифікації та 95,64 % для визначення сценаріїв, причому алгоритми класифікації KNN (K-Nearest Neighbors Algorithm), Decision Trees і Random Forests перевершили Gaussian Naive Bayes і SVM. Алгоритм KNN показав найвищу точність виявлення аномалій та ідентифікації конкретних сценаріїв атак у всіх експериментах. Результати підтвердили важливість використання рівня довіри для підвищення інформативності повідомлень, а також актуальність збільшення обсягу даних і побудови гібридних моделей для оптимізації класифікації подій і сценаріїв. Хоча запропонована модель прискорювала реагування на мережеві атаки, автори зазначили її обмеження у виявленні нових сценаріїв загроз.

Попри високу точність класифікації подій в системах критичної інфраструктури, важливим викликом залишається ефективна обробка сповіщень у масштабних системах безпеки. Дослідження Feng C. та інших [43] акцентує увагу на проблемі високої частоти хибних сповіщень у наявних SIEM, що значно перевищує можливості обробки операційними центрами безпеки (Security Operation Center – SOC). Для її розв’язання запропоновано систему, яка завдяки алгоритмам машинного навчання суттєво знижувала частоту хибних спрацьовувань, підвищуючи ефективність реагування на загрози. Сильною стороною таких підходів є здатність навчатися як на попередніх, так і на поточних даних для прогнозування майбутніх інцидентів безпеки, що може допомогти аналітикам швидше ідентифікувати та реагувати на загрози.

Досягнення досліджень в області аналітики та машинного навчання для SIEM знайшли своє продовження в сучасних системах безпеки для оркестрації, автоматизації та реагування (Security Orchestration, Automation, and Response – SOAR). SOAR-системи у поєднанні зі ШІ та машинним навчанням, демонструють значний потенціал у виявленні, пом'якшенні та запобіганні кіберзагрозам. Постачальники даних інструментів інтегрують алгоритми ШІ та машинного навчання для підвищення ефективності роботи аналітиків SOC [44]. Водночас виникають питання ефективності алгоритмів класифікації та визначення пріоритетності інцидентів, а також необхідність подальших досліджень щодо впровадження глибокого посиленого навчання (Deep Reinforced Learning – DRL) у SOAR-системи. Для вирішення даної проблеми використовують нові моделі інтерпретовного ШІ (Explainable Artificial Intelligence – XAI), які забезпечують зрозумілість та прозорість у поясненні результатів прогнозування. Зокрема, XAI дозволяє аналітикам безпеки виявляти помилкові прогнози шляхом оцінки надійності результатів. Це значно зменшує кількість хибних спрацьовувань і підвищує ефективність роботи SOC, оскільки аналітики отримують змогу швидше та точніше реагувати на реальні загрози [45].

В цілому ж, можна помітити, що сучасні виклики, пов'язані зі складністю виявлення та нейтралізації кіберзагроз, вимагають комплексного підходу. Зокрема, для ефективного функціонування SOC необхідна інтеграція алгоритмів машинного навчання на всіх етапах роботи – від збору та обробки даних до аналізу загроз і управління інформаційною безпекою. Наприклад, для цього у роботі [46] пропонується багаторівнева модель SOC, яка включає збір даних, їх обробку, застосування алгоритмів машинного навчання для аналізу загроз та використання інформаційних панелей для прийняття рішень. Серед алгоритмів машинного навчання дослідники пропонують використовувати як контрольовані алгоритми (SVM, дерева рішень), так і неконтрольовані (кластеризація KNN). В іншої роботі [47] автори запропонували впровадити інструменти на основі ШІ для диференціації загроз і зменшення втоми від численних сигналів зі сповіщеннями безпеки для аналітиків SOC. Також, вони акцентували увагу на необхідності використання алгоритмів SVM для аналізу попередніх даних та оцінки рівня загроз.

Таким чином, інтеграція ШІ та машинного навчання, включно з підходами DRL, дозволяє автоматизувати рутинні процеси, одночасно підвищуючи ефективність безпеки. А всі згадані вище дослідження, що демонструють, як застосування алгоритмів ШІ та машинного навчання може сприяти підвищенню точності виявлення загроз та зниженню кількості помилкових спрацьовувань, зайвий раз підтверджують це та доводять доцільність використання можливостей ШІ в рамках ZTA.

2.3.4. Аналіз загроз

Інформаційний(і) канал(и) про загрози / система аналізу загроз (Threat Intelligence – TI) є одним із ключових елементів в рамках ZTA, що сприяє захищеності підприємства від зовнішніх і внутрішніх атак. Це інформація з внутрішніх або зовнішніх джерел, яка допомагає механізму політики приймати рішення про доступ. З огляду на це, основні техніки системи TI можна поділити на два основні напрямки: використання інформаційних каналів для отримання даних з різних джерел, і безпосередньо аналіз великих обсягів даних для виявлення аномалій. Перший напрямок включає використання служб, які збирають дані про нещодавно виявлені атаки, вразливості, шкідливе програмне забезпечення чи інші загрози з різних джерел. Другий напрямок зосереджений на аналізі даних у внутрішніх системах для виявлення аномальних дій, які можуть вказувати на потенційні атаки, що дозволяє своєчасно реагувати на підозрілі події та мінімізувати шкоду від кібератак.

Інформація, отримана завдяки TI, дозволяє не лише виявляти атаки та вразливості, а й прогнозувати їх розвиток та завчасно оцінювати потенційні ризики. Однак оскільки джерел такої інформації може існувати багато, виникає природна необхідність впровадження автоматизованих систем, у тому числі або насамперед, заснованих на використанні ШІ, здатних збирати дані TI та оцінювати їх достовірність. У зв'язку з цим, наприклад, у роботі [48] авто-

ри розглянули сучасні технології у сфері аналізу загроз та запропонували нову модель прогнозування загроз на основі функції оцінки ризику та вдосконаленого алгоритму апостеріорної ймовірності Баєса (Enhanced Naive Bayes Posterior Probability – ENBPP) з використанням машинного навчання. Запропонований ними алгоритм об'єднує модифіковану функцію ENBPP з адаптованою функцією оцінки ризику, що забезпечує підвищення точності прогнозування загроз та скорочення часу обробки. Для аналізу ефективності рішення вони використали п'ять різних наборів даних, які містили 328 814 зразків загроз. Отримані результати засвідчили про перевагу запропонованого підходу, оскільки точність прогнозування зросла до 92–96 %, а середній час обробки знизився з 0,043 до 0,028 секунди порівняно з альтернативними методами. Крім того, алгоритм продемонстрував здатність ефективно долати проблеми, пов'язані із залежністю від заздалегідь визначених шаблонів дій зловмисників і порогових значень у множинних сценаріях прогнозування. В цілому ж новий підхід здатний забезпечити більш надійний механізм аналізу та прогнозування загроз у різних сценаріях.

Хакерські форуми є також одним із ключових джерел даних для TI, про що свідчить, зокрема, дослідження, проведене в роботі [49], спрямоване на автоматизоване отримання відповідної інформації про кіберзагрози з хакерських форумів за допомогою гібридного процесу машинного навчання. Авторами [49] було розроблено дворівневий алгоритм, що поєднує метод SVM для фільтрації нерелевантних повідомлень та моделювання латентних/прихованих розподілів Дирихле (Latent Dirichlet Allocation – LDA) для кластеризації релевантних постів за відповідною тематикою. У межах експерименту проаналізовано мільйон постів із реального хакерського форуму, що дозволило ідентифікувати такі ключові загрози, як витік облікових даних, шкідливі проксі-сервери та програмне забезпечення. Результати продемонстрували ефективність методу, оскільки використання SVM для відсіювання нерелевантних повідомлень зменшило обсяг даних для аналізу більш ніж на 90 %, що дозволило значно скоротити час обробки. Наприклад, середній час для моделювання тем за допомогою LDA знизився з 238 до 16 хвилин за умови обмеження словникового запасу до 50 000 слів. У сукупності тематичне моделювання дозволило виділити ключові теми, такі як обговорення скомпрометованих облікових записів, IP-адрес шкідливих проксі та програм, що робить цю методику цінним інструментом для виявлення оперативної інформації про загрози. А модель продемонструвала високу гнучкість у питанні налаштування параметрів, що дозволяє в майбутньому адаптувати її до різних типів даних і завдань. Крім того, варто зазначити, що в рамках даної системи важливим є участь людини-експерта для остаточної інтерпретації результатів даного тематичного моделювання, оскільки навіть найбільш досконалі алгоритми можуть не враховувати специфіку рідкісних або складних тем, наприклад, вразливості нульового дня. Але загалом, дана гібридна система є ефективним рішенням для швидкого вилучення важливої інформації, яка може бути доповнена до традиційних засобів захисту для підвищення їх ефективності.

Застосування сучасних методів для аналізу загроз на основі вдосконалених алгоритмів оцінки ризиків та автоматизованих систем обробки великих обсягів даних, сприяє покращенню виявлення та прогнозування потенційних атак. Однак ефективність таких підходів значною мірою залежить від якості вхідних даних, адаптивності моделей до нових типів загроз і можливості інтеграції результатів у комплексні системи кіберзахисту. Отже, можна зробити висновок, що потрібні додаткові дослідження у напрямку вдосконалення наявних підходів в аналізі загроз (і в першу чергу тих, що спираються на можливості ШІ), що дозволяють більш детально оцінити ризики для системи, визначити можливі вектори атак, встановити пріоритетність загроз та розробити відповідні заходи захисту або стратегії запобігання.

Таким чином, розглянуті дослідження та підходи до впровадження компонентів ZTA демонструють ключову роль машинного навчання та ШІ у забезпеченні концепції нульової довіри. Використання ШІ в основних і зовнішніх компонентах ZTA, таких як алгоритм довіри, контроль доступу, SIEM, керування ідентифікацією, журнали активності (в тому числі, моніторинг користувачів та пристроїв) та аналіз загроз, дозволяє автоматизувати аналіз ве-

ликих обсягів даних, виявляти аномалії та адаптивно реагувати на потенційні загрози. Алгоритми ШІ забезпечують постійний моніторинг, оптимізацію політик безпеки та скорочення часу реагування на інциденти, що значно підвищує ефективність захисту. Завдяки цьому модель ZTA у поєднанні з технологіями ШІ створює гнучку й надійну систему кібербезпеки, здатну протистояти сучасним загрозам у динамічному цифровому середовищі.

3. Виклики та подальший напрямок досліджень

З розвитком IoT, хмарних та інших інноваційних технологій, багато пристроїв можуть бути інтегровані до єдиної централізованої системи управління. Однак застаріла інфраструктура, програми, сервіси та інші елементи можуть не відповідати принципам нульової довіри, оскільки в них відсутні концепції мінімальних привілеїв, захисту від бічного переміщення, а також немає динамічної автентифікації. Через це застарілі системи залишаються вразливими до широкого спектра кіберзагроз. Можливим рішенням є додавання модуля для автентифікації до центральної системи управління з подальшим визначенням привілеїв. Хоча це рішення частково вирішує проблему застарілих систем, воно вимагає від суб'єкта прямого проходження через всю інфраструктуру, що порушує принцип мікросегментації, який є також основоположним у концепції ZTA. Такий підхід окреслює значні виклики для інтеграції застарілих систем у сучасні моделі безпеки, засновані на концепції нульової довіри, та вимагає подальших досліджень у напрямку адаптації існуючої інфраструктури до нових стандартів кіберзахисту.

З іншого боку, впровадження ZTA потребує поступового переходу, оскільки різкий перехід може викликати значні труднощі, зокрема збільшення кількості помилкових спрацювань, зниження продуктивності системи та опір з боку персоналу. Тобто впровадження ZTA потребує ретельного планування та має бути поетапним, з урахуванням особливостей підприємства, його бізнес-процесів, критичних активів та рівня кіберзагроз (при цьому з мінімальним негативним впливом на роботу підприємства). Особливо актуальним є питання адаптації персоналу до нових принципів роботи, зокрема шляхом розробки ефективних стратегій навчання та автоматизованих засобів підтримки прийняття рішень у процесі переходу. Крім того, перспективним напрямом є дослідження методів оцінки ефективності впровадження ZTA та розробка відповідних метричних показників, які дозволять об'єктивно аналізувати та оцінювати рівень захищеності підприємств.

Ще одним важливим викликом для ZTA є стандартизація даних. Інформація про загрози може надходити з різних джерел, проте на сьогодні в ZTA немає єдиного стандарту, який може бути використаний алгоритмами оцінки довіри. Це впливає на достовірність даних та фінальну оцінку ефективності, оскільки вхідні дані надаються різними джерелами, а відсутність уніфікованого формату для зібраних даних ускладнює використання відповідних алгоритмів. Важливим аспектом цієї проблеми, також є моніторинг мережевого трафіку та поведінки користувачів у системі, який значною мірою залежить від журналів активності, що надаються різними інструментами безпеки. Це вимагає від систем використовувати різні алгоритми оцінки довіри для адаптації до різних форматів даних. Такий підхід не лише ускладнює процес аналізу та оцінки, але й призводить до зниження продуктивності моделі оцінки довіри. Крім того, кожне джерело даних в ZTA має власні операційні політики та стандарти, що створює додаткові труднощі при автоматизації процесів. Відсутність єдиної політики, яка б регулювала взаємодію компонентів ZTA, зокрема, політики шифрування, специфікації коду тощо, ускладнює впровадження ефективних механізмів кібербезпеки.

Дані виклики підкреслюють необхідність в уніфікації підходів до обробки та стандартизації даних для забезпечення ефективної роботи в рамках моделі нульової довіри. Подальші дослідження доцільно було б направити, за можливістю, на створення єдиних стандартів, які б забезпечили узгодженість даних та процедур безпеки, що дозволило б підвищити ефективність, точність моделей оцінки та узгодженість процесів автоматизації безпеки в рамках ZTA.

ZTA в поєднанні з елементами ШІ має значні переваги в автоматизації процесів, однак покладатися виключно на рішення прийняті ШІ може бути ризиковано, оскільки можливі помилкові або упереджені висновки, що в результаті може призводити до хибних спрацьовувань або невиправданих відмов. У зв'язку з цим, важливим є інтеграція людського досвіду в процес ухвалення рішень. Включення людини до циклу (human-in-the-loop) допоможе знизити або усунути ризики, пов'язані з помилками ШІ. Наприклад, якщо система ZTA на базі ШІ неправомірно відмовляє в доступі легітимному користувачеві, експерт може переоцінити рішення та надати зворотний зв'язок, що дозволить підвищити точність спрацювань системи. В результаті, система зі ШІ буде навчатися на своїх помилках, а, отже, покращувати свою ефективність. Таким чином, використання підходу human-in-the-loop є перспективним напрямом для покращення точності і ефективності рішень ШІ в ZTA. Водночас, ефективність цього підходу значною мірою залежатиме від якості та доступності даних для навчання моделей ШІ, які, у свою чергу, значною мірою залежатимуть від великих наборів даних для навчання. При цьому, слід звернути увагу і на те, що скомпрометовані дані теж можуть серйозно вплинути на ефективність систем на базі ШІ.

Однією з потенційних загроз, як відомо, є атаки типу отруєння даних (data poisoning), коли шкідливі дані вводяться до навчальної вибірки для маніпулювання рішеннями системи, що призводить до некоректних результатів. Для мінімізації ризиків подібних атак необхідно впроваджувати надійні методи очищення даних та перевірки їх цілісності та якості, використовувати набори даних із різних джерел, а також застосовувати методи випадкової вибірки для зниження впливу потенційних загроз. Враховуючи, що якість рішень ШІ залежить від достовірності вхідних даних, важливим аспектом є також забезпечення коректної взаємодії між компонентами безпеки, що здійснюють збір та аналіз даних. У цьому контексті інтеграція систем SIEM та SOAR у ZTA постає як окремий виклик, де ключовою задачею є забезпечення узгодженості між автоматизованими процесами даних систем та принципами ZTA.

SIEM, як система збору й аналізу даних про події безпеки, часто стикається з проблемами уніфікації форматів даних, що ускладнює автоматичну кореляцію подій між різними джерелами. Це призводить до підвищення кількості хибних спрацювань та перевантаження аналітиків, особливо в умовах обробки великих обсягів різнорідної інформації. У свою чергу, SOAR забезпечує автоматизацію IR, але залежить від якості вхідних даних і сценаріїв, створених для обробки загроз. Недоліки у стандартизації та адаптації алгоритмів, які використовуються в цих системах, можуть знижувати точність та ефективність обробки інцидентів у реальному часі. Тому для подолання даних викликів доцільно було б певним чином стандартизувати дані, що надходять до SIEM, а також удосконалити механізми обробки даних, щоб забезпечити відповідність принципам нульової довіри. Наприклад, алгоритми аналізу подій мають бути адаптовані до динамічних політик доступу, характерних для ZTA, а процеси автоматизації SOAR повинні враховувати необхідність постійної перевірки довіри суб'єктів і пристроїв. Подальші дослідження можуть бути спрямовані на інтеграцію алгоритмів машинного навчання для оптимізації виявлення аномалій і мінімізації хибних спрацювань, а також на розробку єдиних протоколів обміну даними між системами SIEM, SOAR та компонентами ZTA. У зв'язку з цим, інтеграція SIEM та SOAR у рамках ZTA вимагає не лише технологічної адаптації, але й розробки уніфікованих стандартів для забезпечення узгодженості й ефективності.

Таким чином, використання можливостей ШІ в рамках ZTA для забезпечення кібербезпеки підприємств є актуальним питанням, але водночас вимагає подальших досліджень. Подальші дослідження мають бути спрямовані на створення надійної методології для впровадження ZTA та алгоритмів ШІ в її компоненти, розробку ефективних механізмів захисту від атак на моделі машинного навчання та стандартизацію обміну даними для підвищення узгодженості та ефективності кібербезпеки. Успішна реалізація даних підходів сприятиме розвитку надійних систем кібербезпеки, здатних реагувати на сучасні загрози в умовах постійної мінливості та динаміки загроз.

Висновки

1. Для забезпечення надійного захисту сучасного цифрового підприємства необхідна комплексна стратегія, концепція, яка забезпечує безпечний доступ до корпоративних ресурсів у будь-який час і в будь-якому місці. Враховуючи сучасні виклики, такою концепцією є парадигма безпеки «нульової довіри». Вона є ефективним підходом для захисту інформаційних систем від новітніх загроз, де кожен доступ має контролюватися та проходити верифікацію.

2. ШІ відіграє важливу роль у розвитку автоматизованих рішень для ZTA, зокрема в таких сферах, як виявлення атак, керування доступом, моніторинг, аналіз загроз тощо. Проте, незважаючи на значний прогрес у цій сфері, залишаються невирішеними питання щодо повної інтеграції ШІ в процес автоматизації для всіх компонентів ZTA. Як показують результати досліджень у цьому напрямі у світі лише в окремих логічних компонентах ZTA використовуються деякі методи автоматизації на основі можливостей ШІ. Насправді ж, механізми, що використовують ШІ для автоматизації процесів виявлення загроз та управління доступом у рамках ZTA, можуть істотно допомогти розробникам та спеціалістам з безпеки досягти більшої ефективності при впровадженні ZTA на підприємствах, підвищити ефективність захисту їх інформаційних систем загалом. Це дозволить створити більш надійні та масштабовані механізми захисту, що відповідають вимогам сучасного цифрового середовища.

3. Представлені результати аналізу сучасного стану використання ШІ в рамках концепції нульової довіри показують, що існуючі виклики та напрямки потребують подальшого дослідження можливостей застосування ШІ для автоматизації прийняття рішень. Встановлено, що подальші дослідження доцільно зосередити на розробці нових методів для покращення взаємодії між ZTA та ШІ, стандартизації механізмів обміну даними та методології поступового впровадження ZTA. При цьому слід не забувати про важливість так званого підходу human-in-the-loop для підвищення точності рішень ШІ, що в цілому сприятиме створенню більш адаптивних, надійних та ефективних систем кібербезпеки.

Застосування технологій ШІ у рамках концепції нульової довіри відкриває значні перспективи для розвитку більш надійних та масштабованих систем захисту інформаційних ресурсів, що є надзвичайно актуальним у сучасному цифровому кіберпросторі.

Список літератури:

1. Pentera: The State Of Pentesting 2024 Survey Report. (2024). URL: https://pentera.io/resources/reports/the-state-of-pentesting-2024-survey-report/.
2. PwC: The macroeconomic impact of artificial intelligence (2018). URL: https://www.pwc.co.uk/economic-services/assets/macroeconomic-impact-of-ai-technical-report-feb-18.pdf.
3. Cost of a data breach (2024). URL: https://www.ibm.com/reports/data-breach.
4. National Cybersecurity Center of Excellence (NCCoE). Implementing a Zero Trust Architecture. URL: https://www.nccoe.nist.gov/projects/implementing-zero-trust-architecture.
5. Єсін В. І., Вілігура В. В., Узлов Д. Ю. Огляд існуючих моделей та основних принципів нульової довіри // Радіотехніка. 2024. Вип. 217. С. 39–54. https://doi.org/10.30837/rt.2024.2.217.03.
6. Rose S., Borchert O., Mitchell S., & Connelly S. Zero Trust Architecture. NIST Special Publication 800-207 // National Institute of Standards and Technology. 2020. 59 p. https://doi.org/10.6028/NIST.SP.800-207.
7. Ahmed I., Nahar T., Urmi S. S., Taher K. A. Protection of Sensitive Data in Zero Trust Model // Proceedings of the International Conference on Computing Advancements. 2020. Vol. 63. P. 1–6. https://doi.org/10.1145/3377049.3377114.
8. Zero Trust Security (2024). URL: https://www.akamai.com/solutions/security/zero-trust-security.
9. Kindervag J. No More Chewy Centers: Introducing The Zero Trust Model Of Information Security. Forrester Research, For Security & Risk Professionals. URL: https://media.paloaltonetworks.com/documents/Forrester-NoMore-Chewy-Centers.pdf.
10. Sarkar S., Choudhary G., Shandilya S. K., Hussain A., Kim H. Security of Zero Trust Networks in Cloud Computing: A Comparative Review // Sustainability. 2022. 14(18). 11213. https://doi.org/10.3390/su141811213.
11. Cunningham C., Balaouras S., Barringham B., Dostie P. The Zero Trust eXtended (ZTX) Ecosystem. Extending Zero Trust Security Across Your Digital Business. Forrester Research, Inc. Cambridge, MA. 2018. URL: https://www.cisco.com/c/dam/m/en_sg/solutions/security/pdfs/forrester-ztx.pdf.

12. Fisher B. Forrester's Zero Trust or Gartner's Lean Trust? 2019.
URL: https://blogs.cisco.com/security/forresters-zero-trust-or-gartners-lean-trust.
13. Ward R., Beyer B. Beyondcorp // A new approach to enterprise security. 2014. 39(6). P. 6–11.
14. Oracle. Zero-trust security model. 2024. URL: https://www.oracle.com/nl/security/what-is-zero-trust/.
15. National Cybersecurity Center of Excellence (NCCoE). Implementing a Zero Trust Architecture. URL: https://www.nccoe.nist.gov/projects/implementing-zero-trust-architecture.
16. Fortinet. The State of Zero Trust. Report. 2023.
URL: https://www.fortinet.com/content/dam/fortinet/assets/reports/report-state-of-zero-trust.pdf.
17. Єсін В. І., Вілігура В. В., Узлов Д. Ю. Архітектура нульової довіри: проблеми та рекомендації щодо успішного впровадження. Радіотехніка. 2024. Вип. 218. С. 7–34. https://doi.org/10.30837/rt.2024.3.218.01.
18. Garbis J., Chapman J. W. Zero Trust Security: An Enterprise Guide. Berkeley, CA : Apress, 2021. 300 p.
19. ManageEngine: Adopting Zero Trust to safeguard against generative AI cyberthreats (2024).
URL: https://www.manageengine.com/active-directory-360/ebooks/zero-trust-approach-to-combating-gen-ai-cyberattacks.html.
20. Wang J. W., Jing X. Y., Yan Z., Fu Y. L., Pedrycz W., Yang L. T. A survey on trust evaluation based on machine learning // ACM Computing Surveys. 2020. 53(5). P. 1–36. https://doi.org/10.1145/3408292.
21. Ajish D. The significance of artificial intelligence in zero trust technologies: a comprehensive review // Journal of Electrical Systems and Inf Technol. 2024. 11(30). P. 1–23. https://doi.org/10.1186/s43067-024-00155-z.
22. Rangaraju S. Secure by intelligence: enhancing products with AI-driven security measures // EPH – International Journal of Science and Engineering. 2023. 9(3). P. 36–41. https://doi.org/10.53555/ephijse.v9i3.212.
23. Suleski T., Ahmed M., Yang W., Wang E. A review of multi-factor authentication in the Internet of Healthcare Things // Digital Health. 2023. Vol. 9. P. 1–20. https://doi.org/10.1177/20552076231177144.
24. Borodavka V., Tsuranov M. Biometrics: analysis and multi-criterion selection // The 9th IEEE International Conference on Dependable Systems, Services and Technologies, DESSERT, Kyiv, Ukraine. 2018. P. 334–339. https://doi.org/10.1109/DESSERT.2018.8409152.
25. Bodepudi A., Reddy M., Gutlapalli S. S., & Mandapuram M. Voice Recognition Systems in the Cloud Networks: Has It Reached Its Full Potential? // Asian Journal of Applied Science and Engineering. 2019. 8(1). P. 51–60. https://doi.org/10.18034/ajase.v8i1.12.
26. Stouffer C. What is facial recognition and how does it work? 2023. URL: https://us.norton.com/blog/iot/how-facial-recognition-software-works.
27. Ryu R., Yeom S., Kim S. H., Herbert D. Continuous multimodal biometric authentication schemes: A systematic review // IEEE Access. 2021. Vol. 9. P. 34541–34557. https://doi.org/10.1109/ACCESS.2021.3061589.
28. Germain K. S., Kragh F. Mobile physical-layer authentication using channel state information and conditional recurrent neural networks. In Proceedings of the 93rd IEEE Vehicular Technology Conference, Helsinki, Finland. 2021. P. 1–6. https://doi.org/10.1109/VTC2021-Spring51267.2021.9448652.
29. Meng R., Xu B., Xu X., Sun M., Wang B., Han S., Lv S., Zhang P. A survey of machine learning-based physical-layer authentication in wireless communications // Journal of Network and Computer Applications. 2024. 111 p. https://doi.org/10.48550/arXiv.2411.09906.
30. Du M., Li F. F., Zheng G. N., Srikumar V. DeepLog: Anomaly detection and diagnosis from system logs through deep learning // Proceedings of the ACM SIGSAC Conference on Computer and Communications Security, Dallas, USA. 2017. P. 1285–1298. https://doi.org/10.1145/3133956. 3134015.
31. Wang Y. M., Ji Z. X. Design and implementation of a semi-supervised anomaly log detection model DDA // Proceedings of International Conference on Computer Communication and Artificial Intelligence, Guangzhou, China. 2021. P. 86–90. https://doi.org/10.1109/CCAI50917.2021. 9447533.
32. Bursic S., Cuculo V., D'Amelio A. Anomaly detection from log files using unsupervised deep learning // Proceedings of International Symposium on Formal Methods, Porto, Portugal. 2019. P. 200–207. https://doi.org/10.1007/978-3-030-54994-7_15.
33. Tang Y. P., Ma B. X., Wu Z. Research on user clustering algorithm based on software system user behavior trajectory // Proceedings of the 2nd International Conference on Big Data Technologies, Jinan, China. 2019. P. 11–14. https://doi.org/10.1145/3358528.3358572.
34. Zhao Z., Chen W., Wu X., Chen P.C.Y., Liu J. LSTM network: A deep learning approach for Short-term traffic forecast // IET Intelligent Transport Systems. 2017. 11(2). P. 68–75. https://doi.org/10.1049/iet-its.2016.0208.
35. Singh M., Mehtre B. M., Sangeetha S. User behavior profiling using ensemble approach for insider threat detection // Proceedings of the 5th IEEE International Conference on Identity, Security, and Behavior Analysis, Hyderabad, India. 2019. P. 1–8. https://doi.org/10.1109/ISBA.2019. 8778466.
36. Sharma B., Pokharel P., Joshi B. User behavior analytics for anomaly detection using LSTM autoencoder-insider threat detection // Proceedings of the 11th International Conference on Advances in Information Technology, Bangkok, Thailand. 2020. Vol. 5. P 1–9. https://doi.org/10.1145/3406601.3406610.
37. Singh M., Mehtre B. M., Sangeetha S. User behaviour based insider threat detection in critical infrastructures // Proceedings of the 2nd International Conference on Secure Cyber Computing and Communications, Jalandhar, India. 2021. P. 489–494. https://doi.org/10.1109/ICSCCC51823.2021.9478137.

38. Marchal S., Jiang X. Y., State R., Engel T. A big data architecture for large scale security monitoring // Proceedings of IEEE International Congress on Big Data, Anchorage, USA. 2014. P. 56–63. https://doi.org/10.1109/BigData. Congress.2014.18

39. Li T. M., Yan L. M. SIEM based on big data analysis // Proceedings of the 3rd International Conference on Cloud Computing and Security, Nanjing, China. 2017. P. 167–175. https://doi.org/10.1007/978-3-319-68505-2_15.

40. El Hajji S., Moukafih N., Orhanou G. Analysis of neural network training and cost functions impact on the accuracy of IDS and SIEM systems // Proceedings of the 3rd International Conference on Codes, Cryptology, and Information Security, Rabat, Morocco. 2019. P. 433–451. https://doi.org/10.1007/978-3-030-16458-4_25.

41. Hossain S. M. M., Couturier R., Rusk J., Kent K. B. Automatic event categorizer for SIEM // Proceedings of the 31st Annual International Conference on Computer Science and Software Engineering, Toronto, Canada. 2021. P. 104–112. https://dl.acm.org/doi/10.5555/3507788.3507803.

42. Hindy H., Brosset D., Bayne E., Seeam A., Bellekens X. Improving SIEM for critical SCADA water infrastructures using machine learning // Proceedings of International Workshop on Security and Privacy Requirements Engineering, Barcelona, Spain. 2019. P. 3–19. https://doi.org/10.1007/978-3-030-12786-2_1.

43. Feng C., Wu S. N., Liu N. W. A user-centric machine learning framework for cyber security operations center. In Proceedings of IEEE International Conference on Intelligence and Security Informatics, Beijing, China. 2017. P. 173-175. https://doi.org/10.1109/ISI.2017.8004902.

44. Kinyua J., Awuah L. AI/ML in security orchestration, automation and response // Future research directions. Intelligent Automation & Soft Computing. 2021. 28(2). P. 527–545. https://doi.org/10.32604/iasc.2021.016240.

45. Aslam N., Khan I.U., Mirza S., AlOwayed A., Anis F.M., Aljuaid R.M., Baageel R. Interpretable Machine Learning Models for Malicious Domains Detection Using Explainable Artificial Intelligence (XAI) // Sustainability. 2022. 14(12), 7375. P. 1–22. https://doi.org/10.3390/su14127375.

46. Yeshwanth M.V., Kalluri R., Rao M.S., Kumar R.K.S., Bindhumadhava B.S. Adoption and Assessment of Machine Learning Algorithms in Security Operations Centre for Critical Infrastructure // Pillai R.K., Ghatikar G., Sonavane V.L., Singh B.P. (eds) ISUW 2020. Lecture Notes in Electrical Engineering, Springer, Singapore. 2022. № 847. P. 395–407. https://doi.org/10.1007/978-981-16-9008-2_38

47. Ban T., Ndichu S., Takahashi T., Inoue D. Combat security alert fatigue with AI-assisted techniques // CSET –21: Cyber Security Experimentation and Test Workshop. 2021. P. 9–16. https://doi.org/10.1145/3474718.3474723.

48. Sentuna A., Alsadoon A., Prasad P. W. C., Saadeh M., Alsadoon O. H. A novel enhanced naive Bayes posterior probability (ENBPP) using machine learning: Cyber threat analysis // Neural Processing Letters. 2021. № 53(1). P. 177–209. https://doi.org/10.1007/s11063-020-10381-x.

49. Deliu I., Leichter C., Franke K. Collecting cyber threat intelligence from hacker forums via a two-stage, hybrid process using support vector machines and latent dirichlet allocation // Proceedings of IEEE International Conference on Big Data, Seattle, USA. 2018. P. 5008–5013. https://doi.org/10.1109/BigData.2018.8622469.

Надійшла до редколегії 10.01.2025

Відомості про авторів:

Бородавка Владислав Вячеславович – Харківський національний університет імені В. Н. Каразіна, аспірант кафедри кібербезпеки інформаційних систем, мереж і технологій навчально-наукового інституту комп'ютерних наук та штучного інтелекту; Україна; e-mail: vladyslav.borodavka@karazin.ua; ORCID: https://orcid.org/0009-0002-3885-1364

Єсін Віталій Іванович – д-р техн. наук, професор, Харківський національний університет імені В. Н. Каразіна, професор кафедри кібербезпеки інформаційних систем, мереж і технологій навчально-наукового інституту комп'ютерних наук та штучного інтелекту; Україна; e-mail: v.i.yesin@karazin.ua; ORCID: https://orcid.org/0000-0003-1977-7269

UDC 004.8 **DOI:10.30837/rt.2025.1.220.03**

Yu. L. GOLIKOV

STUDY OF THE CURRENT STATE AND PROSPECTS OF ARTIFICIAL INTELLIGENCE IN CYBERSECURITY

Introduction

Artificial intelligence (AI) has been changing the cybersecurity space for more than a decade, thanks to machine learning (ML), which accelerates threat detection and detects anomalous behavior of users and objects. That's why AI is gradually becoming an integral part of modern cybersecurity systems, helping to identify threats, automate processes, and increase the level of information protection.

One of the important challenges in using AI for cybersecurity is building trust. The data used to train AI/ML models drives the output of the models. If the training data does not reflect the "real world," the model may distort its ability to deliver the expected results. Some data, such as threat information, "good" and "bad" file characteristics, compromise indicators, etc., are for everyone to see.

Another major challenge is data security. It is important to define and control what training data can be shared and what data remains secret within organizations. In the wrong hands, this data can help attackers in their attacks to undermine the ability of AI/ML to identify their files, programs, and behavior as invalid. In this regard, governments and businesses need to develop regulations, standards, and best practices to prevent new AI threats.

For example, NIST [17, 18] is already leading and participating in the development of technical standards, including international standards, that promote innovation and public trust in systems that use AI. A wide range of standards for AI data, performance, and governance is - and increasingly will be - a priority for reliable and responsible AI.

NIST has developed a plan for global engagement with the promotion and development of AI standards. The goal is to stimulate the development and implementation of consensus standards related to artificial intelligence, collaboration and coordination, and information sharing. Reflecting input from the public and private sectors. On July 26, 2024, after reviewing public comments on the project plan, NIST published the Global AI Standards Engagement Plan [17].

The development of AI technologies has brought not only new opportunities, but also new risks and dangers. The community of scientists and researchers around the world is concerned and warns of potential problems with the spread of AI. In particular, a recent report by the UK National Cyber Security Center (NCSC) [14] warns that over the next two years, AI technologies will likely increase the dynamics of cyberattacks and increase their impact on existing cryptosystems and information security tools. According to the Center [14], AI opens up great opportunities in this area even for those cryptanalysts who do not have the appropriate technical skills. And they argue that after 2025 and beyond, when AI has been trained successfully enough, AI will almost certainly improve, providing faster and more accurate cyber operations.

The role of AI will only grow in the coming years. For example, AI is able to detect threats in real time, meaning it can analyze huge amounts of data, identifying anomalous activities and potential threats faster than humans can. AI algorithms can not only identify threats but also instantly block malicious traffic or change network access rules. What is also important, automated solutions help to avoid mistakes that can occur due to human inattention or lack of skills.

Therefore, the purpose of this article is to study the current state of AI in cybersecurity, as well as the threats and risks associated with its use. The article discusses modern anti-virus solutions, the most popular AI attacks and methods of protodiagnostics. It also discusses the prospects of using AI and proves that in the modern world, AI is an integral part of cybersecurity.

1. Main areas of AI application in cybersecurity

Below, we will consider six main possible options for using AI in the field of cybersecurity (Fig. 1):

1. Automated threat detection and response. Traditional cybersecurity systems require constant monitoring and analysis of large amounts of data, which is difficult to implement manually. AI can perform the following tasks:

- Detect anomalous activity in the network using machine learning algorithms.
- Analyze user and device behavior to detect suspicious activity.
- Automatically respond to threats by blocking potentially dangerous actions without human intervention.

An example of such systems is, for example, an AI-enabled SIEM (Security Information and Event Management) system that analyzes events in real time and warns of possible attacks. SIEM systems will be discussed in more detail in Section 3 of this article.

2. Use of AI in malware analysis. Traditional antiviruses use signatures to detect malware, which makes them less effective against new attacks. Instead, AI allows:

- Use behavioral analysis to detect new viruses and Trojans.
- Recognize different types of attacks that change their code to bypass antiviruses.
- Automatically create and update threat databases without the need for manual changes.

For example, AI antiviruses such as Microsoft Defender ATP or Darktrace are gaining popularity, analyzing program behavior and detecting threats without human intervention. We discuss these methods in more detail in Section 4 of this article.

3. Strengthening cryptography and post-quantum security. It is well known that with the development of quantum computers, traditional cryptographic algorithms can become vulnerable. AI, in turn, can help in:

- Creating adaptive cryptographic solutions that can change keys and algorithms in real time.
- Optimization of encryption and decryption, which will make cryptographic systems more efficient.
- Development of new post-quantum cryptographic algorithms that will be resistant to attacks by quantum computers.

Therefore, AI is actively used to test new strong ciphers. Encryption and key management optimization – machine learning algorithms can improve the efficiency of cryptographic protocols, providing faster and more secure encryption. For example, NIST is actively researching encryption and signature algorithms for post-quantum cryptography [1], and AI can accelerate their testing and implementation [18].

4. AI in countering phishing attacks. Phishing is one of the most widespread cyber threats that is becoming increasingly complex. AI can help in:

- Automatically recognize suspicious emails and URLs.
- Analyzing the language and structure of messages to detect fraudulent schemes.
- Improved authentication mechanisms, for example, through behavioral biometrics or dynamic captchas.

One of the most well-known examples of AI in the fight against phishing is Google, which uses AI in Gmail to filter phishing emails, which allows it to block more than 99% of malicious messages.

5. Using AI to predict attacks. Artificial intelligence can help not only respond to attacks but also predict them by analyzing huge amounts of data:

- Using big data analysis to identify trends in cyberattacks.
- Creating predictive models that allow us to anticipate potential system vulnerabilities.
- Automatic analysis of the Dark Web to identify new threats and hacking tools.

For example, IBM Watson for Cyber Security [7] uses cognitive analysis to identify new threats by analyzing millions of articles, forums, and messages on the darknet.

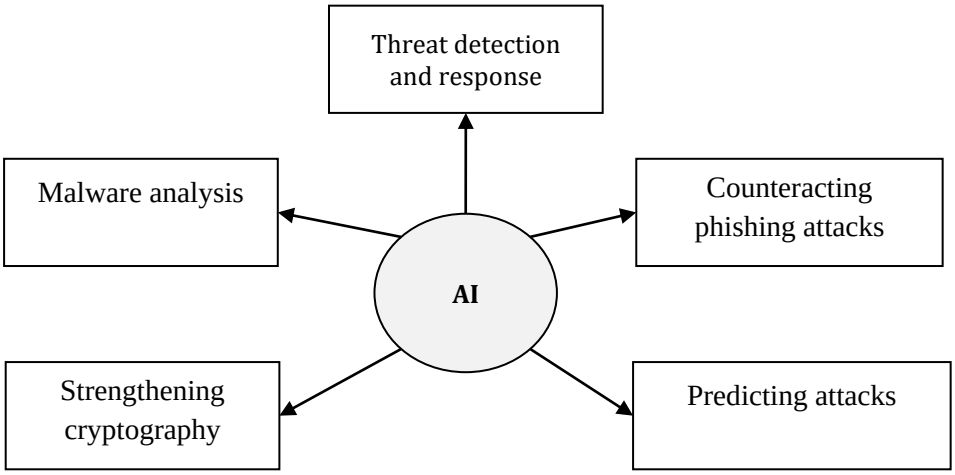


Fig. 1. The use of AI in cybersecurity

2. AI-powered protection and improved cybersecurity efficiency

Artificial intelligence (AI)-based intrusion detection systems (IDSs) are modern cybersecurity tools that use machine learning and data analytics to identify and prevent unauthorized activities on networks and systems. They are able to adapt to new threats by analyzing large amounts of data and detecting anomalies that may indicate potential attacks.

There are two main methods used in IDS:

1) Detection based on known algorithms. This method involves comparing incoming traffic with a database of known attacks. If a match is found, the system generates an alert. However, this approach is limited in detecting new or modified attacks that do not yet have corresponding algorithms.

2) Anomaly-based detection: This method uses models of normal system behavior. Deviations from this norm are considered as potential threats. AI plays a key role in building and updating such models, which allows detecting even previously unknown attacks.

It is clear that the integration of artificial intelligence into intrusion detection systems significantly increases the effectiveness of cybersecurity, allowing for the detection and prevention of both known and emerging threats. However, in order to maximize the potential of such systems, it is necessary to take into account possible limitations and ethical aspects of their application, since, for example, the use of AI may raise privacy issues, especially if the systems analyze personal data without proper control.

3. SIEM system with AI support

Security Information and Event Management, or SIEM, is a security solution that helps organizations recognize and address potential security threats and vulnerabilities before they have a chance to disrupt business operations [7].

SIEM systems help enterprise security teams detect anomalies in user behavior and use artificial intelligence (AI) to automate many of the manual processes involved in threat detection and incident response. Currently, the most well-known modern SIEM systems are the following software: Splunk Enterprise Security (Splunk), Elastic Security, IBM QRadar SIEM, Wazuh SIEM, Microsoft Sentinel.

The initial SIEM platforms were log management tools. They combined the functions of security information management (SIM) and security event management (SEM). These platforms provided real-time monitoring and analysis of security-related events. The term SIEM was coined in 2005 to describe the combination of SIM and SEM technologies.

They also made it easier to track and record security data for compliance or audit purposes. Over the years, SIEM software has evolved to include user and object behavior analytics, as well as other advanced security analytics, artificial intelligence, and machine learning capabilities to detect

anomalous behavior and indicators of advanced threats. Today, SIEM has become a core element of modern security operations centers (SOCs) for security monitoring and compliance management.

The stages of SIEM systems (Fig. 2) can be divided as follows [6]:

- Data collection – All sources of network security information, such as servers, operating systems, firewalls, antivirus software, and intrusion prevention systems, are configured to send event data to the SIEM tool. Most modern SIEM tools use agents to collect event logs from enterprise systems, which are then processed, filtered, and sent to the SIEM. Some SIEMs allow you to collect data without agents. For example, Splunk [8] offers agentless data collection on Windows using WMI.

AI SIEM systems start by aggregating data from various sources, such as network devices, servers, databases, and applications. Once ingested, the raw data is converted into a standardized format to ensure consistent and accurate data analysis regardless of the source. AI and ML significantly automate these processes, increasing the speed and intelligence with which security data is aggregated and normalized, reducing manual effort and time [9].

- Policies – The SIEM administrator creates a profile that defines the behavior of enterprise systems under normal conditions and during predefined security incidents. SIEMs provide standard rules, alerts, reports, and dashboards that can be customized to meet specific security needs.
- Data Consolidation and Correlation – SIEM solutions consolidate, analyze, and parses log files. Events are then categorized based on the raw data and correlation rules are applied to combine individual data events into meaningful security issues.
- AI SIEM systems use predictive analytics to forecast potential future threats by analyzing historical security data and identifying patterns. This capability allows organizations to proactively protect their systems rather than reacting to threats as soon as they occur. This knowledge base allows the artificial intelligence models that are at the heart of the solution to create increasingly accurate security responses and incident prevention approaches as time passes and new data is collected.

Continuously learning from past problems improves the accuracy and reliability of AI-based SIEM systems against increasingly powerful cyber threats. Ultimately, an AI-powered SIEM integrates various components such as AI, ML, deep learning, NLP, and UEBA that extend the capabilities of a traditional SIEM. This integration leads to smarter, more efficient and proactive cybersecurity measures, which is crucial in the ever-changing cyber threat environment [9].

- Alerts – If an event or set of events triggers a SIEM rule, the system notifies security personnel. When a threat is detected, AI enables SIEM systems to automate parts of the incident response process. This includes automatically triggering alerts, implementing predefined response actions, or organizing complex response workflows. One such example is an automated dynamic workflow, where the workflow that is established after a potential threat is tailored to the threat in question.

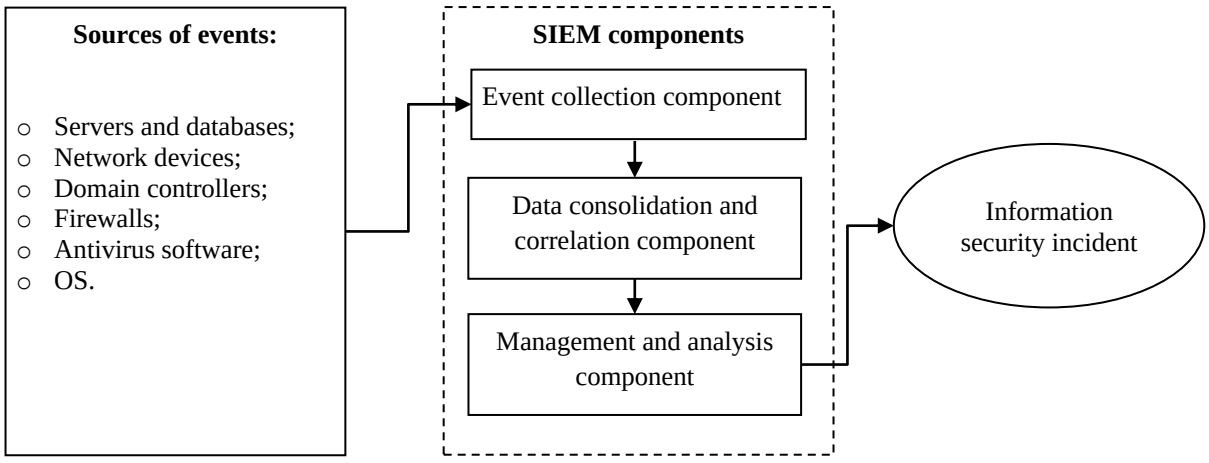


Fig. 2. Diagram of the SIEM system operation

Without the help of a SIEM, the amount of time it would take for security analysts to reliably detect suspicious activity by correlating logs between different types of devices would be very long given the complexity of most networks. It is rarely possible to detect and respond to any threat or attack on their infrastructures in time to prevent any damage. In addition, a SIEM solution can expand the possibilities of using the collected information [3].

It is clear that AI will become increasingly important in the future of SIEM as cognitive capabilities will improve the system's decision-making ability. It will also allow systems to adapt and evolve as the number of endpoints increases. As IoT, cloud computing, mobile, and other technologies increase the amount of data that a SIEM tool must consume. AI offers the potential for a solution that supports more types of data and a comprehensive understanding of threats as they evolve.

4. Anti-virus solutions based on AI

Artificial intelligence plays a key role in modern anti-virus solutions, such as Microsoft Defender Advanced Threat Protection (ATP) [11] and Darktrace [12]. These systems use AI capabilities to improve detection and response to cyber threats.

Microsoft Defender ATP [11] is an enterprise endpoint security platform designed to prevent, detect, investigate, and respond to threats. It integrates endpoint behavioral sensors, cloud-based security analytics, and threat intelligence to provide comprehensive protection. The sensors built into Windows 10 collect and process behavioral signals that are sent to the Microsoft Defender isolated cloud environment for further analysis.

The main features of Microsoft Defender include [11]:

- Reducing the attack surface: minimizing attack vectors to reduce the possibility of intrusion.
- Next-generation defense: using advanced machine learning techniques to detect sophisticated attacks.
- Endpoint Detection and Response (EDR): Provides in-depth analysis and visualization of threats in real time.
- Automated investigation and response: reduce the workload of security teams by automating processes.

Among the advantages of the Microsoft Defender solution is that it has deep integration with Windows, Microsoft 365, and Azure, but at the same time, this can be seen as a disadvantage, as it does not cover all network traffic as effectively as, for example, Daktrace [12], which will be discussed further. Other advantages include automatic threat research and built-in SIEM and SOAR capabilities through Microsoft Sentinel. Let's take a closer look at the Daktrace solution.

Darktrace [12] is a cybersecurity company that uses artificial intelligence and machine learning to detect cyberattacks and vulnerabilities in computer systems. Its technology aims to detect threats quickly and efficiently by using behavioral analysis to identify anomalies that may indicate attacks.

Darktrace uses self-learning AI to provide proactive cyber defense. Darktrace's core principle is the use of machine learning to analyze user, device, and network behavior. Its technology is capable of:

- Detect threats in real time: by analyzing network and user behavior to detect anomalies. And just as importantly, it detects new, unknown threats without using known algorithms or databases of known viruses.
- Autonomously respond to threats: perform automatic actions to neutralize attacks without human intervention.
- Provide protection across multiple environments: networks, email, cloud services, operational technologies and endpoints, as well as external platforms such as AWS, Azure, Google Cloud.

Thus, we can see that both Microsoft Defender for Endpoint [11] and Darktrace [12] use artificial intelligence (AI) to improve cybersecurity, but they have different approaches and areas of application. Let us consider them in a comparative analysis in Table 1.

Table 1

Comparative analysis of modern AI-based anti-virus solutions

Characteristics	Microsoft Defender ATP	Darktrace
Solution type	Endpoint Detection and Response (EDR), SIEM/SOAR	Network Detection and Response (NDR), Autonomous AI security
The main approach	Use behavioral analysis and threat intelligence to protect endpoints	Self-learning AI to analyze anomalies in the network, email, and cloud services
Main features	Endpoint threat detection, attack analysis, automated response	Network threat detection, autonomous response with Darktrace Antigena
Protection against ransomware	Blocks known attacks, analyzes behavior, stops suspicious processes	Detects anomalous activity in real time, blocks malicious activity at the network level
Focus on threats	Viruses, malware, exploits, attack scripts, account compromise	Anomalies in network traffic, insider threats, zero-day attacks
Integration	Deep integration with the Microsoft 365 ecosystem, Azure, Defender XDR	Support for hybrid environments: network, email, cloud, industrial systems
Cloud support	Microsoft 365, Azure	AWS, Google Cloud, Azure, local area networks

Let's consider who each solution is best suited for.

Microsoft Defender for Endpoint:

- Large and medium-sized companies operating in the Microsoft ecosystem.
- Organizations looking for powerful endpoint protection with built-in SIEM analytics.
- Companies with an IT team that is ready to manage security through Microsoft Security Center.

Darktrace would be better integrated into:

- Businesses with extensive networks that require in-depth traffic analysis.
- Organizations that want to detect anomalies in real time and automatically respond to them.
- Companies that use mixed environments (local servers, cloud platforms, IoT).

These examples demonstrate how the integration of AI into antivirus solutions improves the efficiency of detecting and responding to modern cyber threats, ensuring proactive protection of information systems.

5. AI as an attacker's tool – risks and threats associated with AI

The previous sections have discussed the benefits of using AI in cybersecurity, but there are undoubtedly many challenges to its use, as AI not only opens up new opportunities for development, but also becomes a tool in the hands of attackers, creating new risks and threats. The most common of these threats in the modern world are:

- AI-based attacks: Cybercriminals can use AI to launch more sophisticated and targeted attacks. This increases the effectiveness of their actions and makes it more difficult to detect threats.
- Disinformation and deep fakes (Deepfake): AI allows for the creation of realistic fake video, audio, and text that can undermine trust in authoritative sources, manipulate public opinion, and interfere with electoral processes.
- Automation of cyberattacks: Attackers can use AI to automate attacks, allowing them to be carried out faster and less likely to be detected.
- Attacks on AI systems: Attackers can manipulate the data that AI systems are trained on, leading to incorrect decisions and increasing the vulnerability of the systems.

Attackers are using AI to automate and increase the effectiveness of social engineering attacks. For example, neural networks can automatically generate highly believable phishing messages that convince users to share their passwords or other important information. This allows attackers to

gain access to the system without the need to conduct technical attacks, bypassing many levels of protection. Attackers are also actively using AI to carry out various attacks, which requires security professionals to develop new protection strategies. Therefore, let's take a look at the main types of AI-based attacks.

5.1. Data poisoning attacks

The first Data Poisoning attacks [15] were carried out in cybersecurity back in 2006 [19] and 2008 [20] and have since gained popularity among attackers. These attacks occur at the training or retraining stage of an AI model. Attackers inject malicious data into the training database, which leads to malfunctioning of the system and generation of false results. This can cause errors in classification or decision-making. For example, GANs can create artificial data that looks legitimate but is intended to mislead or corrupt machine learning models, which affects their performance and reliability.

Data poisoning can also reinforce existing biases in AI systems [16]. Attackers can target specific subsets of data, such as a particular demographic, to inject biased data. This can cause an AI model to perform unfairly or inaccurately. For example, facial recognition models trained with biased or fake data may incorrectly identify people from certain groups, leading to discriminatory results. These types of attacks can affect both the fairness and accuracy of ML models in different applications.

Data poisoning can also open the door to more sophisticated attacks [16], such as inversion attacks, in which hackers attempt to reconstruct the model's training data. Once an attacker successfully poisons the training data, they can then use these vulnerabilities to launch more serious attacks. In systems designed for sensitive tasks, such as cybersecurity, these risks can be particularly dangerous.

To protect against data poisoning attacks, organizations can implement strategies to help ensure the integrity of training datasets, improve model reliability, and continuously monitor AI models.

5.2. Evasion attacks

Evasion Attacks [18] consist of creating special input data that misleads the AI model, forcing it to make incorrect predictions or classifications. Such attacks can be aimed at bypassing malware detection systems or other protective mechanisms.

The discovery of evasion attacks against machine learning models has sparked increased interest in adversarial machine learning, leading to significant growth in this research area over the past decade. In an evasion attack, the goal of the attacker is to create competitive examples, which are defined as test samples [21].

In cybersecurity applications, competitive examples must respect the constraints imposed by the program semantics and the representation of cyber data features, such as network traffic or program binaries [18].

FENCE is a general framework for creating white-box evasion attacks using gradient optimization in discrete domains and supports a number of linear and statistical characteristic dependencies [22]. FENCE has been applied to two network security applications: malicious domain detection and malicious network traffic classification. In [23], this technique was applied to network intrusion detection and phishing classifiers. It is noted in [23] that continuous domain attacks cannot be easily applied in constrained environments because they result in infeasible adversarial examples. Pierazzi et al. [24] discuss the difficulty of establishing possible evasion attacks in cybersecurity due to constraints in the function space and formalize evasion attacks in the problem space and create possible adversarial examples for Android malware.

5.3. Rapid deployment attacks

In a Prompt Injection attack [18], attackers insert malicious instructions into requests to AI models, forcing them to perform unwanted actions or provide sensitive information, i.e., tricking the model into returning an unexpected response and causing the application to act in unplanned ways.

Successful implementation can lead to the leakage of confidential data, destruction of information, and other types of damage depending on the application.

5.4. Social engineering attacks using AI

AI is used to automate and improve the effectiveness of social engineering attacks, such as phishing or manipulation, making them more difficult to detect.

Attackers use social engineering techniques to conceal their true "identity" by posing as trusted organizations or individuals to victims. These attacks are aimed at obtaining personal information to access the target network through deception and manipulation. Social engineering is used as the first stage of a large cyberattack to penetrate a system, install malware, disclose confidential data, etc.

For example, in the case of phishing [18], it was previously demonstrated that large language models (LLMs) can create persuasive scams such as phishing emails [25]. Now that LLMs can more easily integrate with applications, they can not only create fraudulent activities, but also widely distribute such attacks [26]. Users are likely to be more susceptible to these new attacks, as opposed to phishing emails, because they lack experience and awareness of this new threat technique.

The LLM itself also acts as a computer on which malicious code runs and spreads. For example, an automated message processing tool that can read and create emails and view users' personal data can propagate the injection to other models that can read these incoming messages [26].

So, let's look at measures to counter AI-based attacks. To protect yourself from AI attacks, you need to take the following steps:

- Improving data quality: Ensuring data is clean and reliable for training AI models helps reduce the risk of data poisoning.
- Developing resilient models: Creating AI models that are resistant to attacks by implementing security methods and regular testing.
- Monitoring and auditing: Continuously monitor the operation of AI models and conduct audits to identify possible vulnerabilities.
- Staff training: Raising employees' awareness of possible AI-based attacks and methods of detecting them.

In today's digital environment, it is important to be prepared for new challenges related to the use of AI and implement appropriate cybersecurity measures.

Conclusions

1. This paper reviews and analyzes. This article provides a comprehensive analysis of the current state and prospects of artificial intelligence (AI) in cybersecurity. Both the benefits of implementing AI in security systems and the risks associated with its use are considered.

2. AI allows you to automate the process of detecting and responding to threats, which significantly increases the effectiveness of cyber defense. The use of machine learning algorithms helps to quickly analyze large amounts of data and identify anomalies in the behavior of users and systems.

3. Modern cybersecurity systems, such as SIEM (Security Information and Event Management), benefit greatly from AI integration, as they are able to analyze events in real time and warn of possible attacks. Continuously learning from the past improves the accuracy and reliability of AI-powered SIEM systems against increasingly powerful cyber threats. Ultimately, an AI-powered SIEM integrates various components such as AI, ML, deep learning, NLP, and UEBA. This integration leads to smarter, more efficient and proactive cybersecurity measures, which is crucial in the ever-changing cyber threat environment. At the same time, a large number of integrations with various systems allow SIEM systems to monitor and accumulate data on the current state of cybersecurity of information infrastructure in relation to certain international and national standards, such as ISO 27001, GDPR or PCI DSS.

4. AI can analyze huge amounts of data and identify patterns that indicate potential threats, allowing organizations to stay ahead of hackers. AI can also identify threats faster and more accurate-

ly, and automatically block malicious traffic without human intervention. Thanks to behavioral analysis, AI antiviruses (e.g., Microsoft Defender ATP and Darktrace) can detect threats more effectively than traditional antivirus programs.

5. As for the use of attack detection protection systems, if a company actively uses Microsoft 365, Azure, and Windows, it is better to choose Microsoft Defender for Endpoint. It provides deep integration, automated response, and behavioral analysis of threats on endpoints. If you need flexible and autonomous protection of all levels of your network, you should consider Darktrace. It is suitable for organizations that want to detect anomalies, analyze cyber threats in real time, and respond to them without human intervention. But the ideal option is to combine both solutions: Microsoft Defender for Endpoint for endpoint protection and Darktrace for network analysis and automated threat response.

6. The use of AI not only for defense but also for attack poses a significant threat. Attackers can use AI to automate attacks, manipulate, and engage in social engineering. Attackers are increasingly using AI to create sophisticated malware that can adapt to defenses. Security experts are worried about potential autonomous AI attacks, forcing companies to prepare now. Organizations need to implement comprehensive strategies to take advantage of the benefits of AI while minimizing its potential threats.

7. The prospects for development and recommendations for the use of AI in cybersecurity are as follows:

- Increasing the transparency of AI algorithms and implementing ethical standards are critical to the credibility of AI technologies in the security sector.
- Development of stable AI models that will be less vulnerable to attacks by malicious actors.
- Investing in research on post-quantum cryptography and the latest authentication methods to strengthen cybersecurity systems.
- Strengthening international cooperation in the field of AI standards and regulation, in particular through the initiatives of organizations such as NIST.

8. Thus, artificial intelligence has the potential to completely change the approach to cybersecurity. Its ability to quickly analyze large amounts of data, predict threats, and automatically respond to attacks makes it a key element of protection in the digital world. However, it should be remembered that cybercriminals are also using AI, so the future of cybersecurity will depend on the balance between security innovations and threats from criminal groups.

9. The future of cybersecurity is a symbiosis of humans and artificial intelligence, where analysts and security experts collaborate with smart systems to create a secure cyberspace.

References:

1. NIST standardization process "Post-Quantum Cryptography: Digital Signature Schemes". Access mode: https://csrc.nist.gov/Projects/pqc-dig-sig/round-1-additional-signatures.

2. TAO, Feng; Akhtar, Muhammad Shoaib; Jiayuan, Zhang. The future of artificial intelligence in cybersecurity: A comprehensive survey // EAI Endorsed Transactions on Creative Technologies. 2021. 8.28: e3–e3. https://doi.org/10.4108/eai.7-7-2021.170285.

3. Leung B. K. (2021). Security Information and Event Management (SIEM) Evaluation Report. ScholarWorks. May 2021. Access mode: https://scholarworks.calstate.edu/downloads/41687p49q.

4. González-Granadillo G., González-Zarzosa S., Diaz, R. Security Information and Event Management (SIEM) // Analysis, Trends, and Usage in Critical Infrastructures. Sensors. 2021. 21(14). Access mode: https://doi.org/10.3390/s21144759

5. Muhammad S., et al. Effective Security Monitoring Using Efficient SIEM Architecture // Human-centric Computing and Information Sciences. 2023. 13. Access mode: https://doi.org/10.22967/HCIS.2023.13.017.

6. What is SIEM. Security Information and Event Management Tools. (n.d.). Imperva. Access mode: https://www.imperva.com/learn/application-security/siem/.

7. IBM Security QRadar. What is security information and event management (SIEM)? https://www.ibm.com/think/topics/siem.

8. Splunk. The Splunk SIEM. Access mode: https://www.splunk.com/en_us/products/enterprise-security.html.

9. Stellar Cyber. AI SIEM: The 6 Components of AI-Based SIEM. - Access mode: https://stellarcyber.ai/learn/ai-driven-siem/.

10. ISO/IEC 27001:2022. Information technology - Security techniques - Information security management systems - Requirements. International standard. 3 Edition.
11. Microsoft Defender for Endpoint. 2024. Access mode: https://learn.microsoft.com/uk-ua/defender-endpoint/microsoft-defender-endpoint.
12. Darktrace. Official website. 2025. Access mode: https://darktrace.com/.
13. Mauri L., Damiani E. Modeling Threats to AI-ML Systems Using STRIDE. *Sensors* 2022, *22*(17), 6662; - Access mode: https://doi.org/10.3390/s22176662.
14. The near-term impact of AI on the cyber threat: https://www.ncsc.gov.uk/report/impact-of-ai-on-cyber-threat.
15. Nihad Hassan. What is data poisoning (AI poisoning) and how does it work? Search Enterprise AI, TechTarget, 2024. Access mode: https://www.techtarget.com/searchenterpriseai/definition/data-poisoning-AI-poisoning.
16. Tom Krantz, Alexandra Jonker. What is data poisoning? IBM. Access mode: https://www.ibm.com/think/topics/data-poisoning.
17. NIST Trustworthy and Responsible AI NIST AI 100-5. A Plan for Global Engagement on AI Standards: https://doi.org/10.6028/NIST.AI.100-5.
18. Vassilev A, Oprea A, Fordyce A, Anderson H (2024) Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations. (National Institute of Standards and Technology, Gaithersburg, MD) NIST Artifcial Intelligence (AI) Report, NIST Trustworthy and Responsible AI NIST AI 100-2e2023. Access mode: https://doi.org/10.6028/NIST.AI.100-2e2023.
19. R. Perdisci, D. Dagon, Wenke Lee, P. Fogla, and M. Sharif. Misleading worm signature generators using deliberate noise injection // 2006 IEEE Symposium on Security and Privacy (S&P'06), Berkeley/Oakland, CA, 2006.
20. Blaine Nelson, Marco Barreno, Fuching Jack Chi, Anthony D. Joseph, Benjamin I.P. Rubinstein, Udam Saini, Charles Sutton, and Kai Xia. Exploiting machine learning to subvert your spam flter // First USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET 08), San Francisco, CA, April 2008. USENIX Association.
21. Christian Szegedy, Wojciech Zaremba, Ilya Sutskever, Joan Bruna, Dumitru Erhan, Ian Goodfellow, and Rob Fergus. Intriguing properties of neural networks // International Conference on Learning Representations, 2014.
22. Alesia Chernikova and Alina Oprea. FENCE: Feasible evasion attacks on neural networks in constrained environments // ACM Transactions on Privacy and Security (TOPS) Journal. 2022.
23. Ryan Sheatsley, Blaine Hoak, Eric Pauley, Yohan Beugin, Michael J. Weisman, and Patrick McDaniel. On the robustness of domain constraints // Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security, CCS '21, p. 495–515, New York, NY, USA, 2021. Association for Computing Machinery.
24. Fabio Pierazzi, Feargus Pendlebury, Jacopo Cortellazzi, and Lorenzo Cavallaro. Intriguing properties of adversarial ML attacks in the problem space // 2020 IEEE Symposium on Security and Privacy (S&P). P. 1308–1325. IEEE Computer Society, 2020.
25. Daniel Kang, Xuechen Li, Ion Stoica, Carlos Guestrin, Matei Zaharia, and Tatsunori Hashimoto. Exploiting programmatic behavior of llms // Dual-use through standard security attacks. arXiv preprint arXiv:2302.05733, 2023.
26. Kai Greshake, Sahar Abdelnabi, Shailesh Mishra, Christoph Endres, Thorsten Holz, and Mario Fritz. Not what you signed up for // Compromising realworld llm-integrated applications with indirect prompt injection. arXiv preprint arXiv:2302.12173, 2023.

Received 08.02.2025

Information about the authors:
Yuriy Golikov – CEO and Founder of DevBrother tech company, USA; e-mail: yuriy@devbrother.com ; ORCID: https://orcid.org/0009-0008-7946-4663

УДК 681.3.07 (3.06) **DOI:10.30837/rt.2025.1.220.04**

Д.М. МОРГУЛЬ, О.П. НАРЄЖНІЙ, канд. техн. наук, Т.О. ГРІНЕНКО, канд. техн. наук

КЛАСИФІКАЦІЯ АТАК ТА ВИМОГИ КІБЕРБЕЗПЕКИ ДО ВЕБ-РЕСУРСУ QRNG

Вступ

Квантові генератори випадкових чисел (Quantum Random Number Generator, QRNG) є ключовими компонентами сучасних криптографічних систем, які забезпечують генерацію непередбачуваних чисел на основі квантових ефектів. Це дозволяє уникнути обмежень традиційних псевдовипадкових генераторів (Pseudo Random Number Generator, PRNG), що можуть бути вразливими до прогнозування або відтворення. QRNG використовують фундаментальні принципи квантової механіки, зокрема властивості фотонів або електронів, для створення справжньої випадковості. На відміну від PRNG, які базуються на алгоритмічному підході, QRNG є стійкими до будь-яких спроб прогнозування, навіть з використанням квантових комп'ютерів.

Порівняння характеристик захищеності QRNG та класичних алгоритмічних PRNG приведено в табл. 1.

Таблиця 1

Параметр	QRNG	PRNG
Стійкість до прогнозування	Максимальна	Уразливий до підбору
Вплив бічних каналів	Існує	Обмежений
Фізичний рівень захисту	Необхідний	Мінімальний
Чутливість до середовища	Висока	Низька

Застосування веб-сервісів QRNG стало критично важливим для забезпечення безпеки банківських систем, інтернету речей та інших високочутливих платформ. Наприклад, при шифруванні даних QRNG виступають як надійний інструмент для створення криптографічних ключів. Однак їх інтеграція в реальні системи породжує нові ризики, пов'язані з потенційними атаками на апаратному та програмному рівнях.

Важливим аспектом є ризик атак на QRNG через криптографічні бібліотеки, які можуть бути вразливими до зовнішнього втручання або маніпуляцій на рівні програмного забезпечення. Наприклад, неправильна реалізація екстрактора QRNG у бібліотеках типу OpenSSL може стати причиною генерації передбачуваних чисел, що піддає загрозі всю систему. Зловмисники можуть скористатися цією вразливістю для перехоплення сеансових ключів або доступу до зашифрованих даних.

Ще одним критичним вектором атак є маніпуляція середовищем виконання, що може призводити до спотворення результатів QRNG під час генерації чисел. Якщо зловмисники отримають доступ до програмного середовища, вони зможуть змінювати вихідні значення QRNG, тим самим створюючи криптографічно слабкі ключі.

Крім програмних атак, QRNG також можуть бути вразливими до апаратних дефектів або збоїв під час інтеграції на фізичному рівні. Наприклад, дефекти мікросхем або некоректне налаштування апаратного забезпечення можуть призводити до збоїв у генерації ключів. У випадках масштабних веб-сервісів або хмарних платформ ці ризики є особливо критичними, оскільки навіть незначна похибка може призвести до масштабних витоків даних.

Важливо враховувати і атаки через бічні канали, що використовують витік інформації із систем QRNG шляхом аналізу часу виконання, енергоспоживання або електромагнітних випромінювань. Такі атаки є складними для виявлення, але вони можуть надати зловмисникам цінну інформацію про вихідні дані генератора.

Метою статті є класифікація та аналіз основних типів атак на веб-сервіси QRNG, обґрунтування та дослідження ефективних методів їх запобігання. Основна увага приділяється програмним атакам, атакам через бічні канали та уразливостям апаратного рівня. Також роз-

глядаються сучасні методи захисту, такі як сертифікація QRNG, мультифакторна перевірка даних та алгоритми моніторингу, що дозволяють виявляти потенційні загрози в реальному часі.

1. Атаки на QRNG на програмному рівні

1.1. Атаки на криптографічні бібліотеки

Одним із найпоширеніших векторів атак на QRNG є компрометація криптографічних бібліотек, які забезпечують генерацію та обробку випадкових чисел для захищених з'єднань. Бібліотеки, такі як OpenSSL, використовуються для реалізації протоколів захисту мережевого трафіку, зокрема TLS (Transport Layer Security). Уразливості у цих бібліотеках можуть виникати через помилки в коді екстрактора QRNG або відсутність стандартизованих механізмів перевірки вихідних даних генератора в реальному часі.

Атака може бути здійснена шляхом підміни джерела випадкових чисел під час виконання криптографічних операцій [1]. Якщо бібліотека не виконує належної перевірки джерела генерації чисел, зловмисник може інтегрувати менш стійкий генератор, який дозволяє прогнозувати вихідні значення. У такому випадку TLS-з'єднання стає вразливим до атаки "людина посередині", що дозволить розшифрувати конфіденційні дані.

Ще одним прикладом є атака на рівні ініціалізації QRNG. Під час запуску криптографічної системи QRNG генерує первинні значення, які використовуються як сеансові ключі. Якщо зловмисники отримують доступ до цього етапу генерації, вони можуть маніпулювати ключами або перехоплювати їх до моменту шифрування. Уразливості такого типу часто виникають у результаті недостатньої ентропії на ранніх етапах генерації або внаслідок слабких початкових параметрів бібліотеки.

1.2. Маніпуляція середовищем виконання

Маніпуляція середовищем виконання коду екстрактора QRNG є критичним вектором атак, який дозволяє зловмисникам впливати на процес генерації чисел під час його роботи. Якщо програмне середовище недостатньо захищене або має недоліки в системі доступу, зловмисник може впровадити шкідливий код, що змінить поведінку екстрактора. Наприклад, шляхом ін'єкції коду на рівні операційної системи можливе перехоплення результатів генерації або створення навмисних збоїв у роботі QRNG.

Навіть мінімальні маніпуляції середовищем можуть мати катастрофічні наслідки для криптографічних систем, які залежать від QRNG [2]. Середовище виконання може піддаватися атакам під час віддалених оновлень програмного забезпечення, що дає можливість зловмисникам модифікувати налаштування екстрактора. Уразливості виникають через відсутність контрольних сум або механізмів перевірки цілісності файлів під час оновлення.

Ще одним аспектом є використання вразливостей системної пам’яті. Зловмисники можуть отримати доступ до регістрів QRNG або буферів даних і підмінити вихідні значення випадкових чисел. Такий підхід дозволяє створити передбачувані ключі шифрування, що значно знижує рівень безпеки системи.

1.3. Атаки бічними каналами (Side-channel attacks)

Атаки бічними каналами є одним із найбільш витончених типів атак на QRNG. Вони базуються на аналізі непрямих фізичних характеристик системи під час генерації випадкових чисел, таких як споживання енергії, час виконання операцій, електромагнітне випромінювання або тепловий вплив. Ці фактори можуть містити інформацію про внутрішні процеси QRNG, що дозволяє зловмиснику відновити частину або всі вихідні значення генератора.

Ймовірність успішної атаки через бічний канал можна розрахувати за формулою

$$P_{attack} = 1 - \left(1 - \frac{E_{leak}}{E_{total}}\right)^n, \quad (1)$$

де E_{leak} – кількість енергії, що витікає з QRNG; E_{total} – загальна енергія процесу генерації, n – кількість спроб атаки.

Атаки бічними каналами можуть бути реалізовані навіть на рівні захищених систем із фізичним захистом QRNG [3]. Використання високочутливих датчиків дозволяє аналізувати найдрібніші коливання напруги або температури, що створює можливості для витоку даних. Наприклад, QRNG, що використовують фотонні технології, можуть піддаватися атакам через аналіз випромінювання лазерів або зміну інтенсивності світла.

Щоб мінімізувати ризики таких атак, виробники QRNG впроваджують механізми маскування даних, які додають випадкові шуми або спотворюють фізичні характеристики під час генерації чисел. Проте, ці методи не завжди є ефективними проти сучасних бічних атак, що використовують машинне навчання для аналізу навіть прихованих закономірностей.

Таким чином, атаки на QRNG на програмному рівні є серйозною загрозою для криптографічних систем. Ефективний захист QRNG вимагає комплексного підходу, який включає сертифікацію криптографічних бібліотек, контроль середовища виконання та захист від атак через бічні канали.

2. Уразливості на рівні інтеграції

2.1. Атаки через апаратну інфраструктуру

Інтеграція QRNG на апаратному рівні є важливим, але водночас вразливим етапом у забезпеченні криптографічної безпеки веб-сервісів. Уразливості можуть виникати в результаті фізичних дефектів апаратного забезпечення або недостатньо ретельної перевірки під час виробництва QRNG-чипів. Зловмисники можуть реалізовувати атаки через використання дефектних або підроблених компонентів, що мають вбудовані "бекдори" або інші приховані механізми [4].

Ці "бекдори" можуть активуватися під час криптографічних операцій, надаючи зловмиснику доступ до процесу генерації чисел або навіть можливість підміняти вихідні значення QRNG. Наприклад, у випадку інтеграції QRNG в процесори або мікроконтролери, зловмисники можуть зчитувати частину вихідних ключів через специфічні команди на рівні апаратного інтерфейсу. Такі атаки надзвичайно складно виявити, оскільки вони не залишають видимих слідів на програмному рівні.

Крім того, QRNG можуть бути вразливими до атак типу фізичного доступу. Наприклад, у випадку зламів дата-центрів або фізичного вторгнення до серверних кімнат, зловмисники можуть підміняти QRNG або вбудовувати шкідливі компоненти, які перехоплюють криптографічні ключі під час їхньої генерації. Для мінімізації таких ризиків необхідно впроваджувати багаторівневий контроль обладнання, включаючи регулярну перевірку QRNG за допомогою тестування на сторонні компоненти та приховані модифікації.

2.2. Апаратні дефекти і збої

Апаратні дефекти та збої можуть виникати як на етапі виробництва QRNG, так і під час їхньої експлуатації. Навіть найменші відхилення у процесі виготовлення мікросхем можуть спричинити зниження рівня випадковості, що робить генератор менш надійним для криптографічних задач. QRNG, інтегровані в хмарні обчислювальні системи, можуть піддаватися ризику часткової деградації апаратних компонентів через тривале навантаження або температурні перепади [5].

У таких випадках генератор може видавати некоректні або повторювані значення, що критично знижує криптографічну стійкість системи. Крім того, можливі перебої в електропостачанні або помилки у зв'язку між компонентами QRNG та іншими модулями системи, що може призвести до неповного або пошкодженого процесу генерації чисел.

Для виявлення таких дефектів важливо впроваджувати системи самодіагностики QRNG, які можуть виявляти будь-які відхилення у вихідних даних генератора. Наприклад, регулярна перевірка вихідних чисел на предмет відповідності статистичним критеріям випадковості до-

зволяє оперативно ідентифікувати деградацію апаратного забезпечення. Крім того, розробка резервних механізмів генерації дозволяє миттєво замінювати пошкоджені QRNG, запобігаючи можливості витоків даних.

2.3. Інтеграційні конфлікти з іншими компонентами системи

QRNG часто інтегруються з іншими криптографічними компонентами, такими як традиційні PRNG або системи шифрування на основі апаратних модулів безпеки (Hardware Security Modules, HSM). У таких випадках можливі конфлікти між вихідними значеннями QRNG та іншими генераторами, що може призвести до помилок у криптографічних алгоритмах або навіть повної втрати ентропії. Некоректна конфігурація системи може призвести до зниження рівня випадковості вихідних чисел, оскільки QRNG і PRNG можуть працювати паралельно без належної синхронізації [6].

Додатковим ризиком є конфлікт протоколів передачі даних. У деяких випадках QRNG передають вихідні значення через загальні канали зв’язку, які можуть бути перехоплені або модифіковані. Це створює можливість для атаки підміни вихідних чисел на рівні передачі даних між компонентами системи.

Для захисту від таких атак, необхідно впроваджувати ізольовані канали передачі даних між QRNG та криптографічними бібліотеками, а також застосовувати механізми апаратної автентифікації генератора. Також доцільно використовувати алгоритми перевірки сумісності компонентів та регулярне оновлення системного програмного забезпечення, щоб забезпечити коректну роботу QRNG у комплексних криптографічних системах.

Таким чином, інтеграція QRNG на апаратному рівні створює численні виклики, які потребують детального аналізу та впровадження багаторівневих механізмів захисту. Підходи, що включають регулярну перевірку обладнання, діагностику та ізольовані канали передачі даних, є важливими для забезпечення надійності QRNG у сучасних криптографічних системах.

3. Механізми захисту QRNG від атак

3.1. Валідація та сертифікація QRNG

Валідація та сертифікація QRNG є критичними етапами для гарантування їхньої надійності та стійкості до атак. Ці процеси дозволяють не лише підтвердити відповідність QRNG міжнародним стандартам, але й виявити потенційні вразливості до моменту інтеграції в реальні системи. Важливим елементом є багатоступенева перевірка QRNG як на етапі виробництва, так і в процесі експлуатації.

Процес сертифікації включає кілька рівнів:

1. Тестування випадковості – перевірка QRNG на відповідність критеріям випадковості та статистичним тестам, таким як NIST SP800-90, Dieharder та тест Фур'є-аналізу.

2. Перевірка на фізичні дефекти – аналіз мікросхем QRNG на наявність потенційних апаратних дефектів або вразливостей, які можуть вплинути на генерацію чисел.

3. Програмна сертифікація – тестування програмного забезпечення, яке обробляє вихідні дані QRNG, з метою виявлення вразливостей на рівні алгоритмів.

Оскільки нові методи атак постійно розвиваються, регулярне оновлення сертифікаційних стандартів для QRNG є важливим. Сертифікація має відбуватися в умовах реальних навантажень і включати сценарії атаки через бічні канали, апаратні збої та спроби компрометації середовища виконання.

Крім того, впровадження систем аудиту та постійного моніторингу QRNG дозволяє своєчасно виявляти потенційні відхилення у генерації випадкових чисел. Наприклад, якщо генератор демонструє повторюваність чисел або знижує рівень випадковості, система автоматично сигналізує про необхідність заміни чи повторної сертифікації генератора.

3.2. Мультифакторна перевірка даних

Мультифакторна перевірка є ключовим механізмом підвищення стійкості QRNG до атак та апаратних збоїв. Вона передбачає використання кількох незалежних джерел випадкових чисел для перевірки коректності вихідних даних. У разі розбіжності між джерелами генерації система автоматично блокує подальшу обробку чисел або ініціює повторну генерацію.

Одним із прикладів такої практики є інтеграція QRNG із традиційними PRNG для перевірки відповідності вихідних значень. У такій системі QRNG виконує основну функцію генерації ключів, тоді як PRNG працює як резервний механізм для перевірки статистичних закономірностей.

В роботі [8] представлена гібридна модель, у якій QRNG працює спільно із квантовою ключовою дистрибуцією (Quantum Key Distribution, QKD). Цей підхід дозволяє значно підвищити рівень безпеки, оскільки навіть якщо QRNG буде скомпрометований, QKD забезпечить захист каналів передачі ключів.

Крім того, мультифакторна перевірка включає:

1. Контроль фізичних параметрів QRNG, таких як температура, рівень енергоспоживання та стабільність вихідних даних.

2. Використання кількох QRNG в одній системі з подальшим порівнянням результатів між генераторами.

3. Інтеграція з апаратними модулями безпеки (HSM), які виконують додаткові перевірки та захищають QRNG від зовнішніх атак.

3.3. Моніторинг та виявлення аномалій

Моніторинг та виявлення аномалій є невід'ємною частиною комплексної системи захисту QRNG. Оскільки атаки на QRNG можуть бути як програмними, так і фізичними, необхідно використовувати багаторівневі методи аналізу, які дозволяють виявляти будь-які відхилення у роботі генератора на різних етапах його функціонування.

Системи моніторингу QRNG спрямовані на контроль вихідних даних генератора, аналіз фізичних характеристик генератора, виявлення стороннього втручання та запобігання апаратним збоям. Ці механізми мають бути адаптовані до специфіки QRNG, оскільки квантові процеси є надзвичайно чутливими до зовнішніх факторів, таких як зміни температури, електромагнітні поля або шум.

Також є важливим впровадження алгоритмів машинного навчання (machine learning, ML) для аналізу вихідних даних QRNG у реальному часі [9]. Такі алгоритми здатні виявляти приховані закономірності або повторення у вихідних числах, які можуть бути ознакою компрометації генератора.

До ключових методів моніторингу належать:

1. Аналіз фізичних параметрів генерації чисел.

Моніторинг фізичних параметрів QRNG дозволяє виявити відхилення, які можуть свідчити про можливу атаку або апаратний дефект. Наприклад, зміни в енергоспоживанні або теплових характеристиках QRNG можуть вказувати на атаку через бічні канали або спробу маніпуляції середовищем виконання.

Для підвищення ефективності цього підходу використовуються:

– датчики температури та енергоспоживання, які постійно фіксують дані про роботу QRNG. У разі виявлення відхилень система автоматично переходить у режим діагностики або аварійного відключення.

– спектральний аналіз сигналів QRNG, що дозволяє виявляти частотні відхилення та приховані закономірності у процесі генерації чисел.

2. Часовий аналіз та аналіз продуктивності QRNG

Моніторинг продуктивності QRNG включає аналіз часу генерації чисел та перевірку відповідності вихідних даних заданим криптографічним стандартам. Якщо генератор почи-

нає працювати повільніше або, навпаки, демонструє надто швидку генерацію чисел, це може свідчити про внутрішні збої або зовнішнє втручання.

Особливу увагу слід приділяти:

– затримкам у генерації чисел, що можуть бути ознакою атаки на рівні програмного забезпечення.

– раптовим змінам у швидкості генерації ключів, які можуть свідчити про спробу підміни QRNG або маніпуляції апаратними компонентами.

3. Використання штучного інтелекту (Artificial Intelligence, AI) для моніторингу QRNG

Одним із найперспективніших напрямків у галузі моніторингу QRNG є використання алгоритмів машинного навчання (ML) та штучного інтелекту (AI). AI може аналізувати великі обсяги даних та виявляти приховані закономірності, які не піддаються класичним методам аналізу.

Алгоритми глибокого навчання (DL) здатні навчатися на історичних даних QRNG і виявляти навіть найдрібніші відхилення у вихідних числах або фізичних характеристиках генератора. У разі виявлення аномалій AI може автоматично ініціювати перехід на резервний QRNG або заблокувати компрометований генератор.

Крім того, AI-системи можуть проводити:

– автоматичний аналіз кореляцій вихідних чисел, що дозволяє виявляти повторюваність або закономірності у генерації випадкових чисел.

– детекцію аномалій у реальному часі, яка дозволяє миттєво реагувати на будь-які відхилення у роботі генератора.

4. Автоматизовані системи аварійного моніторингу

Важливим компонентом є впровадження автоматизованих систем аварійного моніторингу QRNG, які працюють у безперервному режимі та миттєво реагують на виявлення підозрілих процесів.

Автоматизовані системи моніторингу включають:

– резервні генератори (Backup QRNG), які активуються у разі виявлення дефектів в основному генераторі.

– аварійне відключення QRNG з подальшим аналізом та діагностикою виявлених проблем.

– логування всіх операцій генератора для подальшого аудиту та аналізу на предмет можливих атак або збоїв.

Моніторинг QRNG має бути інтегрований у загальну систему кібербезпеки організації. Це дозволяє синхронізувати дані з інших компонентів безпеки та виявляти комплексні атаки, які можуть поєднувати програмні, апаратні та фізичні вектори загроз.

Наприклад, система моніторингу QRNG може взаємодіяти з системами управління подіями та інцидентами (SIEM), які забезпечують централізований збір та аналіз даних про безпеку.

Моніторинг QRNG є не лише засобом виявлення аномалій, але й інструментом для довготривалої оцінки ефективності системи. Виявлення поступової деградації апаратних компонентів або зниження рівня ентропії генератора дозволяє своєчасно вжити заходів щодо заміни або оновлення обладнання.

Таким чином, комплексний підхід до моніторингу QRNG, що включає фізичний аналіз, часовий контроль, використання AI та інтеграцію з іншими системами безпеки, забезпечує високий рівень стійкості квантових генераторів до сучасних загроз та атак.

3.4. Автоматизація захисних механізмів

Окремим напрямом розвитку захисних механізмів QRNG є впровадження автоматизованих систем захисту, які здатні самостійно реагувати на аномалії та ініціювати процеси аварійної зупинки генерації чисел або перехід на резервний генератор.

Ключові елементи автоматизації:

– система швидкої заміни QRNG – резервні генератори підключаються до системи миттєво після виявлення аномалій, що забезпечує безперервність генерації чисел.

– автономне оновлення сертифікації – генератор автоматично проходить перетестування після критичних оновлень програмного забезпечення або виявлення потенційних загроз.

– дистанційний контроль – можливість віддалено відключати або перезавантажувати QRNG у разі виявлення фізичних атак або підозрілих процесів.

Завдяки впровадженню таких автоматизованих систем, QRNG стають значно менш вразливими до атак як на програмному, так і на апаратному рівнях.

Таким чином, комплексний підхід до захисту QRNG включає в себе сертифікацію, мультифакторну перевірку та постійний моніторинг. Усі ці елементи дозволяють значно підвищити стійкість квантових генераторів до сучасних атак та забезпечити їхню надійну інтеграцію в криптографічні системи майбутнього.

Висновки

Впровадження QRNG в системи захисту інформації супроводжується низкою викликів, які можуть призвести до серйозних загроз для безпеки даних. У цій роботі були розглянуті потенційні вразливості QRNG на програмному рівні, під час інтеграції та на рівні апаратного забезпечення.

Атаки на QRNG на програмному рівні залишаються одним із найпоширеніших векторів загроз. Зловмисники можуть використовувати вразливості криптографічних бібліотек, маніпулювати середовищем виконання або здійснювати атаки через бічні канали, що призводить до витоку ключів або компрометації вихідних даних. Недостатній захист програмного середовища або відсутність механізмів моніторингу якості QRNG може стати причиною серйозних проблем у роботі систем кіберзахисту.

Атаки на рівні інтеграції QRNG в апаратне забезпечення створюють додаткові загрози, оскільки навіть найменші дефекти мікросхем або неправильно налаштовані системи можуть суттєво знизити рівень випадковості вихідних чисел. Фізичний доступ до QRNG відкриває можливості для зловмисників впровадити апаратні закладки або модифікації, що ускладнює виявлення атак стандартними методами.

Особливу увагу слід приділяти атакам через бічні канали. Ці атаки використовують фізичні параметри роботи QRNG, зокрема енергоспоживання, теплові відхилення або електромагнітні сигнали, щоб отримати інформацію про вихідні дані генератора. Подібні атаки важко виявити та зупинити, оскільки вони не залишають цифрових слідів і експлуатують фізичні характеристики системи.

Для мінімізації цих загроз необхідно впроваджувати комплексні захисні механізми на всіх рівнях роботи QRNG. Важливим етапом є валідація та сертифікація QRNG з дотриманням міжнародних стандартів. Цей процес дозволяє гарантувати, що генератор працює коректно і відповідає вимогам криптографічної безпеки. Регулярне тестування, аналіз статистичної випадковості та виявлення фізичних дефектів забезпечують стабільність роботи генератора в реальних умовах.

Додатковий рівень захисту забезпечується за рахунок мультифакторної перевірки вихідних даних, яка використовує кілька незалежних джерел випадковості для перевірки QRNG. Поєднання QRNG із традиційними PRNG або QKD дозволяє мінімізувати ризики, пов’язані з компрометацією одного джерела генерації.

Важливим компонентом є системи моніторингу та виявлення аномалій, які дозволяють виявляти потенційні відхилення у роботі QRNG у режимі реального часу. Використання алгоритмів машинного навчання та штучного інтелекту для аналізу вихідних даних генератора підвищує ефективність захисту та дозволяє оперативно реагувати на загрози. Постійний моніторинг фізичних параметрів роботи QRNG допомагає виявити спроби атак через бічні канали або апаратні дефекти.

Окремим напрямом є автоматизація захисних механізмів, яка дозволяє автоматично перемикати генератори, перезавантажувати систему або здійснювати аварійну зупинку генерації чисел у разі виявлення аномалій. Це дозволяє зменшити час реакції на загрози та гарантувати безперебійну роботу систем шифрування.

У перспективі розвиток квантових обчислень та квантових комунікаційних систем потребуватиме вдосконалення QRNG та впровадження нових стандартів безпеки. Інтеграція QRNG із квантовими комп'ютерами та квантовими мережами дозволить створити більш стійкі до атак криптографічні системи. Водночас, це створить нові виклики, пов'язані з необхідністю захисту квантових систем від фізичних та апаратних атак.

Впровадження QRNG у веб-сервіси та критичні інфраструктури потребує комплексного підходу до захисту, який поєднує сертифікацію, мультифакторну перевірку, моніторинг та автоматизацію захисних механізмів. Такий підхід дозволить значно знизити ризики та забезпечити максимальний рівень безпеки для криптографічних систем.

Список літератури:

1. Blanco-Romero J., Lorenzo V., & Almenares F. Evaluating integration methods of a quantum random number generator in OpenSSL for TLS // Computer Networks. 2024. Vol 255, article №110877. doi:10.1016/j.comnet.2024.110877
2. Henry Elizabeth. (2024). The Role of Quantum Random Number Generation in Enhancing Encryption Security. SSRN, doi:10.2139/ssrn.4966139
3. Regazzoni F., et al. (2021). A high speed integrated quantum random number generator with on-chip real-time randomness extraction. doi:10.48550/arXiv.2102.06238
4. Bishwas A. K., & Sen M. (2024). Strategic Roadmap for Quantum-Resistant Security: A Framework for Preparing Industries for the Quantum Threat. doi:10.48550/arXiv.2411.09995
5. Pedone I., et al. (2021). Toward a complete software stack to integrate quantum key distribution in a cloud environment // IEEE Access. doi:10.1109/ACCESS.2021.3102313
6. Adetifa, O. E. Comparative Analysis and Applications of Quantum Random Number Generators: Evaluating Efficiency, Statistical Properties, and Real-world Use Cases // Morgan State University. ProQuest Dissertations & Theses, 2024. 31141646. link https://www.proquest.com/openview/0e228ff803da898521302a83a2d3b7d4 preview lang Eng
7. Mehmood A., et al. (2024). Advances and vulnerabilities in modern cryptographic techniques // IEEE Access. doi:10.1109/ACCESS.2024.3367232
8. Huang L., et al. A practical hybrid quantum-safe cryptography scheme between data centers // Proceedings Volume 11540, Emerging Imaging and Sensing Technologies for Security and Defence V; and Advanced Manufacturing Technologies for Micro- and Nanosystems in Security and Defence III; 1154008. 2020. doi:10.1117/12.2573558
9. Cherbal S., Zier A., Hebal S. et al. Security in internet of things: a review on approaches based on blockchain, machine learning, cryptography, and quantum computing // J. Supercomput. 2024. Vol. 80. P. 3738–3816. doi:10.1007/s11227-023-05616-2

Надійшла до редколегії 09.01.2025

Відомості про авторів:

Моргуль Дмитро Миколайович – Харківський національний університет імені В. Н. Каразіна, аспірант кафедри кібербезпеки інформаційних систем, мереж і технологій; Україна; e-mail: dmitriymdn85@gmail.com; ORCID: https://orcid.org/0009-0007-5272-1634

Нарєжній Олексій Павлович – канд. техн. наук, Харківський національний університет імені В.Н. Каразіна, доцент кафедри кібербезпеки інформаційних систем, мереж і технологій; Україна; e-mail: o.nariezhnii@karazin.ua; ORCID: https://orcid.org/0000-0003-4321-0510

Гріненко Тетяна Олексіївна – канд. техн. наук, доцент, Харківський національний університет радіоелектроніки, доцент кафедри безпеки інформаційних технологій; Україна; e-mail: tetiana.grinenko@nure.ua; ORCID: https://orcid.org/0000-0002-8251-8991

УДК 621.317.76.089.68:621.373.82 **DOI:10.30837/rt.2025.1.220.05**

О.А. СНЄОСІКОВ, *О.П. НАРЄЖНІЙ, канд. техн. наук, Т.О. ГРІНЕНКО, канд. техн. наук*

МОДЕЛІ ТА МЕТОДИ ЗАХИСТУ ВІД КІБЕРЗАГРОЗ АВТОНОМНОЇ СИСТЕМИ ДИФЕРЕНЦІАЛЬНОЇ КОРЕКЦІЇ ГЛОБАЛЬНИХ НАВІГАЦІЙНИХ СУПУТНИКОВИХ СИСТЕМ

Вступ

Розвиток глобальних навігаційних супутникових систем (Global navigation satellite systems, GNSS) триває вже понад півстоліття, починаючи з перших експериментальних систем у 1960-х роках до сучасних високоточних глобальних навігаційних систем, що використовуються у всьому світі.

Сучасний ринок GNSS характеризується функціонуванням кількох ключових супутникових навігаційних систем, а саме:

– GPS (Global Positioning System), розроблена Сполученими Штатами Америки (США) – має на орбіті планети близько 31 активних супутників [1, 2];

– GLONASS (Глобальна навігаційна супутникова система), створена Радянським Союзом (тепер Російська Федерація) – має 24 активних супутників [3];

– Galileo – супутникова система навігації Європейського Союзу та Європейського космічного агентства, наразі функціонує з 24 активними супутниками (повна констеляція налічує 30 супутників, враховуючи 6 резервних) [4];

– BeiDou – супутникова система навігації Китайської Народної Республіки, працює з 30 активними супутниками [5].

А також регіональні системи:

– IRNSS (NavIC) – індійська система навігації – має 7 супутників для забезпечення регіонального покриття [6];

– QZSS – японська система навігації – забезпечує регіональне покриття за допомогою 4 супутників [7].

Доповненням до глобальних систем GNSS є супутникові системи корекції та моніторингу, які забезпечують підвищення точності позиціонування за рахунок виправлення похибок супутникових сигналів та моніторингу їх стабільності, забезпечуючи точність до 1-2 метрів.

До таких систем належать:

– WAAS (Wide Area Augmentation System) – система, розроблена у Сполучених Штатах Америки, яка використовує мережу наземних базових станцій для обчислення коригувальних поправок, що передаються супутниками. WAAS дозволяє значно підвищити точність GPS-позиціювання, забезпечуючи горизонтальну точність до 1-2 метрів у багатьох регіонах [8].

– EGNOS (European Geostationary Navigation Overlay Service) – європейська система, що доповнює GPS шляхом передачі коригувальних сигналів із геостаціонарних супутників і наземних базових станцій. EGNOS покращує точність і надійність навігаційних даних у Європі [9].

– СДКМ (Російська система диференційної корекції) – система, що використовується для корекції навігаційних даних супутникової системи GLONASS, забезпечуючи підвищену точність позиціонування в Росії та суміжних регіонах [3].

– GAGAN (GPS Aided Geo Augmented Navigation) – індійська система супутникового підсилення, розроблена для забезпечення високоточних навігаційних послуг в Індії та прилеглих регіонах. GAGAN покращує точність позиціонування завдяки використанню наземної інфраструктури та супутникових сигналів [6].

– MSAS (Multi-functional Satellite Augmentation System) – японська система супутникового підсилення, яка доповнює навігаційні сигнали GPS для забезпечення більшої точності позиціонування в регіоні Японії [10].

Системи корекції і моніторингу значно підвищують ефективність та точність GNSS-систем, дозволяючи користувачам отримувати дані з набагато вищою точністю, що є критично важливим для застосувань у авіації, морській навігації, сільському господарстві, геодезії та інших галузях.

Поєднання GNSS із наземними технологіями, такими як інерційна навігація, диференціальні системи корекції (DGPS, RTK, SBAS), LTE, 5G для передачі поправок, лазерне сканування (LiDAR) та системи машинного зору, відкриває нові можливості для розробки технологій, що забезпечують не лише високу точність, але й підвищену надійність та цілісність навігаційних сигналів.

За прогнозами, встановлена база GNSS-пристроїв буде стрімко зростати: з 5,6 мільярдів одиниць у 2023 р. до майже 9,0 мільярдів одиниць у 2033 р. [9]. Цей суттєвий ріст відображає зростаючу потребу в супутникових навігаційних технологіях у різних секторах економіки, від автомобільної промисловості та землеробства до електронних комунікацій та фінансових послуг.

Очікується, що до 2030 р. глобальний ринок GNSS виросте з рівня 260 мільярдів євро (станом на 2023 р.) до 590 мільярдів євро, що свідчить про суттєве розширення галузі [9].

Екосистема GNSS є багаторівневою та охоплює всі аспекти роботи технології – від супутникових угруповань до кінцевих користувачів. Вона поділяється на три ключові рівні:

1. Інфраструктурний рівень (базовий). Цей рівень включає операторів супутникових систем, таких як GPS (США), GLONASS (Росія), Galileo (Європейський Союз) та BeiDou (Китай). Вони відповідають за розробку, запуск та обслуговування супутників, що забезпечують глобальне покриття навігаційними сигналами.

2. Технологічний рівень (середній). Сюди входять виробники мікросхем та приймачів, які розробляють обладнання для прийому та обробки GNSS-сигналів. Наприклад, компанія Septentrio спеціалізується на високоточних GNSS-приймачах для різних застосувань, включаючи БПЛА.

3. Прикладний рівень (верхній). Цей рівень охоплює кінцеві застосування GNSS-технологій у різних галузях, таких як транспорт, безпека, сільське господарство, геодезія та критична інфраструктура. Наприклад, сервіс високої точності (High Accuracy Service, HAS) від навігаційної системи Galileo надає сантиметрову точність позиціонування в реальному часі, що є критично важливим для геодезичних робіт та точного землеробства [11].

Постановка проблеми

GNSS відіграють ключову роль у забезпеченні стабільної роботи критичних секторів економіки та національної безпеки. Відповідно до Закону України "Про критичну інфраструктуру" № 1882-IX від 15 листопада 2021 р. до критично важливих сфер належать: «15) космічна діяльність, космічні технології та послуги» [12]. Це прямо включає GNSS, оскільки вони є невід'ємною частиною космічних технологій і надають критично важливі послуги для безпеки, економічної та соціальної стабільності держави. Проте, ця технологія стала мішенню для кіберзагроз, що не може не впливати на надійність та безпеку навігаційних систем. Кібератаки на GNSS можуть спричиняти спотворення сигналів, перехоплення даних або навіть повну дезорієнтацію користувачів, що створює значну загрозу функціонуванню критичної інфраструктури.

Транспортні системи, енергетика, аеропорти та морські порти стають об'єктами підвищеного ризику, оскільки їхнє функціонування значною мірою залежить від точних і достовірних даних GPS [13]. Основний перелік споживачів технологій GNSS включає автомобільні навігаційні системи, смартфони та планшети, логістичні та транспортні компанії, повітряну та морську навігацію, туризм і активний відпочинок, сільське господарство, наукові дослідження, аварійно-рятувальні служби, спортсменів та фітнес-програми, банківський сектор, бізнес-корпорації та служби доставки. Враховуючи це, кібератаки на GPS можуть мати значні наслідки для суспільної безпеки та економічної стабільності країни [14]. У зв'язку з

цим забезпечення захисту GPS-систем стає надзвичайно важливим для підтримки функціонування цих критично важливих сфер та забезпечення національної безпеки.

Найбільш відомими прикладами кібератак на GNSS за останні роки є:

– 2017 р. – Кібератака NotPetya та WannaCry. Масштабні кібератаки на інформаційно-комунікаційні системи (ІКС), зокрема ІКС GNSS, вразили навігаційні системи транспортних суден і портів, викликавши перебої в роботі логістичних ланцюгів [15];

– 2017 – 2018 рр. – перешкоди GPS під час військових навчань "Захід-2017" та "Єдиний тризуб-2018". Було здійснено глушіння сигналів GPS у Латвії та Норвегії під час військових навчань, що вплинуло на цивільні авіаційні системи [16];

– 2020 р. – Кібератака на сервери Garmin. Хакерська група Evil Corp здійснила атаку вірусом-вимагачем WastedLocker, що вивело з ладу сервіси ІКС Garmin Connect та інші онлайн-служби. Вимагали викуп у 10 млн. доларів [17];

– 2022 р. – Атака на супутникову мережу KA-SAT. Перед початком повномасштабного вторгнення в Україну була здійснена атака на супутникову мережу KA-SAT, що призвело до перебоїв у роботі інтернет-з'єднання в Україні та Європі [18];

– 2024 р. – Глушіння сигналів GPS у Балтійському регіоні. Велика кількість авіарейсів до Великої Британії зазнала навігаційних проблем через глушіння сигналів GPS у Балтійському регіоні [19].

За період з 2022 – 2025 роки Україна також стала свідком серії інцидентів, пов'язаних із кібератаками на системи глобального позиціонування (GPS). Спостереження приватних компаній бізнес-сегменту держави вказують на різке збільшення відхилень у моніторингу GPS-приймачів, що свідчить про зростання кібератак на GPS у 2022 – 2025 роках (рис. 1).

Рис. 1. Кібератаки на GPS

На сьогодні кібератаки на супутникові навігаційні системи можуть здійснювати як приватні криптоаналітики, так і криптоаналітики третього рівня, використовуючи найпотужніші засоби для кібератак. Таким чином, кібератаки на супутникові системи навігації в Україні вимагають негайної уваги та вивчення через потенційно серйозні наслідки для національної безпеки та економіки.

У цій роботі розглядається реалізація концепції «Створення системи координатно-часового та навігаційного забезпечення України з використанням інформації, отриманої від глобальних навігаційних супутникових систем різних держав» [20]. Відповідно до Концепції реалізації державної політики у сфері космічної діяльності до 2032 р. [21], затвердженої

Розпорядженням КМУ № 238-р від 30 березня 2011 р., планується створення національної системи геоінформаційного забезпечення та проведення моніторингу надзвичайних ситуацій. Ця система буде складовою частиною європейської програми Copernicus, яка до 2012 року мала назву Global Monitoring for Environment and Security (GMES) [22], та світової Global Earth Observation System of Systems (GEOSS), яка буде забезпечувати експлуатацію її інформаційних сервісів зацікавленими користувачами [23].

Проблема, яка набуває особливої актуальності в межах цього дослідження, пов'язана з тим, що на сьогодні ще недостатньо врегульоване на законодавчому рівні питання щодо впровадження діяльності у сфері супутникової навігації, зокрема щодо [24]:

- забезпечення безпечного використання інформації GNSS;
- розроблення та застосування національних стандартів і технічних регламентів щодо виробництва апаратури, засобів супутникової навігації, спеціалізованого програмного забезпечення, надання супутникових навігаційних інформаційних послуг;
- обміну інформацією між вітчизняними та іноземними функціональними доповненнями;
- захисту інформації у сфері супутникової навігації відповідно до вимог Закону України "Про захист інформації в інформаційно-комунікаційних системах" [25];

Очікувані результати після ухвалення проєкту Закону України "Про державне регулювання у сфері супутникової навігації" [24] передбачають такі переваги, як підвищення рівня безпеки та надійності транспортно-логістичного комплексу, розвиток його інфраструктури, а також підвищення якості надання навігаційних послуг користувачам навігаційних послуг України.

Діяльність у сфері супутникової навігації здійснюється за такими напрямами [24, 26]:

1. Моніторинг з використанням функціональних навігаційних інформаційних систем для об'єктів супутникової навігації в галузях будівництва, енергетики та транспортної інфраструктури з метою своєчасного запобігання виникненню надзвичайних ситуацій та ліквідації їх наслідків.

2. Створення, розвиток і експлуатація функціональних доповнень та навігаційних інформаційних систем, а також надання супутникових навігаційних інформаційних послуг користувачам. Це включає обмін інформацією між вітчизняними та іноземними функціональними доповненнями на основі вимог законодавства та міжнародних договорів.

Відповідно до проєкту Закону України "Про державне регулювання у сфері супутникової навігації" користувачі глобальних навігаційних супутникових систем можуть бути тимчасово обмежені в супутникових навігаційних визначеннях власною апаратурою та засобами супутникової навігації (повністю або з бажаним рівнем точності) та в отриманні інших супутникових навігаційних інформаційних послуг у певних районах та/або на певних об'єктах, де існує військова загроза або небезпека терористичної діяльності. Це положення регламентує впровадження заходів протидії атакам по типу GPS spoofing та GPS jamming на GNSS, а також захист від інших хакерских кібератак на ІКС GNSS.

Захист інформації у сфері супутникової навігації в обов'язковому порядку має здійснюватися відповідно до вимог Закону України "Про електронні комунікації" [27]. Захисту підлягає інформація, яка:

- постачається у складі супутникових навігаційних інформаційних послуг користувачам функціональних доповнень та навігаційних інформаційних систем, що виконують завдання у сфері оборони та національної безпеки, цивільного захисту населення та об'єктів інфраструктури, а також охорони правопорядку;
- опрацьовується у функціональних навігаційних інформаційних системах.

Зокрема, проєктом Закону України "Про затвердження Загальнодержавної цільової науково-технічної космічної програми України на 2021 – 2025 роки" (реєстр. № 6129 від 04.10.2021) [28] передбачено захід "Розвиток Системи координатно-часового та навігаційного забезпечення України та забезпечення використання інформаційних сервісів європейської

навігаційної супутникової системи EGNOS/Galileo на території України" з фінансуванням у розмірі 40,78 млрд. гривень до 2025 р.

Аналіз основних досліджень і публікацій.

Проблематиці кіберзахисту супутникового зв'язку присвячено численні наукові праці. Зокрема, у [29] висвітлюються сучасні технології захисту від GPS spoofing, серед яких: аналіз потужності сигналу та його характеристик, застосування диференційного GPS (DGPS), використання мультичастотних та багатосистемних приймачів, автентифікація сигналів, фільтрація на основі методів машинного навчання, а також інтеграція з інерційними навігаційними системами (ІНС). В роботі [30] надано аналіз методів захисту безпілотних літальних апаратів (БПЛА) від атак типу GPS spoofing для забезпечення безпечної навігації. Розглядаються різні підходи до підвищення функціональної ефективності БПЛА в умовах кіберзагроз, а саме, направлені на оптимізацію польотів алгоритми та методи, що дозволяють швидше та точніше вирішувати задачі планування польотів, визначення аномалій у навігаційних даних, інтеграцію штучного інтелекту (генеративний дизайн, алгоритми керування роєм, комп'ютерний зір і метод інформаційно-екстремального навчання), запропоновано використання схеми 2+2, яка складається із ІНС, GNSS, радарів та оптичних систем для підвищення надійності пілотажно-навігаційного обладнання. Додатково автори зазначають, що у науковій літературі існує досить мало робіт, присвячених аспектам надійності та відмовостійкості GNSS пристроїв проти кібератак. В роботі [31] запропоновано комплексний підхід для підвищення стійкості та якості супутникового приймального обладнання до впливу завад типу GPS spoofing та GPS jamming з використанням приймальних антен на базі фазованих антенних решіток. В роботі [32] наголошується, що маніпуляція часом GNSS є серйозною загрозою для навігаційних систем, оскільки атаки можуть здійснюватися як синхронно, так і асинхронно, змінюючи мітку часу приймача GNSS. Дані дослідження підтверджують, що використання комбінації локальних і віддалених джерел міток часу дозволяє ефективно виявляти такі атаки. У роботі [33] дослідники спроєктували та розробили атаку, яка дозволяє підробляти місцезнаходження або рух приймача-жертви без зміни змісту навігаційного повідомлення реального сигналу шляхом ретрансляції сигналів GNSS. В зв'язку з необхідністю запобігання кібератакам, що загрожують цілісності даних диференціальних поправок в автономній системі диференціальної корекції (СДК), науковці запропонували [34] вирішення цієї проблеми шляхом усунення вразливості даних СДК, яка виникає при використанні MD5 у протоколі NTP. Запропоновано модифікацію NTP-сервера часу СДК відповідно до схеми ANSI X9.95 із застосуванням криптографічно стійкої імітовставки (MAC). Також проведено метрологічне дослідження макету NTP-сервера СДК із використанням криптографічно стійкої MAC.

Метою статті є аналіз та дослідження існуючих моделей та методів захисту від кіберзагроз на GNSS шляхом надання та обґрунтування рекомендацій щодо впровадження сучасних рішень в інформаційно-комунікаційні системи автономних СДК з урахуванням вимог національних стандартів до рівня безпеки в постквантовий період.

Основні кіберзагрози для автономної СДК GNSS

1. Глушіння сигналу (GPS jamming).

Використання потужних радіочастотних перешкод може повністю блокувати приймачі GNSS, змушуючи системи втрачати сигнал і припиняти навігацію. Це особливо небезпечно для авіації, морського транспорту та військових операцій. Доступні на ринку пристрої для глушіння GNSS-сигналів, які коштують до 100 $ [14], можна ефективно використовувати для дестабілізації навігаційної інфраструктури.

2. Спуфінг сигналу (GPS spoofing).

Це атака, при якій створюється фальшивий GNSS-сигнал, що змушує приймач визначати неправильне місцеположення або час. Використовується для шахрайських схем, наприклад, викрадення вантажів або введення в оману навігаційних систем автономного транспорту.

У військовій сфері така атака може спричинити дезорієнтацію військових дронів або зброї з супутниковим наведенням.

3. Кібератаки на наземну інфраструктуру GNSS.

GNSS-сигнали слабкі, тому наземні системи корекції та моніторингу мають важливе значення для забезпечення корегувальною інформацією споживачів. Хакерські атаки можуть вивести з ладу ІКС автономної СДК, що суттєво спричинить викривлення навігаційних даних у критичних галузях.

Моделі та методи кібератак на автономну СДК GNSS

1. GPS spoofing. Атака спуфінгу базується на передачі сигналів з параметрами, схожими на справжні сигнали GNSS, але з модифікованими даними навігації. Математично базовий приклад сигналу спуфінга можна описати наступним чином.

Спуфер повинен відтворити радіочастотну (RF – Radio frequency) несучу, псевдовипадковий код (PRN – pseudo-random code) розширення спектра, а також потік бітів даних кожного відкритого супутникового GNSS-сигналу, який він має намір підробити. Типовий прийнятий сигнал GNSS має вигляд [35]:

$$y(t) = Re\left\{\sum_{i=1}^{N} A_i D_i[t-\tau_i(t)] C_i[t-\tau_i(t)]\, e^{j[\omega_c t-\varphi_i(t)]}\right\}, \quad (1)$$

де N – кількість сигналів, кожен з яких відповідає певному супутнику (з унікальним кодом); A_i – амплітуда сигналу i-го супутника; $D_i(t)$ – потік бітів даних сигналу i-го супутника; $C_i(t)$ – код розширення спектра (наприклад, BPSK PRN або BOC/PRN); $\tau_t(t)$ – кодова затримка (тобто, коли приймач "бачить" цей сигнал); $\omega_c t$ – несуча частота; $\varphi_i(t)$ – фазовий зсув (beat carrier phase) для i-го сигналу.

Спуфер передає набір фальшивих сигналів, подібних до:

$$y_s(t) = Re\left\{\sum_{i=1}^{N_s} A_{si} \widehat{D}_i[t-\tau_{si}(t)] C_i[t-\tau_{si}(t)]\, e^{j[\omega_c t-\varphi_{si}(t)]}\right\}, \quad (2)$$

де параметри фейкових сигналів (для $i = 1, \dots, N_s$): A_{si} – амплітуда, τ_{si} – кодова затримка, $\varphi_{si}(t)$ – фаза несучої.

Номінально $N_s = N$, тобто кількість фейкових сигналів дорівнює кількості справжніх. Кожен спуфінговий сигнал повинен мати той самий код $Ci(t)$, що і відповідний справжній сигнал, щоб обдурити приймач. Зазвичай передають найкращу оцінку бітового потоку $\widehat{D}_i(t)$, який мав би бути. Ці параметри можуть трохи відрізнятись від справжніх, оскільки залежні від положення антени спуфера.

Повна модель прийнятого сигналу:

$$y_{tot}(t) = y(t) + y_s(t) + v(t), \quad (3)$$

де $v(t)$ – шум (в основному – білий гаусівський).

У деяких випадках цей шум є основним джерелом перешкод. В інших – саме спуфер створює значну частину сигналу, включаючи як дані, так і шум.

2. GPS jamming. Глушіння реалізується шляхом передачі шумового або узгодженого сигналу з високою потужністю, що перевищує рівень корисного сигналу GNSS. Математично базовий приклад сигналу глушіння можна описати як [36]:

$$x_j(t) = A_j exp\left(j\theta_0 + j2\pi \int_0^{t-\tau_p} f_i(u)du\right), \quad (4)$$

де A_j – амплітуда сигналу глушіння, τ_p – затримка поширення сигналу від генератора заглушення до приймача, θ_0 – фазове зміщення сигналу заглушення, f_i – миттєва частота з періодичним характером.

3. Хакерські атаки на автономну СДК:

– DDoS-атаки на сервери автономної СДК. Розподілені атаки типу "відмова в обслуговуванні" (DDoS) спрямовані на перевантаження серверів автономної СДК

численними запитами, що призводить до їхньої недоступності. DDoS-атаки характеризуються інтенсивним трафіком із багатьох джерел до цільового сервера.

DDoS-атака на сервер-жертву виснажує ресурси цільового сервера, що змушує сервер відмовляти у з'єднанні новим легітимним клієнтам. Виснаження ресурсів сервера може стосуватися як пропускної здатності, так і буферної пам'яті сервера-жертви. Наступне рівняння надає визначення загальної ймовірності виснаження ресурсів на сервері-жертві [37]:

$$Total_{attack} = 1 - \left(1 - P^{\beta}\right)(1 - P^{M}), \tag{5}$$

де $Total_{attack}$ – ймовірність повного виснаження ресурсів жертви внаслідок атаки, P^{β}– ймовірність виснаження пропускної здатності, P^{M} – ймовірність виснаження пам'яті.

Для опису моделі атаки розглянемо два різні випадки в контексті виснаження пропускної здатності та оперативної пам'яті [37].

В и п а д о к А : ймовірність виснаження пропускної здатності визначається рівнянням [37]:

$$P^{\beta} = \frac{\left(\frac{\alpha^{C}}{C!}\right)}{\sum_{i=0}^{C} \frac{\alpha^{i}}{i!}}, \tag{6}$$

де

$$\alpha = \frac{\beta_A + \beta_N}{\beta_{Total}} = \frac{\left(\frac{\delta_{BA}}{\tau_{BA}} + \frac{\delta_{BN}}{\tau_{BN}}\right)}{\beta_{Total}}, \tag{7}$$

C – кількість відкритих каналів або невикористаної пропускної здатності; β_A – пропускна здатність, що споживається атакуючими клієнтами; β_N – пропускна здатність, що споживається легітимними клієнтами; β_{Total} – загальна пропускна здатність; δ_{BA} – розмір переданого пакета для атакуючих клієнтів у контексті пропускної здатності; δ_{BN} – розмір переданого пакета для легітимних клієнтів у контексті пропускної здатності; τ_{BA} – частота прибуття (інтервал) пакетів атакуючих клієнтів; τ_{BN} – частота прибуття (інтервал) пакетів легітимних клієнтів.

Припускаючи, що розмір пакетів подібний у випадках атаки й звичайного трафіку, тобто: $\delta_{BA} = \delta_{BN} = \delta_B$, маємо:

$$\alpha = \frac{\delta_B}{\beta_{Total}}\left(\frac{1}{\tau_{BA}} + \frac{1}{\tau_{BN}}\right) = K \times \frac{1}{\tau_{BA}}, \text{ оскільки } \frac{\delta_\beta}{\beta_{Total}} = K;\ \frac{1}{\tau_{BN}} \to 0, \tag{8}$$

де K – деяка константа. Тобто:

$$\alpha \propto \frac{1}{\tau_{BA}}\ . \tag{9}$$

Інтервал між прибуттям пакетів визначається як час між двома суміжними пакетами від одного клієнта. Використовуючи рівняння (6) та (9), отримуємо два висновки [37]:

$$P^{\beta} \propto \frac{1}{C} \tag{10}$$

та

$$P^{\beta} \propto \alpha \propto \frac{1}{\tau_{BA}}\,. \tag{11}$$

В и п а д о к В : ймовірність виснаження пам’яті або буфера задається рівнянням [37]:

$$P^M = \frac{\left(\frac{\gamma^{M_{Total}}}{M_{Total}}\right)}{\sum_{i=0}^{M_{Total}} \frac{\gamma^i}{i!}}\ , \tag{12}$$

де

$$\gamma = M_A + M_N = \frac{\delta_{MA}}{\tau_{MA}} + \frac{\delta_{MN}}{\tau_{MN}}\left[since\ M_A = \frac{\delta_{MA}}{\tau_{MA}}\ and\ M_N = \frac{\delta_{MN}}{\tau_{MN}}\right],$$

тобто

$$\gamma = \delta_M\left(\frac{1}{\tau_{MA}} + \frac{1}{\tau_{MN}}\right) = \frac{\delta_M}{\tau_{MA}}[since\ \delta_{MA} = \delta_{MN} = \delta_M\ and\ since\ \frac{1}{\tau_{MN}} \to 0].$$

Маємо:

$$\gamma \propto \frac{1}{\tau_{MA}}. \tag{13}$$

Використовуючи рівняння (12) та (13), отримаємо два висновки [37]:

$$P^M \propto \frac{1}{M_{Total}}\ . \tag{14}$$

$$P^M \propto \gamma \propto \frac{1}{\tau_{MA}}\ . \tag{15}$$

Атаки типу "людина посередині" (Man-in-the-Middle, MitM). Такий вид атаки спрямований на перехоплення та можливу модифікацію даних, що передаються між двома сторонами, без їхнього відома. У контексті автономних СДК GNSS це може означати перехоплення даних між приймачем та наземними станціями корекції, що дозволяє зловмиснику змінювати або підробляти навігаційні дані. Така атака ставить під загрозу конфіденційність, цілісність та автентичність переданої інформації.

Припустимо, що дані d передаються від відправника A до отримувача B через канал зв'язку. Зловмисник M перехоплює ці дані, змінює їх на d' і передає B. Математично це можна описати як: $A \to M: d; M(d) = d'; M \to B: d'$. Це призводить до того, що B отримує модифіковані дані d' замість оригінальних d, що може викликати неправильне визначення координат або інших параметрів.

Атаки на програмне забезпечення (ПЗ) автономної СДК GNSS. Криптоаналітики можуть використовувати вразливості в програмному забезпеченні автономної СДК для виконання несанкціонованих дій, таких як виконання шкідливого коду, проникнення в ІКС та отримання доступу до конфіденційних даних. Наприклад, припустимо, що в програмному забезпеченні веб ресурсу автономної СДК є вразливість, яка дозволяє виконати переповнення буфера. Зловмисник надсилає спеціально сформований сигнал $s_{exploit}$, який викликає переповнення буфера і дозволяє виконати шкідливий код. Математично це можна описати як

$$s_{exploit} = \{s_1, s_2, \dots, s_n\}\ , \tag{16}$$

де s_i – частини сигналу, які разом перевищують розмір буфера приймача. Це може призвести до виконання зловмисного коду на стороні веб-ресурса автономної СДК, що може порушити його роботу або сприяти порушенню цілісності даних.

Атаки на фізичне проникнення або пошкодження автономної СДК. Кіберзлочинці можуть здійснювати атаки на наземні станції GNSS, виводячи їх з ладу через фізичне пошкодження. Така атака більш спроможна здійснити саботаж автономної СДК, результатом якої є обмеження до коригувальної інформації певних регіонів СДК. Математичну модель (стійкість автономної СДК до саботажу) можна розрахувати на основі концепції класичної k-out-of-n структури надійності, яка реалізується через біноміальну модель, де для успішної

роботи необхідно, щоб функціонували принаймні k із n компонентів [38,39]. Припустимо, що система має N наземних станцій, і для корекції сигналу потрібно одночасне функціонування N_{req} станцій. Ймовірність нормальної роботи станції після атаки визначається як

$$P_{work} = 1 - P_{fail} \ , \tag{17}$$

де P_{fail} – ймовірність успішного виведення станції з ладу.

Якщо атаки незалежні між станціями, ймовірність того, що хоча б $Nreq$ станцій залишаться працездатними:

$$P_{survive} = \sum_{k=Nreq}^{N} \binom{N}{k} P_{work}^{k} (1 - P_{work})^{N-k} \ . \tag{18}$$

Якщо $P_{survive}$ падає нижче певного значення P_{crit}, система вважається недієздатною, що порушує доступність даних.

Якщо зловмисник одночасно атакує M станцій, то ймовірність знищення кожної:

$$P_{fail} = \frac{M}{N}. \tag{19}$$

Визначення мінімальної кількості станцій M_{crit}, які треба атакувати для виведення системи з ладу:

$$M_{crit} = N - min_k \left(\sum_{k=Nreq}^{N} \binom{N}{k} P_{work}^{k} (1 - P_{work})^{N-k} \leq P_{crit} \right). \tag{20}$$

Моделі та методи захисту автономної СДК GNSS від кібератак

1. *Автентифікація GNSS на рівні сигналу*.

Commercial Authentication Service (CAS) – це сервіс автентифікації сигналів, що надається європейською навігаційною системою Galileo. CAS забезпечує користувачам можливість перевіряти автентичність отриманих навігаційних сигналів, що підвищує захист від спуфінгу та інших видів атак на системи позиціонування.

Основні характеристики CAS. Сигнал E6-C: CAS використовує пілот-компонент сигналу E6 (E6-C), який передається на частоті 1278,75 МГц. Цей компонент може бути зашифрований для забезпечення контрольованого доступу та автентифікації (рис. 2) [40].

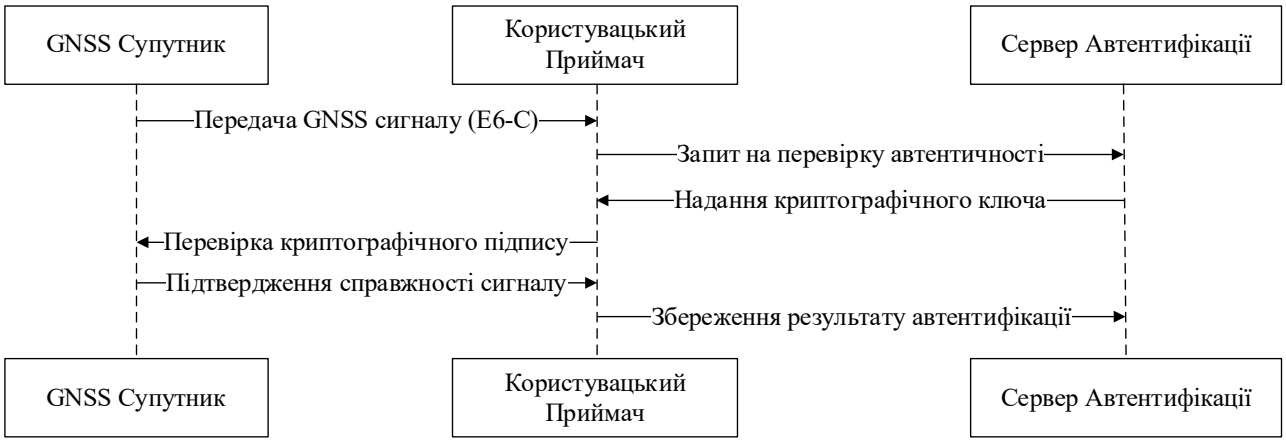


Рис. 2. Автентифікація GNSS на рівні сигналу

2. *Аналіз потужності та його характеристик для виявлення атаки GPS spoofing.*

Принцип аналізу потужності сигналу сигналу та його характеристик для виявлення атаки GPS spoofing наведено на рис. 3.

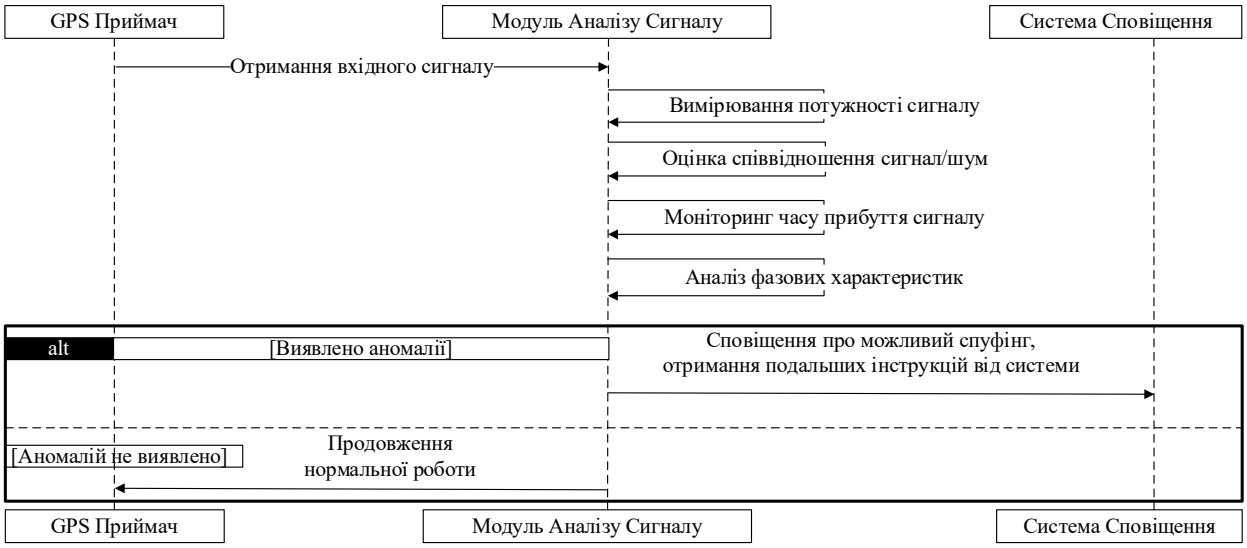


Рис. 3. Аналіз потужності сигналу та його характеристик для виявлення атаки GPS spoofing

Під час спуфінгової атаки дозволяє виявляти такі аномалії. Середня потужність сигналу GPS (L1 C/A) на поверхні Землі ≈ −130 dBm. Спуфінгові сигнали зазвичай мають потужність від −100 dBm зловмисник може передавати сигнали з потужністю, вищою за потужність реальних супутникових сигналів, щоб змусити приймач приймати підроблені дані. Моніторинг вхідної потужності сигналу до −80 dBm, що значно вище від справжнього супутникового сигналу. Допустиме відхилення потужності для автентичного сигналу не більше ±3 dB, що є стандартним допуском у багатьох радіочастотних системах.

Оцінка співвідношення сигнал/шум (SNR – Signal-to-noise ratio). Вимірювання SNR допомагає визначити граничні значення, перевищення яких може вказувати на спуфінгову атаку. Нормальне значення SNR для автентичного GPS-сигналу становить 30 – 50 dB-Hz. Спуфінгові сигнали можуть мати SNR > 55 dB-Hz, що вказує на потенційну атаку. Виявлення аномальних значень > 10 dB вище середнього рівня може свідчити про спуфінг. SNR визначається як відношення потужності сигналу (P_{signal}) до потужності шуму (P_{noise}):

$$SNR = \frac{P_{signal}}{P_{noise}}. \tag{21}$$

Це відношення виражається в децибелах (dB) за допомогою формули

$$SNR_{dB} = 10 \times \log_{10}\left(\frac{P_{signal}}{P_{noise}}\right). \tag{22}$$

(TOA) коливається в межах 10 – 100 нс. При атаці спуфінгом затримки можуть бути від 500 нс до кількох мс, оскільки сигнали передаються зі значно ближчої відстані. Відстеження часу приходу сигналів дозволяє Моніторинг часу прибуття сигналів (Time of Arrival, TOA). Для звичайних супутників затримка сигналу виявляти відхилення, які можуть бути спричинені спуфінгом.

Різницю часу прибуття можна обчислити за формулою [41]:

$$\Delta d = c \times (\Delta t), \tag{23}$$

де c – швидкість світла; Δt – різниця у часі прибуття сигналу в кожну референсну точку.

У двовимірному просторі маємо наступне рівняння:

$$\Delta d = \sqrt{((x^2 - x)^2 + (y^2 - y)^2)} - \sqrt{((x^1 - x)^2 + (y^1 - y)^2)}, \tag{24}$$

де (x_1, y_1) та (x_2, y_2) – відомі координати референсних точок (маяків).

Використовуючи методи нелінійної регресії, це рівняння можна перетворити у форму гіперболи. Після обчислення достатньої кількості таких гіпербол положення цілі можна визначити шляхом знаходження точки їхнього перетину.

Аналіз фазових характеристик. Порівняння фазових характеристик вхідних сигналів допомагає виявити несумісності з реальними супутниковими сигналами. Допустиме відхилення фазової затримки справжніх GNSS-сигналів < 1 рад. Спуфінгові сигнали можуть мати аномальні зміни фазового кута > 3 рад у коротких часових інтервалах.

3. *Інтеграція ІНС з GNSS.* Такий метод є ефективним для підвищення надійності та безпеки навігаційних даних рухомих об'єктів. Ця комбінація дозволяє виявляти та протидіяти атакам типу спуфінгу та глушіння, які можуть спотворювати або блокувати сигнали GNSS. Для поєднання двох систем широко використовується Фільтр Калмана, оскільки від дозволяє вимірювати безперервні вимірювання ІНС (які накопичують похибки з часом) та періодичні, але точні дані від GNSS (які можуть мати перешкоди або спуфінг-атаки). Основна ідея такої інтеграції складається з акселерометрів і гіроскопів, які забезпечують відносне переміщення та орієнтацію рухомого об'єкта. GNSS дає абсолютні координати, які можуть бути хибними через кібератаки. Фільтр Калмана дозволяє компенсувати недоліки обох систем:

ІНС забезпечує безперервність навігації навіть при втраті сигналу GNSS;

GNSS коригує ІНС, зменшуючи накопичення помилок;

ІНС допомагає виявляти атаки на GNSS (якщо дані GNSS не відповідають ІНС, це може бути ознакою спуфінгу).

На рис. 4 наведено приклад інтеграції ІНС та GNSS [42].

4. *Забезпечення захисту ІКС автономної СДК. Захист ІКС автономної СДК є критично важливим для забезпечення надійності та безпеки навігаційних даних*. Моделі та методи захисту ІКС автономної СДК від кібератак мають відповідати вимогам міжнародних стандартів, таких як ISO/IEC 27001, NIST, IEC 62443, та національних НД ТЗІ 2.5-004-99, НД ТЗІ 2.5-005-99 для забезпечення комплексного та системного захисту від хакерських кіберзагроз [43, 44].

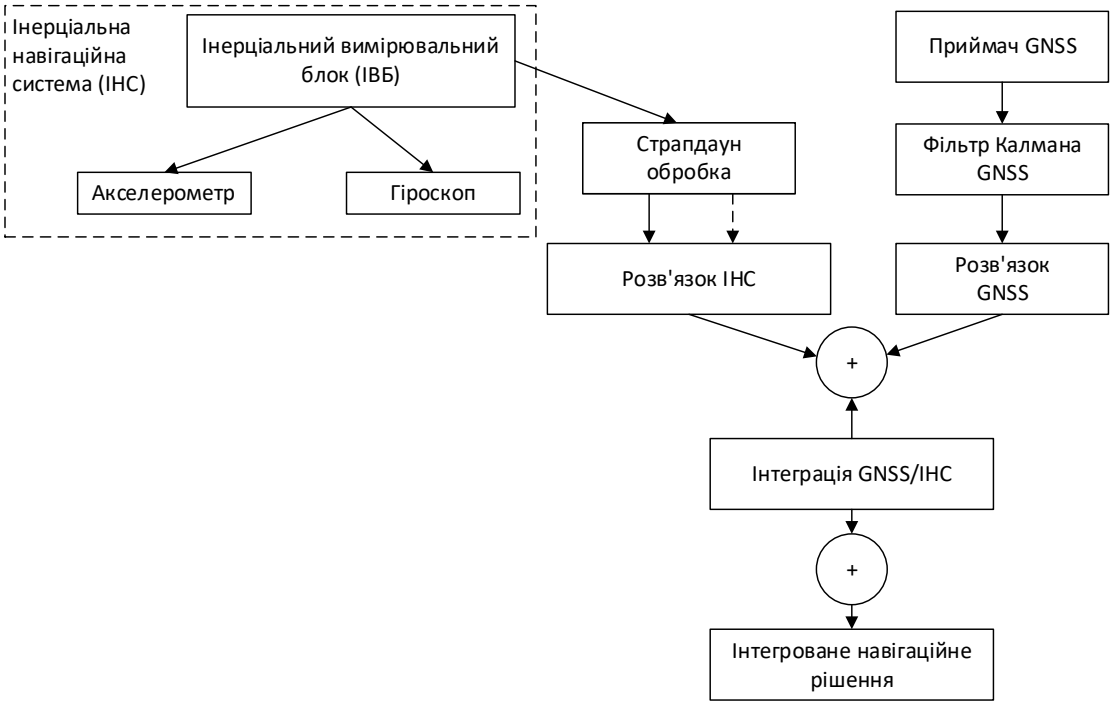


Рис. 4. Приклад інтеграції ІНС та GNSS

4.1. *Захист від DDoS-атак на сервери автономної СДК*. Для захисту веб-сервера автономної СДК від перевантаження шляхом атаки на відмову в обслуговуванні можуть бути розглянуті наступні методи захисту:

Балансування навантаження шляхом розподілу вхідного трафіку між декількома серверами для запобігання перевантаження окремих вузлів. Математично це можна описати як розподіл інтенсивності запитів λ на кількість серверів N:

$$\lambda_{\text{сервер}} = \frac{\lambda}{N}. \tag{25}$$

Фільтрація трафіку за допомогою використання міжмережевих екранів (фаєрволів) для блокування підозрілого трафіку. Ефективність фільтрації визначається коефіцієнтом α, який показує частку заблокованого шкідливого трафіку:

$$\lambda_{\text{ефективна}} = (1 - \alpha)\lambda. \tag{26}$$

Конфігурацію фаєрвола можна представити у вигляді примітивної бінарної матриці доступу A:

$$\begin{bmatrix} A_{1,1}A_{1,2} & \cdots & A_{1,j} \\ A_{2,1}A_{2,2} & \cdots & A_{2,j} \\ \vdots & \ddots & \vdots \\ A_{i,1}A_{i,2} & \cdots & A_{i,j} \end{bmatrix}, \tag{27}$$

де $A_{i,j} = 1$ – означає дозволений трафік між сегментами i та j, а $A_{i,j} = 0$ – заборонений, де $i \in [1, n], j \in [1, m]$; n – кількість сегментів-джерел, m – кількість сегментів-призначень.

Обмеження швидкості запитів (Rate Limiting). Встановлення максимального числа запитів від одного джерела за одиницю часу, щоб запобігти перевантаженню.

4.2. *Захист від атак типу "людина посередині" (MitM).* Для запобігання перехопленню та модифікації даних, що передаються між компонентами автономної СДК, застосовується шифрування даних під час передавання, яке реалізується через функції шифрування E та дешифрування D з використанням ключа K:

$$\mathrm{C} = E_k(M), M = D_k(C). \tag{28}$$

де M – оригінальне повідомлення, C – зашифроване повідомлення.

4.3. *Криптографічний захист інформації шляхом використання протоколів та алгоритмів шифрування для забезпечення конфіденційності та цілісності даних*:

– для цифрових підписів можуть застосовуватися алгоритми RSA, ECDSA і ін.;

– для гешування та перевірки цілісності – SHA-2 (SHA-256, SHA-384, SHA-512).

– управління криптографічними ключами відповідно до стандартів ISO/IEC 11770, 14888, 9796, 27002. Основними вимогами є: генерація ключів з використанням криптографічно стійких генераторів випадкових чисел; зберігання ключів у захищених апаратних модулях (HSM – Hardware Security Module); заміна або оновлення ключів через певні інтервали часу або при підозрі на компрометацію; використання ключів для різних криптографічних систем; реєстрування та аудит діяльності, пов’язаної з управлінням ключами.

– захист каналів зв'язку – наприклад, за допомогою сучасних протоколів шифрування трафіку таких як TLS 1.3, VPN (IPSec, WireGuard, OpenVPN). Забезпечення обов’язкового шифрування між серверами автономної СДК, базами даних та клієнтськими пристроями.

– захист даних у спокої (на дисках, у базах даних, в резервних копіях) доцільно використовувати AES (Advanced Encryption Standard) з ключами не менше 256 біт.

4.4. *Впровадження інфраструктури відкритих ключів (ІВК) для автентифікації та управління цифровими сертифікатами*.

4.5. *Захист від атак на програмне забезпечення автономної СДК* – потрібне для

забезпечення захисту від несанкціонованих дій, таких як впровадження шкідливого коду або отримання несанкціонованого доступу.

Методи захисту:

– регулярне оновлення та патчинг програмного забезпечення;

– використання антивірусних засобів;

– системи виявлення та запобігання вторгнень (IDS/IPS) для моніторингу мережевого трафіку та активності для виявлення підозрілої поведінки в елементах автономної СДК.

4.6. *Захист від атак на фізичну інфраструктуру автономної СДК.* Необхідний для запобігання ризику фізичного доступу до конфіденційних даних. Для запобігання несанкціонованому доступу доречно встановлення систем контролю доступу, відеоспостереження та охорони, а також використання резервних серверів та каналів зв'язку для забезпечення безперервності роботи автономної СДК у разі виходу з ладу основних вузлів.

4.7. *Контроль доступу* – важливий аспект захисту від несанкціонованого доступу до автономної СДК неавторизованих користувачів. Рекомендується впровадження механізмів мультифакторної автентифікації.

4.8. *Розмежування доступу* – використання політик доступу на основі ролей (RBAC – role-based access control). Модель ролей визначає, що кожний користувач U_i має одну або кілька ролей R_k, які визначають доступ до ресурсів P_m: $U_i \in R_k, \quad R_k \in P_m$.

Модель може бути представлена матрицею прав доступу:

$$\begin{bmatrix} P_{1,1}P_{1,2} & \cdots & P_{1,m} \\ P_{2,1}P_{2,2} & \cdots & P_{2,m} \\ \vdots & \ddots & \vdots \\ P_{n,1}P_{n,2} & \cdots & P_{n,m} \end{bmatrix}. \tag{29}$$

де $P_{i,j} = 1$, якщо користувач має доступ, і $P_{i,j} = 0$ – якщо не має доступу.

4.9. *Контроль активності користувачів та адміністраторів*. Обов'язковий елемент ІКС, який включає логування та моніторинг дій користувачів автономної СДК з використанням засобів інтелектуального аналізу поведінкових аномалій.

4.10. *Сегментація мережі* автономної СДК на логічні зони з певними вимогами безпеки та визначення контрольованих каналів зв'язку між ними.

4.11. *Регулярні аудит та тестування всіх елементів безпеки* – сканування ПЗ автономної СДК на наявність вразливостей та тестування на проникнення для проактивного виявлення потенційних кіберзагроз.

На виконання вимог Проєкту Закону України "Про державне регулювання у сфері супутникової навігації" № 10198 від 29.03.2019 [24] щодо застосування національних стандартів, вектор подальших досліджень спрямований на дослідження можливості використання квантового генератора випадкових чисел (QRNG – Quantum Random Number Generation) для управління криптографічними ключами в ІКС автономної СДК, а також застосування постквантових національних стандартів, таких як:

– ДСТУ 7624:2014 – для захисту даних у спокої та для передачі даних. Доцільним є впровадження алгоритму «Калина» з ключами не менше 256 біт;

– ДСТУ 8961:2019 – алгоритм асиметричного шифрування та інкапсуляції ключів «Скеля».

– ДСТУ 9212:2023 – алгоритм електронного підпису «Вершина», заснований на алгебраїчних решітках із відхилами;

– ДСТУ 7564:2014 – алгоритм гешування «Купина».

На рис. 5 представлено прототип загальної схеми архітектури автономної СДК з використанням контрольно коригуючих станцій (ККС), з веб сервісом, який надає користувачам відкориговану GNSS інформацію. На рис. 6 представлено запропонований прототип мережевої архітектури автономної СДК.

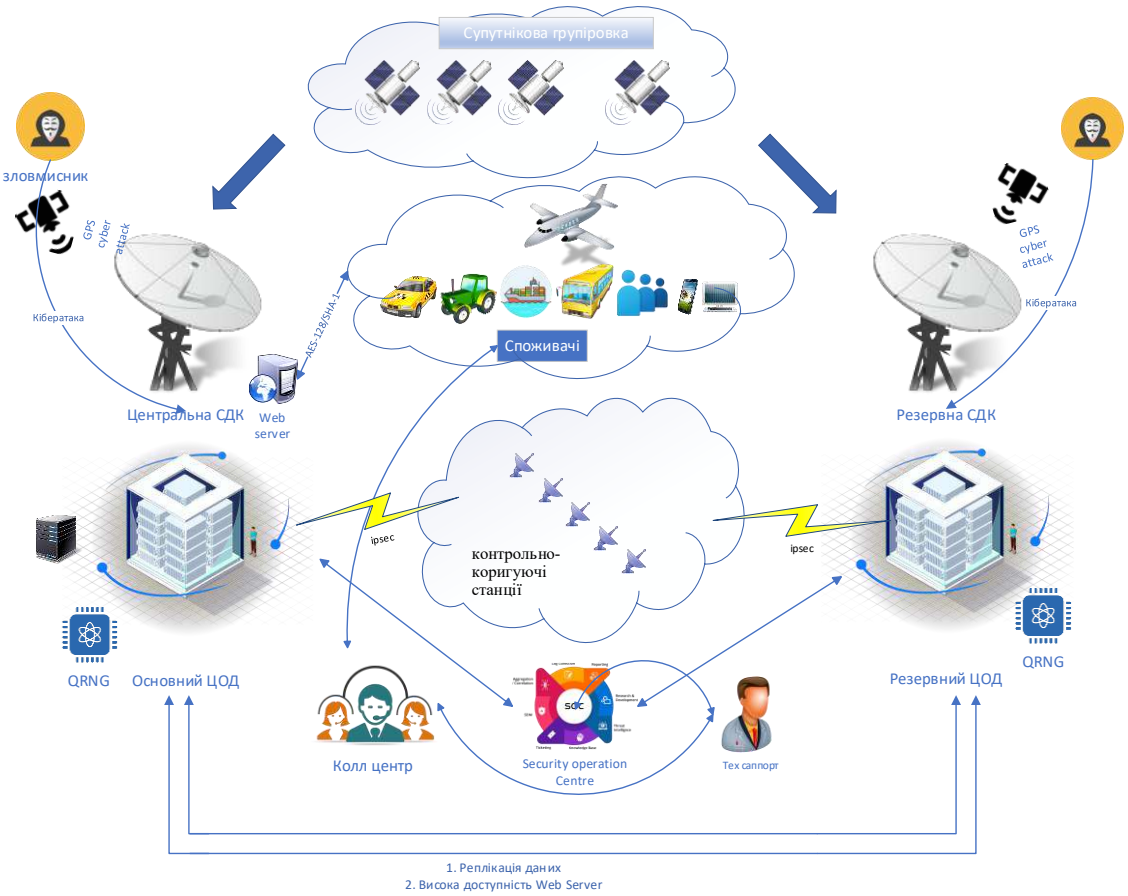


Рис. 5. Прототип архітектури СДК

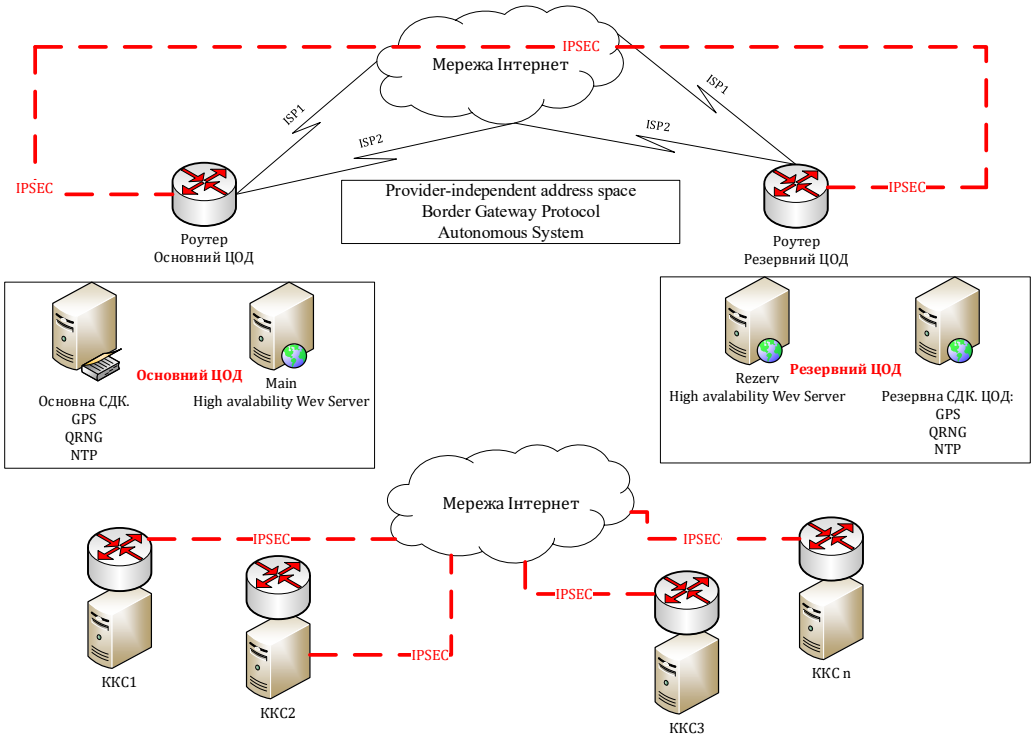


Рис. 6. Прототип мережевої архітектури автономної СДК

Висновки

Зростання використання GNSS супроводжується збільшенням кіберзагроз, які можуть спричиняти фінансові втрати, порушення роботи критичної інфраструктури та створювати небезпеку для життя людей. Атаки на навігаційні системи, такі як спуфінг і глушіння сигналів, а також хакерські атаки на ІКС автономної СДК, є серйозним викликом для транспорту, логістики, військових операцій і комерційних застосувань, що може призводити до значних ризиків використання GNSS.

Забезпечення стабільної, точної та безпечної супутникової навігації вимагає не лише інвестування у системи кібербезпеки GNSS, а ще й постійного дослідження та вивчення нових загроз, а також пошуку ефективних методів їх нейтралізації, зокрема у постквантовий період. Серед ключових механізмів захисту слід виділити: захищені протоколи передачі сигналів, що запобігають перехопленню та підробці даних; механізми автентифікації, які дозволяють ідентифікувати легітимні супутникові сигнали; анти-спуфінгові технології, що виявляють та нейтралізують спроби маніпуляції навігаційними даними; технології захисту ІКС автономних СДК для забезпечення конфіденційності, цілісності та доступності GNSS даних кінцевим користувачам.

Додатково необхідно досліджувати та вивчати можливості застосування автономних СДК, які підвищують точність GNSS і зменшують вплив кібератак, зокрема постквантових. Важливим напрямом є впровадження штучного інтелекту для моніторингу та виявлення загроз та резервних навігаційних технологій для підвищення надійності GNSS у майбутньому.

Отже, ефективний кіберзахист GNSS потребує не лише фінансування, а й активного дослідження, вивчення загроз та розробки інноваційних методів протидії. Комплексний підхід та міжнародна співпраця є ключовими факторами для забезпечення надійної роботи супутникових навігаційних систем у критично важливих сферах.

Проведені дослідження та запропоновані заходи безпеки можуть бути використані як основа для реалізації національної системи координатно-часового та навігаційного забезпечення України. Впровадження відповідного законодавчого регулювання та стандартів дозволить забезпечити кіберстійкість навігаційних систем та інтегрувати їх у європейську супутникову інфраструктуру.

Список літератури:

1. F. T. McClure and R. B. Kershner. The Legacy of Transit: A Dedication // JOHNS HOPKINS APL TECHNICAL DIGEST, vol. 19, no. 1, 1998. URL: https://secwww.jhuapl.edu/techdigest/content/techdigest/pdf/V19-N01/19-01-Pisacane.pdf
2. Department of Defense. Department of Transportation and Department of Homeland Security, 2021 Federal Radionavigation Plan. URL:https://www.navcen.uscg.gov/sites/default/files/pdf/2021_ Federal_Rdionavigation_Plan.pdf
3. V. Vdovin. National Reference Systems of the Russian Federation, used in GLONASS including the user and fundamental segments, 2013. URL: https://www.unoosa.org/pdf/icg/2013/icg-8/wgD/D3_3_2.pdf
4. Redactie De Ingenieur. After 13 years, Galileo satellite navigation complete at last, 2018. URL:https://deingenieur.nl/artikelen/after-13-years-galileo-satellite-navigation-complete-at-last
5. J.A. Ávila Rodríguez. University FAF Munich, Germany. BeiDou Signal Plan – Navipedia. URL: https://gssc.esa.int/navipedia/index.php/BeiDou_Signal_Plan.
6. K.S. Parikh, Deputy Director. IRNSS / GAGAN and its Potential Applications. URL: https://geospatialworld.net/gsi/2016/presentations/benifits-of-IRNSS-GAGAN-satellite-navigation-systems-and-its-potential-applications.pdf.
7. N. S. P. S. C. O. Kenji NUMATA Government of Japan // QZSS System and service Updates. Quasi-Zenith Satellite System, Japanese Regional Navigation Satellite System. URL: https://www.unoosa.org/documents/pdf/icg/2023/ICG-17/icg17.01.06.pdf
8. Greg Thompson. Wide Area Augmentation System (WAAS) – Program Overview. URL: https://www.faa.gov/sites/faa.gov/files/about/office_org/headquarters_offices/ato/WAAS_Program_Status_Update_Jun_2021.pdf
9. European Union Agency for the Space Programme // EUSPA EO and GNSS Market Report. 2024. Iss. 2. LU: Publications Office, 2024. URL: https://data.europa.eu/doi/10.2878/73092

10. J. Siu. Global Navigation Satellite System Overview and Support for PBN Implementation. URL: https://www.icao.int/nacc/documents/meetings/2012/pbngnss2012workshop/pbngnss2-1.pdf

11. Galileo HAS: точність в режимі реального часу – SystemNET – ‘Систем Солюшнс’. URL: https://systemnet.com.ua/galileo-has-tochnist-v-rezhymi-realnoho-chasu/

12. Про критичну інфраструктуру // Офіційний вебпортал парламенту України. URL: https://zakon.rada.gov.ua/go/1882-20

13. Westbrook T. A. Taxonomy of Radio Frequency Jamming and Spoofing Strategies and Criminal Motives // Journal of Strategic Security. 2023. Vol. 16, no. 2. P. 68–80. DOI: https://doi.org/10.5038/1944-0472.16.2.2081.

14. Westbrook T. The Global Positioning System and Military Jamming: The geographies of electronic warfare // Journal of Strategic Security. Vol. 12, № 2. P. 1–16. DOI:10.5038/1944-0472.12.2.1720.

15. Навігаційні ризики в аспекті кібербезпеки транспортних суден і військових кораблів // ResearchGate, 2024. doi: 10.51582/interconf.19-20.08.2022.037.

16. Litvinov N. GPS та його значення у сучасних військових конфліктах // Universe Space Tech. 2022. URL: https://universemagazine.com/borotba-za-koordynaty-globalni-navigaczijni-systemy-ta-yih-znachennya-u-suchasnyh-vijskovyh-konfliktah/

17. Garmin outage caused by confirmed WastedLocker ransomware attack. BleepingComputer. URL: https://www.bleepingcomputer.com/news/security/garmin-outage-caused-by-confirmed-wastedlocker-ransomware-attack/

18. KA-SAT Network cyber attack overview. viasat.com. 30.03.2022.
URL: https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview

19. Kauranen A. Finland detects satellite navigation jamming and spoofing in Baltic Sea, Reuters, 31, 2024. URL: https://www.reuters.com/world/europe/finland-detects-satellite-navigation-jamming-spoofing-baltic-sea-2024-10-31/

20. Розпорядження Кабінету Міністрів України; Концепція від 03.01.2013 № 1-р. Про схвалення Концепції проєкту Закону України “Про державне регулювання у сфері супутникової навігації”// Офіційний вебпортал парламенту України. Розпорядження Кабінету Міністрів України; Концепція від 03.01.2013 № 1-р. URL: https://zakon.rada.gov.ua/laws/show/1-2013-%D1%80#Text.

21. Розпорядження Кабінету Міністрів України; Концепція від 30.03.2011 № 238-р. Про схвалення Концепції реалізації державної політики у сфері космічної діяльності на період до 2032 р. // Офіційний вебпортал парламенту України. Розпорядження Кабінету Міністрів України; Концепція від 30.03.2011 № 238-р. URL: https://zakon.rada.gov.ua/laws/show/238-2011-%D1%80#Text.

22. European Commission. Copernicus: new name for European Earth Observation Programme. URL: https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_12_1345/IP_12_1345_EN.pdf

23. MS4_GEO Strategic Plan 2016-2025 Implementing GEOSS_approved_by_GEO-XII.pdf. URL: https://old.earthobservations.org/documents/ministerial/mexico_city/MS4_GEO%20Strategic%20Plan%202016-2025%20Implementing%20GEOSS_approved_by_GEO-XII.pdf

24. Офіційний портал Верховної Ради України. Проєкт Закону України “Про державне регулювання у сфері супутникової навігації” № 10198 від 29.03.2019.
URL: https://ips.ligazakon.net/document/view/gh7va00a?an=15&ed=2019_03_29

25. Закон України від 05.07.1994 № 80/94-ВР. Про захист інформації в інформаційно-комунікаційних системах // Офіційний вебпортал парламенту України. Закон України від 05.07.1994 № 80/94-ВР. URL: https://zakon.rada.gov.ua/go/80/94-%D0%B2%D1%80

26. Офіційний вебпортал парламенту України. Постанова Кабінету Міністрів України ; Перелік від 07.04.2003 № 486. Про утворення державної мережі моніторингу глобальних навігаційних супутникових систем. URL: https://zakon.rada.gov.ua/go/486-2003-%D0%BF#Text"

27. Офіційний вебпортал парламенту України. Закон України від 16.12.2020 № 1089-IX. Про електронні комунікації. URL: https://zakon.rada.gov.ua/go/1089-20#Text.

28. Проєкт Закону України від 30.09.2021 № 6129. Про затвердження Загальнодержавної цільової науково-технічної космічної програми на 2021–2025 роки. № 6129 від 04.10.2021. URL: https://itd.rada.gov.ua/billinfo/Bills/Card/27922

29. Mustafaiev O. V. Modern technologies of protection against gps spoofing in navigation systems // Scientific notes of Taurida National V.I. Vernadsky University. Series: Technical Sciences. 2024. Vol. 1, 5. P. 58–61. DOI: 10.32782/2663-5941/2024.5.1/10.

30. Вадіс Д., Аврутов В. Методи підвищення функціональної ефективності БПЛА // Механіка гіроскопічних систем. 2024. Вип. 48. DOI: 10.20535/0203-3771482024317891.

31. Narytnik T., Prysiazhnyi V., Kapshtyk S., Denysenko M., Narushkevych O. Improvement of the gps signal receiving resistance against electromagnetic interference, jamming, and spoofing is based on the use of the antenna array system with digital beamforming and NORAD TLE information. 2022.
URL: https://ela.kpi.ua/handle/123456789/54188

32. Spanghero M., Papadimitratos P. Time-based GNSS attack detection // IEEE Transactions on Aerospace and Electronic Systems. 2024. P. 1–18. DOI:10.1109/TAES.2024.3516708.

33. Motallebighomi M., Sathaye H., Singh M. et al. Cryptography Is Not Enough: Relay Attacks on Authenticated GNSS Signals. arXiv, 2022. DOI:10.48550/arXiv.2204.11641.
34. Солдатов В. В., Нарєжній О. П., Гріненко Т. О. Модифікація ntp сервера часу системи диференціальної корекції відповідно до схеми ANSI X9.95. Український метрологічний журнал // Ukrainian Metrological Journal. № 3А. С. 98–102. DOI:10.24027/2306-7039.3a.2020.218165.
35. Psiaki M. L., Humphreys T. E. GNSS Spoofing and Detection // Proceedings of the IEEE. Vol. 104, № 6. P. 1258–1270. DOI:10.1109/JPROC.2016.2526658.
36. Ghizzo E., Djelloul E.-M., Lesouple J. та ін. Assessing jamming and spoofing impacts on GNSS receivers: Automatic gain control (AGC) // Signal Processing. Vol. 228, 03.2025. P. 109762. DOI:10.1016/j.sigpro.2024.109762.
37. Johnson Singh K., De T. and. Mathematical modelling of DDoS attack and detection using correlation // Journal of Cyber Security Technology. Vol. 1, Issue 3–4. P. 175–186. DOI:10.1080/23742917.2017.1384213.
38. Seddighighachkanloo, Morteza. RBDs and Analytical System Reliability Series Systems. ResearchGate. URL: ttps://www.researchgate.net/publication/278678509_RBDs_and_Analytical_System_Reliability_Series_Systems
39. Barlow R. Heidtmann Klaus. Computing k-out-of-n System Reliability. ResearchGate. DOI:10.1109/TR.1984.5221843.
40. European Union. Galileo E6-B/C Codes Technical Note // European Union. 2019. Vol. 1. URL: https://www.gsc-europa.eu/sites/default/files/sites/all/files/E6BC_SIS_Technical_Note.pdf
41. O'Keefe B. Finding Location with Time of Arrival and Time Difference of Arrival Techniques. URL: https://sites.tufts.edu/eeseniordesignhandbook/files/2017/05/FireBrick_OKeefe_F1.pdf
42. Li S., Mikhaylov M., Mikhaylov N. et al. Deep Learning Based Kalman Filter for GNSS/INS Integration: Neural Network Architecture and Feature Selection // 2023 International Conference on Localization and GNSS (ICL-GNSS). 2023. P. 1–7. DOI: 10.1109/ICL-GNSS57829.2023.10148914.
43. Департамент спеціальних телекомунікаційних систем та захисту, інформації Служби безпеки України. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу // Інформаційна безпека та захист інформації. URL: https://tzi.ua/ua/nd_tz_2.5-004-99.html
44. ISO/IEC 27001:2022. ISO: Global standards for trusted goods and services. URL: https://zakon.isu.net.ua/sites/default/files/normdocs/dstu_iso_iec_27001_2023.pdf

Надійшла до редколегії 23.01.2025

Відомості про авторів:
Снєосіков Олег Анатолійович – Харківський національний університет імені В. Н. Каразіна, аспірант кафедри кібербезпеки інформаційних систем, мереж і технологій, Україна; e-mail: oleh.snieosikov@student.karazin.ua, ORCID: https://orcid.org/0009-0001-9468-5965
Нарєжній Олексій Павлович – канд. техн. наук, Харківський національний університет імені В. Н. Каразіна, доцент кафедри кібербезпеки інформаційних систем, мереж і технологій, Україна; e-mail: o.nariezhnii@karazin.ua, ORCID: https://orcid.org/0000-0003-4321-0510
Гріненко Тетяна Олексіївна – канд. техн. наук, доцент, Харківський національний університет радіоелектроніки, доцент кафедри безпеки інформаційних технологій, Україна, e-mail: tetiana.grinenko@nure.ua, ORCID: https://orcid.org/0000-0002-8251-8991

UDC 621.373.8+621.391+681.88 **DOI:10.30837/rt.2025.1.220.06**

V.I. ZABOLOTNYI, Ph.D. of Engineering Sciences, N.O. KHOLIEV, V.S. DOVGAL

TARGETED INTERFERENCE TO LASER ACOUSTIC RECONNAISSANCE

Introduction

At present, methods and characteristics of laser acoustic reconnaissance (LAR) of information voiced at information activity objects (IAOs) are being improved. As a counteraction to this, certain sets of measures and means of protection against technical channels of information leakage (TCIL) of this nature exist and are used [1 – 3].

Methods of protecting speech information include organizational, passive and active. The latter are divided into methods using acoustic devices and methods using vibroacoustic devices.

Organizational methods of protecting speech information from possible leakage include a set of organizational measures aimed at ensuring a minimum risk of speech information leakage from protected premises. These measures include choosing a suitable room for confidential negotiations, ensuring the functioning of the relevant security service on the official territory, closing windows during a confidential conversation in order to prevent the conversation from being monitored by acoustic directional microphones, etc.

In the case of LAR, the passive methods of protecting speech information include choosing the optimal size of the window glass, since the smaller the window pane, the greater the elasticity of the window, which will ensure a lower amplitude of glass oscillation as a result of acoustic wave pressure.

Another passive method of protection against «laser microphones» is to stick a special film on the window pane, which results in the superposition of the beam reflected from the film with the beam reflected from the glass itself in the opposite phase, which ensures that the LAR cannot receive the signal reflected from the window pane. For this purpose, a special film of a given thickness is selected, which should correspond to a quarter of the laser wavelength, although, unfortunately, it is impossible to determine it precisely in advance.

An active method of protecting speech information using special acoustic noise-reducing devices involves creating powerful random acoustic noise in the room, which causes the window pane to vibrate according to a random law and makes it impossible for the LAR to detect a dangerous signal from the reflected laser beam.

By generating powerful acoustic noise, the corresponding devices affect the vibration of the window pane, which ensures the masking of the dangerous signal.

The law of unity of opposites determines the further development and improvement of measures to protect speech information on information activity objects (IAO), which emphasizes the relevance of research in this area.

This paper analyzes the peculiarities of the components of the said TCIL, and presents the corresponding general and individual models of this channel. A new method of protecting information broadcast in a dedicated room (DR) is formulated by using the reflection of the probing signal from the side lobes of the laser beam to influence the processing of a dangerous informative signal in the LAR.

An indirect method for estimating the amplitude of vibration of a window pane

Estimation of the parameters of window pane oscillation under the influence of the acoustic field in the DR is the basis for making a decision on the application of protection measures against LAR.

The determining factor in this is the amplitude of window pane oscillation $\Delta(t)$. The real value of this can be theoretically estimated using the following approach (Fig. 1).

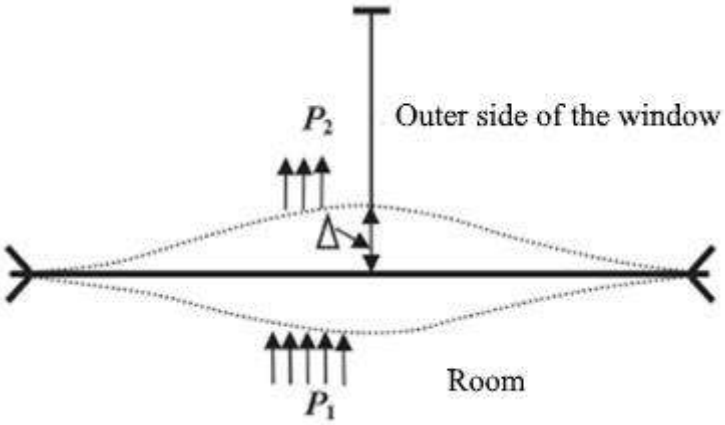


Fig.1. Window pane – the source of the optical part of the TCIL LAR

In the proposed model, P_1 is the sound pressure in front of the glass (in the room), P_2 is the sound pressure behind the glass, and Δ is the amplitude of the window glass vibration.

From the physics course, it is known that at any given time the pressure of a sound wave can be defined as:

$$P(t) = v(t)rc, \tag{1}$$

and for the case of harmonic oscillations as:

$$P(t) = P \sin 2\pi ft, \tag{2}$$

where P – is the pressure value of the sound wave;

$v(t)$ is the vibrational velocity of air molecules under the action of a sound wave;

r is the density of the atmosphere;

c is the speed of sound wave propagation in the atmosphere;

f is the frequency of harmonic oscillation of the acoustic wave.

To estimate the amplitude of window glass oscillation under the action of an acoustic wave, the following model of window glass oscillation with a clamped fixture in the frame was used.

The instantaneous value of the window glass oscillation $\Delta(t)$ is actually an integral of the velocity of the window glass molecules oscillating under the action of the sound wave, which in turn coincides with the velocity of the air molecules behind the window glass $v2(t)$:

$$\Delta(t) = \int v_2(t)dt = -\frac{P_2}{2\pi frc}\cos 2\pi ft \tag{3}$$

From this, it is possible to determine the maximum vibration amplitude of the window pane Δ for a given sound frequency f and sound pressure behind the pane P_2:

$$\Delta = \frac{P_2}{2\pi frc} \tag{4}$$

For normal atmospheric conditions, rc=420Н·С/м^3. Use to determine the maximum amplitude of vibration of the window pane of a window Δ for a given sound frequency f and sound wave pressure in the room P_1:

$$\Delta = \frac{P_1}{2\pi frc \cdot 10^{R/20}} \tag{5}$$

The value of R is taken from the formula for calculating the sound insulation of a window: $R=10lg(R_1/P_2)$.

Generalized illumination model of interference-type LAR photodetector

In this work, we use the LAR model based on the principle of the Michelson interferometer (Fig. 2).

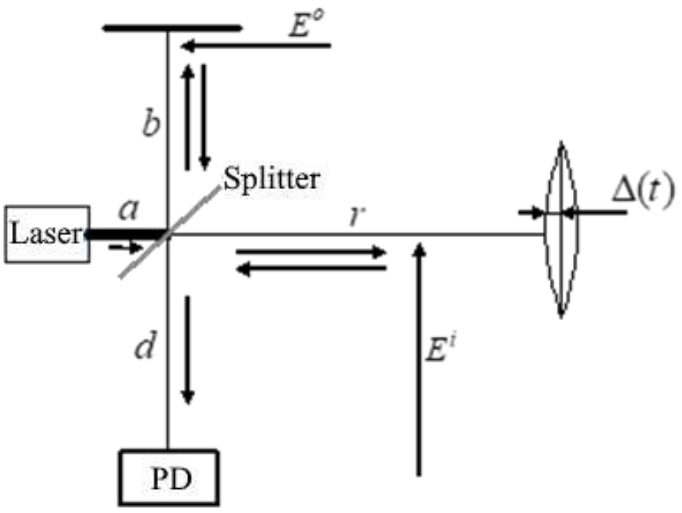


Fig. 2. Laser interference-type acoustic reconnaissance device

The information leakage is carried out through a conventional window pane, which is a kind of membrane that oscillates at the sound frequency under the pressure of acoustic waves of the conversation content. The emission generated by the laser propagates in space and, reflected from the surface of the window pane, is modulated by an acoustic signal. This reflected emission is then perceived by a photodetector, which reproduces the speech information in the room.

The splitter allows the incident and reflected beams to be brought together in one point. This makes it possible to combine the laser and the detector.

Interferometry can increase the sensitivity of a «laser microphone» if the reflected beams are coherent.

The wavelength of the laser can be between visible and infrared radiation. Even the far-infrared spectrum can be used. But the best wavelength is the near-infrared range. Modern lasers operate at frequencies of approximately $3 \cdot 10^{13} \div 3{,}75 \cdot 10^{14}$ Hz, i.e., the wavelength is in the range of 0,8 ÷ 10 micrometers, which is invisible to the human eye.

LAR have a range of 100 ÷ 500 meters or more.

When using a «laser microphone», it should be borne in mind that rain, snow, and fog can significantly affect the reflected signal, weakening it mainly due to scattering.

The illumination of the LAR photodetector is proportional to the square of the sum of the light vectors of the reference $E^o(t)$ and reflected $E^i(t)$ laser beams from the window pane:

$$I(t) \sim \left(E^i(t) + E^o(t)\right)^2, \tag{6}$$

For the field strength of the reference signal $E^o(t)$ of laser emission on the photodetector (PD), we can express (7):

$$E^o(t) = E^o \sin\left(2\pi f t + k(a + 2b + d)\right), \tag{7}$$

and for the field strength of the reflected signal on the PD $E^i(t)$:

$$E^i(t) = E^i \sin\left(2\pi f t + k\left(a + 2r + d + 2\Delta(t)\right)\right), \tag{8}$$

where E^o and E^i – are the amplitudes of the field strength of the reference and reflected signals, respectively;

f is the frequency of laser radiation;

k is the wavenumber;

a is the distance from the laser to the splitter;

b is the distance from the splitter to the laser reference mirror;

d is the distance from the splitter to the PD;

r is the distance from the splitter to the window pane;

Δ(t) is the function of window pane oscillation at the point of laser beam irradiation, which depends on the pressure of acoustic waves of the speech signal in the room.

The neutral filter sets the amplitudes of the field strengths of the reference E^o and reflected E^i signals so that $E^o = E^i = E$.

The illumination of the photodetector will be [4]:

$$I(t) \sim 4E^2 \left(\frac{1+\cos\frac{4\pi}{\lambda}(\Delta(t)-b)}{2} \right), \tag{9}$$

After the conversion, we can express it as:

$$I(t) \sim 2E^2 \left(1 + \cos 2\pi \left(\frac{\Delta(t)-b}{\lambda/2}\right)\right), \tag{10}$$

For the simplest case of a sinusoidal oscillation of a window pane:

$$\Delta(t) = \Delta \sin 2\pi F t, \tag{11}$$

where Δ is the amplitude of oscillation of the window pane at the irradiation point;

F is the oscillation frequency of the window pane.

In this case, the illumination of the photodetector *I(t)* will be determined by the expression:

$$I(t) = 2E^2(1 + \cos 2\pi(\beta - \alpha \sin 2\pi F t)), \tag{12}$$

where β – is the ratio of the difference in the path of the reference and reflected laser beams to half the laser wavelength, otherwise, the relative parameter of the laser reference mirror position setting; a – is the relative amplitude of oscillation of the window pane (relative to half the laser wavelength).

This expression makes it possible to visually check the correct choice of the LAR by minimizing the distortion of the detected signal.

Features of the lateral characteristics of the LAR emissions

LAR beam model plays an important role in the substantiation of the protection method proposed in this work.

The beam of the LAR is formed by an optical system from an infrared light source. On a window pane, the light spot usually has a size between 2 and 20 mm.

The emission pattern of such a beam can be determined theoretically based on the following assumptions characteristic of a circular field source with, for example, a uniform energy distribution [5]. In this case, the diameter of the lens d and the wavelength of the emission λ are determined. It was also determined that the normalized emission pattern of the field *F(θ)* of such a site can be determined quite accurately by the expression:

$$F(\theta) = \frac{sin\left(\frac{\pi d \sin\theta}{2\lambda}\right)}{\frac{\pi d \sin\theta}{2\lambda}}, \tag{13}$$

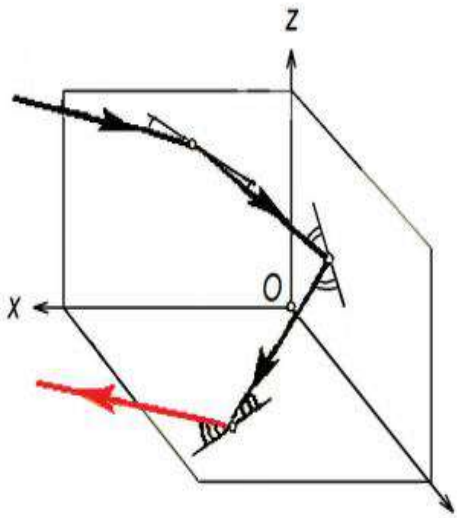
where: θ is the angle relative to the laser beam axis (within the direction of the window pane plane);

d is the diameter of the LAR lens.

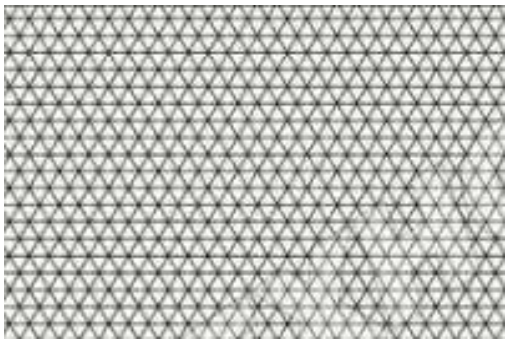
It follows from (13) that, in addition to the main beam of the laser, emission sidelobes also hit the window pane, their intensity decreases with an increase in the angle θ.

Corner reflectors of the LAR beam

The lateral radiation field of a LAR beam represents coherent laser frequency signals. The possibility of using them to create frequency-targeted interference to the photodetector of the laser is almost perfect. The problem of returning these reflected signals to the side of the LAR lens is simply solved by using corner reflectors (Fig. 3).



a - Single corner reflector with the beam paths in it



b - Composite corner reflector – retroflector

Fig. 3. Varieties of corner reflector designs that can be used to create frequency and direction-targeted interference for LAR

The main characteristics of corner reflectors depend on their design and structural dimensions.

The work uses the effective surface, the value of which significantly depends on the ratio of the size of the corner reflector edge *a* and the wavelength of the infrared (IR) emission LAR beam λ.

If a corner reflector with triangular faces of size *a* is used, the radar cross section (RCS) equals

$$\sigma = \frac{4\pi}{3\lambda^2} a^4, \tag{14}$$

If the corner reflector consists of quadrilateral faces, the RCS is

$$\sigma = \frac{4\pi}{3\lambda^2} 3a^4, \tag{15}$$

As reflectors, you can use retroreflectors (cataphote), which are an assembly of several (dozens) corner reflectors.

Effect of a corner reflector on the perception of a reconnaissance signal

The use of corner reflectors to interfere the LAR is based on the addition of the reflected signal onto LAR PD (Fig. 4).

In contrast to the standard interference-type LAR usage scheme with applied settings, a corner reflector (CR) is installed behind the window pane in the DR at a distance R_{cr} from the window pane, in the area of LAR scanning. The RCS value of the CR is known for the working wavelength of the LAR beam.

The mass of the CR is so large that it cannot change its position under the influence of the sound pressure of the dangerous signal field, so as not to be an additional source of this signal.

Alternatively, the CR mount can be moved along the «laser – CR» line. Artificially, the movement can be carried out in time with amplitude M (to create a phase modulation of the reflected signal). This case will be investigated separately in the course of further research.

Optical signals on the PD (expr. 6) will create a light field

$$E(t) \sim E^i(t) + E^o(t) + E^{CR}(t), \tag{16}$$

The amplitude E^i $E^i(t)=E^i(\Delta(t))$, the component of the information signal modulated by the window pane vibration $\Delta(t)$, is determined by the distance *r*, the beam reflection coefficient from the window pane. It should be assumed that the operator can direct the LAR beam to the point of the window plane where the window pane vibrations $\Delta(t)$ have the optimal amplitude value for interception.

The amplitude $E^o(t)$ of the reference signal can be adjusted by the LAR operator to adjust it to receiving a signal with a filter bandwidth (not shown in the figure). In [4], it is determined that the optimal amplitude setting will be when it coincides with the amplitude value of the information signal. The transparency range of the filter should be expected to be from 1 to 0. In addition, the phase of the signal is selected by the location of the distance to the mirror b, to minimize the distortion of the received signal.

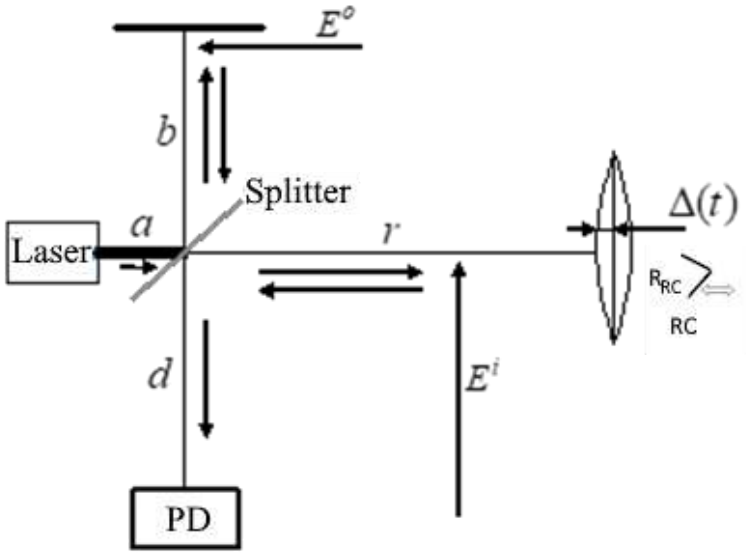


Fig. 4. LAR with an applied corner reflector (CR),
the mark ⇔ shows the option of artificially moving the CR

The amplitude of the $E^{CR}(t)$ component reflected from the CR depends on the level of lateral LAR emission, the distance to the CR (practically, the distance r), and is determined by the value of the CR effective surface σ of formulas (14), (15), which depends on the actions of the IAO protection service.

From the analysis of LAR principle of operation in the conditions of the CR usage, it can be noted that the total signal of the beams $E^o(t)+E^{CR}(t)$ will play the role of a reference (in the Michelson interferometer).

Setting up the optimal LAR performance according to the criterion of amplitude equality with the information signal field $E^i(t)$ will not always be achieved due to the control of settings by different parties – the LAR operator and the IAO protection service, which must counteract each other.

Thus, due to the addition of unmodulated signals $E^n(t)$ from the sidelobes, a component appears that does not allow the reconnaissance device to ensure the optimal reception of signals with a given quality.

The specific ratio of the interference signal to the information signal should be determined when introducing regulations for this method of protection against LAR.

Corner reflectors can be located in dedicated rooms in front of window panes, preferably near the expected location of the LAR beam. The weight of such devices, as mentioned earlier, should ensure their stable position (no vibration) under the influence of the sound field of the conversation).

Evaluation of the corner reflector usage possibility in the protection against LAR

The physical realization for the usage proposal can be assessed on the basis of energy ratios accepted in the practice of electronic warfare research.

The energy assessment of the effect of CR on the received dangerous signal is based on the ratio of the effective illumination of PD I_{CR} from CR to the effective illumination I_i by the dangerous signal from the window pane – the suppression factor:

$$C_s = I_{CR}/I_i, \tag{17}$$

The numerator of this expression can be written as:

$$I_{CR} = \frac{I \cdot F(\theta)^2}{4\pi r^2}\sigma(1-C_R)^2\frac{C_R}{4\pi r^2} = \frac{I \cdot F(\theta)^2}{(4\pi r^2)^2}\sigma(1-C_R)^2, \tag{18}$$

where F(θ) – normalized diagram of the electric field directivity of the LAR (13);

C_r – coefficient of reflection of the LAR beam from the window glass;

$$I_i = \frac{I \cdot C_R \cdot F(\theta=0)^2}{4\pi(2r)^2}, \tag{19}$$

After substituting into (17) and making the necessary simplifications, we can obtain an expression for the suppression coefficient C_s:

$$C_s = \frac{I_{CR}}{I_i} = F(\theta)^2 \cdot \frac{(1-C_R)^2}{C_R} \cdot \frac{4\sigma}{\pi r^2}. \tag{20}$$

From this expression, it is possible to estimate the requirements for the characteristics of a corner reflector that is advisable to use for protection against LAR. So, for example, a square-faceted corner reflector for an infrared wave of 800 nm, a window with $C_R = 0{,}1$ and 3 distances of 100 m should have a face size of 0,053 m to ensure $C_s = 10$ at a laser emission sidelobe level of 0,001. This is quite possible to implement at IAO.

Conclusions

The work analyzes the possibility of using a new method of protection against interference-type LAR when trying to obtain information voiced at the objects of information activity.

Separate quantitative models of the LAR elements and the method of creating targeted interference are proposed.

References:

1. Ivanchenko S., Havrylenko O., Lypskyi O., and Shevtsov A. Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інформації / Репозитарій КПІ ім. Ігоря Сікорського. Accessed: Nov. 3, 2024. [Online]. Available: https://ela.kpi.ua/server/api/core/bitstreams/930d9270-2cb1-4c62-a4ce-ab5404d9b90f/content.
2. Dudykevych V., Sobchuk I. and Rakobovchuk V. Пасивний захист інформації від лазерного зондування // Вісн. Нац. ун-ту "Львів. політехніка". Сер. Автоматика, вимірювання та керування. 2013. № 753. С. 118–123. [Online]. Available: http://nbuv.gov.ua/UJRN/VNULP_2013_753_20.
3. Zabolotnyi V. and Kovalchuk Y. Безшумний" захист від "лазерних мікрофонів"// Прикладная радиоэлектроника. 2009. Т. 8, № 3. С. 377–382.
4. Zabolotnyi V. and Kovalchuk Y. Модель отражающей поверхности лазерного канала разведки информации // Прикладная радиоэлектроника. 2007. Т. 6, № 3. С. 432–434,.
5. Прикладна дифракційна оптика: підручник / V.H. Kolobrodov, H.S. Tymchyk. Київ : НТУУ „КПІ”, 2014. 312 с.

Received 04.01.2025

Information about the authors:

Volodymyr Zabolotnyi – Ph.D. of Engineering Sciences, Associate Professor, Kharkiv National University of Radio Electronics, Professor of the Department of Information Technology Security, Ukraine; e-mail: volodymyr.zabolotnyi@nure.ua; ORCID: https://orcid.org/0000-0003-3258-8489

Nikita Kholiev – Kharkiv National University of Radio Electronics, undergraduate student of cybersecurity, Ukraine; e-mail: nikita.kholiev@nure.ua; ORCID: https://orcid.org/0009-0000-7111-2462

Valeriia Dovhal – Kharkiv National University of Radio Electronics, undergraduate student of cybersecurity, Ukraine; e-mail: valeriia.dovhal@nure.ua, ORCID: https://orcid.org/0009-0004-2243-1650

UDC 004.056.5 **DOI:10.30837/rt.2025.1.220.07**

Yu.L. GOLIKOV, Ye.V. OSTRIANSKA

RESEARCH AND CLASSIFICATION OF THE MAIN TYPES OF ATTACKS ON ARTIFICIAL INTELLIGENCE SYSTEMS IN CYBERSECURITY

Introduction

In today's world, artificial intelligence (AI) is increasingly being integrated into various areas of human activity, from finance and medicine to autonomous vehicles and cybersecurity. Along with the development of AI technologies, new challenges arise, including threats related to attacks on artificial intelligence. Such attacks can have serious consequences, including compromising data security, manipulating algorithms, and creating vulnerabilities in critical systems.

Machine learning, as the basis of most modern AI systems, allows them to find patterns in data, adapt to changes, and improve over time. However, since ML models rely heavily on the quality of the input data and the hypotheses they are based on, they are vulnerable to certain types of attacks. Attackers can manipulate training data, spoof input parameters, or exploit algorithmic weaknesses to achieve their goals.

In essence, the machine learning methodology used in modern AI systems is susceptible to attacks through publicly available APIs that expose the model and against the platforms on which they are deployed. For attacks on security models, attackers can compromise the privacy and data protection of both the model and the data simply by using publicly available interfaces and providing input data that is within an acceptable range. In this sense, the challenges faced by AML are similar to those faced by cryptography. Modern cryptography relies on secure algorithms in the theoretical sense of information. Thus, people should only focus on their reliable and secure implementation, which is the primary task for the cryptographic research community. Unlike cryptography, there are no information-theoretic security proofs for widely used machine learning algorithms. As a result, many advances in the development of mitigation tools for various classes of attacks are empirical and limited.

But many companies and organizations have been actively working in recent years to regulate the use of AI in their systems. For example, among a wide range of activities, NIST contributes to the research, standards, assessments, and data needed to develop, use, and ensure reliable artificial intelligence (AI). In 2024, NIST published a report [1] on machine learning threats, and in 2025 it updated it [25]. This report developed a taxonomy of concepts and defined terminology in the field of adversarial machine learning (AML).

Attacks on AI/ML systems can be divided into several categories depending on the attacker's goals, implementation methods, and the level of impact on the model. Among the most common types of attacks are poisoning attacks, evasion attacks, privacy attacks, and denial-of-service attacks. Each of these types of attacks uses different mechanisms of influence, from spoofing training data to exploiting vulnerabilities in already trained models.

The relevance of the study is due to the growing number of cases of hacking and manipulation of AI systems, which can lead to financial losses, security threats, and loss of trust in technology. Therefore, the purpose of this article is to study the threats and risks associated with the use of AI. The article identifies the types of attacks that can be directed at AI/ML models, the stages of the attack life cycle, the goals and objectives of the attacker, as well as the attacker's capabilities and knowledge of the learning process. The study allows us to better understand current risks in the field of artificial intelligence and identify measures to improve the security of such systems.

1. Classification of AI-based attacks

An AI-based attack can be classified according to many different parameters. For example, several attack classification systems were presented in [7, 8]. NIST also presented different types of

classification in its report on AI machine learning attacks [1]. In this section, we will consider some types of classifications.

1.1. Main types of attacks

Attacks based on machine learning and AI are usually classified according to the following general parameters [1]:

1) the training method and the stage of the training process when the attack is established;
2) goals and objectives of the attacker;
3) capabilities of the attacker;
4) the attacker's knowledge of the training process.

Fig. 1 shows a general classification of attacks aimed at AI/ML models.

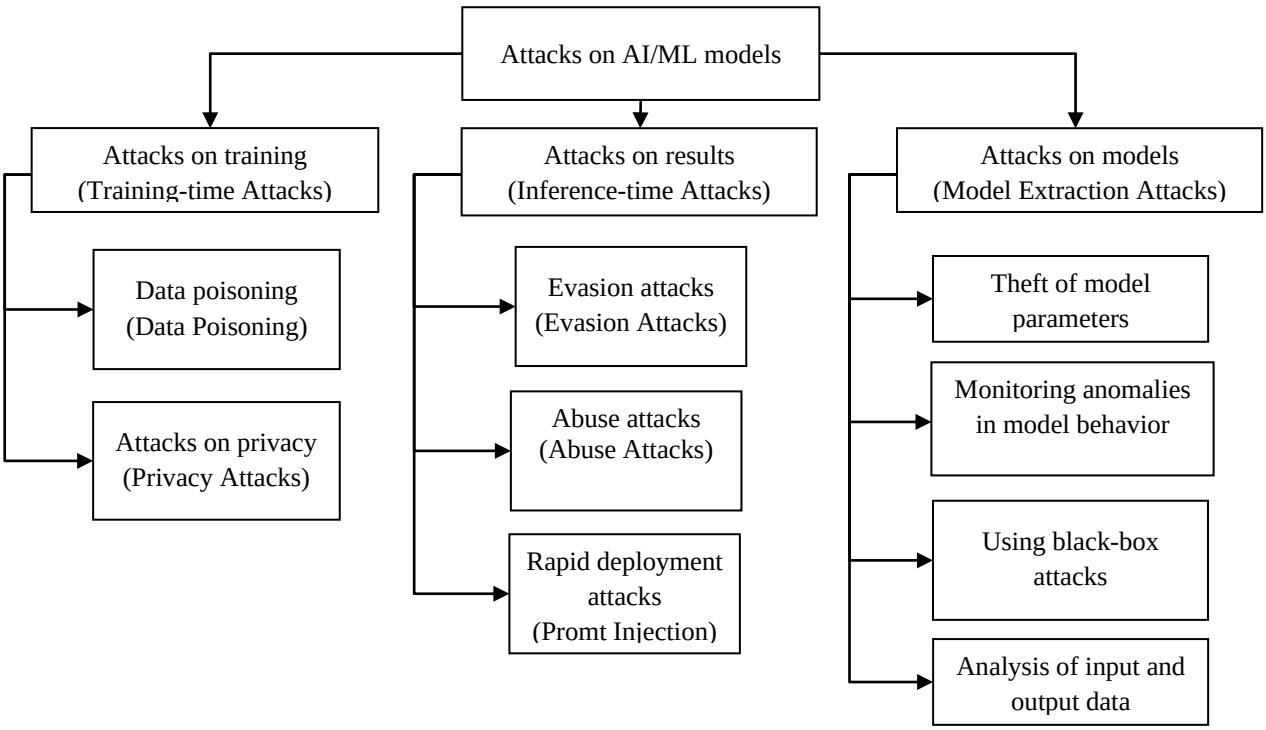


Fig. 1. Classification of attacks on AI systems

Fig. 1 shows a scheme of classification of attacks on AI systems. In turn, each of these attacks can be divided into the following main subgroups:

– Data Poisoning:
  - Introducing malicious data into the training set.
  - Label-flipping Attack.
  - Using hidden triggers (Backdoor Attack).
  - Manipulation of neural network weights.
– Privacy Attacks:
  - Extract data from the training set.
  - Model Inversion Attack.
  - Membership Inference Attack.
  - Hacking the model parameters.
– Evasion Attacks:
  - Manipulation of input data.
  - Image/text/audio attack.
  - Bypassing anti-virus systems.
  - Change the recognition parameters.

– Abuse Attacks:
  - Using generative AI to create fake content.
  - Deepfake (video, audio, images).
  - Social engineering attacks.
  - Creating malicious code.
– Prompt Injection attacks:
  - Influence on text models (ChatGPT, Bard, etc.).
  - Imposing unwanted answers.
  - Bypassing model limitations.
  - Generation of fake information.

1.2. Classification of attacks by attacker's goal

The attacker's goals are classified by three criteria in accordance with the three main types of security breaches [1] that are considered when analyzing system security: availability, integrity, and data confidentiality compromise. Accordingly, an attacker's success indicates the achievement of one or more of these goals.

An availability attack is an indiscriminate attack on machine learning (ML) in which an attacker attempts to disrupt the performance of a model during deployment. Availability attacks can be launched through data poisoning, where an attacker controls a portion of the training set, or through model poisoning, where an attacker controls the model parameters.

An integrity attack targets the integrity of the ML model's output, resulting in incorrect predictions made by the ML model. An attacker can cause an integrity breach by performing a bias attack during deployment or a poisoning attack during training. Evasion attacks require modifying test samples to create competitive examples that are misclassified by the model to a different class while remaining hidden and unnoticed by humans. Examples of such attacks can be found in [12, 13].

In privacy attacks, attackers may be interested in obtaining information about the training data or the ML model (resulting in data and model privacy attacks, respectively). An attacker may have different goals for compromising the privacy of training data, such as data modification (extracting the content or features of training data), data injection [14, 15] (the ability to extract training data from generative models), and injection of properties regarding the distribution of training data [16].

1.3. Classification of attacks by attacker's knowledge

Another criterion for classifying attacks is the extent to which the attacker has knowledge of the machine learning system. There are three main types of attacks according to this criterion [1]: white box, black box, and gray box.

- White box attacks. They assume that an attacker operates with full knowledge of the machine learning system, including training data, model architecture, and additional model parameters. Although these attacks operate under very strong assumptions, the main reason for analyzing them is to test the vulnerability of the system against the worst attackers and evaluate potential mitigations.
- Black box attacks. These attacks involve minimal knowledge of the ML system. An attacker can gain access to query the model, but they have no other information about how the model is trained. These attacks are the most practical because they assume that the attacker does not know the AI system and uses system interfaces that are easily accessible for normal use.
- Gray box attacks. There are a number of gray box attacks that capture conflicting knowledge between black box and white box attacks. Paper [17] presents a framework for classifying gray box attacks. An attacker may know the model architecture but not its parameters, or an attacker may know the model and its parameters but not the training data. Other common assumptions for gray box attacks are that the attacker has access to data distributed identically to the training data and knows the function representation. The latter assumption is important in applications where feature extraction is used before training an ML model, such as cybersecurity, finance, and healthcare.

That is, generally speaking, from an information perspective, if an attacker has complete knowledge of the model, such as parameters, functions, and training data, we speak of a white box attack. Conversely, if the attacker has no knowledge of the model's inner workings and only has access to its predictions, we call it a black box attack. Everything in between falls into the gray box category [22]. This is shown schematically in Fig. 2.

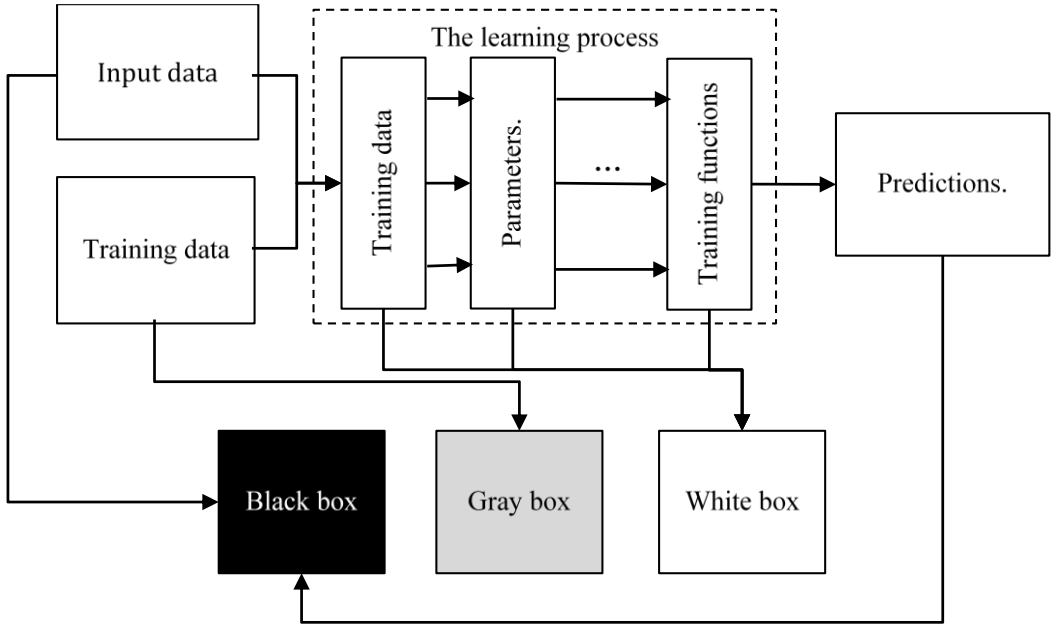


Fig. 2. Diagram of the degree of awareness of the attacker

In practice, the attacker often starts from a black box perspective and tries to increase his knowledge, for example by performing logical inference or oracle attacks, where the attacker queries the model to get clues about the model's internal elements or training data. Often, sensitive information about the target model can be obtained through more traditional means, such as open source intelligence (OSINT), social engineering, cyber espionage, etc.

2. Data poisoning attack

Attacks at the ML training stage are called poisoning attacks [1, 9]. In a data poisoning attack [5, 9], an attacker controls a subset of the training data by inserting or modifying training samples. In a model poisoning attack [10], the attacker controls the model and its parameters. Data poisoning attacks can be applied to all learning paradigms, while model poisoning attacks are most common in federated learning [11], where clients send local model updates to the server that processes the input, and in supply chain attacks, where malicious code can be added to the model by the model technology providers. Here, federated learning refers to a machine learning method focused on settings in which multiple entities (often called clients) jointly train a model, with the data used for training distributed in a decentralized manner. This distinguishes it from machine learning, in which data is stored centrally.

The first poisoning attacks detected in cybersecurity applications were availability attacks against the generation of worm profiles and spam classifiers that indiscriminately affect the entire machine learning model and essentially cause a denial-of-service attack for users of the AI system.

Poisoning attacks are considered to be one of the most dangerous among AI attacks and can cause either availability or integrity violations. In particular, availability attacks cause degradation of the machine learning model at all stages, while targeted and backdoor poisoning attacks are more stealthy and cause integrity violations on a small dataset. Poisoning attacks utilize a wide range of competitive capabilities such as data poisoning, model poisoning, label control, source code control, and test data control, resulting in several subcategories of poisoning attacks. According to the threat

model, they can be used in both white-box and black-box scenarios [18], which were discussed in Section 1.3 of this article.

Among the methods of preventing data poisoning attacks, there are two most effective ones [1]:

- Cleaning the training data. These methods exploit the fact that poisoned sets are usually different from normal training sets that are not controlled by attackers. Thus, data cleaning techniques are designed to clean the training set and remove the poisoned sets before performing machine learning training.
- Robust training. An alternative approach to mitigating availability attacks is to modify the ML learning algorithm and perform robust learning instead of regular learning. Several articles have identified robust optimization methods, such as using a reduced loss function [20] or random smoothing to add noise during training [21].

3. Evasion attack

Evasion Attacks are a type of cyberattack in which attackers modify input data to bypass a machine learning system and cause misclassification or false decisions. Such attacks usually occur at the stage of using the model, when it is already trained and deployed. Attackers make minor, often unnoticeable changes to the input data, which, however, significantly affect the model's performance.

The types of evasion attacks according to the NIST AI 100-2e2025 classification [25] include the following:

1. Gradient-based attacks: Attackers use information about the gradients of the model's loss function to determine the most effective input changes that will lead to misclassification [22].
2. Score-based attacks: Attackers gain access to the model's confidence scores and use optimization techniques to create fake examples that the model misclassifies.
3. Decision-based attacks: Attackers have access only to the final decisions of the model (e.g., class labels) and use optimization techniques to create fake examples that cause the model to make mistakes.
4. Transfer attacks [23]: Attackers train a replacement model, generate fake examples on it, and transfer these attacks to the target model by exploiting similarities between the models.

Evasion attacks pose a serious threat to cybersecurity systems. Attackers can change the characteristics of malware to bypass antivirus systems or modify network traffic to avoid detection by intrusion systems.

Currently, the main methods of protection [1] against evasion attacks are:

1. Adversarial training: Incorporating fake examples into the model training process to increase its resistance to attacks.
2. Use of ensembles of models (Ensemble methods) [24]: Combining multiple models to reduce the likelihood of a successful attack on all models at once.
3. Continuous monitoring and updating: Regularly updating detection models and systems to adapt to new attack strategies and improve resilience.

However, these methods have various limitations, such as reduced accuracy for adversarial learning and random smoothing, and computational complexity for formal methods. Therefore, a trade-off between robustness and accuracy should always be sought. Understanding and implementing these security techniques is critical to ensuring the security and reliability of machine learning systems in the face of increasing threats from evasion attacks.

4. Attack on privacy

Privacy attacks are a type of cyberattack aimed at obtaining sensitive information from artificial intelligence (AI) models, their training data, or output. These attacks can be used to steal personal data, compromise commercial information, or hack machine learning models.

Below, we'll look at the main types of privacy attacks:

1. Data Reconstruction Attacks: Attackers attempt to recreate the original data by accessing the AI model or its output. This can happen when the model produces overly detailed answers or has vulnerabilities that allow parts of the training data to be recovered.

2. Model Inversion Attacks: In this case, attackers use the output of the model to recreate the inputs or characteristics used in training. This can reveal sensitive information about the parties represented in the training data.

3. Membership Inference Attacks: Attackers try to determine whether specific records were included in the model's training dataset. This can be used to reveal a person's participation in certain events or membership in certain groups.

4. Metadata-based attacks: Even if the data itself remains secure, attackers can use metadata (e.g., access times, file sizes) to obtain sensitive information or establish patterns that can be used in further attacks.

5. Side-channel attacks: Attackers can analyze the behavior of an AI system, such as response time or energy consumption, to gain information about internal processes or model data.

It is recommended to protect against such attacks:

- Increasing anonymity and aggregating data. Use methods that reduce the risk of identifying individual records in training data.
- Federated Learning – training models on local devices without transferring data to the server.
- Differential privacy. Adding controlled noise to the data or model results to prevent the original data from being recovered without significantly affecting the model's accuracy.
- Access restriction and monitoring: Control access to models and data, and continuously monitor usage to detect suspicious activity.
- Vulnerability assessment: Regularly testing models for resistance to privacy attacks and implementing appropriate security measures.

Privacy attacks pose a serious threat to AI systems, including in the field of cybersecurity. Therefore, protecting privacy in AI systems is critical to maintaining user trust and regulatory compliance. Attackers use various methods to gain access to sensitive data or model parameters. Protecting such systems requires a comprehensive approach, including modern cryptographic methods, activity monitoring, and raising user awareness of risks.

5. Attack of abuse

Another type of attack on AI systems is abuse attacks [25]. These attacks are aimed at abusing or manipulating artificial intelligence (AI) systems to produce undesirable or harmful results. These attacks exploit vulnerabilities in the structure or implementation of AI models to cause the system to behave inappropriately.

Examples of abuse attacks:

1. Bias Exploitation: An attack in which an attacker exploits existing biases or weaknesses in an AI model to produce certain results or amplify discriminatory tendencies.

2. Functionality Misuse: Manipulating an AI system to perform actions that were not intended by the developers, such as using a chatbot to generate unwanted content or spam.

3. Prompt Injection Attacks: Injecting specially crafted queries or commands that cause the AI model to generate unwanted or malicious content.

To prevent such attacks, NIST recommends the following security measures:

- Improvement of anomaly detection algorithms – development of mechanisms that can recognize suspicious interactions with AI.
- Stricter data verification policies – analyzing incoming data to identify possible manipulations.
- Increase the transparency of AI systems by improving the documentation of decision-making processes in models.

- Mechanisms to counteract malicious intrusion, such as the introduction of additional levels of verification in security models.
- Development of standards for the ethical use of AI – active regulation and control over the implementation of such technologies.

Thus, misuse attacks pose a serious threat to AI systems, as they allow attackers to use them in unexpected ways. The use of AI to automate fraud, manipulate public opinion, or circumvent restrictions creates new challenges for cybersecurity. Preventing such attacks requires a comprehensive approach, including improving security algorithms, developing policies for the responsible use of AI, and continuously monitoring threats.

6. General summary of attacks on AI systems

In Sections 2-5 of this article, we have discussed the 4 most influential types of attacks on ML/AI systems, namely:

Data poisoning attacks – are carried out during the training phase and can have a long-term impact on the model's accuracy, causing it to draw incorrect conclusions.

Evasion attacks are runtime attacks where attackers try to trick the model by injecting specially created data into it.

Privacy attacks – aimed at extracting sensitive data from the model, which jeopardizes the security of users' personal information.

Abuse attacks are associated with the misuse of AI capabilities, for example, to create fake videos, malicious code, or manipulate social media.

The results of the analysis of the considered attacks are summarized in Table 1 below.

Table 1

Comparative characteristics of attacks on AI/ML systems

Type of attack	The purpose of the attack	The attack phase	Methods	Consequences
Poisoning Attack (data poisoning attack)	Impact on the quality of education	Model training	Adding malicious data to the training set	Deterioration in the quality of decisions, false alarms, and reduced security for further attacks
Evasion Attack (evasion attack)	Bypassing model security mechanisms	Execution of the model	Manipulation of source data, generation of special malicious data	Bypassing defense mechanisms, reducing model accuracy
Privacy Attack (privacy attack)	Theft of data used to train the model	Execution of the model	Analyzing model responses, data recovery	Confidential data leakage
Abuse Attacks (misuse attacks)	Using AI to create malicious data	After deploying the model	Generative models for attacks, manipulation	Information manipulation, fraud automation

Conclusions

1. AI is a good tool for automating the processes of detecting and responding to attacks and threats, and significantly increases the efficiency of protecting systems and companies. The use of machine learning algorithms helps to quickly analyze large amounts of data and identify anomalies in the behavior of users and systems.

2. However, AI not only provides effective protection, but also creates new threats due to its possible use by malicious actors. That is why the issue of detecting and counteracting attacks is a very important issue in the modern cyberspace. Therefore, in this article, we have reviewed and comprehensively analyzed attacks on modern ML/AI models.

3. The reliability of an AI system depends on all the attributes that characterize it. For example, an AI system that is accurate but easily susceptible to aggressive actions is unlikely to be trustworthy. Likewise, an AI system that produces harmfully biased or unfair results is unlikely to be trusted, even if it is reliable. There are also trade-offs between transparency and competitiveness. Unfortunately, it is not possible to maximize the performance of an AI system with respect to these attributes simultaneously. For example, AI systems optimized only for accuracy tend to underperform in terms of competitive reliability and fairness. Conversely, an AI system optimized for competitiveness may demonstrate lower accuracy and poorer reliability results.

4. Data poisoning attacks are the most dangerous type of AI-based attacks in the long run, as they affect the model itself and can remain undetected for a long time.

5. Privacy attacks and abuse attacks are particularly dangerous because of the possibility of leaking sensitive data and creating malicious content.

6. The study revealed the general consequences of AI-based attacks:

- Undermining trust in AI – constant attacks and manipulations can make AI a less reliable decision-making tool.
- Confidential information leakage – privacy attacks lead to large-scale losses of personal and corporate data.
- Defense bypassing – model evasion and poisoning jeopardize modern cybersecurity systems, reducing their effectiveness.
- Scalability of attacks – attackers can use AI to automate and accelerate attacks, which increases their impact.
- State-level risks – AI-based attacks can threaten national security, the economy, and critical infrastructure.

7. Therefore, the main ways to protect against AI-based attacks are as follows:

- Developing resilient AI models that are less vulnerable to poisoning or evasion.
- Implementation of attack detection mechanisms, such as monitoring changes in training data and algorithms.
- Increasing the transparency of AI by creating explainable models that can be checked for manipulations.
- Strengthening regulation and standards – governments and organizations should set rules for the use of AI.

8. Each type of attack on AI systems has different mechanisms of influence, but all of them can significantly reduce the efficiency and security of machine learning models. Protection against such attacks requires a comprehensive approach. In addition to the above methods of counteracting attacks, the human factor remains important – training of specialists and users, as many attacks are based on social engineering.

9. In most cases, organizations will have to make a trade-off between desirable attributes and decide which to prioritize depending on the AI system, use case, and potentially many other considerations regarding the economic, environmental, social, cultural, political, and global implications of AI technology.

10. It is important to note that with the development of AI technologies, new types of attacks are emerging, so constant monitoring and updating of knowledge in this area is essential to ensure cybersecurity.

11. To summarize, it is important to note that the safe use of AI in cybersecurity is a balance between technological innovations and threats arising from their development. The development of adaptive security methods and the improvement of machine learning models will help reduce the risks associated with attacks and ensure a reliable level of cyber defense in the future.

References:

1. Vassilev A., Oprea A., Fordyce A., Anderson H (2024) Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations. (National Institute of Standards and Technology, Gaithersburg, MD) NIST Ar-

tifcial Intelligence (AI) Report, NIST Trustworthy and Responsible AI NIST AI 100-2e2023. Access mode: https://doi.org/10.6028/NIST.AI.100-2e2023.

2. Booth H., Souppaya M., Vassilev A., Ogata M., Stanley M., Scarfone K. (2024) Secure Development Practices for Generative AI and Dual-Use Foundation AI Models: An SSDF Community Profile. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-218A. Access mode: https://doi.org/10.6028/NIST.SP.800-218A.

3. Oprea A., Singhal A. and Vassilev A. Poisoning Attacks Against Machine Learning: Can Machine Learning Be Trustworthy? // Computer. 2022. Vol. 55, no. 11. P. 94–99. doi: 10.1109/MC.2022.3190787.

4. Hui Wei, Hao Tang, Xuemei Jia, Zhixiang Wang, Hanxun Yu, Zhubo Li, Shin'ichi Satoh, Luc Van Gool, Zheng Wang. Physical Adversarial Attack Meets Computer Vision: A Decade Survey // IEEE Transactions on Pattern Analysis and Machine Intelligence. 2024. Vol. 46, no. 12. P. 9797–9817.

5. Anjan K. Koundinya S. S. Patil, Chandu B. R. Data Poisoning Attacks in Cognitive Computing // IEEE 9th International Conference for Convergence in Technology (I2CT). 2024. P.1–4.

6. National Institute of Standards and Technology. Artifcial Intelligence Risk Management Framework. 2023. (AI RMF 1.0). Access mode: https://doi.org/10.6028/NIST.AI.100-1.

7. Battista Biggio and Fabio Roli. Wild patterns: Ten years after the rise of adversarial machine learning. Pattern Recognition, 84:317–331, December 2018.

8. Octavian Suciu, Radu Marginean, Yigitcan Kaya, Hal Daume III, and Tudor Dumitras. When does machine learning FAIL? generalized transferability for evasion and poisoning attacks // 27th USENIX Security Symposium (USENIX Security 18). 2018. P. 1299–1316.

9. Battista Biggio, Blaine Nelson, and Pavel Laskov. Poisoning attacks against support vector machines // Proceedings of the 29th International Conference on International Conference on Machine Learning, ICML, 2012.

10. Yingqi Liu, Shiqing Ma, Yousra Aafer, Wen-Chuan Lee, Juan Zhai, Weihang Wang, and Xiangyu Zhang. Trojaning attack on neural networks // NDSS. The Internet Society, 2018.

11. Kairouz, Peter; McMahan, H. Brendan; Avent, Brendan; Bellet, Aurélien; Bennis, Mehdi; Bhagoji, Arjun Nitin; Bonawitz, Kallista; Charles, Zachary; Cormode, Graham (June 22, 2021). Advances and Open Problems in Federated Learning // Foundations and Trends in Machine Learning 14 (1-2): doi:10.1561/2200000083. ISSN 1935-8237.

12. Yingqi Liu, Shiqing Ma, Yousra Aafer, Wen-Chuan Lee, Juan Zhai, Weihang Wang, and Xiangyu Zhang. Trojaning attack on neural networks // NDSS. The Internet Society, 2018.

13. Kairouz, Peter, McMahan, H. Brendan, Avent Brendan, Bellet Aurélien, Bennis Mehdi, Bhagoji Arjun Nitin, Bonawitz Kallista, Charles Zachary, Cormode Graham (June 22, 2021). Advances and Open Problems in Federated Learning // Foundations and Trends in Machine Learning 14 (1-2). doi:10.1561/2200000083. ISSN 1935-8237.

14. Christian Szegedy, Wojciech Zaremba, Ilya Sutskever, Joan Bruna, Dumitru Erhan, Ian Goodfellow, and Rob Fergus. Intriguing properties of neural networks // International Conference on Learning Representations, 2014.

15. Ian Goodfellow, Jonathon Shlens, and Christian Szegedy. Explaining and harnessing adversarial examples // International Conference on Learning Representations, 2015.

16. Nicholas Carlini, Chang Liu, Ulfar Erlingsson, Jernej Kos, and Dawn Song. The Secret Sharer: Evaluating and testing unintended memorization in neural networks // USENIX Security Symposium, USENIX 19). 2019. P. 267–284. Access mode: https://arxiv. org/abs/1802.08232.

17. Nicholas Carlini, Florian Tramer, Eric Wallace, Matthew Jagielski, Ariel Herbert - Voss, Katherine Lee, Adam Roberts, Tom Brown, Dawn Song, Ulfar Erlingsson, Alina Oprea, and Colin Raffel. Extracting training data from large language models // 30th USENIX Security Symposium (USENIX Security 21). 2021. P. 2633–2650. USENIX Association, August 2021.

18. Karan Ganju, Qi Wang, Wei Yang, Carl A. Property inference attacks on fully connected neural networks using permutation invariant representations // Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, CCS '18, pages 619-633, New York, NY, USA, 2018. Association for Computing Machinery.

19. Octavian Suciu, Radu Marginean, Yigitcan Kaya, Hal Daume III, and Tudor Dumitras. When does machine learning FAIL? generalized transferability for evasion and poisoning attacks // 27th USENIX Security Symposium (USENIX Security 18). 2018. P. 1299–1316.

20. Battista Biggio, Blaine Nelson, and Pavel Laskov. Poisoning attacks against support vector machines // Proceedings of the 29th International Conference on International Conference on Machine Learning, ICML, 2012.

21. Nihad Hassan. What is data poisoning (AI poisoning) and how does it work? Search Enterprise AI, TechTarget, 2024. Access mode: https://www.techtarget.com/searchenterpriseai/definition/data-poisoning-AI-poisoning.

22. Ilias Diakonikolas, Gautam Kamath, Daniel Kane, Jerry Li, Jacob Steinhardt, and Alistair Stewart. Sever: A robust meta-algorithm for stochastic optimization. In International Conference on Machine Learning. PMLR, 2019. P.1596–1606.

23. Elan Rosenfeld, Ezra Winston, Pradeep Ravikumar, and Zico Kolter. Certified robustness to label-fipping attacks via randomized smoothing. In International Conference on Machine Learning. PMLR, 2020. P. 8230–8241.

24. The Tactics & Techniques of Adversarial Machine Learning. HiddenLayer. 2022. Access mode: https://hiddenlayer.com/innovation-hub/the-tactics-and-techniques-of-adversarial-ml.

25. Chi Zhang, Zifan Wang, Ravi Mangal, Matt Fredrikson, Limin Jia, Corina Pasareanu. Transfer Attacks and Defenses for Large Language Models on Coding Tasks. November 22, 2023. Access mode: https://doi.org/10.48550/arXiv.2311.13445.
26. D. Li and Q. Li. Adversarial Deep Ensemble: Evasion Attacks and Defenses for Malware Detection // IEEE Transactions on Information Forensics and Security. June 30, 2022. Access mode: https://doi.org/10.48550/arXiv.2006.16545.
27. Vassilev A., Oprea A., Fordyce A., Anderson H. (2025) Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations. (National Institute of Standards and Technology, Gaithersburg, MD) NIST Artifcial Intelligence (AI) Report, NIST Trustworthy and Responsible AI NIST AI 100-2e2025. Access mode: https://doi.org/10.6028/NIST.AI.100-2e2025.

Received 11.01.2025

Information about the authors:
Yuriy Golikov – CEO and Founder of DevBrother tech company, USA; e-mail: yuriy@devbrother.com; ORCID: https://orcid.org/0009-0008-7946-4663
Yelyzaveta Vadymivna Ostrianska – V.N. Karazin Kharkiv National University, junior researcher, JSC "IIT", information security systems analyst, Ukraine; e-mail: antelizza@gmail.com; ORCID: https://orcid.org/0000-0003-1412-8470

УДК 621.391:519.2 **DOI:10.30837/rt.2025.1.220.08**

Є.В. КОТУХ, канд. техн. наук, Г.З. ХАЛІМОВ, д-р техн. наук,
М.В. КОРОБЧИНСЬКИЙ, д-р техн. наук, І.Є. ДЖУРА

АНАЛІЗ ОБМЕЖЕНЬ КВАНТОВИХ ОБЧИСЛЕНЬ У ЗАДАЧАХ КРИПТОАНАЛІЗУ

Вступ

Ера NISQ (Noisy Intermediate-Scale Quantum) визначає поточний стан розвитку квантових обчислень та характеризується квантовими процесорами, які містять від десятків до тисяч кубітів, але не мають механизмів повноцінної корекції помилок, що зумовлює недосяжність стабільної квантової переваги над класичними комп'ютерами. Розвиток технологій квантових обчислень в умовах обмежених ресурсів у період з 2020 по 2025 р. демонструє поступовий перехід від теоретичних досліджень до прикладного застосування, а також підготовку до впровадження повноцінних обчислень із виправленням помилок. Починаючи з 2020–2021 рр. основна увага була зосереджена на фундаментальних дослідженнях і розробці базових алгоритмів, що працюють у шумному квантовому середовищі. Протягом цього етапу відзначалося стабільне зростання кількості наукових публікацій у галузі квантових обчислень, що зумовлено загальним технологічним проривом у галузі після 2015 р. та його суттєвим прискоренням з 2020 р. Дослідницькі ініціативи зосереджувалися на пошуку шляхів ефективного використання обмежених квантових ресурсів, зокрема через адаптацію алгоритмів до шуму, що притаманний апаратному забезпеченню проміжного рівня. У період 2021–2022 рр. відбувся перехід до практичної демонстрації можливостей квантових алгоритмів на фізичних пристроях. Значущим кроком стало виконання алгоритму квантової приблизної оптимізації (QAOA) на квантовому комп’ютері Google Sycamore із 53 кубітами [1]. Цей експеримент продемонстрував здатність NISQ-систем виконувати обчислювальні задачі з реальним практичним значенням навіть за умов суттєвого рівня шуму та обмеженого контролю над квантовими станами. Це також стало свідченням того, що квантова перевага можлива до досягнення повної толерантності до помилок. Наступний етап в 2023–2024 рр. демонстрував рішення щодо зниження рівня шуму та масштабування архітектури. Було досягнуто важливих результатів у підвищенні точності квантових операцій, зокрема двокубітних гейтів, що перевищили 99,9 % точності. Водночас активно розроблялися нові варіанти алгоритмів, оптимізованих для наявного квантового заліза, які краще враховують фізичні обмеження кубітів, їх зв’язність та топологію. Значну увагу було приділено розробці методів гібридних обчислень, що поєднують класичні та квантові ресурси, а також методам мітігації шуму без використання повноцінної корекції помилок. У 2024–2025 рр. спостерігається стратегічний зсув у напрямку початкової реалізації квантових комп’ютерів із виправленням помилок (FTQC). Це позначає завершення етапу суто шумних обчислень і поступовий перехід до більш стабільних архітектур, здатних підтримувати тривале квантове когерентне обчислення. Провідні компанії у сфері квантових технологій все частіше спрямовують свої зусилля на розробку систем квантової корекції помилок (QEC), що підтверджується зростаючою кількістю інвестицій у відповідні дослідження. За деякими оцінками, близько двох третин індустріальних гравців активно працюють у цьому напрямку або вже інтегрують QEC у свої розробки, що свідчить про нову фазу у розвитку квантових технологій. Таким чином, період 2020–2025 рр. можна охарактеризувати як критично важливий перехідний етап у формуванні основ майбутніх квантових обчислень з повною корекцією помилок та масштабованими архітектурами.

Мета статті – проведення аналізу щодо обмежень поточних квантових архитектур та підходів до організації квантових обсчилень в задачах квантового криптоаналізу.

Етапи розвитку квантових обчислень

NISQ-ера є перехідною фазою розвитку квантових обчислень, що характеризується наявністю пристроїв із обмеженою кількістю кубітів та високим рівнем шуму, що унеможливлює повноцінну реалізацію алгоритмів із квантовою корекцією помилок. У відповідь на ці обмеження в рамках NISQ-парадигми було розроблено низку спеціалізованих алгоритмів та обчислювальних стратегій, здатних працювати в умовах нестабільного квантового середовища. Одним із найбільш поширених підходів є варіаційний квантовий алгоритм знаходження власних значень (VQE), який базується на гібридному квантово-класичному циклі оптимізації. Цей алгоритм знайшов широке застосування у квантовій хімії для моделювання молекулярних структур та визначення енергетичних рівнів, що становить значний інтерес як для наукових, так і для промислових задач.

Іншим перспективним алгоритмом, розробленим спеціально для пристроїв NISQ-типу, є QAOA, призначений для вирішення складних комбінаторних оптимізаційних задач, зокрема задач на графах, маршрутизації та розміщення ресурсів. QAOA вирізняється здатністю досягати хороших апроксимаційних результатів навіть за обмеженої кількості квантових операцій, що робить його одним із провідних кандидатів на демонстрацію так званої квантової переваги в реальних умовах. Оскільки пристрої NISQ характеризуються високим рівнем помилок, важливим напрямом досліджень стали методи зниження впливу шуму на обчислення. Серед найбільш ефективних стратегій можна виділити рандомізовану компіляцію (RC), яка перетворює квантові схеми у форму, більш стійку до шуму, та екстраполяцію до нульового шуму (ZNE), що дозволяє оцінити результат імовірного обчислення за ідеального (безшумного) середовища. Синергічне застосування цих методів, зокрема в контексті алгоритмів на кшталт VQE, дало змогу значно підвищити точність результатів без потреби в повноцінній реалізації системи квантової корекції помилок [2].

У межах NISQ-епохи також активно розвивалися гібридні квантово-класичні підходи. Ці архітектури поєднують квантову частину, яка відповідає за генерацію та маніпуляцію квантовими станами з класичними методами оптимізації та обробки результатів. Серед них вирізняються варіаційні методи, техніки схемного "плетіння" (Circuit Knitting), розділення великих задач на менші підзадачі, а також використання класичної постобробки для зменьшення помилок. Такі інтегровані підходи дозволяють розширити можливості квантових обчислень в умовах апаратних обмежень та слугують основою для подальшого переходу до квантової толерантності до помилок.

Потенційні сфери застосування технологій NISQ є надзвичайно широкими, охоплюють як фундаментальні наукові дослідження, так і прикладні галузі з високим економічним потенціалом. У сфері оптимізації квантові обчислення вже застосовуються до логістичних задач, фінансового моделювання та оптимізації ланцюгів постачання. Алгоритми на кшталт QAOA дозволяють шукати оптимальні або близькі до оптимальних рішення для складних задач, таких як маршрутні задачі, розміщення виробничих потужностей або вибір інвестиційних стратегій, що раніше вимагали значних обчислювальних ресурсів. Квантова перевага в таких випадках може виявлятися у пришвидшеному знаходженні глобальних екстремумів у багатовимірних і складних просторах рішень.

Стратегічною галуззю, де активно розвиваються квантові підходи, є криптографія. Хоча NISQ-пристрої наразі не здатні зламати стійкі класичні криптографічні схеми, вони стимулюють розвиток квантово-стійких (post-quantum) алгоритмів шифрування, які залишатимуться захищеними навіть у випадку появи потужних квантових комп’ютерів [3–6]. Окрім цього, активно досліджується вплив квантових обчислень на надійність сучасних протоколів, що зумовлює перегляд криптографічних стандартів на міжнаціональному рівні.

Попри стрімкий прогрес у сфері квантових обчислень, ера NISQ супроводжується низкою фундаментальних викликів, які досі обмежують практичне застосування цих технологій. Однією з ключових проблем є обмежена масштабованість існуючих систем. Хоча значні інвестиції з боку університетів, урядових структур та індустрії дозволили досягти поточного

рівня розвитку, квантові комп'ютери NISQ-класу ще не демонструють переваг над класичними системами у вирішенні реальних задач. Водночас оптимістичні оцінки припускають, що перехід до пост-NISQ технологій відбудеться вже найближчими роками.

Одним із головних технічних бар'єрів залишається проблема шуму та помилок у квантових системах. Через надзвичайну чутливість кубітів до навколишніх впливів результати обчислень можуть бути суттєво спотворені. Гібридні підходи, що поєднують класичну обробку даних з квантовими обчисленнями, дозволяють досягати значного зменшення похибок, що підтверджується числовими експериментами.

Паралельно з цим триває активний пошук нових квантових архітектур, які можуть забезпечити подолання поточних обмежень. У 2024 р. було оголошено про створення першого у світі топологічного кубіта, важливого кроку на шляху до реалізації відмовостійких квантових комп'ютерів. Крім того, інновації у вигляді «скляних» чіпів, що забезпечують більш стабільне середовище для роботи кубітів, вказують на прагнення до "чистої" і стійкої квантової інфраструктури. Важливо, що у квантовій галузі спостерігається технологічне розмаїття: від надпровідникових схем і пасток для іонів до фотонних і топологічних систем. Саме така різноманітність дозволяє компаніям створювати рішення, придатні до використання в умовах існування ринку квантових обчислень – фази, коли квантові комп'ютери виконуватимуть реальні прикладні задачі з економічною ефективністю.

Однією з найважливіших тенденцій у сучасному розвитку квантових обчислень є поступовий перехід до ери квантових комп'ютерів із повноцінною толерантністю до помилок (FTQC). Очікується, що в період з 2025 по 2029 рр. з'являться перші FTQC-машини, здатні працювати в обчислювальних режимах масштабу MegaQuops або навіть GigaQuops, використовуючи декілька сотень логічних кубітів. У рамках NISQ-парадигми основна увага приділяється методам зниження та пом'якшення шумів, включаючи рандомізовану компіляцію, екстраполяцію до нульового шуму та різні стратегії класичної постобробки результатів. У свою чергу, FTQC базується на реалізації повноцінної квантової корекції помилок (Quantum Error Correction, QEC), що дозволяє масштабувати обчислення без втрати точності за умови дотримання суворих вимог до точності фізичних операцій і надлишковості кубітів для побудови логічних одиниць.

Із технічної точки зору, сучасні NISQ-пристрої зазвичай оперують кількома сотнями до кількох тисяч фізичних кубітів із типовою двокубітною точністю в діапазоні 99–99,9 %. Ці параметри дозволяють виконувати демонстраційні обчислення та тестувати нові алгоритми, але не забезпечують масштабованості для обробки складних задач. Натомість, ранні FTQC-системи, навіть із порівняно невеликою кількістю (~100) логічних кубітів, демонструватимуть значно вищу надійність – із точністю понад 99,9999 % завдяки використанню кодів квантової корекції, таких як поверхневі коди (surface codes) або LDPC-коди (Low-Density Parity-Check).

Важливо зазначити, що найближчим часом кінцеві користувачі опиняться перед вибором між двома платформами: з одного боку NISQ-пристрої з великою кількістю (до 10000) фізичних кубітів і вдосконаленими методами пом'якшення шуму, а з іншого – FTQC-пристрої з меншою, але більш надійною кількістю логічних кубітів. Цей вибір буде залежати від характеру задачі. Деякі наукові проблеми (особливо пов'язані з хімічним моделюванням або квантовою симуляцією) можуть залишатися ефективно вирішуваними на NISQ-архітектурах, тоді як інші, зокрема криптографічні обчислення, великомасштабна оптимізація або точне моделювання квантових систем, потребуватимуть надійності та масштабованості FTQC.

Отже, перехід до FTQC не означає негайного відкидання NISQ-моделі, а радше знаменує початок співіснування двох типів квантових платформ, кожна з яких займатиме своє місце в інноваційній екосистемі квантових технологій.

Таким чином, квантові обчислення перетворилися з суто академічної дисципліни на сферу з чіткою комерційною стратегією. Сьогодні почали з'являтися перші практичні реалізації квантових алгоритмів, системи стали доступними у хмарі, а промислові гіганти розгор-

нули дорожні карти до FTQC. Цей етап ознаменував кінець епохи "невідомого" у квантових обчисленнях та початок періоду активного інженерного вдосконалення та комерціалізації. Таким чином, попри обмеження, властиві періоду NISQ, наявні досягнення вже відкривають реальні можливості для прикладного використання квантових обчислень у різних галузях, що підкреслює важливість продовження досліджень у сфері квантових алгоритмів, методів зниження шуму та гібридних архітектур, що у сукупності формують базис майбутньої ери повноцінних квантових обчислень.

Постквантова криптографія в еволюційонму процесі квантових обчислень

Із зростанням обчислювальної потужності квантових комп'ютерів під загрозою опиняються традиційні криптографічні протоколи (зокрема, RSA, ECC), вразливі до алгоритму Шора. У відповідь на це зростає інтерес до квантово-безпечної (post-quantum) криптографії, яка включає розробку алгоритмів, стійких до атак квантових комп’ютерів. Паралельно з цим розвиваються квантові протоколи захисту інформації, зокрема квантового розподілу ключів (QKD), що базується на принципах квантової механіки й гарантує виявлення будь-якої спроби прослуховування. На відміну від класичних криптоаналітичних підходів, квантові алгоритми, зокрема алгоритм Шора, здатні ефективно зламувати криптографію з відкритим ключем, засновану на таких математичних задачах, як факторизація цілих чисел, обчислення дискретного логарифма та дискретного логарифма на еліптичній кривій [7]. Хоча сучасні квантові пристрої ще не є криптографічно релевантними (CRQC), прогрес у галузі передбачає необхідність завчасної підготовки. У період NISQ-ери ці системи ще не здатні виконувати обчислення з довгими ланцюгами квантових гейтів, необхідні для реалізації квантових криптоаналітичних атак на практиці. Наприклад, розв’язання задачі факторизації 2048-бітного RSA-ключа вимагатиме тисячі коректованих від помилок кубітів та мільйони логічних гейтів, що виходить далеко за межі сучасних NISQ-систем [8].

Квантові обчислення мають значно сильніший вплив на алгоритми з відкритим ключем, ніж на симетричні криптографічні схеми. Асиметричні алгоритми, такі як RSA, DSA та алгоритми на еліптичних кривих, базуються на складності математичних задач факторизації, дискретного логарифмування та логарифмування на еліптичних кривих. Відповідно, ці методи є уразливими до атак криптографічно релевантних квантових комп’ютерів (CRQC), які передбачають наявність тисяч коректованих від помилок кубітів. Алгоритм Гровера є ще одним прикладом квантової загрози. Він забезпечує квадратичне прискорення для пошуку в невпорядкованих структурах, знижуючи складність з $O\ N\ O\ N\ O\ N$ до $O\ N\ O\ \sqrt{N}\ O\ N$. Хоча така перевага не настільки драматична, як у Шора, вона може мати серйозні наслідки для симетричних криптосистем.

Оскільки атаки квантових алгоритмів уже змодельовано й підтверджено теоретично, світова спільнота вживає заходів щодо заміни вразливих схем. Зокрема, NIST (Національний інститут стандартів і технологій США) завершив відбір стандартів постквантової криптографії. 3 серпня 2024 р. NIST опублікував перші три фіналізовані стандарти, які мають захистити цифрові дані від потенційних атак квантових комп’ютерів: FIPS 203 (ML-KEM), алгоритм для направленого шифрування, заснований на CRYSTALS-Kyber, FIPS 204 (ML-DSA), алгоритм цифрового підпису, заснований на CRYSTALS-Dilithium та FIPS 205 (SLH-DSA), алгоритм цифрового підпису, заснований на SPHINCS+, який використовує хеш-функції для забезпечення безпеки.

Багато квантових алгоритмів для HSP спираються на принципи визначення періоду. Для абелевих груп складність залишається поліноміальною, але для неабелевих груп складність значно зростає (часто стає експоненціальною), оскільки квантове перетворення Фур’є стає важчим для інтерпретації. Хоча алгоритми Шора та Саймона пропонують ефективний пошук періоду для певних типів періодичностей (модульних та XOR відповідно), їхня складність залишається поліноміальною. Однак для неабелевих груп або інших складних структур квантові алгоритми можуть не мати такої переваги [9, 10].

У сучасних умовах розвитку квантових обчислень особливу увагу криптоаналітиків привертає реалізація фундаментальних квантових алгоритмів на NISQ-пристроях. Значну долю дослідженнь становить вивчення впливу цих обчислень на криптографічні методи та перспективи використання симетрії PT (парність-час) для подолання апаратних обмежень. Спочатку вивчена в контексті негерметичних гамільтоніанів, PT-симетрія була обґрунтована в роботах Карла Бендера і Стефана Беттчера наприкінці 1990-х років. Автори продемонстрували, що, незважаючи на неермітову природу, гамільтоніани з непорушеною PT-симетрією можуть мати дійсні власні значення, а за відповідного визначення внутрішнього добутку – унітарну еволюцію, яка є необхідною умовою для фізичної реалізації квантових систем. Останні експерименти на надпровідних квантових процесорах показали можливість моделювання еволюції квантової системи під дією PT-симетричних негерметичних гамільтоніанів із застосуванням допоміжних кубітів. Такі дослідження відкривають нові перспективи для реалізації складних квантових симуляцій у відкритих системах, зокрема періодично керованих квантових фаз, включно з реалізацією дискретних часових кристалів. Таким чином, PT-симетрія розглядається як інноваційний підхід до подолання обмежень сучасних NISQ-пристроїв і розширення арсеналу ефективних методів квантової симуляції.

Узагальнюючи, можна стверджувати, що сучасні дослідження в галузі квантових обчислень, зокрема в рамках NISQ-парадигми, демонструють значний поступ у реалізації теоретичних моделей, водночас висвітлюючи існуючі технічні та фізичні обмеження. Криптографічні виклики, що постають унаслідок розвитку квантових алгоритмів, актуалізують необхідність розгортання постквантових криптографічних протоколів. У свою чергу, розробка нових підходів, таких як впровадження PT-симетрії, відкриває нові горизонти у підвищенні ефективності квантових обчислень і розширенні їх застосувань у фундаментальній фізиці та прикладних інформаційних технологіях.

Аналіз критерієв квантових обчислень в контексті квантового криптоаналізу

Розглянемо ключові математичні моделі, що формалізують процес розвитку NISQ, EFTQC та FTQC обчислювальних систем. Одним з ключових математичних описів переходу між різними епохами квантових обчислень є модель масштабованості, представлена у статті [11]. Перехідний період між епохами NISQ та FTQC характеризується законом зменшення віддачі у квантовій корекції помилок (QEC), де здатність архітектури підтримувати якісні операції при масштабуванні визначає точку зменшення віддачі. Модель масштабованості опишемо наступним чином:

$$f\ \ Z\ = P_{база} \cdot \left(\frac{n_{фіз.куб.}}{n_0} \right)^{1/\alpha}$$

де $P_{база}$ – базовий рівень помилки для одного кубіта, $n_{фіз.куб.}$ – кількість фізичних кубітів, n_0 – нормалізаційний параметр, α – параметр масштабованості (scalability). Параметр масштабованості α є ключовим для класифікації: NISQ: $\alpha < 2$, EFTQC: $2 \le \alpha \le 3.5$, FTQC: $\alpha > 3.5$ (див. табл. 1). Проаналізуємо результати класифікації наступним чином.

При значеннях параметра масштабованості менших за 2, спостерігається стрімке зростання загального рівня помилок із збільшенням кількості кубітів у системі. Даний режим характерний для сучасного етапу розвитку квантових обчислень з використанням NISQ-пристроїв. Основними чинниками, що зумовлюють низьке значення α, є недостатня ізоляція кубітів від навколишнього середовища, наявність перехресних перешкод між сусідніми кубітами (crosstalk), обмежена точність контролюючих сигналів та високий рівень декогеренції. При таких значеннях параметра масштабованості застосування квантової корекції помилок є неефективним, оскільки процедури виявлення та виправлення помилок вносять більшу кількість нових помилок, ніж здатні виправити.

Таблиця 1

Еволюція квантових обчислень

Критерій	NISQ (Noisy Intermediate-Scale Quantum)	EFTQC (Early Fault-Tolerant Quantum Computing)	FTQC (Fault-Tolerant Quantum Computing)
Часові рамки практичних реалізацій	2018 – 2025	2025 – 2030	2030+
Класи складності	Слабший за BQP, сильніший за BPP	Між NISQ і BQP	BQP
Теорема про поріг помилки	Не застосовується (помилки вищі за поріг)	Частково застосовується (близько до порогу)	Повністю застосовується (нижче порогу)
Математична характеристика фізичної помилки	$P_{error} > P_{th}$	$P_{error} \approx P_{th}$	$P_{error} = P_{th}$
Модель масштабованості (scalability)	$\alpha < 2$	$2 \le \alpha \le 3.5$	$\alpha > 3.5$
Принцип корекції помилок	Пом'якшення помилок	Обмежена корекція помилок	Повна корекція помилок

Діапазон значень параметра масштабованості від 2 до 3.5 відповідає перехідному режиму ранніх відмовостійких квантових обчислень (EFTQC). У цьому режимі зростання рівня помилок при збільшенні кількості кубітів є помірним, що дозволяє імплементувати обмежені схеми корекції помилок з позитивним ефектом. Цей режим вимагає суттєвого покращення якості фізичних кубітів та систем контролю, включаючи: підвищену ізоляцію від оточення, зменшення перехресних перешкод, більш точне управління квантовими гейтами та ефективні методи пом'якшення помилок. Оскільки зростання помилок є достатньо повільним, стає можливим застосування часткової квантової корекції помилок, що дозволяє реалізувати обмежені відмовостійкі квантові схеми. Нижня межа α = 2 для цього режиму відповідає мінімальному значенню, при якому квантова корекція помилок починає давати позитивний ефект і є теоретично обґрунтованою точкою, в якій кількість виправлених помилок починає перевищувати кількість нових помилок, внесених схемами корекції.

Значення параметра масштабованості, що перевищують 3.5, характеризують режим повноцінних відмовостійких квантових обчислень (Fault-Tolerant Quantum Computing). У цьому режимі рівень помилок зростає настільки повільно з розширенням системи, що стає можливим ефективне застосування повномасштабних схем квантової корекції помилок. Досягнення таких значень параметра α вимагає надзвичайно високої якості фізичних кубітів з мінімальним рівнем декогеренції, практично відсутніми перехресними перешкодами та прецизійним квантовим контролем. При α > 3.5 рівень помилок зростає достатньо повільно, щоб забезпечити масштабування до систем з тисячами або навіть мільйонами логічних кубітів, що необхідно для вирішення практично значущих задач. Верхня межа α = 3.5 для EFTQC (яка є одночасно нижньою межею для FTQC) визначає значення, при якому ефективність корекції помилок стає достатньою для реалізації великомасштабних відмовостійких квантових обчислень з довільною кількістю логічних кубітів.

Проаналізуємо критерії співвідношення між фізичними та логічними кубітами в реалізації задач криптографічних квантових обчислень (див. табл. 2).

Таблиця 2

Оцінки характеристик кубітів для систем NISQ, EFTQC та FTQC

Характеристика	NISQ	EFTQC	FTQC
Кількість фізичних кубітів	50-1,000	10^3-10^6	$>10^6$
Кількість логічних кубітів	0	10-100	100-10,000+
Формула для кількості фізичних кубітів на логічний кубіт	не існує	$O\ d^2$	$>O\ d^2$
Рівень фізичної помилки	10^{-2}-10^{-3}	10^{-3}-10^{-4}	$<10^{-4}$
Рівень логічної помилки	N/A	: $p_{phys}^{d/2}$	: $p_{phys}^{d/2}$

NISQ-пристрої оперують з обмеженою кількістю фізичних кубітів (50-1,000) без реалізації логічних кубітів, що унеможливлює застосування квантової корекції помилок. Вони характеризуються високими рівнями фізичних помилок (10^{-2} – 10^{-3}), що суттєво обмежує глибину реалізованих квантових схем. Такі системи, як IBM Eagle (127 кубітів) та Atom Computing Phoenix (понад 100 кубітів), є типовими реалізаціями. Перехід до EFTQC-ери передбачає драматичне збільшення кількості фізичних кубітів (10^3 – 10^6) та реалізацію обмеженої кількості логічних кубітів (10 – 100). Це дозволяє імплементувати часткову корекцію помилок та виконувати квантові алгоритми середньої складності. У таких системах кількість фізичних кубітів на один логічний кубіт масштабується як $O\ d^2$, де d – відстань коду, а рівень фізичних помилок знижується до 10^{-3} – 10^{-4} . FTQC-системи характеризуються використанням понад мільйона фізичних кубітів для забезпечення сотень і тисяч логічних кубітів (100 – 10,000+) з повноцінною корекцією помилок. Рівень фізичних помилок у таких системах нижчий за 10^{-4} , що в поєднанні з більшою відстанню коду забезпечує достатньо низький рівень логічних помилок. Для поверхневого коду та аналогічних кодів рівень логічної помилки масштабується приблизно як: $p_{phys}^{d/2}$, де p_{phys} – рівень фізичної помилки. Дані співвідношення ґрунтуються на теоремі про поріг для квантової корекції помилок, яка стверджує, що для фізичних рівнів помилок нижче порогового значення логічний рівень помилки може бути знижений до довільно малого значення шляхом збільшення відстані коду. Ця теоретична база визначає фундаментальні вимоги до масштабування квантових систем та відкриває шлях до практичної реалізації потужних квантових алгоритмів у майбутньому.

Проаналізуємо квантові обчислювальні підходи (див. табл. 3).

Таблиця 3

Порівняння квантових обчислювальних підходів

Підхід	Обчислювальна парадигма	Математична складність схеми	Логічні кубіти	Глибина схеми
VQE та QAOA (NISQ)	Гібридна	$O\ p$ з глибиною p	Фізичні кубіти	Обмежена
RFE (EFTQC)	Робастні квантові алгоритми	$O\ K$ з параметром K	Обмежена кількість	Середня
QPE (FTQC)	Повна квантова корекція помилок	$O\ 1/\varepsilon$ для точності ε	Необмежена	Висока

Табл. 3 демонструє прогресію від більш обмеженого, але практично доступного NISQ-підходу (Noisy Intermediate-Scale Quantum) до теоретично потужнішого, але технологічно вимогливішого FTQC (Fault-Tolerant Quantum Computing). Підходи VQE (Variational Quantum Eigensolver) та QAOA (Quantum Approximate Optimization Algorithm) працюють в гібридній парадигмі, поєднуючи класичні та квантові обчислення, використовуючи доступні сьогодні фізичні кубіти з обмеженою глибиною схеми. Підхід RFE (Randomized Fourier Estimation) у контексті EFTQC (Error-Free Topological Quantum Computing) знаходиться посередині, пропонуючи кращу стійкість до помилок при середній глибині схеми. Підхід QPE (Quantum Phase Estimation) представляє повну квантову корекцію помилок, що теоретично дозволяє необмежену кількість логічних кубітів і високу глибину схеми, але має складність, що залежить від бажаної точності ε.

Проаналізуємо показникі якості квантових операцій (див. табл. 4).

Таблиця 4

Порівняння показників якості квантових операцій

Метрика	NISQ	EFTQC	FTQC
Точність двокубітного гейта	99 – 99.9 %	99.9 – 99.999 %	>99.9999 %
Кількісна формула для Quops	KiloQuops $\approx 10^3$	MegaQuops $\approx 10^6$ -GigaQuops $\approx 10^9$	TeraQuops $\approx 10^{12}$
Час когерентності відносно часу операції	$T_2 / T_{gate} \approx 10^2 - 10^3$	$T_2 / T_{gate} \approx 10^3 - 10^5$	$T_2 / T_{gate} > 10^5$

Аналіз показників якості квантових операцій демонструє радикальне зростання продуктивності та надійності квантових систем у процесі переходу від ери шумних проміжних квантових пристроїв (NISQ) до ери повноцінних відмовостійких квантових обчислень (FTQC). Ключовими метриками, що характеризують цю еволюцію, є точність двокубітних гейтів, обчислювальна потужність (Quops) та співвідношення між часом когерентності та часом виконання операції. Точність двокубітних гейтів, що є фундаментальним показником якості квантових операцій, зростає від 99 – 99.9 % у NISQ-пристроях до понад 99.9999 % у FTQC-системах. Це експоненційне підвищення точності є критичним фактором для реалізації складних квантових алгоритмів, оскільки навіть незначне покращення у точності гейтів призводить до суттєвого зменшення накопичених помилок під час виконання глибоких квантових схем. Обчислювальна потужність квантових систем, виражена в кількості квантових операцій за секунду (Quops), демонструє зростання на дев'ять порядків від KiloQuops (10^3) у NISQ-ері до TeraQuops (10^{12}) у FTQC-системах. Цей прогрес відображає не лише збільшення кількості кубітів, але й підвищення частоти операцій та впровадження паралельного виконання квантових гейтів, що в сукупності забезпечує безпрецедентне зростання обчислювальної потужності. Співвідношення між часом когерентності та часом виконання операції (T_2 / T_{gate}) зростає від 10^2 – 10^3 у NISQ-системах до понад 10^5 у FTQC-пристроях. Це відображає принципове покращення як технологій збереження квантової когерентності, так і методів швидкого та точного виконання квантових гейтів. Збільшення цього співвідношення означає, що квантові системи зможуть виконувати суттєво більше послідовних операцій до того, як декогеренція зруйнує квантовий стан, що є критичним для реалізації складних квантових алгоритмів з глибокими схемами.

Ці метрики колективно демонструють траєкторію розвитку квантових обчислень від експериментальних систем з обмеженими можливостями до повноцінних квантових комп'ютерів, здатних реалізувати практичні квантові алгоритми з обчислювальною потужністю, що значно перевищує можливості класичних систем. Проаналізуємо EFTQC та FTQC підходи як перспективні з огляду на рішення криптоаналітичних задач (див. табл. 5).

Таблиця 5

Порівняльний аналіз EFTQC та FTQC у вирішенні задач криптоаналізу

Характеристика	Традиційний FTQC підхід	EFTQC підхід	Математичне співвідношення
Кількість операцій на схему	Висока	Знижена в ≈ 100 разів	$O\ T_{FTQC} / 100$
Кількість запусків схеми	Низька	Збільшена в ≈ 10000 разів	$O\ R_{FTQC} \cdot 10^4$
Загальний час виконання	$T_{total} = T_{FTQC} \cdot R_{FTQC}$	$T_{total} = T_{EFTQC} \cdot R_{EFTQC}$	Збільшення в ≈ 100 разів
Розмір задачі (досяжність)	Обмежений кількістю кубітів	Розширений на $\approx 40 - 50\%$	Від ≈ 90 до ≈ 130 логічних кубітів

Порівняльний аналіз підходів EFTQC та FTQC має особливе значення в контексті криптоаналітичних задач, де квантові алгоритми потенційно демонструють експоненційне прискорення порівняно з класичними методами. Принципові відмінності цих підходів визначають різні траєкторії розвитку криптоаналітичних можливостей у квантову еру.

EFTQC підхід із характерним зниженням кількості операцій на схему $O\ T_{FTQC} / 100$ відкриває можливість для раннього впровадження модифікованих версій алгоритму Шора та алгоритму Гровера з обмеженою глибиною. Критичною особливістю такого підходу для криптоаналізу є компенсація обмеженої глибини схем через інтенсивне статистичне накопичення результатів $O\ R_{FTQC} \cdot 10^4$ запусків. Це дозволяє атакувати криптографічні системи з редукованою складністю, вибірково таргетуючи вразливі компоненти або використовуючи часткове знання про структуру криптографічного ключа.

Збільшення розміру задач на 40 – 50 % (від ~90 до ~130 логічних кубітів) у EFTQC підході є особливо значущим для криптоаналізу, оскільки уможливлює атаки на криптоси-

стеми з більшою довжиною ключа. Це дозволяє, наприклад, застосовувати квантові методи для факторизації RSA-модулів більшого розміру або для обчислення дискретних логарифмів у більших елліптичних кривих, навіть при обмеженій глибині схем. Такий підхід потенційно надає можливість проводити "доказові концепції" атак на криптосистеми, які вважаються безпечними в сучасних умовах.

Фундаментальна зміна парадигми в EFTQC ері для криптоаналізу полягає в переході від повномасштабних атак, які вимагають глибоких квантових схем високої точності, до гібридних класично-квантових атак з інтенсивним статистичним післяопрацюванням. Такі атаки можуть включати квантові підпрограми для вирішення специфічних, обчислювально складних підзадач, інтегровані в класичні криптоаналітичні frameworks. Збільшений загальний час виконання (приблизно в 100 разів) залишається прийнятним для криптоаналітичних застосувань, де час атаки не є критичним фактором порівняно з можливістю принципового зламу криптосистеми.

Пріоритезація кількості запусків схеми над її глибиною є особливо релевантною для таких криптоаналітичних алгоритмів, як квантовий варіант meet-in-the-middle атак та квантові версії диференціального та лінійного криптоаналізу, де статистичне накопичення результатів є невід'ємною частиною атаки. Цей підхід дозволяє розширити спектр криптоаналітичних методів, доступних на ранніх етапах квантових обчислень, стимулюючи розвиток постквантової криптографії та прискорюючи транзицію до криптографічних систем, стійких до квантових атак.

Висновок

Проведений аналіз математичних критеріїв різних епох розвитку квантових обчислень має наслідки для вирішення криптоаналітичних задач, трансформуючи розуміння часових рамок та методологічних підходів до подолання криптографічного захисту класичних криптосистем.

Еволюція параметра масштабованості α від $\alpha < 2$ у NISQ до $\alpha > 3.5$ у FTQC системах визначає фундаментальні обмеження для імплементації алгоритму Шора та інших криптоаналітичних алгоритмів, що вимагають низького рівня помилок. Перехід від рівня характеристики фізичної помилки $P_{error} > P_{th}$, характерної для NISQ, до рівня $P_{error} = P_{th}$ у FTQC є критичною точкою біфуркації для практичної реалізації повномасштабних квантових атак на асиметричні криптосистеми в недалекому майбутньому. Співвідношення між фізичними та логічними кубітами, що описується функцією $O\ d^2$, має вирішальне значення для криптоаналізу, оскільки визначає максимальний розмір криптографічних ключів, які можуть бути атаковані. Збільшення кількості доступних логічних кубітів від 10 – 100 у EFTQC до 100 – 10,000+ у FTQC в недалекому майбутньому відкриває можливість для атак на криптосистеми з ключами від 2048 до 4096 біт та більше, що охоплює значну частину сучасної криптографічної інфраструктури. Показники якості квантових операцій демонструють експоненційне покращення від NISQ до FTQC, що безпосередньо корелює з ефективністю криптоаналітичних алгоритмів. Зростання точності двокубітних гейтів від 99 –99.9 % до >99.9999 % критично важливе для реалізації квантового перебору в алгоритмі Гровера та для точного оцінювання фази в алгоритмі Шора. Збільшення обчислювальної потужності від KiloQuops до TeraQuops та співвідношення T_2 / T_{gate} від 10^2 – 10^3 до $>10^5$ визначає швидкість виконання криптоаналітичних операцій та максимальну глибину квантових схем, достатніх для факторизації чи обчислення дискретних логарифмів. EFTQC-підхід пропонує революційний компроміс для квантового криптоаналізу: зниження кількості операцій на схему в ~100 разів при збільшенні кількості запусків у ~10,000 разів уможливлює реалізацію модифікованих версій алгоритму Шора та Гровера, оптимізованих для роботи з обмеженою глибиною схеми. Це дозволяє атакувати криптосистеми більшого розміру (на 40 – 50 % більше логічних кубітів) значно раніше, ніж передбачалося в традиційних моделях квантового криптоаналізу, хоча й з пропорційно більшими часовими

витратами. Еволюція від VQE та QAOA алгоритмів через робастні EFTQC-алгоритми до повноцінних FTQC-алгоритмів трансформує методологію квантового криптоаналізу. В NISQ-ері можливі лише гібридні атаки з обмеженою квантовою складовою; EFTQC-ера відкриває шлях до робастних квантових атак зі складністю O(K), які, хоча й не є оптимальними, але вже становлять реальну загрозу для окремих криптосистем; і, нарешті, FTQC-ера уможливлює повномасштабні квантові атаки зі складністю $O\ 1/\varepsilon$, що повністю компрометують уразливі криптографічні примітиви.

Запропонована модель переходу від NISQ до FTQC із чіткими математичними критеріями дозволяє більш точно прогнозувати часові рамки виникнення квантової загрози для різних криптографічних систем. Особливо важливим є висновок щодо прискореної досяжності квантових атак в EFTQC-ері, що скорочує очікуваний час до компрометації сучасних асиметричних криптосистем. Ці результати підкреслюють нагальну необхідність активної міграції до постквантових криптографічних рішень, спроможних протистояти як повноцінним FTQC-атакам, так і модифікованим EFTQC-атакам, які можуть стати реальністю значно раніше, ніж передбачалося у традиційних моделях квантової загрози.

Список літератури

1. Arute F., Arya K., Babbush R., Bacon D., Bardin J. C., Barends R., Biswas R., Boixo S., Brandao F. G. S. L., Buell D. A., Burkett B., Chen Y., Chen Z., Chiaro B., Collins R., Courtney W., Dunsworth A., Farhi E., Foxen B., ... Martinis J. M. Quantum supremacy using a programmable superconducting processor // Nature. 2019. Vol. 574(7779). P. 505–510. https://doi.org/10.1038/s41586-019-1666-5
2. Kandala A., Mezzacapo A., Temme K., Takita M., Brink M., Chow J. M., Gambetta J. M. Hardware-efficient variational quantum eigensolver for small molecules and quantum magnets // Nature. 2017. Vol. 549(7671). P. 242–246. https://doi.org/10.1038/nature23879
3. Kotukh E., Severinov O., Vlasov A., Tenytska A., Zarudna E. Some results of development of cryptographic transformation schemes using non-abelian groups // Radiotekhnika. 2021. No 204. P. 66–72. https://doi.org/10.30837/rt.2021.1.204.07
4. Khalimov G., Kotukh Y., Sergiychuk Y., Marukhnenko A. Analysis of the implementation complexity of the cryptosystem on the Suzuki group // Radiotekhnika. 2018. No 193. P. 75–81. https://doi.org/10.30837/rt.2018.2.193.08
5. Kotukh Y., & Khalimov G. Hard problems for non-abelian cryptography // 2021: Fifth International Scientific and Technical Conference "computer and information systems and technologies" https://doi.org/10.30837/csitic52021232176
6. Kotukh Y., Khalimov G. Towards practical cryptoanalysis of systems based on word problems and logarithmic signatures // Information security: problems and prospects. https://shorturl.at/IaByX
7. Shor P. W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer // SIAM Journal on Computing. 1997. No 26(5). P. 1484–1509. https://epubs.siam.org/doi/10.1137/S0097539795293172
8. Gidney C., & Ekerå M. How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits. Quantum. 2021. No 5. 433 p. https://doi.org/10.22331/q-2021-04-15-433
9. Kotukh Y., Khalimov G. Advantages of logarithmic signatures in the implementation of crypto primitives // Challenges and Issues of Modern Science. https://cims.fti.dp.ua/j/article/download/119/158
10. Kotukh Y. Quantum cryptoanalysis of prospective asymmetric cryptosystems // Proceedings of conference “Cybersecurity in energy sector”. https://shorturl.at/1pbcK
11. Preskill J. Quantum Computing in the NISQ era and beyond // Quantum. 2018. No 2. P. 79. https://doi.org/10.22331/q-2018-08-06-79

Надійшла до редколегії 05.02.2025

Відомості про авторів:

Котух Євген Володимирович – канд. техн. наук, доцент, професор кафедри кібербезпеки; Національний технічний університет «Дніпровська політехніка»; Дніпро, Україна; e-mail: yevgenkotukh@gmail.com; ORCID: https://orcid.org/0000-0003-4997-620X

Халімов Геннадій Зайдулович – д-р техн. наук, професор, завідувач кафедри безпеки інформаційних технологій; Харківський національний університет радіоелектроніки; Харків, Україна; e-mail: hennadii.khalimov@nure.ua; ORCID: https://orcid.org/0000-0002-2054-9186

Коробчинський Максим Володимирович – д-р техн. наук, професор, начальник другої кафедри Другого Навчально-наукового інституту Воєнної Академії імені Євгена Березняка; Київ, Україна; e-mail: maks_kor@ukr.net; ORCID: https://orcid.org/0000-0001-8049-4730

Джура Ілля Євгенович – студент 4-го курсу, Національний Авіаційний Університет; Київ, Україна; e-mail: illya773823@gmail.com; ORCID: https://orcid.org/0009-0002-5470-4479

УДК 004.932 **DOI:10.30837/rt.2025.1.220.09**

І.Ш. НЕВЛЮДОВ, д-р техн. наук, О.М. ЛІСТРАТЕНКО, канд. техн. наук, І.В. БОРЩОВ

АВТОМАТИЗОВАНА ІНФОРМАЦІЙНО-ВИМІРЮВАЛЬНА СИСТЕМА ОПТИЧНОГО КОНТРОЛЮ ГНУЧКИХ НАДТОНКИХ МІКРОКАБЕЛІВ

Вступ

Сьогодні важко уявити подальший розвиток багатьох галузей промисловості без розвитку досягнення найбільшої точності при вимірюваннях, меншої кількості помилок при контролі та підвищенні ймовірності виявлення критичних дефектів при виробництві. Таким чином, підвищення ефективності в умовах промислової революції Індустрії 4.0 насамперед пов’язане з автоматизацією технологічних процесів, які використовуються на сучасному етапі промислового розвитку [1]. Сучасні високотехнологічні електронні засоби (ЕЗ) створюються на основі друкованого монтажу, коли згідно з існуючими прогнозами у подальші роки очікується збільшення використання гнучких друкованих плат (ДП) для різноманітного використання [2]. Максимально високі вимоги щодо надійності вимагають ЕЗ спеціального призначення, в тому числі сенсорні модулі для приймачів електромагнітних випромінювань, а саме рентгенівського і гамма-випромінювання, концентрованого сонячного випромінювання та ін. Це відноситься також до багатосенсорних матричних приймачів, які мають жорсткі вимоги до точності їх встановлення на друковані плати. Останні інновації в галузі кремнієвих технологій візуалізації подій в експериментах фізики високих енергій відкрили виняткові можливості для нових концепцій детекторних систем, у тому числі можливість використання інтеграції кремнієвих піксельних сенсорів, електроніки зчитування та обробки інформації для створення єдиного чутливого кремнієвого елемента. Такий підхід був прийнятий та успішно реалізований при створенні монолітних активних піксельних сенсорів (MAPS) ALPIDE 4 для вирішення одного з основних завдань сучасної фізики високих енергій, яка полягає у вивченні фазової діаграми стану сильно взаємодіючої матерії. Зокрема MAPS піксельні сенсори ALPIDE 4 також успішно застосовуються у детекторних системах нового покоління для дослідження частинок високих енергій на основі гнучких тонких безадгезивних алюміній-поліімідних (Al-Pi) міжз'єднань (мікрокабелів) зі значно зниженою матеріаломісткістю та підвищеною роздільною здатністю [3].

Оптичні методи контролю гнучких Al-Pi мікрокабелів з надтонкими алюмінієвими (Al) провідниками (15 – 30 мкм), що застосовуються для перевірки якості мікрокабелів, дозволяють забезпечити відповідність продукції встановленим вимогам ще до її надходження у виробництво. Оптичний метод дослідження мікрокабелів ґрунтується на таких явищах, як відображення, поглинання, інтерференція та дифракція світла. При виготовленні фотошаблонів та мікрокабелів застосовуються різні матеріали, які по-різному взаємодіють із оптичним випромінюванням. Вони знайшли широке застосування під час виробництва мікрокабелів спеціального призначення для виявлення таких дефектів як раковини, тріщини, вириви на тонких провідниках і навіть неточностей розміщення контактних майданчиків і провідників; зміни ширини провідників; підтравлювання та нависання провідників; дефекти металізації та ін. Однак оптичний контроль за допомогою оператора має ряд недоліків – суб'єктивність і низька достовірність, а також низька продуктивність для складних виробів з надтонкою топологією, що може призвести до пропуску критичних дефектів. Метод автоматичного оптичного контролю (автоматична перевірка зовнішнього вигляду) всебічно використовує технологію аналізу зображення та автоматичного управління процесом виявлення дефектів, що виникають у виробництві різноманітних гнучких друкованих плат та друкованих вузлів. Таким чином, можливості автоматизованих систем для оптичного контролю мікрокабелів спеціального призначення з надтонкою топологією дозволяють здійснювати більш якісний контроль на всіх етапах виробництва компонентів і складання друкованих виробів з виключенням грубих помилок, які допускаються під час ручного візуального контролю [4, 5].

Метою даної роботи є створення інформаційно-вимірювальної системи (ІВС) автоматизованого оптичного контролю для розширення її функціональних можливостей за рахунок комплексної автоматизації отримання та обробки інформації при виявленні критичних поверхневих дефектів, що впливають на якість і надійність надтонких гнучких Al-Pi мікрокабелів та перевірки відповідності провідних малюнків розроблених мікрокабелів вимогам конструкторської документації.

1. Предмет та методи дослідження

1.1. Завдання роботи

1) Проведення аналізу видів критичних та малозначних дефектів Al-Pi гнучких ДП та ДВ на їх основі та розроблення їх систематизації.

2) Проведення аналізу методів виявлення дефектів та отримання і обробка інформації, що реалізують ці методи.

3) Розробка структурної схеми ІВС для оптичного контролю гнучких надтонких мікрокабелів для гнучко-жорстких сенсорних модулів та друкованих виробів (ДВ) для цифрових трекових калориметрів у протонних комп'ютерних томографах.

4) Розробка програмного забезпечення для автоматизації контрольно-перевірочних операцій гнучких надтонких мікрокабелів на основі стандартних методів програмування.

5) Технічне забезпечення та оснащення робочого місця для автоматизованого оптичного контролю гнучких надтонких мікрокабелів.

1.2. Методи дослідження

Методи дослідження в рамках даної роботи базуються на використанні теорії інформаційно-вимірювальних систем, обробки зображень, а також принципів системного аналізу. Для автоматизації процесів контролю використовуються стандартне програмне забезпечення, розроблене із застосуванням сучасних методів програмування, а також спеціалізовані алгоритми для аналізу топології провідників та ідентифікації дефектів. Апаратне забезпечення базується на методах схемотехніки для забезпечення точності й надійності оптичного контролю.

1.3. Критерії виявлення дефектів при оптичному контролі друкованих мікрокабелів

Основним стандартом за вимогами до дефектів ДП є IPC-A-600H "Acceptability of Printed Boards", в якому описано прийнятні (і неприйнятні) дефекти для різних класів точності та критеріїв при прийманні мікрокабелів. У стандарті IPC-A-600H виділено критерії приймання друкованих мікрокабелів за зовнішніми ознаками – ознаками дефектів, які можна спостерігати та вимірювати з поверхні мікрокабелю. До характеристик критеріїв надтонких гнучких мікрокабелів за зовнішніми ознаками, контрольованих на поверхні відносять:

- дефекти поверхні – задирки, вибоїни, подряпини, виїмки, забруднення, частинки, що налипли, та інші;
- дефекти під поверхнею – включення сторонніх матеріалів, розшарування, порожнечі у ламінаті тощо;
- дефекти провідного малюнка – втрата адгезії, зменшення ширини чи товщини провідника через вибоїни, мікроотвори, подряпини, дефекти металізації чи захисного покриття поверхні. Характеристики отворів – діаметр, помилка усунення, сторонній матеріал та дефекти металізації чи захисного покриття;
- дефекти маркування – положення, розмір та точність;
- розмірні характеристики – розміри та товщина мікрокабелів, розміри отворів та точність їх розташування, ширина та відстань між провідниками, точність положення монтажних площин.

Поділ дефектів за значимістю на критичні, значні та малозначні має велике значення при обґрунтуванні планів при проведенні оптичного контролю мікрокабелів. Критичним називається дефект, за наявності якого використання виробу за призначенням є практично неприпустимим. Значний дефект – це дефект, який суттєво впливає на використання виробу за призначенням та (або) на його довговічність, але він не є критичним. Малозначним називається дефект, який суттєво не впливає на використання виробу за призначенням та його довговічність.

При оптичному контролі гнучки надтонки мікрокабелі повинні проходити 100 %-ну перевірку зовнішнього вигляду на відповідність конструкторській документації, перевірку на відсутність видимих забруднень поверхні мікрокабелів та пошкоджень елементів топології у провідних малюнках та відсутність налиплих частинок.

На гнучких мікрокабелях не допускаються:

- забруднення, які не знімаються пензликом;
- відсутність маркування;
- відшарування алюмінієвих Al елементів від поліімідної (Pi) плівки, які визначаються візуально по задирці країв алюмінієвих елементів;
- розрив Al провідників та закоротки між ними;
- наявність залишків Pi плівки на Al провідниках у вікнах в Pi плівці;
- наскрізні протрави в Al провідниках у зонах зварювання;
- деформація мікрокабелів, що призводить до заломів;
- деформація Al провідників у зонах зварювання.

На гнучких мікрокабелях допускаються:

- локальні подряпини, вириви і раковини в Al провідниках як наскрізні до Pi шару, так і не наскрізні поза зоною зварювання, якщо частина Al провідника, що залишилася, не менше 0,5 його ширини;
- локальне зменшення ширини зазору між сусідніми провідниками Al не більше 0,5 ширини зазору;
- раковини у Pi діелектрику з розмірами не більше 200 мкм на 1см^2 при кількості не більше 2 шт.;
- протрави в Pi діелектрику з розмірами не більше ширини Al провідника;
- розрив сусідніх перемичок у перфорації при кількості не більше 4 шт.

1.4. Критичні дефекти та пошкодження при зовнішньому огляді та контролі мікрокабелів на відповідність конструкторській документації

1) Забруднення, які не знімаються пензликом.
2) Наскрізні протрави Al провідників у зонах зварювання.
3) Наявність розривів Al провідників та закороток у провідному малюнку мікрокабелю.
4) Відшаровування Al провідників від Pi покриття.
5) Залишки Pi у зоні зварювання.
6) Деформація мікрокабелів, що призводить до зламів.
7) Деформація Al провідників у зонах зварювання.
8) Відсутність маркування.
9) Відстань між знаками суміщення по осі X, мм.
10) Відстань між знаками суміщення по осі Y, мм.
11) Ширина перфорації, що відокремлює технологічні області, мм.
12) Ширина Al провідників у зонах зварювання, мм.
13) Розміри вікон у Pi шарах у зонах зварювання, мм.
14) Відстань між Al провідниками у верхніх частинах зон зварювання, мм.
15) Відстань між Al провідниками у нижніх частинах зон зварювання, мм.

2. Розробка структурної схеми та програмного забезпечення ІВС оптичного контролю гнучких Al-Pi надтонких мікрокабелів

2.1. Структурна схема автоматизованої ІВС

До складу ІВС для автоматизованого оптичного контролю гнучких мікрокабелів входять: оптична система, система освітлення, система фіксації та позиціонування а також програмне забезпечення. За допомогою цифрової відеокамери здійснюється оптичний огляд мікрокабелів, а також здійснюється перевірка наявності сторонніх включень до них. Система побудована на основі цифрової відеокамери з матриці на приладах з зарядовим зв'язком (CCD – charge-coupled devices). Кольорове зображення з високою роздільною здатністю виводиться на монітор персонального комп'ютеру. Область захоплення зображення та програмне забезпечення, що застосовується, дозволяють здійснювати огляд, створювати базу даних зображень і проводити вимірювання геометричних параметрів елементів мікрокабелів.

Розроблена укрупнена блок-схема алгоритму виявлення та класифікації критичних дефектів і пошкоджень при загальному зовнішньому огляді мікрокабелів представлена на рис. 1.

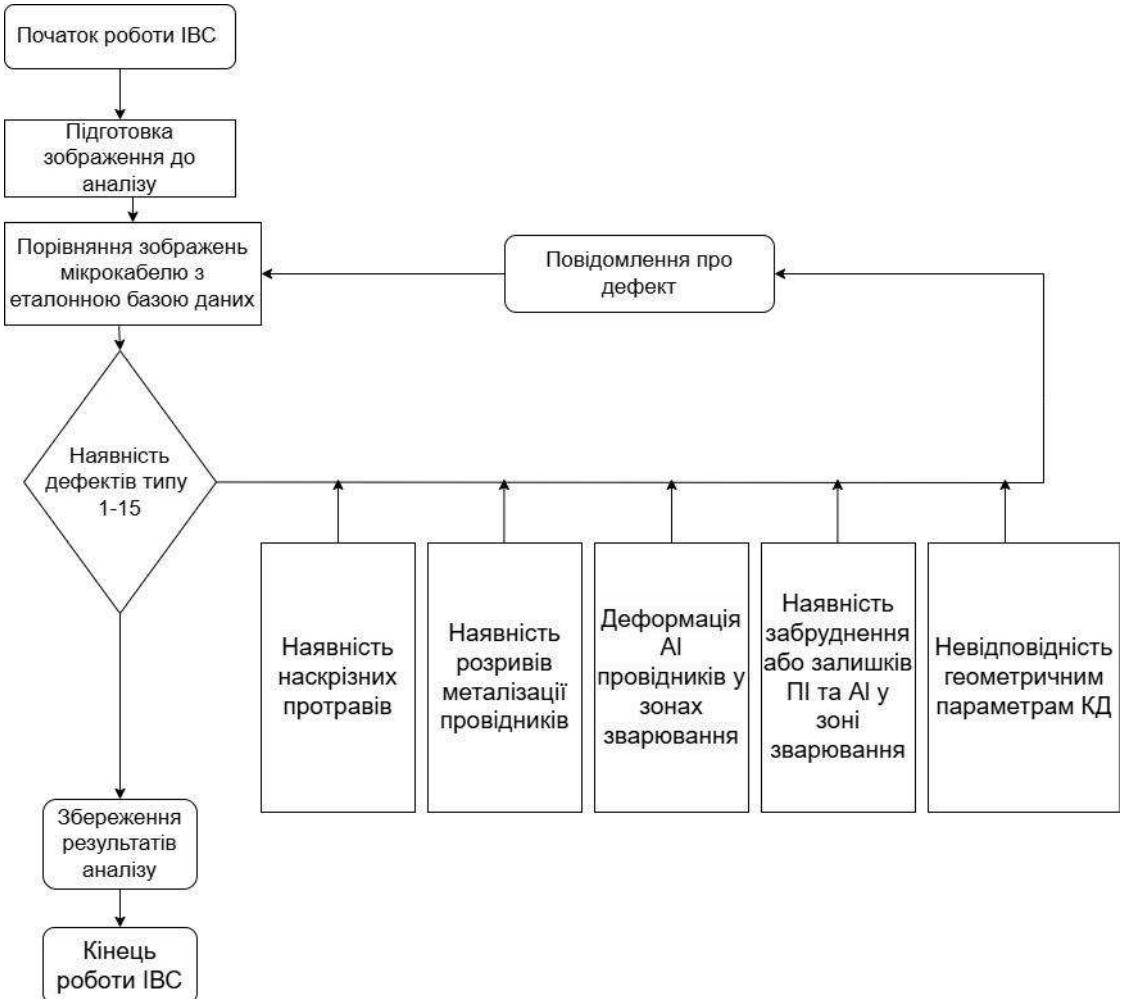


Рис. 1. Блок-схема алгоритму виявлення та класифікації дефектів

2.2. Програмне забезпечення автоматизованої ІВС

Програмне забезпечення ІВС на основі середовища MATLAB поєднує високорівневу технічну обчислювальну мову та інтерактивне середовище для автоматизованного детектування поверхневих дефектів гнучких мікрокабелів, що може використовуватися на виробнц-

тві. Дана система надає користувачеві багатофункціональне та ефективне середовище цифрової обробки двовимірних зображень Image Processing Toolbox як сукупність функцій, написаних мовою MATLAB, для вирішення широкого кола завдань цифрової обробки зображень, що значно розширює базову функціональність середовища програмування. У середовищі MATLAB розробляються алгоритми для автоматизованого аналізу зображень гнучких Al-Pi мікрокабелів для виявлення ключових критеріїв дефектів і параметрів. Алгоритми передобробки відповідають за покращення якості зображень, видалення шуму та підготовку до подальшого аналізу. Сегментація об'єктів виділяє зони інтересу, такі як провідники та зварювальні області, для детального дослідження. Алгоритми вимірювання геометричних параметрів забезпечують автоматичне визначення відстаней, розмірів вікон та ширини провідників з подальшою перевіркою на відповідність технічної документації. Для виявлення дефектів застосовуються методи аналізу провідного малюнка, що дозволяє виявляти розриви, наскрізні протрави, забруднення та деформації. Також реалізуються алгоритми класифікації дефектів за їх значимістю та автоматизована система формування звітів, де фіксується результати контролю та місцезнаходження виявлених дефектів.

3. Технічне забезпечення та оснащення робочого місця для автоматизованої ІВС

У табл. 1 представлено перелік типів пристроїв, які включені до складу ІВС.

Таблиця 1

Перелік та типи пристроїв для ІВС

Найменування	**Тип**
Цифрова кольорова ПЗЗ відеокамера для отримання зображення	AmScope MU1403
Світлодіодний освітлювач	TY-60
Мікроскоп	Konus Crystal
Система фіксації та позиціонування мікрокабелю	Пластикова рамка TAB-70022
Ноутбук	Lenovo IdeaPad 520-15 Ikb

3.1. Основні характеристики пристроїв, які включені до складу ІВС

Вимірювальний мікроскоп Konus Crystal. Сучасний модульний вимірювальний мікроскоп відбитого світла з тринокулярною насадкою складається з високоякісних компонентів та надійного і міцного штатива. Мікроскоп поставляється з освітлювачем падаючого світла з тринокулярною насадкою для підключення цифрової кольорової відеокамери. Мікроскоп призначений для проведення візуального контролю та вимірювання дрібних об'єктів та має серійний вихід для передачі даних статистичного контролю технологічного процесу на комп'ютері.

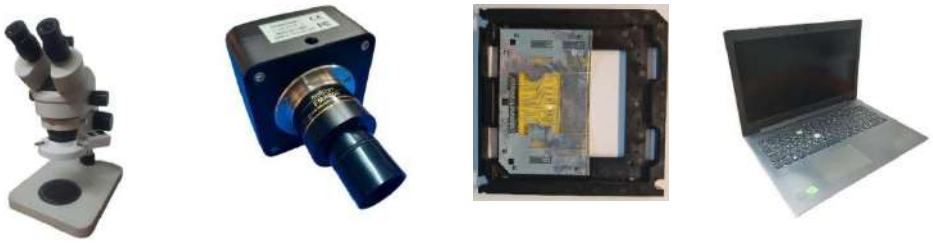
Відеокамера для отримання зображення AmScope MU1403. Для вибору камери проведено аналіз існуючих моделей відеокамер за основними характеристиками, що забезпечують точність і зручність контролю: роздільна здатність не гірша за 1920 х 1080, розміри не більше 75 х 45 мм, маса не більше 500 г. У цифровій камері AmScope MU1403 забезпечується необхідна якість зображення, також вона має прийнятні габаритні розміри і вагу, що визначає можливість її встановлення в блоці переміщення.

Світлодіодний освітлювач TY-60. Ефективне висвітлення має вирішальне значення для оптичного контролю. Різні системи освітлення (наприклад, світлодіодні матриці) використовуються для освітлення гнучкого мікрокабелю, покращуючи видимість потенційних дефектів. Швидкість обробки зображення менше 10 мс.

Составна пластикова рамка TAB-70022 для фіксації та позиціонування гнучкого мікрокабелю. Пластикова рамка TAB-70022 забезпечує механічну стійкість та стабільність положення мікрокабелю у площині.

Фіксація та позиціювання гнучких Al-Pi мікрокабелів при оптичному контролі здійснюється достатньо просто за допомогою пластикової рамки TAB-70022. Пластикова рамка TAB-70022 від адаптера socket IC51-4364-1221-1 забезпечує механічну стійкість та стабільність положення мікрокабелю у площині. Составна пластикова рамка TAB-70022 для фіксації та позиціювання гнучкого мікрокабелю має розміри вікна у рамці 52 х 52 мм. У рамку встановлюється гнучкий Al-Pi мікрокабель з розмірами не більше 70 х 70 мм.

На рис. 2 представлено основні пристрої для оснащення робочого місця з ІВС для автоматизованого оптичного контролю гнучких Al-Pi надтонких мікрокабелів.



а *б* *в* *г*

Рис. 2. Основні пристрої для оснащення робочого місця: *а* – мікроскоп Konus Crystal з світлодіодним освітлювачем TY-60; *б* – відеокамера AmScope MU1403; *в* – составна рамка TAB-70022 у зборі з мікрокабелем; *г* – ноутбук Lenovo IdeaPad 520-15 Ikb

Процес встановлення гнучкого надтонкого Al-Pi мікрокабелю у составну рамку показано на рис. 3.

а *б* *в*

Рис. 3. Процес встановлення гнучкого надтонкого Al-Pi мікрокабелю у составну рамку TAB-70022 для фіксації та позиціювання: *а* – нижня рамка-основа; *б* – верхня рамка для кріплення мікрокабелю; *в* – составна рамка TAB-70022 у зборі з мікрокабелем

4. Результати та їх обговорення

У роботі створено ІВС автоматизованого оптичного контролю, що може використовуватися на виробництві для розширення функціональних можливостей за рахунок комплексної автоматизації отримання та обробки інформації при виявленні критичних дефектів, що впливають на якість і надійність гнучких Al-Pi надтонких мікрокабелів та перевірки відповідності їх вимог до конструкторської документації, що надходять до складально-монтажних операцій.

ІВС має широкий набір функцій та характеристик, які дозволяють ефективно виявляти різноманітні дефекти при забезпеченні якості та надійності виготовлення мікрокабелів.

У тому числі:

- висока роздільна здатність, що дозволяє точно визначати розміри та положення дефектів на гнучких мікрокабелях;
- спеціалізоване програмное забезпечення, яке забезпечує автоматичний процес виявлення дефектів;
- висока швидкодія виявлення дефектів;
- надійність та точність виявлення дефектів, що дозволяє впевнено встановлювати якість мікрокабелів та уникати дефектних екземплярів.

Програмне забезпечення ІВС виявлення дефектів гнучкого Al-Pi мікрокабелю реалізовано у вигляді виконуваного файлу, який призначений для запуску на комп'ютері зі встановленою ОС Windows 10 і вище та за наявності необхідних зовнішніх бібліотек. Процес автоматизованого оптичного контролю гнучкого Al-Pi надтонкого мікрокабелю починається з ініціалізації ІВС та підготовки її до аналізу. Після запуску система формує зображення мікрокабелю, яке потім проходить попередню обробку для покращення якості зображення поверхні та підготовки його до детального аналізу. На наступному етапі система порівнює отримане зображення з еталонними даними бази, щоб виявити відхилення від норми. У процесі оптичного контролю перевіряється наявність критичних дефектів та пошкоджень у мікрокабелі при зовнішньому огляді поверхні, а також забруднень, які не знімаються пензликом. Додатково система контролює відповідність геометричних розмірів вимогам конструкторської документації. При виявленні будь-якого критичного дефекту система формує повідомлення, фіксуючи інформацію про характер і місцезнаходження дефекту (проблеми). Отримана інформація зберігається для формування звітів та для подальшого аналізу.

Робоче місце для оптичного контролю параметрів надтонких Al-Pi мікрокабелів наведено на рис. 4.

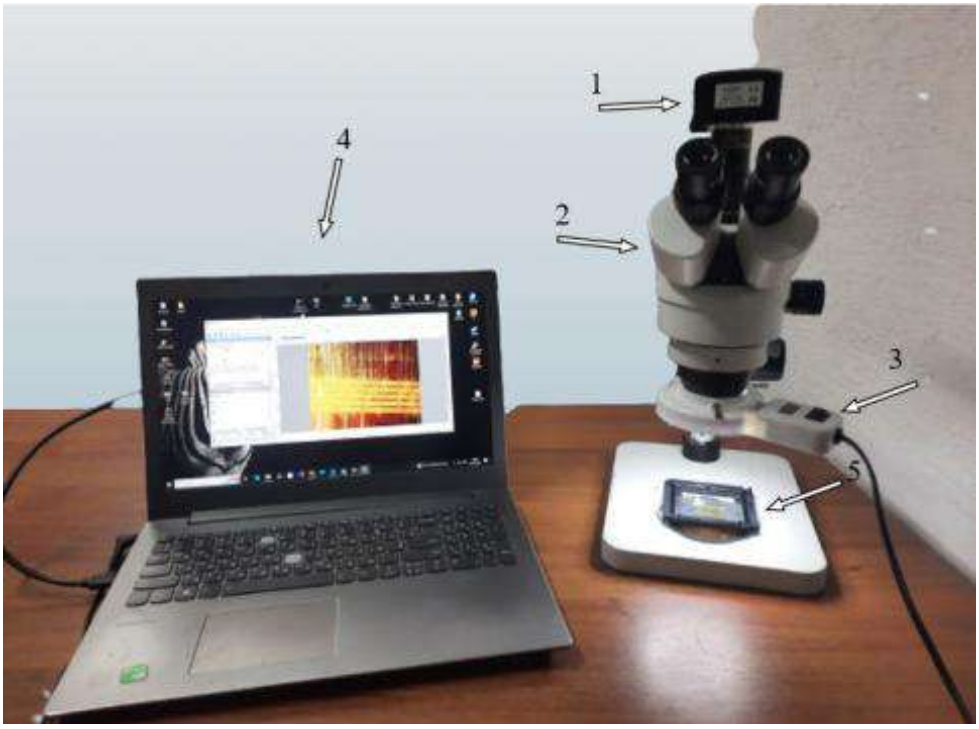


Рис. 4. Робоче місце для автоматизованого оптичного контролю мікрокабелів:
1 – цифрова кольорова відеокамера для отримання зображення(AmScope MU1403); 2 – Мікроскоп (Konus Crystal); 3 – світлодіодний освітлювач(TY-60); 4 – ноутбук(Lenovo IdeaPad 520-15 Ikb); 5 – мікрокабель у рамці (Пластикова рамка TAB-70022)

Надтонкі мікрокабелі розроблені та виготовлені на основі нового типу безадгезивного Al-Pi лакофольгового діелектрику власного виробництва марки ЛТУ-ФПА15-10

(Al – 15 мкм, Pi – 10 мкм) компанії ТОВ «НВП «ЛТУ» для тестування ІВС. Тестування ІВС виконано при оптичному контролі партії надтонких мікрокабелів, кожний з яких має 128 тонких Al ланцюгів з шириною порядку 60 – 95 мкм, кроком 200 мкм та відстанню між Al провідниками близько 140 – 105 мкм. У тому числі:

- відстань між знаками суміщення по осі X, 64,06±0,030 мм;
- відстань між знаками суміщення по осі Y, 30,03±0,015 мм;
- розміри вікна у ПІ (Зона II), 0,15±0,015 мм;
- розміри вікна у ПІ (Зона III), (0,25x0,4)±0,02 мм;
- розмір вікна у ПІ (Зона V), (0,25x0,4) ±0,02 мм;
- відстань між Al провідниками у верхній частині зони, 17,6±0,01 мм;.
- відстань між Al провідниками в нижній частині зони, 25,96±0,01 мм.

ІВС забезпечує виконання основних вимог до перевірки геометричних розмірів високотехнологічних гнучких надтонких Al-Pi мікрокабелів на відповідність конструкторській документації та отримання і обробки інформації при виявленні критичних поверхневих дефектів, що впливають на якість і надійність надтонких гнучких Al-Pi мікрокабелів MAPS піксельних сенсорів детекторних модулів нового покоління зі значно зниженою матеріаломісткістю та підвищеною роздільною здатністю для частинок високих енергій, що досліджуються у детекторних системах нового покоління для досліджень у фізиці високих енергій.

Проте, для ще більшого поліпшення якості автоматизованої системи оптичного контролю гнучких Al-Pi мікрокабелів, яка була розроблена та протестована для виробництва, перспективним напрямком є включення до складу ІВС глибоких нейронних мереж. Наприклад, у роботі [6] успішно використана нейронна мережа YOLOv5 – одна з найпотужніших та найефективніших глибоких нейронних мереж для оптичного огляду об'єктів, яка поєднує високу швидкість та точність роботи. Серед доступних рішень модель YOLOv5 виявилася оптимальною, оскільки забезпечує високу швидкість і точність аналізу, що критично важливо для контролю дефектів ДП у виробничих умовах. Завдяки своїй ефективності YOLOv5 дозволяє виконувати аналіз зображень у реальному часі, виявляючи та класифікуючи дефекти із мінімальними затримками.

YOLO (You Only Look Once) – це серія моделей глибокого навчання, призначених для швидкого та точного виявлення об'єктів на зображеннях. Основна ідея моделей YOLO полягала в тому, щоб замість традиційних підходів, які розбивають процес на кілька етапів (спочатку пошук об'єкта, а потім його класифікація), виконується вся обробка за один прохід через нейронну мережу. Це зробило YOLO однією з найшвидших архітектур для детекції об'єктів у ДП. YOLO знайшла широке застосування у різних сферах, включаючи автоматизовані системи відео спостереження, безпілотні транспортні засоби, медичну діагностику, контроль виробничих дефектів та аналіз супутникових зображень.

Впровадження цього підходу дозволяє значно підвищити точність і швидкість виявлення дефектів, автоматизувати класифікацію різних типів пошкоджень та мінімізувати кількість хибних спрацьовувань. Однією з ключових переваг YOLOv5 є її здатність до роботи в режимі реального часу, що особливо важливо для промислових процесів, де необхідний швидкий і точний аналіз кожного контрольованого зразка. Дана модель дозволяє не лише детектувати наявність дефектів, а й класифікувати їх на основі навчальних вибірок, що включають різні типи механічних пошкоджень, забруднень, порушень геометрії тощо. Впровадження YOLOv5 у систему контролю дасть можливість адаптувати її до нових видів дефектів шляхом до навчання моделі на актуальних даних, що підвищить її ефективність при зміні технологічних параметрів виробництва. Технологічна реалізація цього підходу базується на використанні OpenCV для попередньої обробки зображень, що включає фільтрацію шумів, корекцію контрастності та підсилення видимості дефектів перед передачею в нейромережу. Використання платформи PyTorch забезпечить ефективне навчання та виконання моделі YOLOv5, а при застосуванні апаратного прискорення на базі CUDA або TensorRT можна значно підвищити швидкодію системи. Це дозволить інтегрувати рішення в реальні вироб-

ничі умови, де критичними параметрами є швидкість аналізу та надійність контролю. Принцип роботи вдосконаленої системи передбачає кілька основних етапів. На першому етапі здійснюється автоматизований збір зображень мікрокабелів у процесі контролю, після чого вони проходять попередню обробку для покращення якості аналізу. Далі підготовлені зображення передаються в модель YOLOv5, яка виконує детекцію дефектів і класифікує їх відповідно до типів. Отримані результати порівнюються з еталонними зображеннями, що дозволяє виявляти навіть незначні відхилення від норми та корелювати виявлені дефекти з відповідною конструкторською документацією. Після завершення аналізу формується автоматизований звіт, який містить інформацію про типи виявлених дефектів, рівень браку та можливі причини їх виникнення. Очікувані результати впровадження YOLOv5 включають значне скорочення часу аналізу зображень, що підвищить продуктивність контролю без зниження його якості. Гнучкість та адаптивність моделі дозволить автоматично підлаштовувати систему до змін у виробничому процесі, а глибоке навчання на нових даних сприятиме підвищенню точності детекції навіть складних та нетипових дефектів. Важливим аспектом є й підвищення загальної ефективності оптичного контролю, що забезпечить зменшення відсотка браку та покращення якості виготовлених мікрокабелів. Попередні обчислення показали, що після впровадження цієї технології час на контроль однієї плати скорочується до 0,1 с, якщо використовувати потужні прискорювачі обчислень – блоки обробки тензорів (TPU) та графічні процесори (GPU) [6, 7].

Висновки

Виконано аналіз видів критичних та малозначних дефектів гнучких Al-Pi мікрокабелів та розроблено їх систематизацію. Проведено детальне дослідження методів виявлення дефектів, отримання та обробки інформації, що дозволило вибрати оптимальні підходи для автоматизованого оптичного контролю. Розроблено структурну схему ІВС оптичного контролю, яка забезпечує ефективне виявлення дефектів у гнучких надтонких мікрокабелів, що застосовуються у сенсорних модулях та цифрових трекових детекторних калориметрів. Виконано технічне забезпечення та оснащення робочого місця ІВС, що включає сучасні засоби оптичного аналізу та комп'ютерної обробки даних.

Створено ІВС автоматизованого оптичного контролю, що може використовуватися на виробництві і має широкий набір функцій та характеристик, які дозволяють ефективно виявляти різноманітні поверхневі дефекти при забезпеченні високої якості та надійності гнучких надтонких Al-Pi мікрокабелів.

Проаналізовано сучасні методи покращення точності та швидкості оптичного контролю системи, що була розроблена та протестована, що дозволило визначити перспективні напрямки подальшого вдосконалення системи.

Зокрема, досліджено можливість впровадження у ІВС, сучасної нейронної мережі YOLOv5, яка дозволяє значно підвищити ефективність аналізу, скоротити час обробки зображень та ще більше автоматизувати процес класифікації дефектів. Впровадження YOLOv5 забезпечує швидке виявлення найдрібніших дефектів у реальному часі та адаптацію системи до дослідження та перевірки нових типів дефектів завдяки можливості до навчання моделі. Розробка та навчання нейронної мережі та впровадження елементів штучного інтелекту до складу ІВС оптичного контролю гнучких Al-Pi надтонких мікрокабелів дозволяють надійно поєднати автоматизацію, високу швидкість та точність роботи розробленої системи оптичного контролю у промисловому виробництві.

Список літератури:

1. Сторожик Д.В. Технології опрацювання зображень на основі комплексування даних : огляд / Д. В. Сторожик, А. Г. Протасов // Технічна діагностика та неруйнівний контроль. 2022. № 4. С. 17–26.

2. Романов В. Перспективи розвитку друкованих плат // Електронні компоненти і системи. 2024. № 1. С. 40–42.

3. Innovative microelectronic technologies for high-energy physics experiments / V. M. Borshchov, O. M. Listratenko, M. A. Protsenko, I.T. Tymchuk I. et al. // Functional materials. 2017. Vol. 24, № 1. P. 143–153. (включено до міжнародної науково-метричної бази даних Scopus).

4. Sharma A, Garg S. Automated Optical Inspection Systems for Defect Detection on Printed Circuit Boards Garg // The international journal of Advanced Manufacturing Technology. 2016. P. 32–37.

5. Khan M., Khan K., Anwar N. Automated Visual Inspection for Quality Control of Printed Circuit Boards // Annual technical Symposium. 2022. P. 9–19.

6. Крецул В.В. Прилад для автоматизованого контролю друкованих плат : дипломна робота бакалавра. 2023. 85с.

7. Qin, L. Printed Circuit Board Defect Detection Methods Based on Image Processing, Machine Learning and Deep Learning // Survey. 2021. P. 449–458

Надійшла до редколегії 07.01.2025

Відомості про авторів:

Невлюдов Ігор Шакирович - д-р техн. наук, професор, Харківський національний університет радіоелектроніки, завідувач кафедри комп'ютерно-інтегрованих технологій, автоматизації та робототехніки; Україна; e-mail: igor.nevliudov@nure.ua; ORCID**:**https://orcid.org/0000-0002-9837-2309

Лістратенко Олександр Михайлович – канд. техн. наук, ТОВ «Науково-виробниче підприємство «ЛТУ», провідний науковий співробітник; Україна; e-mail: sasha.listratenko.12@gmail.com; ORCID:https://orcid.org/0000-0001-7643-5295

Борщов Ілля Вячеславович – Харківський національний університет радіоелектроніки, асистент кафедри комп'ютерно-інтегрованих технологій, автоматизації та робототехніки; Україна; e-mail: illia.borshchov1@nure.ua**;** ORCID**:** https://orcid.org/0000-0002-6598-6988.

УДК 621.396.96 **DOI:10.30837/rt.2025.1.220.10**

В.М. КАРТАШОВ, д-р техн. наук, Р.О. БОБНЄВ

МЕТОДИ АКУСТИЧНОГО ЗОНДУВАННЯ АТМОСФЕРИ З ВИКОРИСТАННЯМ АНТЕННИХ РЕШІТОК

Вступ

Системи акустичного зондування (АЗ) атмосфери – содари є відносно недорогим і ефективним засобом дистанційного вимірювання параметрів атмосфери. Системи АЗ дозволяють вимірювати швидкість і напрямок вітру, параметри турбулентності, вологість атмосферного повітря [1, 2]. Метод базується на зондуванні атмосфери акустичними хвилями, формуванні сигналу, розсіяного природними атмосферними турбулентними неоднорідностями, прийомі розсіяного акустичного сигналу та визначенні параметрів атмосфери за параметрами розсіяного сигналу [1].

Моніторинг атмосфери з використанням систем АЗ здійснюється в інтересах авіації, екології, радіозв'язку, радіолокації. Основні фактори, що обмежують ефективність функціонування систем акустичного зондування, – значне затухання акустичних хвиль в атмосфері, яке має суттєву частотну залежність, та вплив зовнішнього акустичного шуму на роботу содарів [3,4].

Метод АЗ розвивається вже декілька десятиліть, з початку 60-х років минулого століття. Розроблено фізичні основи методу, сформовано принципи побудови систем акустичного зондування. Спочатку системи виконувалися, як правило, стаціонарними і будувалися з використанням безперервних за простором дзеркальних антен. З розвитком електроніки та комп'ютерної техніки зменшилася вага, габаритні розміри станцій, з'явилися мобільні варіанти акустичних локаторів [5, 6]. Розробка ефективних п'єзоелектричних акустичних випромінювачів забезпечила можливість створення дискретних за простором акустичних антен – антенних решіток (АР) [7]. Застосування фазованих акустичних антенних решіток дозволяє здійснювати електричне управління променем діаграми спрямованості при вимірюванні швидкості і напрямку вітру методом зондування в кількох напрямках. Раніше, при використанні дзеркальних акустичних антен, випромінювання сигналу в різних напрямках здійснювалося шляхом механічної зміни орієнтації антен.

З появою АР з'явилася також можливість реалізації методів адаптивної антенної обробки з метою підвищення захищеності содарів від завад. Однак використання акустичних антенних решіток у содарах має ряд особливостей, тому перш ніж впроваджувати методи акустичного зондування атмосфери з використанням АР на практиці, необхідно провести додаткові дослідження з метою з'ясування меж потенційних можливостей содарів, що відкриваються, шляхом виконання математичного комп'ютерного моделювання розроблених методів та їх подальшої експериментальної перевірки.

1. Аналіз методів і систем акустичного зондування атмосфери

Публікації, присвячені методу акустичного зондування атмосфери, з'явилися на початку 60-х років минулого століття [1, 5]. Внаслідок інтенсивного розвитку методу АЗ у різних країнах були створені теоретичні основи методу, сформульовані принципи побудови систем акустичного зондування та розроблена узагальнена структура содарів. На початковому етапі системи акустичного зондування атмосфери, як правило, виконувалися стаціонарними, їх будували з використанням безперервних за простором дзеркальних акустичних антен.

Методи та засоби захисту содарів від перешкод (звукоізоляційні бленди, укриття різного роду), що використовувались на початкових етапах розвитку методу АЗ, мали ряд недоліків: значні габаритні розміри та вага, складність транспортування, недостатня ступінь захисту від перешкод, що потрапляють у головний і боковий пелюстки діаграми спрямованості. Усе це в значній мірі впливає на якісні показники системи в цілому [5, 6].

Значним драйвером удосконалення систем АЗ є використання останніх досягнень електроніки, теорії обробки сигналів та комп'ютерної техніки. Використання науково-технічних досягнень у зазначених областях дозволяє розробляти багатофункціональні, зручні в управлінні та експлуатації станції.

Поява ефективних п'єзоелектричних акустичних випромінювачів, які дозволяють здійснювати випромінювання акустичних хвиль в атмосферу, забезпечила можливість використання антенних решіток у содарах [7 – 9]. Попередні спроби побудови акустичних антенних решіток у содарах на основі електродинамічних випромінювачів не були успішними. Електродинамічні випромінювачі характеризуються значним впливом погодних умов на їх роботу та нестабільністю фазочастотних характеристик.

Застосування фазованих п'єзоелектричних акустичних антенних решіток (ААР) у содарах дозволяє шляхом електричного управління променем діаграми спрямованості реалізовувати методику зондування в кількох напрямках для вимірювання швидкості та напрямку вітру [10 – 12]. Раніше, при використанні дзеркальних акустичних антен, випромінювання сигналу в різних напрямках здійснювалося шляхом механічної зміни орієнтації антен.

Важливою перевагою систем зондування з АР є можливість як електронного управління променем (променями) діаграми спрямованості, так і можливість реалізації адаптивної просторової вибірковості залежно від наявної завадової обстановки, що дозволяє формувати «нулі» діаграми спрямованості в напрямку перешкоди, забезпечує можливість суттєво підвищити захищеність систем акустичного зондування від перешкод [11 – 13]. Наразі існує ряд закордонних систем акустичного зондування з АР та електронним управлінням променем діаграми направленості [15]. При цьому адаптивні методи просторово-часової обробки сигналів у них практично не використовуються. Тому розробка методів і засобів адаптації систем акустичного зондування атмосфери до метеорологічної та завадової обстановки, що змінюється, є актуальним науково-прикладним завданням сучасної теорії та техніки акустичного зондування.

В даний час содари для зондування атмосфери виробляються рядом науково-виробничих фірм [14 – 17]. Наприклад, содари марки FAS фірми Scintec є імпульсними акустичними локаторами [16]. Структурна схема содарів XFAS, FFAS, SFAS, які працюють у різних діапазонах частот і мають різну максимальну дальність дії, включає в себе плоску антенну решітку, модуль попередньої обробки сигналів та переносний комп'ютер для подальшої обробки результатів вимірювання параметрів атмосфери. Усі содари марки FAS (XFAS, FFAS, SFAS) аналогічні за конструкцією і відрізняються розмірами, вагою, діапазоном висот зондування та значенням роздільної здатності.

Кількість антенних елементів в антенній решітці содарів складає, як правило, кілька десятків (зазвичай 50-60 випромінювачів) [17]. Содари працюють у діапазоні частот від 600 до 5000 Гц. Помилки вимірювання швидкості вертикального вітру становлять 0,03...0,1 м/с, горизонтального вітру – 0,1...0,3 м/с, помилка вимірювання напрямку вітру складає 2-3 градуси. Максимальна висота зондування залежить від використовуваної частоти випромінювання і досягає 5000 м.

Содари FAS є представниками нової серії содарів, які використовують у якості антенної системи плоску фазовану антенну решітку. При порівняно невеликих розмірах (72×74×25 см) і масі 32 кг содар MFAS забезпечує вимірювання тривимірних профілів швидкості вітру та параметрів турбулентності з досить високими характеристиками. Діапазон висот зондування – від 15 до 1000 м, просторове розділення – від 10 м.

Плоска акустична антенна решітка, що входить до складу содарів серії FAS, є інновацією компанії Scintec. Оригінальне виконання елементів решітки, показане на рис. 1, базується на використанні концепції оберненого рупора, що забезпечує досить добре узгодження з атмосферою, дозволяє досягти покращення направлених властивостей антенної системи, збільшення динамічного діапазону та коефіцієнта перетворення електричної енергії в акустичну, а добре демпфування робить антенну систему менш чутливою до впливу опадів [16].

Кожен з елементів антенної решітки оснащений малошумливим попереднім підсилювачем для випромінювання та прийому коливань. З метою зменшення впливу електромагнітних наводок попередні підсилювачі розташовуються в безпосередній близькості від елементів решітки.

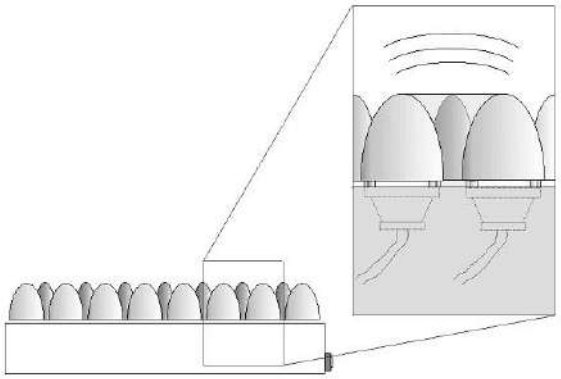


Рис.1. Акустична антенна решітка фірми Scintec

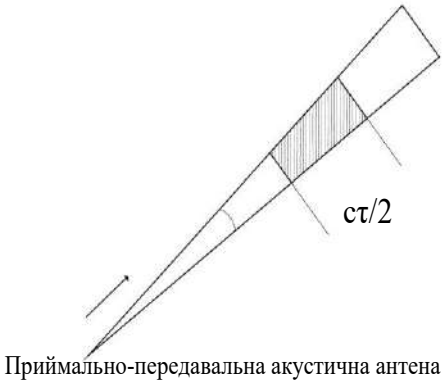


Рис. 2. Промінь діграми спрямованості акустичної антени при зондуванні атмосфери

Акустичні локатори німецької фірми Metek – PCS.2000 (PCS.2000-24, PCS.2000-64). PCS.2000 є мінісодарами, призначеними для вимірювання швидкості вітру та характеристик турбулентності [14]. В якості антени в PCS.2000-24 та PCS.2000-64 використовуються акустичні плоскі ФАР, що складаються з 24 та 64 антенних елементів відповідно. Содари дозволяють вимірювати вертикальні профілі вітру в діапазоні висот від 15 до 1000 м. Особливістю серії акустичних локаторів PCS.2000 є можливість віддаленого доступу до вимірюваних даних. Для цього в содарах застосовано радіомодем GSM-стандарту.

В США фірмою AeroVironment розроблено та серійно виробляються содари – Model 4000, MiniSODAR з 32-елементною ФАР в якості антени. В Японії розроблено та введено в експлуатацію мобільний содар КАР-1000, реалізований з використанням ФАР [17].

Схема акустичного зондування атмосфери в одному напрямку представлена на рис. 2. Радіальна (по променю діаграми спрямованості антени) складова швидкості вітру в досліджуваному обсязі атмосфери визначається співвідношенням [18]

$$\vec{V}_r = \frac{c}{2 \cdot f} \cdot f_d, \tag{1}$$

де c – швидкість поширення звуку в повітрі; f_d – доплерівський зсув частоти зондувального сигналу; f – частота прийнятого акустичного сигналу.

Вимірювання радіальної швидкості вітру здійснюється в обсязі простору, обмеженому за дальністю величиною $c\tau/2$ (τ – тривалість зондувального імпульсу), а в поперечному напрямку – тілесним кутом випромінювання (прийому) діаграми спрямованості акустичної антени локатора.

Найчастіше швидкість і напрямок вітру в атмосферному прикордонному шарі за допомогою содарів визначають методом зондувань у трьох різних напрямках [19]. В результаті такого зондування для кожного висотного шару атмосфери виконуються три вимірювання, результати яких входять у систему трьох рівнянь з трьома невідомими – ортогональними складовими швидкості вітру. Далі система рівнянь розв'язується відносно шуканих параметрів – складових швидкості вітру. Кількість зондувань може бути і більшою, ніж три, при цьому зберігається можливість визначення трьох невідомих атмосферних параметрів, а точність їх визначення зростає.

2. Постановка задачі дослідження

Розроблення останнім часом п'єзоелектричних випромінювачів, що забезпечують ефективне випромінювання акустичних хвиль у повітряне середовище, дало змогу створити акустичні антенні решітки та інтегрувати їх у структуру акустичного локатора, що виконує завдання дистанційного зондування атмосфери. Використання фазованих акустичних антенних решіток у структурі содара дає змогу здійснювати електричне сканування променем діаграми спрямованості під час вимірювання швидкості та напряму вітру методом зондування в декількох напрямках. З'являється також можливість реалізації одночасного зондування атмосфери в декількох напрямках. Такий метод зондування підвищує оперативність і суттєво скорочує час, необхідний для вимірювання профілів швидкості та напрямку вітру. Крім того, підвищуються якісні характеристики результатів вимірювань, зумовлені виконанням послідовного зондування в різних напрямках.

З появою АР забезпечується також можливість реалізації методів адаптивного просторового оброблення сигналів з метою підвищення завадозахищеності содарів. Однак використання акустичних антенних решіток у содарах має і низку особливостей, зумовлених виконанням одночасного зондування в кількох напрямках, особливостями поля акустичних завад, наявністю суттєвої рефракції під час поширення акустичних хвиль в атмосфері. Тому необхідно провести додаткові дослідження з метою реалізації значних потенційних можливостей содарів, що відкриваються, при використанні акустичних антенних решіток. Необхідно розробити адекватні математичні моделі акустичних сигналів, виконати математичне комп'ютерне моделювання методів, що розробляються, і здійснити їх подальшу експериментальну перевірку.

3. Метод одночасного зондування атмосфери у кількох напрямках

У задачах радіолокації, де напрямок приходу корисного сигналу зумовлений наявністю дискретних зосереджених цілей, а оптимізація здійснюється, наприклад, за критерієм максимуму відношення сигнал-перешкода на виході антени [18, 20], у задачах акустичного зондування атмосфери напрямок випромінювання зондувального сигналу і напрямок приймання розсіяних акустичних сигналів може змінюватись у деяких доволі широких межах. При цьому звукові хвилі, що зондують простір, розсіюються на природних турбулентних неоднорідностях середовища, які розподілені практично ізотропно в атмосфері. Ця обставина є фізичною передумовою для виконання зондування атмосфери в різних напрямках, які можна вибирати залежно від наявної метеорологічної або завадостійкої обстановки.

Розглянемо особливості зондування атмосфери акустичними локаторами, у складі яких використовуються акустичні антенні решітки. Нехай є ААР з N акустичними елементами. Вектор вагових коефіцієнтів (ВВК) антенної решітки $\vec{Z}^T = [Z_1, Z_2 \dots Z_N]$, що формує діаграму спрямованості антени, в умовах, коли в середовищі присутній тільки власний шум приймальних антенних елементів, повністю збігається з вектором управління (вектором кореляції) $\vec{V}(\beta_0)$, який визначає вигляд, форму діаграми спрямованості $E(\beta_0, \beta)$ системи та напрямок її головної пелюстки. При цьому максимум діаграми спрямованості припадає на напрямок β_0. Вираз, що визначає вектор керування системи, має вигляд [18]

$$\vec{V}^T = [V_1, V_2, \dots, V_N], \tag{2}$$

де елемент вектору управління V_k записується у вигляді $V_k = v_k \cdot exp(j[2\pi(\kappa - 1)d \cdot sin\theta_0]/\lambda)$, $k = 1, \dots N$.

Значення коефіцієнтів v_k, що описують розподіл акустичного поля апертурою антенної системи, обирають таким чином, щоб забезпечити необхідну форму і параметри діаграми спрямованості – основної та бічних пелюсток. Якщо, наприклад, розподіл поля по апертурі буде рівномірним, «стілоподібним», то значення параметрів v_k=1, $k = 1, \dots N$, β=0 і рівень

першої бічної пелюстки діаграми спрямованості становитиме -13,5 дБ, а діаграма спрямованості антенної системи описуватиметься співвідношенням [6]

$$|E(\beta_0,\beta)| = \left|\vec{S}^T \cdot \vec{V}^*(\beta_0)\right| = \left|\sum_{k=1}^{N} v_k \cdot exp\left(\frac{j(k-1)2\pi d}{\lambda}[sin\,\beta - sin\beta_0]\right)\right|, -\pi/2 \le \theta \le \pi/2, \quad (3)$$

де d – відстань між елементами антенної решітки; λ – довжина хвилі акустичного сигналу.

Вектор корисного сигналу $\vec{S}$ у формулі (3) являє собою вектор-стовпчик сигналів одиничної амплітуди, які приймає антенна решітка з напряму β (або які випромінюються в зазначеному напрямку). Зміна (оптимізація) значень коефіцієнтів v_k дає змогу змінювати форму діаграми спрямованості, домагаючись необхідної її форми, або максимізувати коефіцієнт спрямованої дії антенної решітки.

Багатопелюсткова діаграма спрямованості (рис.3), що формується за допомогою акустичної антенної решітки содара, яка забезпечує виконання одночасного зондування атмосфери в декількох різних напрямках, визначається формулою

$$\left|\sum_{i=1}^{I} E(\beta_i,\beta)\right| = \left|\sum_{i=1}^{I} \vec{S}^T \cdot \vec{V}^*(\beta_i)\right| = \left|\sum_{i=1}^{I}\sum_{k=1}^{N} v_k \cdot exp\left(\frac{j(k-1)2\pi d}{\lambda}[sin\,\beta - sin\beta_i]\right)\right|, \quad (4)$$

де β_i – напрямок i-го зондування.

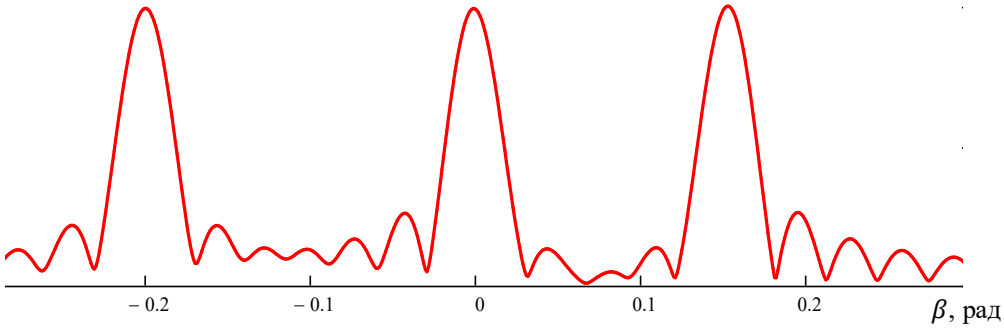


Рис. 3. Діаграма спрямованості антенної решітки содара, що забезпечує одночасне зондування атмосфери в трьох різних напрямках на частоті 1140 Гц

Діаграма спрямованості акустичної антенної решітки (рис. 4), що забезпечує виконання одночасного зондування атмосфери в декількох різних напрямках і на різних частотах зондувального сигналу, описується співвідношенням

$$\left|\sum_{i=1}^{I} E(\beta_i,\beta)\right| = \left|\sum_{i=1}^{I} \vec{S}^T \cdot \vec{V}^*(\beta_i)\right| = \left|\sum_{i=1}^{I}\sum_{k=1}^{N} v_k \cdot exp\left(\frac{j(k-1)2\pi d}{\lambda_i}[sin\,\beta - sin\beta_i]\right)\right|, \quad (5)$$

де β_i – напрямок i-го зондування, λ_i – довжина хвилі, яка визначає частоту зондування в i-му напрямку).

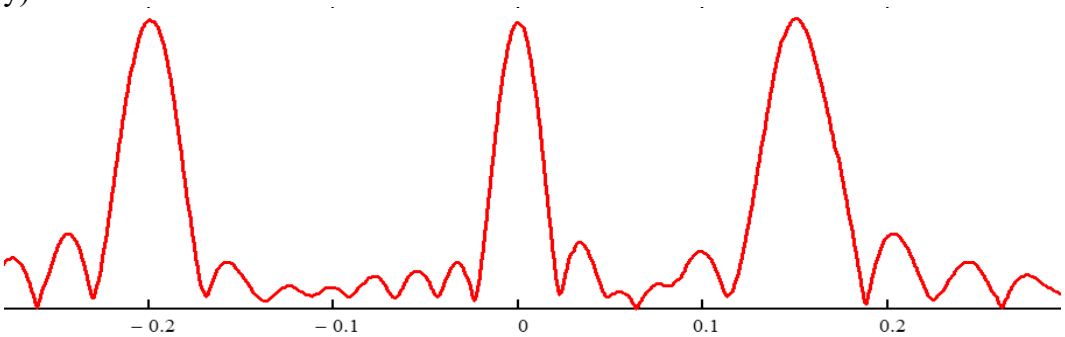


Рис. 4. Діаграма спрямованості антенної решітки содара, що забезпечує одночасне зондування атмосфери в трьох різних напрямках і на трьох різних частотах (1140 Гц, 1460 Гц, 930 Гц)

Як випливає з рис. 4, оскільки зондування атмосфери в різних напрямках здійснюється на різних частотах, то і ширина кожного променя багатопелюсткової діаграми спрямованості при цьому формується різна.

4. Реалізація адаптивної просторової вибірковості у содарах

Розглянемо можливості використання антенних решіток содарів для боротьби із зовнішніми акустичними завадовими коливаннями, що формуються різноманітними зовнішніми джерелами акустичного випромінювання.

У цьому разі акустична решітка содара використовується як адаптивна акустична антенна решітка (АААР). За появи джерел зовнішніх акустичних перешкод діаграма спрямованості АААР видозмінюється таким чином, що в напрямках, з яких діють джерела зовнішніх шумів, у діаграмі спрямованості антени формуються локальні мінімуми – «нулі». При цьому, рівень кожного мінімуму діаграми спрямованості та швидкість адаптації антенної решітки залежатимуть від величини відношення «завада-тепловий шум», а оптимальний у сенсі максимуму відношення «сигнал-завада» ВВК обчислюється згідно з виразом

$$\vec{Z}_{opt}(\beta_0) = \eta \cdot \vec{R}^{-1} \cdot \vec{V}^*(\beta_0), \tag{6}$$

де η – комплексний нормувальний множник; $\vec{R} = E\{\vec{N}^* \cdot \vec{N}^T\}$ – кореляційна матриця суміші зовнішньої активної шумової завади і власного шуму приймальних елементів акустичної решітки; $\vec{N}^T = [n_1, n_2, \dots, n_N]$ – вектор миттєвих значень напруг завади на виходах елементів акустичної антенної решітки; $\vec{V}$ – вектор управління діаграмою спрямованості АААР.

Вираз (6), що визначає процес адаптації антенної решітки, є відомим вінерівським рішенням в області просторової фільтрації корисного сигналу на фоні перешкод. Адаптація, або знаходження оптимального значення ВВК АААР відповідно до зазначеного алгоритму, здійснюється в паузах між приходом корисних луна-сигналів, що несуть інформацію про стан атмосфери. Таким чином, цей алгоритм адаптації виявляється практично інваріантним до структури і параметрів розсіяного, а також зондувального акустичних сигналів за умови, що вказані сигнали є вузькосмуговими в просторово-часовому сенсі.

Якщо ця умова не виконується, то алгоритм адаптації акустичної антенної решітки содара буде значною мірою залежить від властивостей зондувального та розсіяного акустичного сигналів. Коли сигнал є відносно вузькосмуговим, прийнятий просторово-часовий сигнал відповідає умові факторизації (вузькосмуговості в просторово-часовому сенсі), часова і просторова структури сигналу в цьому разі розділяються і можливе роздільне виконання спочатку просторової, а потім і часової обробки.

Умова факторизації просторово-часового акустичного сигналу записується у вигляді [21]

$$|R(0)|^{-2} \int_{-\infty}^{\infty} |R(\tau)|^2 d\tau = \tau_{e\phi} >> \Delta t_{max} \quad , \tag{7}$$

де $R(\tau)$ – часова автокореляційна функція акустичного сигналу, що приймається; $\tau_{e\phi}$– ефективна ширина пелюстки автокореляційної функції; Δt_{max} – максимальний час затримки акустичного сигналу під час поширення його вздовж апертури антенної решітки. Для широкосмугового в просторово-часовому сенсі акустичного сигналу умова факторизації не виконується і розділення обробки на просторову і часову неможливе.

Результати моделювання процесу адаптації акустичної антенної решітки під час впливу на вхід системи шумоподібної акустичної завади, що діє з напрямку 40 градусів, показано на рис. 5. Як видно, вихідна діаграма спрямованості акустичної антенної решітки в процесі адаптації видозмінюється, і в напрямку дії акустичної завади формується «нуль» діаграми спрямованості, внаслідок чого співвідношення сигнал-шум на виході системи обробки підвищується та поліпшуються умови приймання корисного сигналу, що несе інформацію про стан атмосфери.

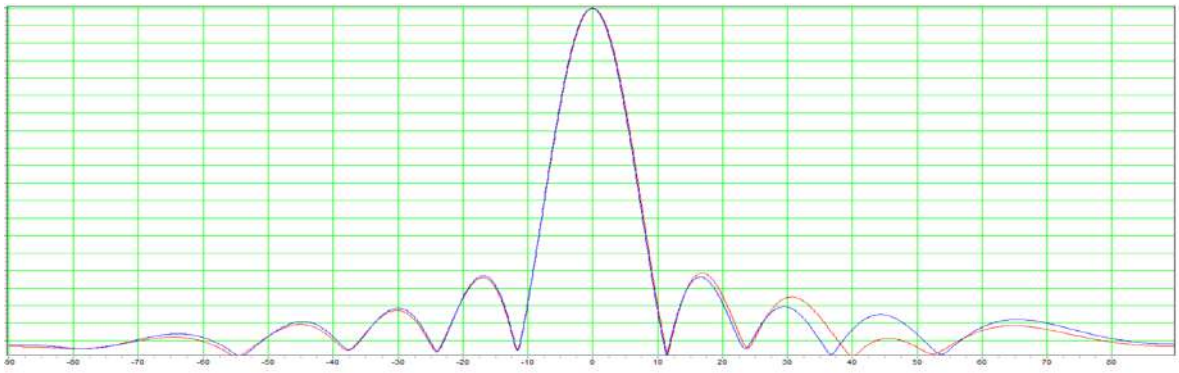


Рис. 5. Діаграми спрямованості акустичної антенної решітки:
1 – неадаптованої; 2 – адаптованої, під час впливу акустичної завади з напрямку 40 градусів

Висновки

1. Метод дистанційного акустичного зондування атмосфери інтенсивно розвивається в останні десятиліття. Він надає можливість отримувати висотні профілі швидкості та напрямку вітру, профілі характеристик турбулентності атмосфери. Результати зондування можуть бути використані для метеорологічного забезпечення зльоту і посадки літальних апаратів, метеорологічного забезпечення екологічних завдань запобігання забрудненню повітря, у задачах вивчення атмосферних процесів.

2. Техніка акустичного зондування також динамічно розвивається останнім часом. Внаслідок інтеграції досягнень електроніки та комп'ютерної техніки в структуру акустичного локатора, він став менш габаритним, легшим, більш функціональним. Розроблення ефективних п'єзоелектричних акустичних випромінювачів забезпечило можливість створення акустичних антен содарів у вигляді антенних решіток, що справило значний вплив на структуру акустичного локатора і надає змогу суттєво розширити його потенційні можливості. Процес, що розглядається, можна порівняти зі зміною технічного вигляду і можливостей систем радіолокації та систем радіозв'язку під час впровадження в них антенних решіток.

Однак використання акустичних антенних решіток у содарах має і низку особливостей, зумовлених можливістю виконання одночасного зондування в кількох напрямках, особливостями поля акустичних завад, наявністю суттєвої рефракції під час розповсюдження акустичних хвиль в атмосфері. Тому необхідно провести додаткові дослідження з метою реалізації значних потенційних можливостей содарів, що відкриваються, під час використання акустичних антенних решіток: розробити адекватні математичні моделі акустичних сигналів, виконати математичне комп'ютерне моделювання методів, що розробляються, та їхню подальшу експериментальну перевірку.

3. Розглянуто методи дистанційного зондування атмосфери содарами з антенною решіткою при виконанні одночасного зондування у декількох напрямках. Розроблено адекватні математичні моделі акустичних сигналів і методів багатоканального зондування, виконано математичне комп'ютерне моделювання процесів зондування. Проаналізовано запропонований метод при виконанні одночасного зондування атмосфери в декількох напрямках на одній частоті, а також при використанні різних частот зондувальних сигналів у різних напрямках. Реалізація розглянутих методів на практиці забезпечить підвищення оперативності та скорочення часу вимірювання характеристик атмосфери.

4. Виконано математичне моделювання методів адаптивної просторової вибірковості акустичних локаторів з адаптивною антенною решіткою. Показано їхні значні потенційні можливості. Реалізація таких методів на практиці дозволить суттєво підвищити завадозахищеність акустичних локаторів, особливо за їхньої роботи в умовах складної завадової обстановки, наприклад в умовах аеропорту або в межах мегаполісу.

Список літератури:

1. Bradley S. Atmosphere Acoustic Remote Sensing. Principes andApplication. CRC Press. 2007. 267 p.
2. Lataitis R.J. Theory and Application of a radio-acoustic sounding system (RASS): NOAA Technical Memorandum ERL WPL-230 // Nat. Oceanic and Atmos. Admin. Environ, Res. Labs. Boulder, CO, 1993. 207 p.
3. Kartashov V.M., Tikhonov V.A., Oleinikov V.N. Signal processing in radio electronic systems for remote monitoring of the atmosphere. Kharkiv, KNURE, 2014. 312 p.
4. Remtech Radio Acoustic Sounding System (RASS) for remote sensing of temperature. URL: https://remtechinc.com/wp-content/uploads/RASS3.pdf.
5. Kartashov V., Babkin S., Kartashov A., Pershyn Y. Development of the Atmosphere Radio-Acoustic Sounding Method in Ukraine and in the World in the Period of 1961-2000 // 2023 IEEE 6th International Conference on Information and Telecommunication Technologies and Radio Electronics, UkrMiCo 2023, 13–15 November 2023, Kyiv, Ukraine. P. 372–376. DOI: 10.1109/UkrMiCo61577.2023.10380339
6. Карташов В.М. Моделі і методи обробки сигналів систем радіоакустичного і акустичного зондування атмосфери. Харків : ХНУРЕ, 2011. 234 с.
7. Kartashov V.M. Estimation of Signal Parameters Scattered by an Acoustic Wave Packet // Telecommunications and Radio Engineering., 2004. Vol. 61, №2. P. 125–129.
8. Muradyan P., Richard Coulter R. Radar Wind Profiler (RWP) and Radio Acoustic Sounding System (RASS) Instrument Handbook. March, 2020. Environmental Science Division, Argonne National Laboratory. 20 p. URL: https://www.arm.gov/publications/tech_reports/handbooks/rwp_handbook.pdf .
9. Kartashov V.M. Signal Scattering Functions of Atmospheric Sounding System // Telecommunications and Radio Engineering, 2003, Vol. 59, №7-8-9, pp. 88–94.
10. Kartashov V. M., Tikhonov V. A., Voronin V. V. Features of Construction and Application of Complex Systems for the Atmosphere Remote Sounding // Telecommunications and Radio Engineering. 2017. Vol. 76, №8. P.743–749.
11. V. Kartashov, V. Oleynikov, I. Koryttsev, S. Sheiko, O. Zubkov, S. Babkin. Processing of Wide Band Acoustic Signals During Detection of Unmanned Aerial Vehicles // 2020 IEEE Ukrainian Microwave Week (UkrMW). Kharkiv, Ukraine, September 21 – 25, 2020. Vol. 1 on 2020 IEEE 12th International Conference on Antenna Theory and Techniques (ICATT). P. 35–39.
12. Developing and Applying Optoelectronics in Machine Vision/ O. Sergiyenko, J.C. Rodriguez-Quiñonez, IGI Global, 2016. 341p.
13. Oleynikov V. N , Zubkov O. V., Kartashov V. M., Korytsev I. V., Babkin S. I., Sheiko S. A. Investigation of detection and recognition efficiency of small unmanned aerial vehicles on their acoustic emission // Telecommunications and Radio Engineering. 2019. Vol. 78, Issue 9. P. 759–770.
14. Doppler SODAR PCS.2000. URL: https://metek.de/product-group/doppler-sodar/.
15. Remtech introduces the miniature PA-XS acoustic wind profiler. URL: https://remtechinc.com/.
16. Wind Profilers. URL: https://www.scintec.com/catalogs/wind-profilers
17. AeroVironment Inc. URL: http://www.aerovironment.com
18. Ситнік О.В., Карташов В.М. Радіотехнічні системи : навч. посіб. Харків : Сміт, 2009. 448 с.
19. Chandrasekhar Sarma, T. V., Narayana Rao, D., Furumoto, J., and Tsuda, T. Development of radio acoustic sounding system (RASS) with Gadanki MST radar – first results // Ann. Geophys. 2008. Vol. 26. P. 2531–2542. https://doi.org/10.5194/angeo-26-2531-2008
20. Kartashov V.M., Tikhonov V.A., Voronin V.V. and Tymoshenko L.P. Complex model of random signal in problems of acoustic sounding of atmosphere // Telecommunications and Radio Engineering. 2016. V. 75, Iss. 20. P.1885–1892.
21. Beyrich F., Engelbart D., Gorsdorf U., Neisser J. Simultaneous Measurements of Vertical Profiling Systems-a Contribution to the “Lindenberg Column // Proc. 8th Int. Symp. on Acoustic Remote Sensing of the Atmosphere and Oceans (ISARS). Moscow, 1996. P. 3.73–3.78.

Надійшла до редколегії 19.01.2025

Відомості про авторів:

Карташов Володимир Михайлович – д-р техн. наук, професор, Харківський національний університет радіоелектроніки, завідувач кафедри медіаінженерії та інформаційних радіоелектронних систем; Україна; email: volodymyr.kartashov@nure.ua; ORCID: https://orcid.org/0000-0001-8335-5373

Бобнєв Роман Олександрович – Харківський національний університет радіоелектроніки, аспірант кафедри медіаінженерії та інформаційних радіоелектронних систем; Україна; email: roman.bobniev@nure.ua; ORCID: https://orcid.org/0000-0002-9322-9722

УДК 621.39:534.87]:004.056.5 **DOI:10.30837/rt.2025.1.220.11**

А.М. ОЛЕЙНІКОВ, канд. техн. наук, Ю.В. ЛИКОВ, канд. техн. наук, Я.С. ПАВЛЕНКО

ОСОБЛИВОСТІ ВИЯВЛЕННЯ АКУСТОЕЛЕКТРОМАГНІТНИХ КАНАЛІВ ВИТОКУ ІНФОРМАЦІЇ

Вступ

У сучасному технологічному середовищі, що характеризується стрімким розвитком інформаційних технологій та цифрових систем, забезпечення інформаційної безпеки набуває критичного значення. Однією з основних загроз для конфіденційності даних є технічні канали витоку інформації, серед яких особливу увагу привертають акустоелектромагнітні канали. Ці канали формуються внаслідок акустоелектромагнітних перетворень, коли акустичні хвилі взаємодіють із елементами технічних пристроїв, перетворюючи звукову енергію на електричну або електромагнітну. Такі канали часто мають прихований характер і залишаються непомітними під час стандартних перевірок систем інформаційної безпеки, що робить їх надзвичайно небезпечними.

Акустоелектромагнітні канали витоку інформації є особливо підступними через свою здатність виникати навіть у повсякденних умовах. Звичайні пристрої, що оточують, можуть стати джерелами небажаних сигналів, які потенційно можуть бути використані для несанкціонованого доступу до даних. Ці канали утворюються завдяки дії акустичних хвиль на чутливі елементи технічних засобів, такі як трансформатори, п’єзоелементи, котушки індуктивності, гучномовці, мікрофони або інші компоненти з високою реакцією на звукові коливання. Вплив акустичних хвиль на ці елементи викликає зміну електричних параметрів або генерує нові сигнали, які можуть містити конфіденційну інформацію [1].

Окрім технічних особливостей, проблема виявлення акустоелектромагнітних каналів витоку інформації посилюється складністю аналізу їх фізичних властивостей. Сигнали такого типу можуть бути слабкими, маскуватися під природний шум або зливатися з робочими сигналами пристроїв. Це вимагає розробки нових підходів до моніторингу, виявлення та аналізу акустоелектромагнітних явищ у технічних засобах.

1. Типи акустоелектомагнітних каналів витоку інформації та фізичні процеси, що відбуваються в них

Акустоелектричні канали витоку інформації поділяються на два основні типи: прямі та модуляційні. Прямі акустоелектричні канали утворюються внаслідок безпосереднього перетворення акустичних коливань в електричні сигнали (рис. 1). Модуляційні акустоелектричні канали виникають тоді, коли акустичні коливання впливають на елементи високочастотнних генераторів, викликаючи модуляцію їх сигналів за частотою або амплітудою відповідно до параметрів мовного сигналу.

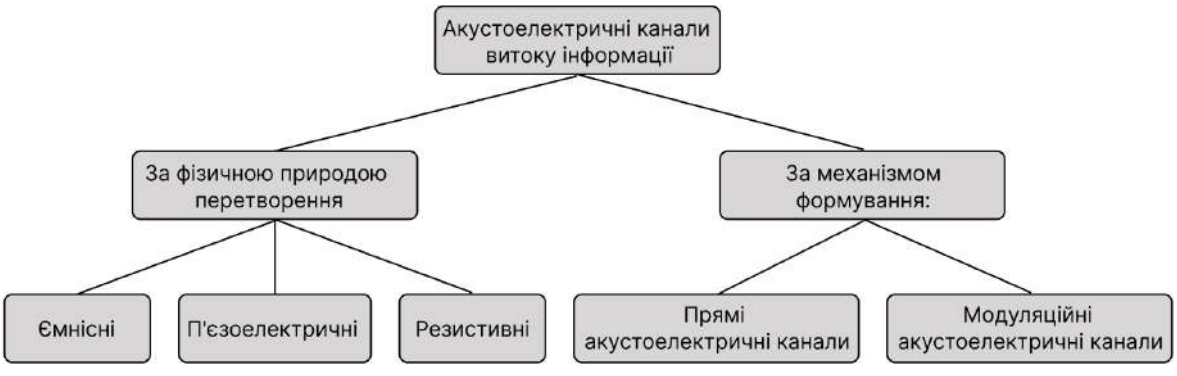


Рис. 1. Класифікація акустоелектричних каналів витоку інформації

Акустомагнітні канали також поділяються на прямі та модуляційні. Прямі акустомагнітні канали формуються через індукцію магнітних полів у феромагнітних матеріалах під впливом акустичних хвиль. У цьому випадку звуковий вплив створює магнітну індукцію, яка може бути виявлена в магнітопроводах чи обмотках пристроїв (рис. 2). Модуляційні акустомагнітні канали виникають тоді, коли звукові коливання змінюють параметри магнітної індукції, впливаючи на характеристики магнітопроводів чи котушок, що використовуються у технічних системах [2].

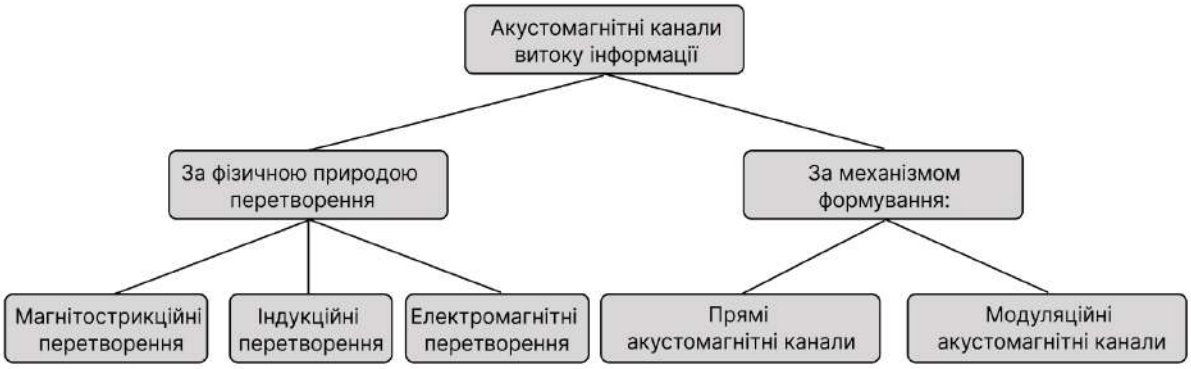


Рис. 2. Класифікація акустомагнітних каналів витоку інформації

Серед акустичних перетворювачів розрізняють індуктивні, ємнісні, п'єзоелектричні, електромагнітні, оптичні, магнітострикційні та акусторезистивні пристрої. Індуктивні перетворювачі працюють за принципом зміни індуктивності під впливом механічної дії. Ємнісні перетворювачі змінюють свою ємність під впливом акустичного тиску, що робить їх надзвичайно чутливими до звукових впливів. П'єзоелектричні перетворювачі базуються на використанні п'єзоелектричного ефекту, коли механічне навантаження викликає появу електричного заряду. Ці елементи мають високу стабільність параметрів перетворення і широко застосовуються в радіотехнічних пристроях, але можуть стати потенційним джерелом витоку інформації.

Фізичні процеси, що лежать в основі акустоелектричних перетворень, пов'язані з механічними коливаннями, які змінюють електричні параметри сигналів. Наприклад, акустичний сигнал впливає на дифузор гучномовця, внаслідок чого акустична енергія перетворюється в механічну, змінюючи положення котушки в магнітному полі, що викликає появу електрорушійної сили в електричному колі котушки. Якщо гучномовець підключений до мережі через трансформатор, небезпечний сигнал може збільшитися в кілька разів, поширюючись мережею живлення [3].

У трансформаторах зміна параметрів обмоток під впливом звукових хвиль може призводити до модуляції сигналів, що передаються мережею. П'єзоелементи перетворюють механічні коливання на електричний заряд, а оптичні перетворювачі можуть змінювати свій вихідний сигнал під впливом акустичних хвиль, які модулюють світловий потік.

Іншим прикладом є домофонні апарати, де динаміки або дзвінкові механізми можуть генерувати сигнали під впливом звукових хвиль, передаючи їх телефонною лінією. Особливу небезпеку становлять датчики охоронно-пожежної сигналізації, які оснащені п'єзоелементами, що реагують на звукові хвилі, створюючи електричні сигнали, які можуть бути використані для перехоплення інформації.

Для оцінки ефективності перетворення звукової енергії в електричну чи магнітну використовують коефіцієнт перетворення (КПД). Це безрозмірна величина, що визначає, яка частка вхідної акустичної енергії перетворюється у вихідний сигнал. Ефективність перетворення п'єзоелементів може досягати 20 – 30 %, що робить їх потенційно небезпечними у контексті витоку інформації.

Формули для розрахунку КПД для акустичного перетворювача:

$$K_{ae} = \frac{P_{\text{вих}}}{P_{\text{вх}}} \cdot 100\%, \quad (1)$$

де $P_{вих}$ – вихідна потужність сигналу, $P_{вх}$ – вхідна акустична потужність.

Для визначення $P_{вих}$ для акустоелектричного перетворення проводиться розрахунок ЕРС.

1) Для п'єзоелектричного перетворення:

$$E = k_0 \cdot F \cdot v, \quad (2)$$

де E – електрорушійна сила (ЕРС); k_0 – коефіцієнт п'єзоефекту; F – механічна сила; v – швидкість деформації.

Для визначення $P_{вих}$ для акустомагнітного перетворення проводиться розрахунок:

2) Для акустомагнітного перетворення:

$$B = \mu \cdot \frac{F}{S}, \quad (3)$$

де B – магнітна індукція, μ – магнітна проникність, F – акустична сила, S – площа магнітопроводу.

Для акустоелектричних каналів, таких як гучномовці та п'єзоелементи, напруга сигналу, що наводиться у гучномовцях, зазвичай становить 2 – 3 мВ/Па. У модуляційних акустоелектричних каналах, які базуються на високочастотних генераторах, величина модуляції сигналу може становити 0,5 – 1 % від амплітуди несучої частоти. Цього рівня достатньо, щоб забезпечити можливість перехоплення інформації. Щодо акустомагнітних каналів, таких як трансформатори або магнітопроводи, індуковані сигнали в них можуть досягати 1 – 5 мВ, залежно від параметрів магнітної проникності та акустичного тиску звукової хвилі. Проте коефіцієнт перетворення магнітного типу зазвичай не перевищує 10 – 15 % через значні втрати у магнітних матеріалах, що обмежує ефективність таких каналів у порівнянні з акустоелектричними [4].

2. Методики виявлення акустоелектричних каналів витоку інформації та їх особливості

Виявлення акустоелектричних каналів витоку інформації (АЕКВІ) базується на використанні експериментальних підходів, які дозволяють визначити взаємозв'язок між акустичними впливами та електричними сигналами, що генеруються технічними пристроями. Основними методами є дослідження прямих і модуляційних каналів витоку інформації. Кожен із цих підходів вимагає окремих схем випробувань, налаштування відповідного обладнання та специфічних методик вимірювань.

Для прямого акустоелектричного каналу використовується функціональна схема (рис. 3.), яка складається:

- з джерела акустичних сигналів (акустичний генератор), який створює електричний сигнал з визначеною частотою та амплітудою;
- випромінювача звуку (динамік або ультразвуковий випромінювач), який передає акустичний сигнал у зону дослідження;
- об'єкта дослідження (потенційне джерело АЕКВІ) – це технічний пристрій (гучномовець, п'єзоелемент, трансформатор, тощо), який піддається впливу звукових хвиль;
- пристрою реєстрації сигналів – спектроаналізатор вимірює електричні сигнали, які виникають у досліджуваному об'єкті;
- комп'ютера з АЦП та програмним забезпеченням для обробки даних і побудови залежностей між акустичними і електричними параметрами.

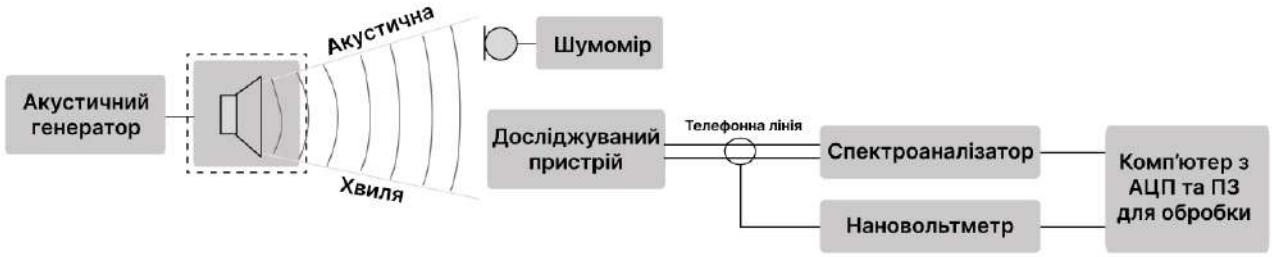


Рис. 3. Функціональна схема для дослідження прямого каналу витоку інформації

Методика дослідження включає поступове підвищення частоти звукового сигналу, вимірювання амплітуд вихідних електричних сигналів та їх аналіз для визначення рівня чутливості об'єкта до акустичних впливів (рис. 4).

Для модуляційного каналу схема включає наступні компоненти:

- акустичний генератор, який створює коливання змінної частоти;
- випромінювач акустичних хвиль передає сигнал у зону розташування високочастотного генератора;
- досліджуваний пристрій, у якому утворюється модуляція сигналу через акустичний вплив;
- антена, радіоприймач та аналізатор спектра реєструють модульовані сигнали та оцінюють їх характеристики;
- комп'ютер з програмним забезпеченням для аналізу частотного спектра, визначення глибини модуляції та виявлення небезпечних сигналів.

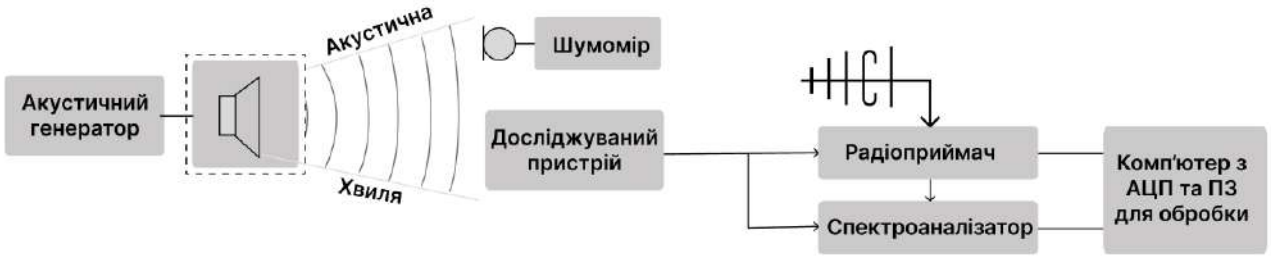


Рис. 4. Функціональна схема для дослідження модуляційного каналу витоку інформації

У цьому випадку проводиться аналіз вихідних сигналів досліджуваного пристрою, їх амплітудної чи частотної модуляції під впливом акустичних хвиль, а також оцінка параметрів модуляції, які можуть бути використані для витоку інформації.

Для проведення експериментів використовуються акустичний генератор із широким діапазоном частот, випромінювач звукових хвиль (динаміки, ультразвукові перетворювачі), осцилограф для візуалізації електричних сигналів у реальному часі, спектроаналізатор для аналізу частотного спектра сигналів, що генеруються об'єктом, нановольтметр із високою чутливістю для точного вимірювання низькоамплітудних сигналів, АЦП, комп'ютер із програмами для обробки даних і побудови графіків залежності сигналів від акустичного впливу.

Акустичні системи (АС), що використовуються для дослідження акустоелектричних каналів витоку інформації, повинні створювати контрольовані акустичні сигнали з параметрами, що дозволяють моделювати вплив звукових хвиль на технічні засоби. АС мають працювати у широкому частотному звуковому та ультразвуковому діапазоні, забезпечувати стабільну амплітуду сигналу з мінімальними спотвореннями (менше 1 %) та зберігати стабільність випромінювання з відхиленням не більше ±1 – 2 %. Важливі вимоги включають спрямованість звуку, можливість регулювання потужності випромінювання (0,1 – 50 Вт),

а також стійкість корпусу до вібрацій і відсутність побічних електромагнітних або механічних випромінювань. Для забезпечення такого захисту використовується щільне електромагнітне екранування колонок, яке зменшує вплив електромагнітних випромінювань на досліджуваний пристрій. Інколи для спеціальних завдань використовуються так звані механічні свистки які не створюють електромагнітного випромінювання, тому їх часто використовують у дослідженнях, де важливо уникнути впливу електромагнітних полів.

АС повинні підтримувати калібрування та забезпечувати сумісність з вузькосмуговими чи ультразвуковими випромінювачами для розширення можливостей дослідження. Виконання цих вимог гарантує точність і надійність експериментів, спрямованих на виявлення і аналіз потенційних загроз [5].

Важливо забезпечити ізольованість досліджуваної зони від сторонніх акустичних та електромагнітних перешкод. Приміщення має бути звукоізольованим, а кабелі – екранованими. Для прямого каналу основна увага приділяється виявленню сигналів, які генеруються технічними засобами безпосередньо під впливом звукових хвиль. Для модуляційного каналу ключовим є визначення параметрів модуляції (частоти, амплітуди), які можуть бути використані для перехоплення мовної інформації.

Важливим етапом в виявленні акустоелектричних каналів витоку інформації є спеціальні перевірки та обстеження, що мають на меті ідентифікацію потенційних каналів витоку, оцінку їхньої небезпеки та розробку заходів для їх нейтралізації. Це комплексна процедура, яка базується на використанні сучасного обладнання, програмних засобів і методик, спрямованих на захист конфіденційної інформації.

Проведення перевірок починається з попереднього аналізу об'єкта. На цьому етапі визначаються можливі джерела витоку інформації, включаючи технічні засоби, які можуть бути вразливими до акустичних, електромагнітних чи інших впливів. Аналізуються планування приміщень, типи використовуваних технічних засобів і комунікаційні мережі [6].

Для визначення першопричини виникнення акустоелектричного каналу витоку інформації необхідно провести комплексний аналіз об'єкта дослідження, враховуючи можливість впливу як електромагнітних, так і акустичних хвиль для прояви електричного відгуку. Основна мета – з'ясувати, чи джерелом небезпечного сигналу є акустична хвиля, а не електромагнітна.

Методика виявлення акустоелектричних каналів витоку інформації включає кілька етапів, які дозволяють визначити природу виникнення сигналу та встановити основні причини витоку.

На першому етапі здійснюється попередній аналіз об'єкта дослідження. Пристрій або система перевіряється на наявність фізичних елементів, які можуть спричинити витік інформації. Аналізуються конструктивні особливості, такі як наявність котушок, конденсаторів чи п'єзоелементів, магнітострикційні елементи, тип матеріалів, з яких виготовлено елементи (феромагнітні, п'єзоелектричні або діелектричні), а також робочі режими пристрою, включно з напругою, частотою та потужністю.

На другому етапі проводиться вимірювання електричних параметрів у контрольованих умовах. Об’єкт ізолюється від будь-якого акустичного впливу і досліджується його робота в звичайних режимах. Вимірюється рівень електричних сигналів, які генеруються пристроєм, перевіряється наявність побічних випромінювань у спектрі частот і електромагнітних завад, що можуть вказувати на внутрішні електричні джерела сигналу.

На третьому етапі моделюється акустичний вплив. Використовується акустичний генератор і випромінювач для створення контрольованого звукового сигналу з заданими параметрами частоти й амплітуди. Об'єкт піддається дії звукових хвиль у різних частотних діапазонах, а результати впливу фіксуються. Реєструються вихідні електричні сигнали, що виникають у пристрої, досліджується їхня амплітудно-частотна залежність та визначається затримка між акустичним впливом і генеруванням сигналу, що дозволяє виявити можливі

механічні ефекти. Зрозуміло, що навіть добре екранована колонка створює деякі електричні та магнітні поля, наведення від яких не повинні вносити похибки у вимірювання [7].

Найпростіший спосіб визначити, що ми спостерігаємо – наведення тест-сигналу від акустичного випромінювача, вимірювального тракту генератор-підсилювач потужності та з'єднувальних кабелів або безпосередньо сигнал АЕП, полягає в закриванні лицьової панелі акустичного випромінювача звукопоглинальною шторкою з метою зміни (зниження) рівня акустичного сигналу, що впливає на технічний засіб (ТЗ), контрольованого за допомогою шумоміра. У цьому випадку наведення через вплив електромагнітного поля генераторного обладнання на технічний засіб, якщо воно існує, залишиться незмінним, тобто показання вимірювального приладу, підключеного до технічного засобу, не зміняться або, в крайньому разі, зміняться непропорційно зниженню рівня акустичного сигналу. У першому випадку вимірювана величина тест-сигналу – це «чисте» наведення, у другому – суміш порівнюваних за рівнями сигналів наведення та акустоелектричних перетворень.

Інший, досить ефективний спосіб визначення достовірності вимірювання саме сигналу акустоелектричного перетворення при тій же вимірювальній схемі полягає в зміні відстані між генераторним обладнанням, включаючи акустичний випромінювач, і досліджуваним технічним засобом. При лінійній зміні сигналу акустоелектричного перетворення залежно від відстані вимірюваний сигнал є наслідком акустичного впливу на технічний засіб, а при зміні вимірюваного сигналу за законом $1/R^2 – 1/R^3$ – наведення через електричні або магнітні поля генераторного обладнання. Цей спосіб зручно використовувати для визначення того, яка з компонент електромагнітного поля переважає у сигналі наведення [8].

Далі проводиться порівняльний аналіз результатів. Якщо електричні сигнали виникають в умовах відсутності акустичних впливів, то першопричина має електричну природу, наприклад, через електромагнітну взаємодію між компонентами або конструктивні недоліки пристрою. Якщо ж сигнали з’являються лише під впливом звукових хвиль, це вказує на акустичну природу явища, наприклад, механічні коливання або п'єзоелектричний ефект. У випадку, коли спостерігається комбінація електричних і акустичних впливів, аналізуються їх характеристики, такі як амплітуда, частота й затримка, щоб встановити домінуючий вплив.

Розуміння природи утворення сигналу наведення визначає і заходи боротьби з ним. При електричному наведенні, як правило, достатньо організувати правильну схему заземлення вимірювального комплексу в цілому. При магнітному наведенні значне зниження можна досягти тільки симетруванням, застосуванням екранованих симетричних кабелів зі скрученими парами та рознесенням елементів вимірювального (генераторного) тракту і технічних засобів.

Ця методика дозволяє не тільки виявити акустоелектричний канал витоку, але й зрозуміти його основні первопричини, що є ключовим для ефективного усунення загроз.

Окремим напрямом є виявлення модуляційних каналів, де високочастотні генератори модулюються акустичними сигналами. Такі канали можуть виникати в складних системах, які включають автогенератори, резонансні контури чи волоконно-оптичні кабелі. Методика передбачає аналіз змін частоти чи амплітуди сигналів, що генеруються пристроями.

Обстеження приміщень також включає виявлення паразитних електромагнітних випромінювань. Наприклад, деякі пристрої можуть випромінювати сигнали, що відображають мовну інформацію. Перевірки такого типу проводяться із застосуванням антен для виявлення сигналів у різних діапазонах частот.

Під час перевірок увага приділяється виявленню пристроїв із мікрофонним ефектом, які можуть діяти як непрямі джерела витоку. Для цього використовуються методики створення акустичного резонансу, що дозволяє точно визначити чутливість пристрою до звукового впливу.

Таким чином, спеціальні перевірки та обстеження є обов'язковим компонентом комплексного захисту інформації. Вони дозволяють виявити приховані технічні канали витоку та

розробити ефективні заходи для їхньої нейтралізації, забезпечуючи надійну конфіденційність даних [9].

3. Рекомендації щодо захисту технічних каналів від витоку за рахунок акустоелектромагнітних перетворень

Рекомендації щодо захисту технічних каналів від витоку інформації через акустоелектромагнітні перетворення спрямовані на мінімізацію ризику перетворення акустичних хвиль у електричні та електромагнітні сигнали, які можуть бути використані для несанкціонованого доступу до даних. Ефективний захист включає технічні, конструктивні та організаційні заходи.

Одним із ключових методів є екранування технічних засобів для зменшення впливу акустичних хвиль. Металеві або композитні екрани можуть ефективно блокувати проникнення звукових хвиль до чутливих елементів пристроїв. Особливо це актуально для гучномовців, трансформаторів і п’єзоелементів. Використання шумопоглинальних матеріалів також є важливим. Акустично поглинаючі панелі чи ізоляційні матеріали навколо пристроїв допомагають знижувати інтенсивність звукових хвиль, які можуть спричинити акустоелектричні перетворення. Оптимізація конструкцій пристроїв дозволяє знизити їх чутливість до акустичних впливів. Наприклад, ущільнення обмоток трансформаторів, використання матеріалів із низьким п’єзоефектом або зміна геометрії деталей може зменшити ефект перетворення [10].

Пасивний захист від мікрофонного ефекту та ВЧ нав'язування здійснюється обмеженням слабких сигналів та фільтрацією або вимкненням лінії, якою поширюється небезпечний сигнал. У схемах обмежувачів використовують зустрічно-паралельно включені напівпровідникові діоди, опір яких для малих (перетворених) сигналів, що становить десятки мегаом, перешкоджає їх проходженню в слаботочну лінію.

Для зниження небезпеки слід застосовувати фільтри на електричних лініях живлення та передачі сигналів. Вони блокують поширення небажаних сигналів поза робочим діапазоном пристрою, що виникають через акустичні перетворення.

Організаційні заходи включають регулярні перевірки приміщень і обладнання на наявність акустоелектричних каналів витоку. Сюди також входить моніторинг акустичного середовища за допомогою спеціалізованих пристроїв, наприклад, спектроаналізаторів, що дозволяють виявляти небажані сигнали [11].

Рекомендується використовувати маскувальні сигнали у приміщеннях із високими вимогами до інформаційної безпеки. Це можуть бути звукові генератори шуму, які створюють фон, що ускладнює роботу акустоелектричних каналів.

Для особливо важливих об’єктів слід розглядати ізоляцію технічних засобів у спеціальних приміщеннях зі звукоізоляційними конструкціями. Це гарантує, що акустичні хвилі не потрапляють до пристроїв, а отже, ймовірність витоку зменшується [12].

Навчання персоналу також відіграє важливу роль. Співробітники повинні знати про потенційні загрози акустоелектричних каналів і дотримуватися заходів безпеки, таких як вимкнення допоміжних пристроїв під час обробки конфіденційної інформації.

Загалом, реалізація цих заходів у комплексі дозволяє значно знизити ризик витоку інформації через акустичні перетворення та забезпечити високий рівень захисту технічних засобів.

Висновки

Акустоелектричні та акустомагнітні канали становлять серйозну загрозу інформаційній безпеці через свою здатність перетворювати акустичну енергію на електричні або магнітні сигнали, що можуть містити конфіденційні дані. Встановлено, що такі канали можуть виникати в технічних пристроях повсякденного використання, зокрема в трансформаторах, п’єзоелементах, телефонних апаратах і датчиках, завдяки прямим або модуляційним ефектам.

Запропоновані методики виявлення акустоелектричних каналів базуються на створенні контрольованих акустичних впливів, аналізі електричних вихідних сигналів та оцінці їхніх характеристик. Важливу роль у дослідженнях відіграють спектроаналізатори, осцилографи та інше сучасне обладнання, яке дозволяє визначати взаємозв'язок між акустичними та електромагнітними параметрами.

Рекомендації з нейтралізації каналів витоку охоплюють технічні, конструктивні та організаційні заходи, включаючи екранування пристроїв, використання шумозаглушувальних матеріалів, оптимізацію конструкцій технічних засобів і впровадження маскувальних сигналів. Особлива увага приділяється організації перевірок і навчання персоналу, що забезпечує високий рівень захисту в умовах зростання технологічних загроз.

Таким чином, виявлення і запобігання акустоелектричним каналам витоку інформації є важливою складовою забезпечення інформаційної безпеки. Складність цих каналів, їх прихований характер і залежність від фізичних властивостей технічних засобів вимагають комплексного підходу до їх виявлення і нейтралізації.

Подальший розвиток технічних засобів аналізу і захисту дозволить знизити ризики витоку інформації, забезпечуючи надійний захист навіть в умовах зростання технічних загроз.

Список літератури:

1. Бобала Ю. Я., Горбатий І. В. Інформаційна безпека. Львів : Львів. політехніка, 2019. 580 с.
2. Голев Д., Кононович В., Хомич С. Методики оцінки інформаційної захищеності телекомунікацій. Одеса : ОНАЗ, 2013. 218 с.
3. Остапов С.Е., Євсеєв С.П., Король О.Г..Технології захисту інформації. Львів : Новий світ-2000, 2023. 678 с.
4. Бузов Г. А. Захист від витоку інформації по технічним каналам. Москва : Гаряча лінія, 2015. 586 с.
5. Солодкий В., Тимофеєв В. Технічні засоби захисту інформації з обмеженим доступом. Харків : ХНУРЕ, 2013. 229 с.
6. Засоби та системи технічного захисту інформації : навч. посіб. для студентів ЗВО / І. Є. Антіпов, А. М. Олейніков, Ю. В. Ликов, В. Д. Кукуш, І. О. Милютченко. 2-е вид., перероб. і доп. Харків : ХНУРЕ, 2024. 266 с.
7. Луньова С.А. Електроакустика. Київ : КПІ, 2020. 198 с.
8. Пашорін В. І., Костюк Ю. В. Безпека інформаційних систем. Київ : Держ. торг.-екон. ун-т, 2023. 376 с.
9. Олейніков А. М. Методи та засоби захисту інформації. Харків : НТМТ, 2014. 298 с.
10. Громико І. А. Загальна парадигма захисту інформації: проблеми захисту інформації в аспектах математичного моделювання. Харків : ХНУ ім. В. Н. Каразіна, 2014. 216 с.
11. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. Київ : ДУТ-КНУ, 2016. 178 с.
12. Іванов В. М., Дмитрієв О. М. Безпека інформаційних систем. Київ : Вид-во "Центр учбової літератури", 2018. 368 с.

Надійшла до редколегії 15.01.2025

Відомості про авторів:

Олейніков Анатолій Миколайович – канд. техн. наук, професор, Харківський національний університет радіоелектроніки, професор кафедри комп'ютерної радіоінженерії та систем технічного захисту інформації; Україна; e-mail: anatoly.oleynikov@nure.ua; ORCID: https://orcid.org/0000-0002-4458-8833

Ликов Юрій Володимирович – канд. техн. наук, доцент, Харківський національний університет радіоелектроніки, доцент кафедри комп'ютерної радіоінженерії та систем технічного захисту інформації; Україна; e-mail: yurii.lykov@nure.ua; ORCID: https://orcid.org/0000-0001-7120-3276

Павленко Ян Сергійович – Харківський національний університет радіоелектроніки, студент кафедри комп'ютерної радіоінженерії та систем технічного захисту інформації; Україна; email:yan.pavlenko@nure.ua; ORCID: https://orcid.org/0009-0000-9378-9319

UDC 621.396; 550.388 **DOI:10.30837/rt.2025.1.220.12**

L.Ya. EMELYANOV, V.O. PULYAYEV, N.O. KUZMENKO, D.A. DZYUBANOV

IMPROVEMENT SOUNDING MODES IN THE INCOHERENT SCATTER TECHNIQUE

Introduction

The study of the state of the Earth's ionosphere occurs in the process of conducting geophysical experiments, when information is obtained about the structure and dynamics of the ionospheric plasma simultaneously in a wide range of altitudes. Currently, this opportunity is provided by the most informative and accurate method, namely the incoherent scatter (IS) technique that includes radio pulse sounding of the ionosphere (in particular, vertically), reception of a signal incoherently scattered by the ionosphere, and its processing [1]. This method makes it possible to obtain the characteristics of the signal: its spectral and autocorrelation functions (ACF) with the subsequent calculation of parameters characterizing the altitude-time behavior of the ionospheric plasma [2]. Using this method, the IS radar, created by Kharkiv Polytechnics [3, 4], simultaneously determines several ionospheric parameters for a number of altitudes (h) and discrete instants of time (t): electron density $N_e(h, t)$, electron $T_e(h, t)$ and ion $T_i(h, t)$ temperatures, plasma drift velocity $V_{dr}(h, t)$, components of the ion composition $\gamma(h, t)$ in the form of the relative content of oxygen $O^+(h, t)$, hydrogen $H^+(h, t)$ and helium $He^+(h, t)$.

The scientific and practical value of these results is very high. They are necessary for solving a significant number of applied problems, including for the purpose of ensuring reliable operation of ground and space radio communication systems, navigation and radar systems. After all, the functioning of many systems depends on the conditions of propagation of an electromagnetic wave in geospace along the route “space object – consumer” [5, 6]. A number of studies examine the operational and technical requirements for such a radar signal, which has increased noise immunity against the background of emerging electromagnetic interference, including in the ionosphere [7, 8].

In general, subsequent geophysical analysis of the obtained parameters of the ionized environment makes it possible to observe variations in the ionosphere caused by both natural and anthropogenic influences, including the appearance of anomalies in the near-Earth environment. All this has a direct impact on critical infrastructure, which determines the relevance of these studies.

Since the main carrier of data containing the necessary information about the state of the ionospheric plasma is ACF (or spectrum) of the scattered signal obtained during experiments, it is necessary to implement further efforts to improve radiation, reception, and signal processing methods aimed at increasing the accuracy and reliability of measuring ionospheric parameters.

This paper considers the case when the carrier of information about the state of the ionosphere is the correlation function $r(\tau)$ of the IS signal. *The purpose* of the work is to improve the process of its determination and analysis. To do this, the article discusses different options for determining the ACF of the IS signal. In particular, various options for coded pulses have been proposed, each of which depends on the goals of the geophysical experiment.

Analysis of Sounding Modes

Ionospheric plasma has a complex structure. This situation indicates the need to use sounding pulses of different durations in order to be able to obtain the ACF shape over a significant range of correlation delays (τ) (preferably up to the appearance of the second zero of the function). On the other hand, proper resolution in height and time must be ensured.

Let us analyze the sounding modes that currently exist while carrying out experimental studies of the ionosphere and that enable to determine these statistical characteristics of the IS signal.

Long Pulse Sounding Mode

The study of the lower ionosphere began and continues today with the use of vertical sounding stations [9–11]. IS radars make it possible to study the ionosphere both below and above its peak.

The sounding mode with a pulse of long duration (T_p, Fig. 1a) is intended for estimating ionospheric parameters along a relatively extended altitude range, over which these parameters change monotonically and insignificantly [12]. In the case of correlation analysis, the procedure for obtaining ACF ordinates involves recording samples of the received IS signal at times t_0, t_1, t_2, ., t_n in the process of propagating the sounding pulse along the height (Fig. 1c). The computer multiplies the corresponding quantized samples, as a result of which, for a selected altitude section of length Δh with a center at height $h_0 = ct_0/2$, an algorithm is implemented to obtain the power $R(0) = u_0^2$ of the IS signal (at time t_0 according to the voltage reading u_0), and also, during the same radar scan (pulse repetition period), n ordinates of normalized ACF are calculated with a correlation lag step $\Delta\tau$: $r(i\Delta\tau) = u_0 u_i / R(0)$, where $i = 1, 2, \ldots, n$ are indices of u_i samples during the scan, c is the speed of light, t_0 is the time delay between transmission and reception of the signal from height h_0. After statistical accumulation of the results of calculating the ACF for this and other heights (usually during a session lasting 1 minute) and subsequent taking into account a number of instrumental factors, these ordinates take the form shown in Fig. 1b (dots). Their discrete nature quite accurately reflects the behavior of a real correlation function, suitable for use in an algorithm for identifying ionospheric parameters using it.

The duration of the sounding signal in this case provides a correlation interval from 0 to τ_2 ($\tau_2 \geq 600$ μs), sufficient for further analysis, where τ_2 is the correlation lag when the correlation function crosses the abscissa for the second time. Therefore, when the radar operating wavelength $\lambda_0 = 2$ m, we actually have $T_p \geq \tau_2 \geq 600$ μs (Fig. 1a) for the case shown in Fig. 1b.

This radio pulse duration corresponds to the height resolution $\Delta h = c\tau_2/2 \approx 100$ km, promotes sufficient statistical accumulation of the results of processing a random IS signal, determines the high energy of the sounding signal and thereby contributes to a sufficient signal-to-noise ratio for studying the ionosphere at altitudes above the ionization maximum. However, such height resolution does not allow us to distinguish in detail the layer structure of the lower ionosphere to study its characteristic features. Such a signal is especially unsuccessful for IS radars with a significant operating wavelength, such as, for example, for the IS radar in Jicamarca (Peru) with $\lambda_0 = 6$ m, $T_p = 3$ ms and $\Delta h = 450$ km. The situation is somewhat more favorable in installations with operating frequencies 400 and 1300 MHz (Hystack, USA and EISCAT, Northern Scandinavia) [2, 13].

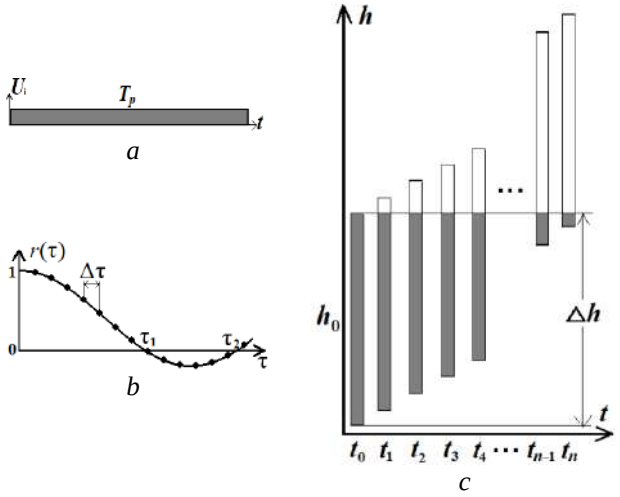


Fig. 1. Envelope of the sounding pulse (*a*), normalized ACF of the scattered signal for the altitude section $\Delta h = cT_p/2$ centered at height h_0 (*b*), and the process of propagation of a long sounding pulse in space (*c*)

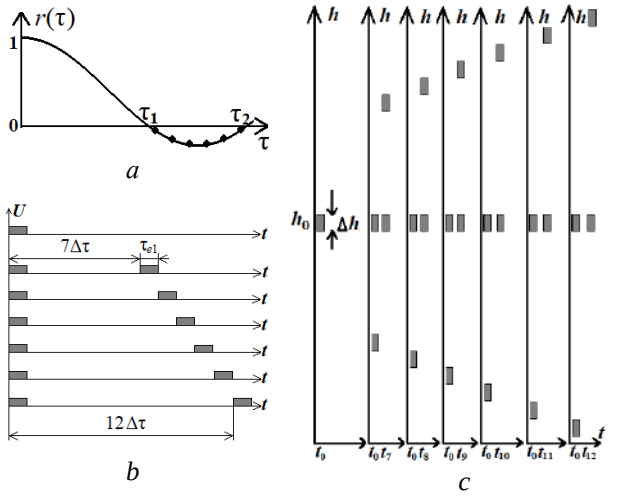


Fig. 2. Normalized ACF of the scattered signal for the section $\Delta h = c\tau_{el}/2$ centered at height h_0 (*a*), envelopes of the elements of the sounding signal (*b*), and the process of alternate propagation of pairs of short pulses in space (*c*)

Mode of Sounding using a Two-Element Signal with Varying Distance between its Elements

To provide better height resolution when studying the lower ionosphere (h < 400 km), the duration of the sounding pulse is reduced [12].

At the same time, they take into account the fact that due to the predominant presence of oxygen ions at these altitudes, the spectrum of the IS signal is narrower than at high altitudes, where light ions are present, the correlation interval increases, and the interval of correlation lags from τ_1 to τ_2 becomes the most informative, that is, from the first to the second zero of the ACF (Fig. 2a). Therefore, the interval of correlation delays from 0 to τ_1 is ignored, which allows the use of sounding signals with a more complex structure.

In this case, short double pulse elements of the sounding signal are emitted (Fig. 2b) with a corresponding interval between them, which varies from scan to scan. At least 7 sounding periods are required [12]. Six periods of double-pulse sounding are intended to determine the ACF ordinates, and one period of sounding with the single pulse of the same duration (for example, 30 μs) is to obtain the power of the IS signal.

The determination of the ACF ordinates consists of the registration of quantized samples u_i of the scattered signal at time instants t_0 (u_{01} when the single pulse propagates along the height), as well as at time instants t_0 і t_7, t_0 і t_8, …, t_0 і t_{12} in the process of alternate propagation of double pulses (Fig. 2c). The computer multiplies the corresponding samples, as a result of which, for the altitude section centered at the altitude h_0, an algorithm for determining the power of the IS signal $\left(R(0)=u_0^2\right)$ is implemented; the ordinates of the normalized ACF calculate for different corresponding sounding periods: $r(i\Delta\tau) = u_0u_i / R(0)$, where i = 7, 8, …, 12 (indices of the instants t_i of voltage readings u_i relative to the corresponding instants t_0 in alternating periods of double-pulse sounding).

The result is a significantly better altitude resolution, which corresponds to $\Delta h = c\tau_{el}/2 \approx 4.5$ km for the pulse element duration presented above. However, such a sounding signal has a significant drawback: the time of statistical accumulation of data for each ordinate of the ACF has decreased by (n+1) times, due to which the calculation error significantly increases for the same duration of the measurement session. To ensure acceptable measurement accuracy, the duration of measurement sessions is increased; and this is associated with a deterioration in temporal resolution, which is not acceptable in the case of studies of fast processes in the ionosphere.

Improving the Structure of Sounding Signals Due to Coding their Elements

As the practice of ionospheric research shows, it is possible to use more complex combinations of elements in the sounding signal to improve resolution. The efficiency of measurements increases significantly if you transmit not an ordinary pair, but several (five or more) elements with certain correctly selected intervals between them. Such composite signals should contribute as much as possible to the effective study of variations in ionospheric parameters, both in height and in time. At the same time, the level of methodological and statistical errors must satisfy the requirements so that the local characteristics of the ionospheric plasma obtained as a result of correlation processing form the basis for further reliable analysis of processes in near-Earth space.

According to this requirement, a computer program was developed to search for such combinations of coded elements in the signal structure that make it possible to calculate the ACF ordinates for a larger number of correlation lags. Fig. 3 shows the results found by the program for options for using codes from 4 to 8 elements. In particular, two combinations are demonstrated (highlighted in dark), providing a uniform correlation lag step, on the basis of which the modernization of the sensing modes discussed above is proposed.

It should be noted that these encoded structures do not make it possible to obtain the power $R(0)$ of the IS signal for the purpose of normalizing the ACF ordinates (a single pulse is needed). This problem was solved in such a way that in each radar sending, when the proposed combinations of elements are emitted, we add another element at the beginning of the radar scan.

To ensure that the signal scattered from it does not interfere with the reception of scattered signals from other coded elements, its radiation is assumed to be in the opposite circular polarization [14]. This will make it possible to select the echo signal received from it in the antenna-feeder device of the IS radar, and transmit it through a separate receiving channel to a separate processing device (see below).

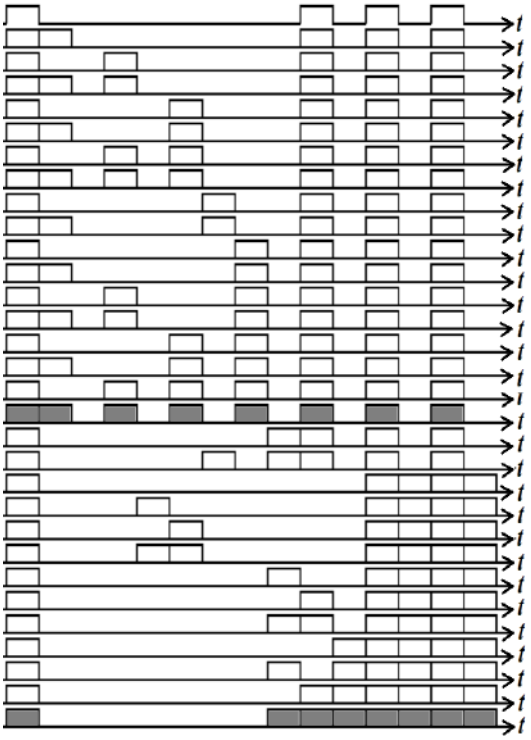


Fig. 3. Results of the search for multi-element coded signals
that provide simultaneous determination of 3 to 7 ordinates of the scattered signal ACF

Multi-Element Pulse Sounding Mode for Lower Ionospheric Altitudes

Based on the above, in order to study the ionosphere at altitudes near the ionization maximum and below, it is proposed to use a sounding signal, the code combination of which is shown in Fig. 4a. Its first element is emitted with the right-hand circular polarization of the radio wave, and the received echo signal is used to determine the power and normalize the ordinates of the IS signal ACF. The remaining elements, intended to determine the correlation coefficients, are emitted with the left-hand circular polarization. In this case, we choose the same duration (τ_{el} = 30 μs) of each code element that ensures good height resolution (Δh). The seven resulting ordinates of the ACF (Fig. 4b) quite informatively reflect the nature of it right-hand side. The procedure for obtaining them is demonstrated in Fig. 4c, which depicts the process of propagating this type of coded sounding signal in space and receiving echo signal at appropriate times by two independent receivers.

In this mode, the computer still multiplies the corresponding quantized samples u_i obtained at times t_i. As a result, for a selected altitude section centered at height h_0, in one radiation cycle, both the powers $\left(R(0)=u_0^2\right)$ of the IS signal (instant t_0) and n = 7 normalized ACF ordinates are calculated: $r[(i-1)\Delta\tau] = u_1 u_i / R(0)$, where i = 9, 10,…, 15 (indices of voltage samples u_i at times t_i).

Multi-Element Pulse Sounding Mode for Upper Ionospheric Altitudes

In a similar way, coded sequences can be used to study the upper altitude range of the ionosphere. To do this, it is proposed to use a sounding signal, the code combination of which is shown in Fig. 4d. The first element still involves the use of right-handed circular polarization of the radio wave, which makes it possible to separately determine the power of the IS signal and, using it, to normalize the ordinates of the ACF, and the remaining elements are intended to determine the correlation coefficients.

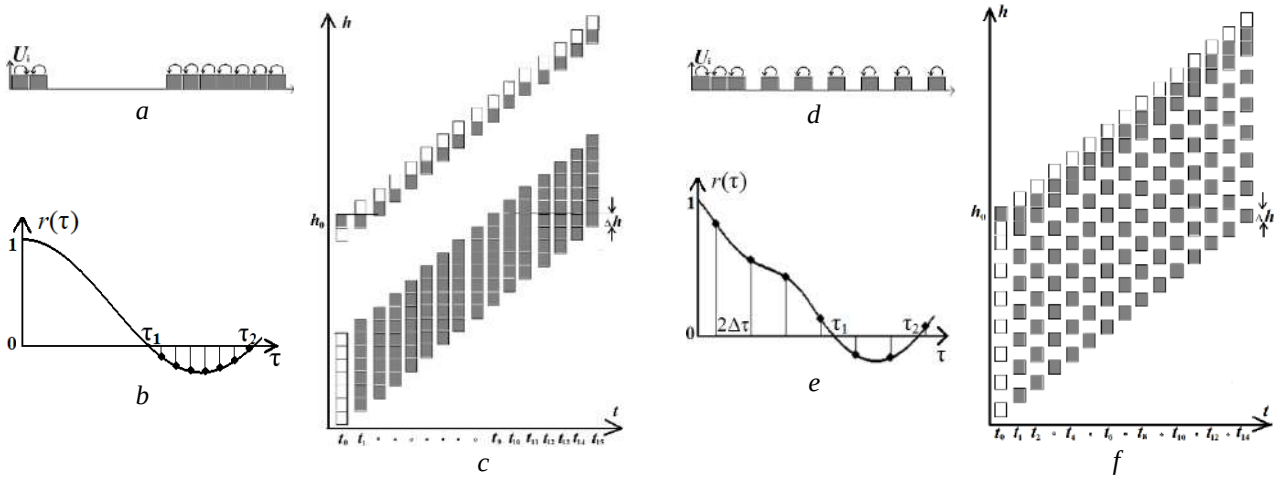


Fig. 4. Envelope of the sounding signal elements (*a*, *d*), normalized ACF of the scattered signal for a narrow altitude section Δh centered at height h_0 (*b*, *e*), and the process of propagation of the coded sounding signal in space (*c*, *f*). The arrows indicate the direction of circular polarization for each element of the sounding signal

The appearance of hydrogen ions, characteristic of high ionospheric altitudes, is additionally reflected in a change in the ACF shape in the range of correlation lags from 0 to τ_1 (Fig. 4e). The ACF becomes informative throughout the entire correlation interval, i.e. from 0 to τ_2. Therefore, in the new mode, the resulting ordinates should reflect the nature of the ACF in a uniform step throughout this interval. This option for determining the ACF ordinates is demonstrated in Fig. 4f, which depicts the case of propagating this type of coded sounding signal in space and subsequent reception of the scattered signal by two independent receivers.

In this mode, the computer, multiplying the corresponding quantized samples u_i, implements an algorithm for calculating the power $\left(R(0)=u_0^2\right)$ of the IS signal (instant t_0) for a selected narrow altitude section with center h_0. In the same radiation cycle, all $n = 7$ normalized ACF ordinates are calculated: $r[(i-1)\Delta\tau] = u_1 u_i / R(0)$, where $i = 2, 4, 6, \ldots, 14$.

It is important to note that this sounding mode makes it possible to average the results obtained over several adjacent altitude sections. Naturally, in order to achieve satisfactory statistical accuracy in determining the IS signal ACF (and, as a consequence, ionospheric parameters), the number of sections for averaging is different for different height ranges. It can also vary depending on the space weather state that affects the shape of the ACF.

Hardware Implementation

The final requirements for the structure of the sounding signal additionally set the features and real capabilities of the radio equipment of the IS radar. Naturally, the computing processor and control system must correspond to the selected structure of the encoded signal.

The proposed manipulation of the direction of radio wave circular polarization involves the use of two transmitter channels and two receiving channels. Their structure may be as follows (Fig. 5).

A circularly polarized sounding signal is generated by a transmit-receive antenna with two orthogonally located vibrators, to which signals from transmitters with a phase difference of 90º are supplied (through the transmit/receive antenna switches AS1 and AS2). Manipulation of the direction of circular polarization is ensured by a corresponding change in the phase of the transmitter excitation signal. When the phase of the excitation signal of the first or second transmitter changes by 90º, a corresponding change occurs in the direction of rotation of the electric field vector of the emitted wave.

Reception of IS signals with circular polarization is carried out by the same vibrators in the pause between radiations of the sounding signal. The signals from vibrators are supplied through antenna switches AS1 and AS2 to the inputs of a ring bridge configured to receive a signal with an operating wavelength λ_0.

The operating principle is based on the fact that a circularly polarized signal can be decomposed into two linearly polarized orthogonal signals, which are received by orthogonal antenna vibrators. When receiving the signal with right-hand circular polarization, signals from vibrators with equal amplitudes and a phase difference of 180° are present at inputs 1 and 2 of the bridge, and the resulting signal is transmitted to output 1 of the ring bridge, while there is no signal at output 2. With opposite (left-hand) circular polarization, the signal is transmitted only to output 2, and there is no signal at output 1. To implement this mode, two controlled phase shifters are designed, through which excitation signals are supplied to the transmitters. Alternating phasing of the transmitter input signals (0°/90° and 90°/0°) is carried out under the control of control system signals. The necessary phasing of received signals with circular polarization is carried out by a phase shifter at input 1 of the ring bridge.

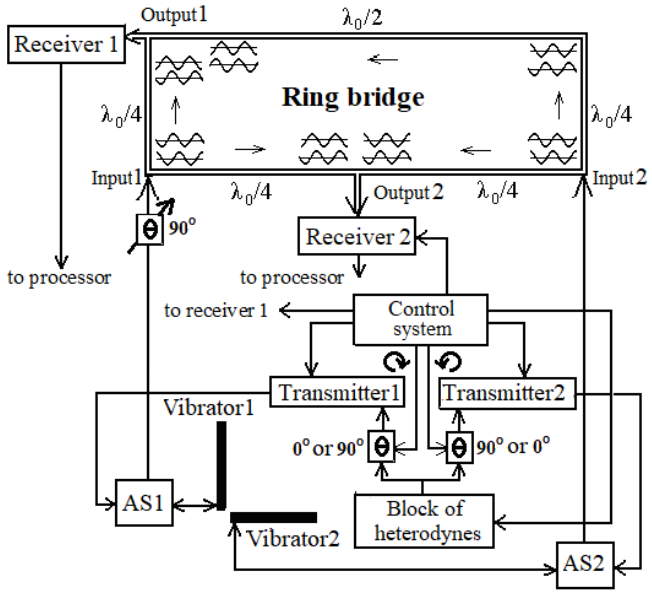


Fig. 5. System for transmitting and receiving signals

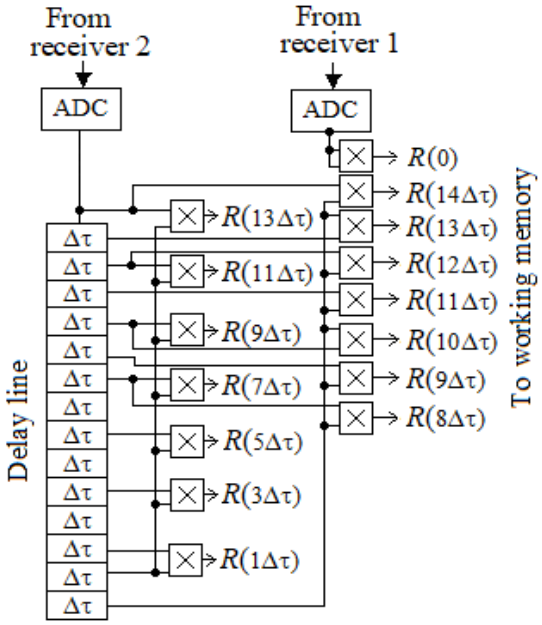


Fig. 6. Multichannel computing processor for calculating the ordinates of the scattered signal ACF

The phase switching signals from the control system are supplied alternately to the phase shifters, as a result of which, during the radiation of the first element (right-hand circular polarization), the phase of the high-frequency oscillation in the path of the first transmitter is shifted by 90° relative to the signal in the path of the second transmitter. In this case, at the inputs of the ring bridge, the signals are received in antiphase, that is, they are compensated at output 2, and their total signal is present at output 1 (see the upper diagrams along the arms of the bridge). And vice versa, when emitting the following pulse elements (left-hand circular polarization), the phase of the high-frequency oscillation in the path of the second transmitter shifts by 90° relative to the signal in the path of the first transmitter. In this case, the signals are received in phase at the inputs of the ring bridge, they are compensated at output 1, and their total signal is present at output 2 (see the lower diagrams). Signals from the outputs of the receivers, in which they were converted, amplified, synchronously detected and filtered, are fed to a multi-channel computing processor, at the inputs of which ADC blocks are installed (Fig. 6).

This processor calculates the powers and autocorrelation functions of the received signal as for the case of the sounding mode shown in Fig. 4 (a, b, c), and for the mode presented in Fig. 4 (d, e, f), depending on the situation. The lag (τ) in the correlation channel is a multiple of the sampling step Δτ [15]. This processor structure makes it possible to obtain results at the outputs of channel multipliers, which vary with altitude. At each instant of time t_j, all ACF ordinates refer to a common height section at altitude h_j. These results fill the corresponding column in working memory, where they are statistically accumulated from scan to scan during the measurement session.

Conclusions

As a result of the analysis, examples of the use of certain modes of pulsed radiation of radio waves with subsequent processing of received signals incoherently scattered by ionospheric plasma are considered. The equipment used is the IS radar designed for remote sensing of near-Earth space. The advantages and disadvantages of the sounding mode with single long radio pulses (intended for studying the upper ionosphere) and the sounding mode with a cyclic sequence of double short pulses with a varying distance between them depending on the radar scan number (intended for studying the ionosphere at altitudes near the ionization maximum and below) are shown.

Options have been proposed for improving the structure of the radio sounding signal by coding its elements, taking into account the nature of scattering in the ionospheric plasma. The results of the search for multi-element coded signals are presented, intended for studies of the lower and upper altitude ranges, providing the calculation of the ordinates of the scattered signal ACF with high resolution in both space and time.

The hardware implementation of sounding modes using these multi-element signals is presented. In particular, a block diagram of the IS radar is presented for working with signals with opposite circular polarizations, which uses for this purpose-controlled phase shifters of the transmitter excitation system, orthogonal antenna vibrators and ring bridge of the receiving feeder path. The structure of the specialized multi-channel correlator for calculating the ACF of a scattered signal using the proposed multi-element coded signals is presented. In general, this makes it possible to transmit and receive signals with various options for the arrangement of their elements, most suitable for specific conditions, as well as to use the manipulation of sounding signals with a change in the direction of the radio wave circular polarization and the separation of received scattered signals in the receiver path.

Thus, the goal of research into further development of the key hardware capabilities of the IS technique, the introduction of new algorithmic approaches aimed at improving the process of obtaining ionospheric information with improved altitude and time resolution of the scattered signal statistical characteristics has been achieved. Using the above approach to the process of searching for coded sequences, in a similar way it is possible to offer many options for the arrangement of elements in the structure of sounding signal, depending on the requirements for the conditions for carrying out radar measurements.

It can be noted that the importance of the conducted research is to obtain better ionospheric information by using the potentially high metrological characteristics of the IS radar. This information is intended for the optimal solution of practical problems in areas covering the activities of space weather systems, the safety of satellite communications and critical infrastructure, problems of positioning objects in space, warning systems for adverse biogeophysical conditions, man-made accidents and disasters.

References:

1. J. Brent Parham; Jason Li; Mark Dickson; Greg Ginet; Philip J. Erickson; Frank D. Lind. Debris plasma density perturbations as seen through a modern collective Thomson scatter radar processing chain // 2024 International Conference on Electromagnetics in Advanced Applications (ICEAA), 02-06 September 2024, doi:10.1109/ICEAA61917.2024.10701844.

2. J. Stamm, J. Vierinen, B. Gustavsson, and A. Spicher. A technique for volumetric incoherent scatter radar analysis // Ann. Geophys. 2023. Vol. 41, is. 1. P. 55–67. https://doi.org/10.5194/angeo-41-55-2023.

3. V. I. Taran. Study of the ionosphere using the incoherent scatter radar in Kharkov // Vestn. KhSPU: Sat. scientific Proceedings, 1999. Vol. 31. P. 3–9.

4. S. V. Panasenko, D. V. Kotov, Y. Otsuka et al. Coupled investigations of ionosphere variations over European and Japanese regions: observations, comparative analysis, and validation of models and facilities // Progress in Earth and Planet Science. 2021. Vol. 8, no. 45. https://doi.org/10.1186/s40645-021-00441-8.

5. N. Beck, J. R. Duval, and P. T. Taylor. GPS processing methods: comparison with precise trilateration // *Journal of Surveying Engineering*. 1989. Vol. 115, no. 2. P. 181–197. https://doi.org/10.1061/(ASCE)0733-9453(1989)115:2(181).

6. S. M. Lichten and R. E. Neilan. Global networks for GPS orbit determination // Proceedings of the Second International Symposium on Precise Positioning with the Global Positioning System. Ottawa, Canada, 1990. P. 164–178.

7. A. Serkov, V. Breslavets, M. Tolkachov, and V. Kravets. Method of coding information distributed by wireless communication lines under conditions of interference // Advanced Information Systems. 2018. Vol. 2, no. 2. P. 145–148. https://doi.org/10.20998/2522-9052.2018.2.25.

8. R. R. Imanov and A. A. Bayramov. Development of field signal centers based on the modern telecommunication technologies // Advanced Information Systems. 2020. Vol. 4, no. 1. P. 136–139, https://doi.org/10.20998/2522-9052.2020.1.21.

9. L. Guo and J. Xiong. Multi-scale attention-enhanced deep learning model for ionogram automatic scaling // Radio Science. 2023. Vol. 58, no. 3. p.e2022RS007566, https://doi.org/10.1029/2022RS007566.

10.M. Fagre, J. A. Prados, J. Scandaliaris, B. S. Zossi, M. A. Cabrera, R. G. Ezquer and A. G. Elias. Algorithm for automatic scaling of the F-layer using image processing of ionograms // IEEE Transactions on Geoscience and Remote Sensing. 2020. Vol. 59, no. 1. P. 220–227. https://doi.org/10.1109/tgrs.2020.2996405.

11.T. Liu, G. Yang, and C. Jiang. High-resolution sporadic E layer observation based on ionosonde using a cross-spectrum analysis imaging technique // Space Weather. Vol. 21, no. 2. Feb. 2023, doi:10.1029/2022SW003195.

12.V. Pulyayev, L. Emelyanov, E. Rogozhkin, and N. Kuzmenko. Hardware method for determination of the characteristics of incoherent scatter signals in radar remote sensing // 2023 IEEE 4rd KhPI Week on Advanced Technology (KhPI Week), October 02-06, 2023, Kharkiv, Ukraine, Conference Proceedings. 2023. P. 227–232. https://doi.org/10.1109/KhPIWeek61412.2023.10312897.

13.G. Wannberg. History of EISCAT – Part 5: Operation and development of the system during the first 2 decades // Hist. Geo Space. Sci. Vol. 13. P. 1–21, https://doi.org/10.5194/hgss-13-1-2022, 2022.

14.L. Emelyanov, E. Rogozhkin, and V. Pulyayev. Features of reception of signals with linear and circular polarization in the incoherent scatter technique // 2022 IEEE 41st International Conference on Electronics and Nanotechnology (ELNANO). 2022. P. 529–534. https://doi.org/10.1109/ELNANO54667.2022.9927099.

15.E. Rogozhkin, V. Pulyayev, and N. Kuzmenko. Peculiarities of using the digital format in computational processing of coherent radar signals // 2022 IEEE 3rd KhPI Week on Advanced Technology (KhPI Week), October 03-07, 2022, Kharkiv, Ukraine., Conference Proceedings, 2022. P. 196–200. https://doi.org/10.1109/KhPIWeek57572.2022.9916377.

Received 06.01.2025

Information about the authors:

Emelyanov Leonid Yakovych – Candidate of Physical and Mathematical Sciences, Senior Researcher, National Technical University "Kharkiv Polytechnic Institute", Leading Researcher, Ukraine; e-mail: leonid.ya.emelyanov@gmail.com; ORCID: https://orcid.org/0000-0002-2117-2675.

Pulyayev Valeriy Oleksandrovych – Doctor of Technical Sciences, Professor, National Technical University "Kharkiv Polytechnic Institute", Leading Researcher, Ukraine; e-mail: v.pulyayev@gmail.com; ORCID: https://orcid.org/0000-0001-6705-2006.

Kuzmenko Nataliia Oleksiivna – Candidate of Historical Sciences, docent, National Technical University "Kharkiv Polytechnic Institute", Associate Professor of the Department of Micro- and Nanoelectronics, Ukraine; e-mail: nkuzmenk@i.ua; ORCID: https://orcid.org/0000-0002-9039-9494.

Dziubanov Dmytro Anatoliyovych – Candidate of Physical and Mathematical Sciences, Senior Researcher, National Technical University "Kharkiv Polytechnic Institute", Professor of the Department of Micro- and Nanoelectronics, Ukraine; e-mail: dzyubanov@gmail.com; ORCID: https://orcid.org/0000-0003-0682-2673.

УДК 621.396.6 **DOI:10.30837/rt.2025.1.220.13**

Д.В. СОКІРКАЄВ, О.А. ЗАРУДНИЙ, канд. техн. наук

ТЕНДЕНЦІЇ РОЗВИТКУ БЕЗДРОТОВОЇ ЛАЗЕРНОЇ ПЕРЕДАЧІ ЕНЕРГІЇ

Вступ

Технологія бездротової передачі енергії привернула значну увагу в останні роки завдяки застосуванню нових матеріалів та технологій для генерації та прийому лазерного випромінення, що покращило характеристики лазера і підвищило ефективність всієї ланки бездротової передачі [1, 2].

Лазерна передача енергії (ЛПЕ) вважається потенційно ефективним способом постачання енергії, особливо в бездротових системах на великі відстані і в суворих небезпечних умовах навколишнього середовища. На відміну від інших методів бездротової передачі енергії (БПЕ), ЛПЕ має свої переваги, наприклад менший розмір пристрою, сфокусований напрямок передачі енергії, відсутність радіочастотних перешкод для існуючих засобів зв'язку і висока щільність потужності.

Завдяки таким перевагам систему ЛПЕ можна використовувати для бездротової передачі енергії в нафтовій промисловості, де така система може допомогти уникнути проблем пов'язаних з електромагнітними перешкодами і високими температурами. Також, за допомогою лазерів можна забезпечити бездротове живлення акумуляторів БПЛА, мобільних пристроїв, робототехніки і аерокосмічних апаратів, що може підвищити надійність і термін їх служби.

Бездротова лазерна передача енергії – це технологія передачі електроенергії, в якій енергія передається за допомогою лазерного променя. Лазерний промінь випромінюється оптичним джерелом і потім поглинається фотоелектричною панеллю для перетворення лазерного променя в електрику, як показано на рис. 1.

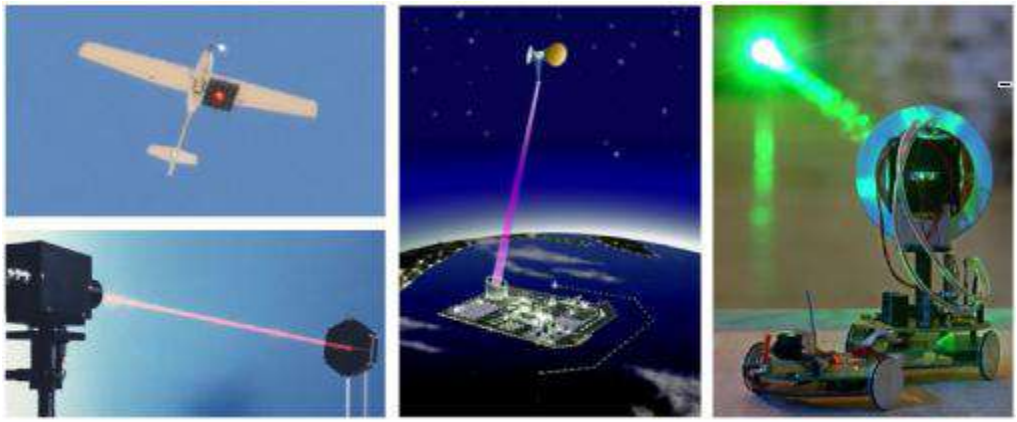


Рис. 1. Використання лазерів в бездротових системах передачі енергії

Загальна структура ЛПЕ зображена на рис. 2. Блок живлення лазера використовується для генерації необхідного і стабільного струму для лазерного випромінювача (ЛВ). ЛВ перетворює електроенергію в лазерне випромінювання, а потім передає його через канал передачі. Приймач складається з фотоелементів, які використовуються для поглинання лазерного випромінювання і перетворення його в струм. Крім того, до системи може бути доданий контролер потужності для випрямлення електричного струму.

Рис. 2. Загальна структура системи бездротової лазерної передачі енергії.

Таким чином, ефективність системи ЛПЕ залежить від потужності лазерного випромінення і ефективності поглинання цього випромінення на приймальній стороні для перетворення його в струм, а також, слід враховувати втрати в середовищі через яке проходить лазерний промінь [1 – 3].

Лазерні випромінювачі, що використовуються в системах ЛПЕ

Лазерний випромінювач відіграє вирішальну роль у системі ЛПЕ. Для забезпечення максимальної ефективності електрооптичного перетворення енергії необхідно використовувати лазер з високою ефективністю. В даний час широко використовуються потужні напівпровідникові лазери завдяки їх компактній і міцній структурі, низькій вартості і простоті експлуатації. Однак такі лазери мають низьку когерентність вихідного лазерного променя і великий кут розбіжності, що робить їх непридатними для безпосереднього використання в бездротовій передачі енергії на великі відстані. Щоб подолати цю проблему, лазерний промінь повинен пройти колімацію, гомогенізацію та інші процеси формування для покращення його однорідності та спрямованості. Дослідження та їх результати щодо ефективності бездротової передачі за допомогою лазерів по відношенню до довжини хвилі наведено у табл. 1 [1 – 16].

Таблиця 1

Довжина хвилі, нм	ККД (%)	Потужність лазера, Вт	Рік
266	28 23 24,7	1,4 23 28,4	1999 2001 2006
355	7 25 35,6	12 1,62 3,1	2000 2009 2011
490	25	1,8	2002
532	14,2 65,2 61 74,6 48 40,9	20 131 62 11,2 32 321	1998 2000 2007 2013 2019 2021
670	42	0,9	2003
808	50 42	8	2003
885	52,4 63	2,1 1,36	2008 2001
912	38,8	6,9	2018
915	72,6	15,3	2022

940	53	200	2013
980	25 27 31 51	0,0012 0,0027 0,0031 3500	1995 1996 2007 2008
1028	45	99,6	2012
1060	44 21	11 6,9	2006 2018
1120	71 53,5	322 25,3	2014 2018
1908	43,5	5,49	2019
2070	31	4,8	2004
2100	42	43	2005

У 2013 р. в [4] розробили лазерні системи на прямих діодах, які могли виробляти багатокіловатні рівні потужності з ефективністю перетворення, яка перевищувала 50 % для промислових застосувань. Подальший прогрес призвів до розробки діодних лазерних платформ, які об'єднали кілька випромінювачів в єдину потужну систему. В цих системах використовувалася спеціалізована оптика, така як волоконні з'єднувачі і коліматори, для об'єднання і фокусування променів, максимізуючи при цьому потужність і ефективність [4]. До 2015 р. лужнопарові лазери з діодним накачуванням досягли потужності 2,5 кВт, причому 90 % загальної потужності було сконцентровано в межах лазерної спектральної лінії, як заначено в [5]. Потужність діодних лазерів з волоконним накачуванням може досягати до 100 Вт за допомогою щільного мультиплексування з поділом по довжині хвилі [5]. У [6] показали, що високояскраві прямі діодні лазери досягли 44 % ефективності перетворення при потужності4 кВт. Тонкоплівкові фільтри були розроблені для полегшення комбінування щільного пучка хвиль з ефективністю 40 % [6]. У 2017 р. стеки лазерних установок виробляли 50-400 Вт, а упоєднання з пластинчастими радіаторами з водяним охолодженням та налаштовані на одну довжину хвилі дозволило досягти навіть рівня потужності 4 кВт [7]. У 2018 р. в [8] запропонували раманівський волоконний лазер на основі раманівського розсіювання до 8 порядків. Максимальна вихідна потужність становила 6,9 Вт, а ефективність накачування – 21 У 2019 р. один широкозонний лазерний діод випромінив 3,5 Вт,а група з восьми таких лазерних діодів – 38 Вт [9]. У 2020 р. 1,5 см силікатне волокно, леговане Nd^{3+}, використали як волокно підсилення для побудови одночастотної волоконної лазерноїсистеми DBR (distributed Bragg reflector – розподілений бреггівський відбивач). Ця система випромінювала центральну довжину хвилі 1120 нм, порогова потужність становила 10 мВт з шириною смуги пропускання 71,5 кГц [10]. Того ж року в роботі [11] продемонстрували безперервний двохвильовий лазер з композитним кристалом $Nd:GdVO_4/Nd:YVO_4$ на довжинах хвиль 1063 і 1064 нм. На довжині хвилі 912 нм використовувалася діодна накачка при цьому регулювання спектрального співвідношення потужностей двох довжин хвиль лазера відбувалось за допомогою зміни температури. Максимальна сумарна вихідна потужність, що генерувалася лазером, становила 4,48 Вт. Ефективність перетворення світло-світло – 38,8 % [11]. У 2021 р. автори роботи [12] виготовили двоступеневі біполярні каскадні 905 нм лазери під назвою VCSELs (Vertical-Cavity Surface-Emitting Laser), ефективність електрооптичного перетворення становила 52,4 %. У 2022 р. було розроблено п'ятиперехідний вертикально-порожнинний поверхнево-випромінюючий лазер з довжиною хвилі 905 нм, а також підготували 19-елементну матрицю з максимальною вихідною потужністю 58,3 Вт, а ККД становило 55,4 % [13]. В [14] представили дизайн, конструкцію та характеристики компактного діодного лазера з розширеною порожниною у конфігурації Літтроу. Він працює на довжині хвилі 780,24 нм з максимальною вихідною потужністю 35 мВт. Результати показали спектральну ширину лінії 340 кГц з використанням гомодинного методу і стабільність частоти 0,47 МГц [14]. В одному з останніх досліджень продемонстрували LD-лазер з ефективністю перетворення потужності, що досягає 72,6 %

при робочій потужності 15,3 Вт і 67,3 % при робочій потужності 30 Вт при температурі радіатора 25 ◦C [15].

Завдяки інтенсивним дослідженням і розробкам лазерні випромінювачі за останнє десятиліття досягли значного покращення потужності, ефективності та щільності випромінення. Досягнення в техніці комбінування променів, методах з'єднання волокон і діодних лазерних платформ зробили можливим виробництво потужних промислових лазерних систем. У майбутньому, ймовірно, відбудуться подальші вдосконалення технологій виробництва і джерел накачування лазеру для підвищення його ефективності.

Високоефективні приймачі лазерного випромінювання

У приймальній частині системи ЛПЕ головним завданням є прийом і перетворення енергетичного сигналу, що передається у вигляді лазерного випромінення, в електричний струм, який може бути використаний для електроживлення приладів або зарядки акумулятора. Для приймання лазерної енергії зазвичай використовують оптично-електроні перетворювачі (ОЕП), спеціально розроблені для ефективного перетворення монохроматичної світлової енергії. В останніх дослідженнях використовують кремній (Si) або арсенід галію (GaAs) як світлопоглинаючі матеріали, оскільки вони підтримуються добре налагодженими виробничими лініями у фотоелектричній промисловості. Нещодавні роботи показали, що ОЕП на основі GaAs досягли вражаючого ККД понад 70 % [30].

Основні параметри цих двох матеріалів наведені в табл. 2 [16].

Таблиця 2

Матеріал	**Довжина хвилі, нм**	**ККД, %**	**Густина потоку енергії, кВт/м^2**
GaAs	810	30-53,5	60-430
Si	950	28-60	110

Кремній є дуже поширеною речовиною, і вартість його виробництва низька. Але ефективність передачі енергії через повітря теж низька через чутливість довжини хвилі до атмосферних втрат. GaAs є типовим напівпровідниковим матеріалом III-V групи, хоча він має таку ж кристалічну структуру, як і Si. Однак, на відміну від кремнію, арсенід галію є матеріалом з прямою забороненою зоною і її ширина становить 1,42 еВ, що є оптимальним для перетворення світлової енергії в електричну.

Переваги GaAs матеріалу над Si [16]:

- більший коефіцієнт поглинання світла, тобто швидше поглинає падаюче світло;
- хороша радіаційна стійкість, особливо в аерокосмічній галузі вплив GaAs нижчий, ніж вплив Si;
- високотемпературна стійкість, матеріали GaAs мають нижчий температурний коефіцієнт і можуть адаптуватися до більш високих робочих температур;
- краща ефективність фотоелектричного перетворення, оскільки GaAs має ширшу ширину забороненої зони і краще відповідає сонячному світлу.

Триперехідний ОЕП на основі арсеніду галію, розроблений компанією Spire Semiconductor, досяг пікової ефективності 42,3 % [17]. Одноперехідні фотоелектричні матеріали мають гарні показники ефективності перетворення енергії. Але вони можуть поглинати лише одну певну довжину хвилі і меншу яскравість падаючого світла ніж багатоперехідні матеріали. Це не сприяє зменшенню розміру приймального пристрою. Для підвищення загальної ефективності фотоелектричного перетворення, враховуючи, що різні типи фотоелектричних матеріалів можуть поглинати різну довжину хвилі світла, дослідники комбінують різні елементи III-V колонок періодичної таблиці відповідно до різної ширини забороненої зони, щоб отримати багатоперехідні фотоелектричні матеріали. Такі матеріали можуть поглинати багато різних довжин хвиль, щоб підвищити загальну ефективність перетворення енер-

гії. У триперехідного фотоелектричного матеріалу InGaP/AsGa/Ga ефективність фотоелектричного перетворення вища, ніж у одноперехідних матеріалів.

У 2006 р. в [24] вивчали характеристики триперехідного фотоелектричного матеріалу InGaP/AsGa/Ga при зміні яскравості падаючого світла і температури. У лабораторії досліджували напругу холостого ходу, струм короткого замикання, коефіцієнт заповнення та ефективність перетворення енергії. Діапазон яскравості падаючого лазерного випромінювання становив від 1 до 200 разів більше сонячного світла, а діапазон температур матеріалу – від 30 до 240 °С. Лабораторні результати показали, що коли температура залишається постійною, зі збільшенням яскравості падаючого лазерного випромінювання, напруга холостого ходу, струм короткого замикання і ефективність перетворення потужності також зростають. Якщо яскравість залишалася постійною, при підвищенні температури напруга холостого ходу, коефіцієнт заповнення і ефективність фотоелектричного перетворення зменшувалися, а струм короткого замикання зростав [24].

У 2008 р. [25] вивчали електричні властивості триперехідних GaAs матеріалів C1MJ і C2MJ в діапазоні температур від ~0 до 120 °С і падаючого світла в діапазоні від 1 до 1000 разів більше сонячного світла. Результат показав, що зі збільшенням яскравості падаючого світла ефективність фотоелектричного перетворення спочатку зростає, а потім падає. Підвищення температури призводить до зниження ефективності фотоелектричного перетворення, а коли температура була постійною, то пік ефективності фотоелектричного перетворення був при 500-кратному перевищенні сонячного світла [25].

У 2010 р. дослідники з Хебейського технологічного університету протестували триперехідний фотоелектричний матеріал GaAs. Експеримент показав, що максимальна ефективність фотоелектричного перетворення склала 22,24 %, а максимальна вихідна потужність – 23,56 Вт за умови 500-кратного освітлення сонячним світлом. Крім того, при підвищенні температури на 1 °С струм короткого замикання зменшився до 1,9 мА [26].

У 2013 р. Шанхайський університет науки і технологій успішно побудував математичну модель матеріалу GaAs з трьома переходами і теоретично проаналізував вплив зміни яскравості падаючого світла та температури, виміряв напругу холостого ходу і ефективність матеріалу. З результатів видно, що збільшення яскравості падаючого світла збільшує напругу холостого ходу та ефективність перетворення. Зі збільшенням температури напруга холостого ходу і ефективність перетворення знижуються [27].

У [28] дослідили, як різні температури впливають на фотоелектричні матеріали GaAs, під час експерименту діапазон температур становив від ~5 до 170 °С. Триперехідні фотоелектричні матеріали GaAs на основі Ga знижують ефективність в умовах високих температур (25+^{o}C), як показано в результаті [28].

В [31] представили одно-фотоелектричний ОЕП з використанням структур $Al_xGa_{1-x}As$-GaAs, досягнули вражаючого ККД 46 % при лазерному опроміненні 0,5 Вт/см^2 з довжиною хвилі 850 нм. Продовжуючи цей прогрес, в [32] отримали підвищений показник ККД до 52,1 %, використовуючи $Al_{0.3}Ga_{0.7}As$ з довжиною хвилі806 нм. Більшість дослідників при розробці ОЕП покладаються на GaAs завдяки надійному виробничому досвіду у фотоелектричній промисловості. Нещодавні звіти показують, що ОЕП в парі з лазерами на довжині хвилі 858 нм досягли значного ККД на рівні 68,9 % [33]. У той же час, поєднання ОЕП з лазерами на довжині хвилі 808 нм призвело до ще більш високого показника ККД – 74,7 % [30]. Крім того, ретельна заміна атомів ґратки на індій дозволяєточно налаштувати ширину забороненої зони відповідно до ближнього інфрачервоного спектру.

У [29] досліджували оптимізацію фотоелектричного матеріалу InGaAs, за допомогою якого можна було досягти ефективності перетворення енергії >50 % при довжині хвилі падаючого лазерного випромінювання 1064 нм. Як наслідок, ОЕП на основі InGaAs продемонстрував ККД в 50,8 % [29].

Також ЛПЕ використовується для бездротової передачі під водою. Для підводного застосувань потрібні синьо-зелені лазери, в яких ширина забороненої зони поглинача повин-

на бути налаштована на ~2,2 еВ. Хоча GaInP з узгодженою шириною забороненої зони можна отримати епітаксійним вирощуванням і отримати 40 % ККД при довжині хвилі 532 нм [34], його висока виробнича вартість і крихка природа створюють серйозні перешкоди для отримання комерційних підводних ОЕП. У цьому випадку основним кандидатом був би органічно-неорганічний гібридний матеріал перовскіт. За допомогою цього матеріалу можливо регулювати енергетичну смугу відповідно до довжини хвилі підводного лазера, таким чином можна збільшити ефективність поглинання лазерної енергії [34]. В [36] продемонстрували перспективність перовскітних матеріалів для підводної передачі енергії, в яких під дією лазера з довжиною хвилі 532 нм було отримано ККД близько 43,02% [36]. Існують також звіти про застосування органічних елементів для ОЕП, наприклад, органічні лазерні перетворювачі потужності демонструють ефективність 36,2 % для лазерного випромінення з довжиною хвилі 660 нм і густиною потоку випромінення 9,5 мВт/см^2 і забезпечують бездротову мікропередачу енергії з потужністю 0,5 Вт на відстані двох метрів, з використанням матеріалу PBDB-TF-Btp-eC9 [37].

Таким чином, завдяки зазначеним вище дослідженням можна переконатися, що матеріал GaAs є частим вибором серед фотоелектричних матеріалів для передачі енергії. Він має найвищу ефективність фотоелектричного перетворення на даний час, має невеликий розмір пристрою та зручне застосування. Більше того, багатоперехідний матеріал GaAs може адаптуватися до багатохвильового лазерного випромінювання, тим самим зменшуючи вимоги до випромінювача і підвищуючи енергоефективність.

Досягнуті результати

На шляху розвитку ЛПЕ було багато перепон, але і було чи мало досягнуто значного прогресу за підтримки науково-дослідних робіт, таких як розробка високоефективних лазерів, збагачення теорії передачі енергії та розробка пристроїв, що приймають енергію. Як результат, ефективність передачі енергії в бездротових системах з часом значно покращилася.

У [21] використали Nd:YAG з довжиною хвилі 532 нм і вихідною потужністю 5 Вт для керування невеликим автомобілем, оснащеним матеріалом InGaP. Відстань передачі становила 300 м, а ефективність перетворення енергії фотоелектричного матеріалу – 25 %. В японському університеті Кінкі використали вихідну потужність оптичного випромінювача 200 Вт з довжиною хвилі 808 нм для опромінення фотоелектричних матеріалів на машині для польотів повітряних приладів. Фотоелектричні матеріали були виготовлені з восьми фотоелектричних батарей GaAs площею 28 см^2 кожна. Максимальна вихідна потужність становила близько 42 Вт, а ефективність перетворення падаючих фотонів в електрони становила 21 % [22]. NASA встановило фотоелектричні матеріали на основі кремнію для живлення та керування прототипу альпініста, використовуючи систему телескопів для передачі безперервного лазерного випромінювання з довжиною хвилі 1030 нм і потужністю 8 кВт. Фотоелектричний масив, який складався з 333 монокристалічних кремнієвих чіпів площею 1 м^2. Використання кремнієвих концентраторів з лазером 1030 нм виявилося ефективним, досягнувши ефективності 35 % для окремих елементів, хоча остаточна конструкція масиву працювала погано [23].

У 2019 р. у Військово-морській лабораторії США провели другий етап проєкту "Power Transmitted Over Laser" (PTROL) на військово-морській експериментальній базі в штаті Меріленд. Під час експериментів було передано 2 кВт лазерної потужності на відстань 325 м, в результаті було отримано близько 400 Вт електричної потужності [38].

У 2021 р. шведська телекомунікаційна компанія Ericsson та американська компанія PowerLig Aerospace успішно продемонстрували повністю бездротову базову станцію 5G з використанням лазерної технології PowerLig Aerospace для передачі 100 Вт потужності на відстань 300 м. Обидві компанії назвали цю демонстрацію важливою віхою на шляху до кінцевої мети передачі кіловат енергії на великі відстані. Демонструючи, як можна розподіляти енергію бездротовим способом, щоб забезпечити розгортання мережі та варіанти викорис-

тання, PowerLig Aerospace Technologies of America заявила, що технологія лазерної бездротової зарядки задовольняє потребу в швидкому живленні бездротових базових станцій для розгортання в надзвичайних ситуаціях [39].

У 2022 р. DARPA (Defense Advanced Research Projects Agency) США опублікувало запит на інформацію щодо модифікації літаків-заправників для підзарядки дронів. Ідея полягає в тому, щоб розробити капсулу під назвою "бортова енергетична свердловина", яку можна було б встановити під крилами діючих літаків-заправників ВПС США, таких як KC-135 і KC-46, для бездротової зарядки БПЛА за допомогою лазера. Капсула потребуватиме потужності лазера щонайменше 100 кВт і відповідної системи терморегуляції. DARPA вважає, що "повітряні енергетичні свердловини" можуть стати частиною енергетичної мережі, яка дозволить Міністерству оборони динамічно розподіляти енергетичні ресурси для забезпечення більшої гнучкості військових операцій [40].

Однією з найважливіших сфер застосування ЛПЕ виявилися космічні сонячні енергетичні супутники/станції (SSPS) [41]. Ці системи використовують геостаціонарні супутники на навколоземній орбіті (ГСО) для збору і перетворення сонячного випромінювання в електричну енергію. Зібрана енергія потім трансформується і передається до визначеного місця прийому на Землі за допомогою мікрохвильового або лазерного випромінювання. У порівнянні з традиційними фотоелектричними джерелами живлення, система SSPS дозволяє отримувати енергію в режимі 24/7, будучи при цьому географічно незалежною. Таким чином, її завершення забезпечить значну кількість енергії на планеті, тим самим пом'якшивши зростаючу енергетичну кризу.

На додаток до SSPS, ще одним важливим застосуванням ЛПЕ є лазерна передача енергії для дослідницьких апаратів на поверхнях планет [42]. Малим космічним апаратам або наземним засобам пошуку корисних копалин може бути важко генерувати достатньо енергії для роботи потужних радіостанцій і приладів корисного навантаження, які можуть знадобитися для завершення майбутніх місій. Малі супутники і наземні марсоходи можуть потребувати нетрадиційного способу виробництва енергії під час сонячних затемнень або під час роботи в затінених ділянках поверхні планети. Для вирішення цієї проблеми супутник, що знаходиться в полі зору Сонця, використовується як ретрансляційна станція для бездротової підзарядки енергії для цих посадкових пристроїв [43].

Лазер може передавати промінь безпосередньо в точне місце, що забезпечує мобільність і простоту базової станції та безперервну передачу енергії. Марсохід може безперервно працювати в кратерах і на зворотному боці Місяця. Сучасні місяцеходи та марсоходи використовують радіоізотопний термоелектричний генератор (RTG) для підзарядки енергії. Однак, через обмежені розміри марсоходів, малі RTG не можуть задовольнити довгострокові потреби у підзарядці енергії [44]. Крім того, використання ракет для перевезення великої кількості радіоізотопів є дуже ризикованим. Тому використання систем SSPS для передачі накопиченої енергії сонячного світла за допомогою лазерів для бездротової підзарядки марсохода має значний потенціал у місячному або марсіанському середовищі.

Висновки

Зроблено загальний огляд розвитку системи ЛПЕ. Дослідження систем ЛПЕ мають величезне значення для майбутнього енергетичної галузі, і очікується, що вони не тільки змінять наявні методи передавання, а й розширять відповідні сфери застосування, бездротових технологій. Хоча концепція бездротової лазерної передачі енергії була запропонована ще в 1960-х роках, ЛПЕ все ще знаходиться на початковій стадії, оскільки показники кожного модуля ЛПЕ стримуються його технічним обмеженнями. В даний час технологія ЛПЕ в основному спрямована на потреби військових та космічних застосувань. До них належать живлення супутників, передача енергії для планетарних роверів і аварійна підзарядка безпілотних літальних апаратів (БПЛА).

Проаналізовано аспекти лазерного випромінювача, фотоелектричних матеріалів та їх ефективність перетворення енергії. Технолгія БПЕ на основі лазеру має невеликий розмір, простий у реалізації та використанні, має значне вирівнювання променя і високу ефективність перетворення фотоелектричної енергії. Точність, стабільність і типи хвиль впливають на ефективність роботи системи ЛПЕ, що може бути одним з напрямків підвищення ефективності. На ефективність лазерної передачі сильно впливає середовище передачі; ефективність передачі у вакуумі і в повітрі або воді дуже відрізняється і в кінцевому підсумку впливає на розподіл інтенсивності випромінення на приймальному кінці. Незважаючи на найбільш оптимізовані конструкції ЛПЕ, на поточному етапі ефективність повної системи ЛПЕ досягає лише близько 20 – 25 %. Таким чином, дослідження слід зосередити на розвитку та оптимізації окремих модулів для підвищення ефективності всієї ланки ЛПЕ.

Слід зазначити, якщо одного лазеру недостатньо для задоволення потреби в енергії, можна розглянути можливість використання діодної лазерної системи. Проте такий підхід ускладнить виготовлення випромінювального пристрою, що призведе до значного підвищення ціни. Інший спосіб досягнення кращої продуктивності лазерних випромінювачів це підвищенні ефективності променя накачування. Можна цього досягти за допомогою джерела накачування. Крім того, можна вжити заходів для зменшення дефектів в епітаксійних кристалах, таких як підвищення чистоти сировини, поліпшення якості кристалічної ґратки, епітаксійних структур і більш точний контроль товщини і концентрації легування. Ці стратегії допомагають покращити якість кристалів і потужність лазера. Слід також зазначити, що ефективність лазерного перетворення чутлива до температури [24 – 28], і велика кількість тепловиділення є неминучим наслідком роботи потужних лазерів. Для забезпечення оптимального температурного контролю лазера важливо використовувати високоефективні охолоджувачі і корпуси з високим коефіцієнтом теплопередачі. Ці методи сприяють підвищенню ефективності лазерної передачі і прокладають шлях для подальших досліджень і розробок в галузі ЛПЕ.

Для підвищення ефективності прийому лазерного випромінювання необхідно використовувати високоефективні ОЕП, адаптовані до довжини хвилі лазера; ОЕП працюють за принципом, подібним до фотоелектричних пристроїв, але вони перетворюють енергію конкретно на цільовій довжині хвилі лазера. Щоб підвищити ефективність перетворювача лазерного випромінювання на одній довжині хвилі, можна використовувати дизайн мікропорожнин для оптимізації діелектричної проникності на довжині хвилі лазера [12 – 14].

Іншим важливим фактором є вибір матеріалу відповідно до середовища, в якому використовується ЛПЕ. Наприклад, у космосі ОЕП виготовлені з GaAs, є більш придатними, ніж ОЕП, виготовлені з матеріалів Si. У підводному середовищі з низькою щільністю окрім GaInP, також можна використовувати гібридні халькогенідні матеріали на основі органічних і неорганічних сполу [33 – 36]. Проте в багатьох дослідженнях використовуються матеріали на основі GaAs, тому цей матеріал є одним з найпоширеніших для поглинання оптичного [43 – 33].

Таким чином, ЛПЕ є перспективною технологією для бездротової передачі енергії, яка може застосовуватися як у військовому, так і в цивільному секторах. Через технічні обмеження окремих модулів, ефективність повної системи ЛПЕ становить лише 20 – 25 %. Проте, завдяки подальшим дослідженням в галузі лазерів і ЛПЕ, очікується, що в недалекому майбутньому ефективність повного каналу ЛПЕ перевищить 30 %.

Список літератури:

1. Electrodynamic Approach to Designing WPT Systems with Accounting for Non-system Interactions / A.I. Luchaninov, D.V. Gretskih, A.V. Gomozov, V.A. Katrich, M.V. Nesterenko // IEEE 2nd Ukraine Conference on Electrical and Computer Engineering UKRCON-2019. 2019. P. 80–85.

2. Modeling the WPT system with the multistate transmitting subsystem / D. Gretskih, A. Luchaninov, A. Gomozov, V. Katrich, M. Nesterenko // Proceedings of the 2020 IEEE Ukrainian Microwave Week. 2020. P. 110–115.

3. Xu W., Wang X., Li W., Li S., Lu C. Research on test and evaluation method of laser wireless power transmission system // Eurasip Journal Advances Sigignal Processing. 2022. Vol. 2022 (1). P. 1–10.

4. Rohner M., Wagner L. Fiber-coupled high-power diode-lasers with highest radiance // Proceedings of the 2013 High Power Diode Lasers and Systems Conference, HPD. 2013. P. 36–39.

5. McCormick D., Irwin D., Stapleton D. Ultra-narrow spectral linewidth diode lasers for the pumping of alkalis // Proceedings of the 2015 High Power Diode Lasers and Systems Conference (HPD). 2015. P. 25–26.

6. Huang R. K., Samson B., Chann B. Recent progress on high-brightness kw-class direct diode lasers // Proceedings of the 2015 High Power Diode Lasers and Systems Conference, HPD. 2015. P. 29–30.

7. Kleine K., Balu P. High-power diode laser sources for materials processing // High Power Diode Las. 2017. P. 3–4.

8. Dong J., Zhang J., Yang X., Pan W., Cui S. High order cascaded Raman random fiber laser with high spectral purity // Opt. Express. 2018. Vol. 26 (5). P. 5275–5280.

9. Krasnoshchoka A., Xu J., Thorseth A., Thorseth A. High luminous flux laser lighting using single-crystal Ce, YAG phosphor // Proceedings of the 2019 IEEE High Power Diode Lasers and Systems Conference, HPD. 2019. P. 31–32.

10. Wang Y., Wu J., Zhao O. Single-frequency DBR Nd-doped fiber laser at 1120 nm with a narrow linewidth and low threshold // Opt. Lett. 2020. Vol. 45 (8). P. 2263–2266.

11. Nadimi M., Onyenekwu C., Major A. Continuous-wave dual-wavelength operation of the in-band diode-pumped Nd, GdVO4/Nd, YVO4 composite laser with controllable spectral power ratio // Appl. Phys. B. 2020. Vol. 126 (5). P. 75.

12. Pan G., Xun M., Zhao Z. High slope efficiency bipolar cascade 905 nm vertical cavity surface emitting laser // IEEE Electron. Dev. Lett. 2021. Vol. 42 (9). P. 1342–1345.

13. Fei Y.Z., Li Y., Tang Z.T. High-power, multi-junction, 905 nm vertical-cavity surface-emitting laser with an AlGaAsSb electron-blocking layer // Opt. Lett. 2023. Vol. 48 (8). P. 2142–2145.

14. Alvarez J., Pimienta J., Mercado E., Sarmiento R. An extended laser cavity centered at 780 nm for high-resolution laser spectroscopy applications // Las. Phys. 2023. Vol. 33 (5). P. 550.

15. Liu Y., Yang G., Zhao Y. 48 W continuous-wave output from a high-efficiency single emitter laser diode at 915 nm // IEEE Photonic Tech. L. 2022. Vol. 34 (22). P. 1218–1221.

16. Han M. Research on photoelectric conversion efficiency of GaAs concentrated cell under laser irradiation: dissertation. Nanjing University of Aeronautics and Astronautics, 2018. URL: https://kns.cnki.net/kcms/detail/detail.aspx?dbcode=CMFD&dbname=CMFD201901&filename=1019800556.nh&uniplatform=NZKPT&v=sFiHMT7eJYbThD4O4CbBMLlncq0HXdeU9F7R2QzvnVxHVzxWYMSpjhbuYNccxBuo3

17. King R. R., Bhusari D., Larrabee D., Liu X.-Q. Solar cell generations over 40% efficiency // Progress in Photovoltaics: Research and Applications. 2012. Vol. 20 (6). P. 801–815.

18. Ermer J., Jones K. R., Hebert P., Pien P. Status of C3MJ+ and C4MJ production concentrator solar cells at Spectrolab // 2011 37th IEEE Photovoltaic Specialists Conference. 2011. P. 941.

19. Miyazawa K., Watanabe Y. Shiseido develops innovative technology to convert ultraviolet light into light that brings about beneficial effects on the skin // Shiseido Company. 2024. URL: https://corp.shiseido.com/en/news/detail.html?n=00000000003256

20. Carroll D. A brighter idea: Wake Forest receives patent for new fiber solar cells // Wake Forest News. 2010. URL: https://news.wfu.edu/2010/04/08/a-brighter-idea-wake-forest-receives-patent-for-new-fiber-solar-cells / Steinsiek F., Foth W. P., Weber K. H. Wireless power transmission experiment as an early contribution to planetary exploration mission // Proceedings of the 54th International Astronautical Congress. 2003. P. 169–176.

21. Kawashima N., Takeda K., Yabe K. Application of the laser energy transmission technology to drive a small airplane // Chinese Optics Letters. 2007. Vol. 5 (101). P. 109–110.

22. Becker D. E., Chiang R., Keys C. C. Photovoltaic concentrator-based power beaming for space elevator application // AIP Conference Proceedings. American Institute of Physics, 2010. Vol. 1230 (1). P. 271–281.

23. Nishioka K., Takamoto T., Agui T., Kaneiwa M., Uraoka Y., Fuyuki T. Annual output estimation of concentrator photovoltaic systems using high-efficiency InGaP/InGaAs/Ge triple-junction solar cells // Solar Energy Materials and Solar Cells. 2006. Vol. 90 (1). P. 57–67.

24. Kinsey G. S., Hebert P., Barbour K. E., Krut D. D., Cotal H. L., Sherif R. A. Concentrator multijunction solar cell characteristics under variable intensity and temperature // Progress in Photovoltaics: Research and Applications. 2008. Vol. 16 (6).P. 503–508.

25. Nishioka K., Sueto T., Uchina M., Ota Y. Detailed analysis of temperature characteristics of an InGaP/InGaAs/Ge triple-junction solar cell // Journal of Electronic Materials. 2010. Vol. 39 (6). P. 704–708.

26. Wang Z., Zhang H., Liu Y. Theoretical and experimental analysis of electrical characteristics of InGaP/GaAs/Ge three-junction GaAs photovoltaic cells // Proceedings of the CSEE. 2013. Vol. 33 (27). P. 168–174.

27. Zimmermann S., Helmers H., Tiwari M. K., Paredes S. A high-efficiency hybrid high-concentration photovoltaic system // International Journal of Heat and Mass Transfer. 2015. Vol. 89. P. 514–521.

28. Kalyuzhnyy N. A., Emelyanov V. M., Evstropov V. V., Mintairov S. A. Optimization of photoelectric parameters of InGaAs metamorphic laser (λ = 1064 nm) power converters with over 50% efficiency // Solar Energy Materials and Solar Cells. 2020. Vol. 217. P. 100-107.

29. Fafard S., Masson D. P. 74.7 % efficient GaAs-based laser power converters at 808 nm at 150 K // Photonics. 2022. Vol. 9 (8). P. 579.

30. Merz J. L., Logan R. A., McBride P. L., Sergent A. M. GaAs double-heterostructure photodetectors // Journal of Applied Physics. 1977. Vol. 48 (8). P. 3580–3587.

31. Olsen L. C., Huber D. A., Dunham G., Addis F. W. High-efficiency monochromatic GaAs solar cells // The Conference Record of the 22nd IEEE Photovoltaic Specialists Conference. 1991. P. 419–424.

32. Helmers H., Lopez E., Hohn O., Lackner D. 68.9% efficient GaAs-based photonic power conversion enabled by photon recycling and optical resonance // Rapid Research Letters. 2021. Vol. 15 (7). P. 2100113.

33. Steinsiek F. Wireless power transmission experiment as an early contribution to planetary exploration missions // International Astronautical Congress. 2003. P. 169–176.

34. Li Q., Zheng Y., Guo X., Zhang G., Ding G. Interface engineering enhances the photovoltaic performance of wide bandgap FAPbBr3 perovskite for application in low-light environments // Adv. Functl. Mater. 2023. Vol. 33 (40). P. 1–23.

35. Guo X., Chen X., Li Q., Zhang G., Ding G., Li F. High-efficiency widebandgap perovskite solar cells for laser energy transfer underwater // Energy Technology. 2023. Vol. 11 (7).

36. Wang Y., Zheng Z., Wang J., Bi P., Chen Z. Organic laser power converter for efficient wireless micro power transfer // Nature Commun. 2023. Vol. 14 (1). P. 5511.

37. Cavallaro E. Researchers transmit energy with laser in historic power-beaming demonstration // U.S. Naval Research Laboratory. URL: https://www.nrl.navy.mil/Media/News/Article/2504007/researchers-transmit-energy-with-laser-in-historic-power-beaming-demonstration/

38. Irving M. Wireless power transmission tech demo uses lasers to run 5G station // New Atlas. URL: https://newatlas.com/energy/wireless-power-transmission-ericsson-powerlight

39. Uppal R. DARPA Airborne Energy Well seeks laser propulsion on Aircrafts to power Rechargable Unmanned Aerial Systems – International Defense Security & Technology // International Defense Security & Technology. URL: https://idstch.com/military/air/darpa-airborne-energy-well-seeks-laser-propulsion-on-aircrafts-to-power-rechargable-unmanned-aerial-systems/ .

40. Cavallaro E. Researchers transmit energy with laser in ‘historic’ power-beaming demonstration // U.S. Naval Research Laboratory. URL: https://www.nrl.navy.mil/Media/News/Article/2504007/researchers-transmit-energy-with-laser-in-historic-power-beaming-demonstration/.

41. Abdullah S., Mulles P. J. S., Amaya R. E. A new adaptive wireless power transfer solution for use with space rovers and vehicles // 2022 IEEE international conference on wireless for space and extreme environments (wisee). 2022. P. 49–54.

42. Sanders M., Kang J. S. Utilization of Polychromatic Laser System for Satellite Power Beaming // 2020 IEEE Aerospace Conference, Big Sky. 2020. P. 1–7.

43. Kerslake T. W., El-Genk M. S. Lunar Surface-to-Surface Power Transfer, AIP Conf. Proc. 964. 2008. P. 466–473.

Надійшла до редколегії 18.01.2025

Відомості про авторів:

Сокіркаєв Денис Вадимович – аспірант, Харківський національний університет радіоелектроніки; Україна; e-mail: denys.sokirkaiev@nure.ua; ORCID:https://orcid.org/0009-0003-4659-529X

Зарудний Олександр Андрійович – канд. техн. наук, Харківський національний університет радіоелектроніки, доцент кафедри радіотехнологій інформаційно-комунікаційних систем; Україна; e-mail: oleksandr.zarudnyi@nure.ua; ORCID: https://orcid.org/0000-0002-1612-0256

УДК 621.372 **DOI:10.30837/rt.2025.1.220.14**

С.М. КУХТІН, канд. фіз.-мат. наук, Є.П. ФЕДОРЕНКО

ОСОБЛИВОСТІ ПОБУДОВИ СИСТЕМ ПЕРЕДАВАННЯ ДАНИХ ВІДКРИТИМИ ОПТИЧНИМИ ТРАСАМИ

Вступ

На сьогодні більшість бездротових систем і мереж передавання даних працюють, як правило, в радіохвильовому діапазоні. Однак історія розвитку телекомунікаційних технологій демонструє поступовий перехід до більш високих несівних частот, зокрема, від кілогерц – з часів упровадження радіозв'язку до терагерцового діапазону сучасних ВОЛЗ-систем. Досягнення у галузі волоконно-оптичних ліній зв'язку і супутні переваги використання оптичного діапазону сприяють значному інтересу щодо дослідження можливостей застосування оптичного діапазону для передавання інформаційних сигналів у відкритому просторі. Це, насамперед, продиктовано обсягом даних, які можуть бути передані, зважаючи на збільшення пропорційно несійної частоти. Враховуючи, що більшість систем і методів у радіодіапазоні вже досягли теоретичної межі, перехід до оптичної області спектру стає абсолютно неминучим. Особливості оптичного діапазону і лазерних джерел випромінювання, що активно застосовуються у цій сфері, відкривають низку унікальних можливостей, серед яких підвищена безпека передавання даних, можливість передавання пакетів оптичних сигналів на великі відстані, впровадження квантової криптографії тощо.

Галузі, в яких можуть застосовуватись системи передавання даних відкритими оптичними трасами, є досить різноманітними. До них, насамперед, можна віднести міські і локальні телекомунікаційні мережі, допоміжні канали передавання даних для наявної телекомунікаційної інфраструктури, швидке впровадження широкосмугового зв'язку у разі надзвичайних подій або у випадку, коли звичайні оптоволоконні мережі не можуть бути застосовані, передавання відеосигналів високої роздільної здатності, телемедицину, широкосмуговий супутниковий зв'язок тощо.

Незважаючи на переваги та широкі перспективи систем передавання даних відкритими оптичними трасами, існує ціла низка труднощів, які стримують їхній розвиток. До них, передусім, слід віднести вплив атмосфери та погодних умов на спотворення сигналу, а також високі вимоги щодо юстування оптичних елементів і необхідності застосування трекінгових систем. Однак у даний час активно ведуться дослідження з метою подолання цих обмежень.

У цій статті опрацьовано стан сучасних систем передавання даних відкритими оптичними трасами, історію їхнього розвитку, структуру побудови мереж та приймально-передавального обладнання. Проведено аналіз впливу атмосферних умов на передавання оптичних сигналів, розглянуто різноманітні методи підвищення ефективності передавання даних за допомогою цих систем.

Оптичні комунікації відкритими оптичними трасами. Історія розвитку

Використання оптичного випромінювання для передавання інформації не є новою ідеєю, і застосовується в тому чи іншому вигляді досить давно. Насамперед, можна навести приклад сигнальних вогнів, геліографів, оптичних телеграфів як примітивних систем передавання оптичних сигналів відкритими оптичними трасами. У 1880 р. Гремом Белом було винайдено фотофон, який використовував голосову модуляцію відбитого сонячного випромінювання, зі зворотнім перетворенням приймачем сигналу [1]. Ідеї, сформовані Гремом Белом, обмежено застосовувались у військових розробках протягом 30–40 років із використанням ламп розжарювання як джерел випромінювання. Поява лазерних джерел і світлодіодів сприяла поштовху для більш активного розвитку систем передавання інформації оптичним випромінюванням. Так, уже в 1960 р. було продемонстровано на практиці передавання телевізійного сигналу за допомогою рубінового лазера на відстань понад 25 миль [2]. У 1962 р.

дослідниками з лабораторії Лінкольна MIT було передано телевізійний сигнал на відстань близько 48 км із використанням *GaAs* світлодіода [3]. Протягом декади було проведено низку досліджень з використанням різноманітних лазерних джерел, які показали на той час досить сумнівну цінність комерційного використання. Більш детальний огляд цих систем можна знайти в роботі [3]. Тут можна виділити передавання даних групою Хьюга у 1962 р. за допомогою *He-Ne* лазера на відстань 30 км. У 1963 р. було продемонстровано передавання акустично-модульованого сигналу на відстань 190 км Electro-optic Systems, а також телевізійного сигналу з полосами 1,7 і 5 МГц. У 1970 р. Nippon Electric Company продемонструвала дуплексну комерційну лінію зв'язку на відстані 14 км за допомогою *He-Ne* лазера 632,8 нм [4]. З появою та впровадженням ВОЛЗ інтерес до систем із відкритими оптичними трасами значно зменшився, обмежуючись, насамперед, військовим і космічним застосуванням. Враховуючи гостру необхідність щодо розроблення надійних високошвидкісних систем передавання даних у космосі, за останні десятиріччя дослідники досягли досить суттєвого прогресу в цій сфері. Національне управління з аеронавтики та досліджень космічного простору продемонструвало оптичну систему передавання даних у своїй програмі Mars Laser Communication Demonstration [5]. Європейське космічне агентство реалізувало експеримент з міжсупутникового зв'язку з використанням напівпровідникового лазера [6] Починаючи з 1990 р. дослідження в галузі оптичного атмосферного і космічного зв'язку значно зросли з появою комерційно доступних платформ. Тут можна навести приклади передавання зображень під час олімпійських ігор 2020 р. у Сіднеї, запуск супутника Optical Inter-orbit Communications Engineering Test Satellite компанії JAXA у 2015 р., а також супутника Terra SAR-X з модулем LCT у 2007 р., що продемонстрував практичні швидкості передавання даних понад 5,5 Гбіт/с [7]. Останні роки також ознаменувались появою комерційних зразків обладнання для передавання даних у видимому діапазоні [8, 9]. Слід також згадати дослідження, пов'язані із забезпеченням оптичним зв'язком наносупутників [10], а також наявність наземних систем із швидкостями передавання даних понад 100 Гбіт/с [11].

Застосування систем з відкритими оптичними трасами та їхні переваги

Фактично передавання інформації відкритими оптичними трасами може реалізовуватись для більшості сфер залежно від відстані й умов застосування, починаючи від з'єднань оптики вільного простору в інтегральних схемах, побудови локальних інформаційних мереж, закінчуючи супутниковим зв'язком. Тут можна виділити окремі категорії:

1) оптичні з'єднання надкороткої дії, наприклад, оптичні зв'язки між елементами або схемами оптичних і гібридних обчислювальних систем [12];

2) оптичні з'єднання малого і середнього радіусу дії, а саме – побудова локальних бездротових оптичних мереж, а також забезпечення зв'язку між транспортними засобами [13 – 15];

3) оптичні з'єднання дальньої дії, для впровадження муніципальних інформаційних мереж;

4) оптичні з'єднання надвеликої дії, наприклад, забезпечення міжсупутникового зв'язку, дальніх інформаційних з'єднань у космосі [16].

У цій статті більш детально розглянуто особливості застосування оптичних інформаційних мереж середньої і дальньої дії в атмосфері, зважаючи на значний інтерес з комерційної точки зору і чималі труднощі практичної реалізації. Такі системи, здебільшого, застосовують відкриті атмосферні оптичні траси значної довжини, що перевищує декілька кілометрів, для забезпечення високошвидкісного передавання даних. У порівнянні з системами радіозв'язку вони характеризуються наявністю широкого каналу передавання даних. На сьогодні комерційно доступні системи, що забезпечують швидкісне передавання понад 100 Гбіт/с, експериментальні системи наближаються за швидкістю передавання даних до волоконно-оптичних ліній зв'язку, в тому числі із застосуванням мультиплексування з поділом довжин хвиль [17]. Загалом системи з відкритими оптичними трасами будуються з використанням лазерних

джерел. Характерні параметри лазерного випромінювання дають низку переваг, серед яких високий показник захищеності каналу передавання даних, невразливість до електромагнітних завад, можливість мультиплексування інформаційних сигналів. Наявність чималої кількості лазерних джерел та оптоелектронних компонентів ВОЛЗ значно розширюють можливість впровадження таких систем. Крім того, враховуючи наявну компонентну базу, системи з відкритими оптичними трасами можуть використовуватись як доповнення до наявних ВОЛЗ мереж, у разі, коли оптоволоконний кабель не може бути прокладений до кінцевого абонента.

Серед ключових напрямків застосування систем з відкритими оптичними трасами можна виділити такі:

– побудова високошвидкісних локальних мереж. У даний час міська офісна чи житлова забудова значної щільності потребує широкого каналу передавання даних, до того ж у деяких випадках існує необхідність забезпечення значного трафіку передавання даних між окремими будівлями (багатоповерхові офісні будівлі);

– відеоспостереження. Відеоспостереження все частіше використовується для забезпечення громадської безпеки, контролю дорожнього руху тощо. Відеосигнал генерує значний потік інформації, особливо якщо мова йде про відеосигнал високої роздільної здатності. В умовах, коли фізично об’єднати камери в дротовій мережі неможливо і бездротовий зв’язок не забезпечує необхідної швидкості передавання даних, системи з відкритими оптичними трасами можуть стати чудовою альтернативою;

– забезпечення додаткових каналів передавання даних між вишками мобільного зв’язку. Як правило, інфраструктура мобільного зв’язку має додаткові канали, як дротові, так і бездротові, для забезпечення надійного функціонування мережі. Зростаюча кількість абонентів і високі швидкості інтернет-трафіку потребують збільшення каналу передавання даних між окремими базовими станціями. Враховуючи, що існуючі технології мають обмеження, системи з відкритими оптичними трасами можуть забезпечити потреби у збільшенні інформаційного трафіку таких мереж;

– упровадження міжсупутникового зв’язку. Сучасні супутникові мережі обмежені пропускною спроможністю радіоканалу. Передавання даних оптичним каналом може суттєво розширити можливості супутникових систем. Крім того, оптичний канал також може бути реалізований між супутниками і приймально-передавальними станціями на Землі;

– швидке впровадження інформаційних мереж. Під час надзвичайних ситуацій та катастроф наявні інформаційні мережі можуть бути пошкоджені, причому їхнє відновлення та ремонт можуть бути неможливі чи потребувати значного часу. Системи передавання даних відкритими оптичними каналами, навпаки, можуть бути встановлені швидко, забезпечуючи високошвидкісний зв'язок в екстремальних умовах;

– упровадження новітніх методів захисту інформації. Ґрунтуючись на законах квантової механіки, квантова криптографія пропонує радикально інше рішення для шифрування та сприяє безпрецедентній безпеці передавання даних. Насамперед, розглядаються системи квантової криптографії, що функціонують у поєднанні з діючою волоконно-оптичною інфраструктурою;

– забезпечення мереж у важкодоступних районах. У деяких ландшафтах дуже складно забезпечити розгортання інформаційних мереж. Це можуть бути як гірські райони, так і райони з агресивним кліматом або райони морських акваторій. Використання супутникового зв’язку має обмеження з точки зору доступного інформаційного каналу та вартості наданих послуг. У цьому випадку впровадження систем із відкритими оптичними трасами стає єдиною логічною альтернативою.

Основи передавання інформації відкритими оптичними трасами

Типова схема передавання містить передавач модульованого оптичного сигналу через атмосферний канал і приймач, що забезпечує збір і трансформацію оптичного сигналу на

електричний. Схема типового приймально-передавального обладнання представлена на рис. 1. Сучасні системи передавання оптичних сигналів працюють, здебільшого, в ближньому ІЧ-діапазоні 800–1600 нм. Вибір цього діапазону продиктовано оптичною прозорістю в атмосфері, за виключенням поглинання деякими молекулярними газами [18]. Так, на полосах 850, 1060, 1250, 1550 нм типове згасання складає лише близько 02 дБ/км. Існують також експериментальні системи в УФ і середньому ІЧ-діапазонах (10 мкм), що демонструють менші помилки, що пов'язані з блокуванням сигналу, впливом сонячного випромінювання та кращими характеристиками передавання даних у тумані [19, 20].

Передавач складається з джерела оптичного випромінювання, оптичного модулятора, оптичного підсилювача (опціонально), пристрою для кодування оптичного сигналу, оптичних елементів для формування оптичного променю. Спершу інформаційний сигнал кодується, потім проводиться модуляція оптичного сигналу. Як джерела випромінювання найбільшого використання набули лазерні діоди, в деяких випадках застосовують звичайні світловипромінювальні діоди. Так, *VCSEL* лазерні діоди є найбільш популярними джерелами на 850 нм, а на 1550 нм – Фабрі–Перо та *DFB* лазерні діоди. Враховуючи доступність останніх як розповсюджених джерел ВОЛЗ, їхню температурну стабільність, а також відносну безпеку для здоров'я людини, саме *DFB* лазерні діоди вважаються найбільш перспективними джерелами для передавання оптичних інформаційних сигналів на значні відстані.

У системах з відкритими оптичними трасами для приймального обладнання застосовують дві розповсюджені схеми, зокрема, некогерентну та когерентну. Некогерентні схеми ґрунтуються на прямому детектуванні амплітудної модуляції оптичного сигналу. Когерентні схеми є більш складними, в яких разом із амплітудою враховується частота та фаза оптичного сигналу. В самому приймачеві використовується окреме джерело оптичного сигналу для змішування з сигналом, який приймається, перед детектуванням. Когерентні системи демонструють значно кращі характеристики з огляду на вплив фонового шуму, врахування згасання сигналу, викликаного турбулентністю повітряних мас, і кращої чутливості приймача [21].

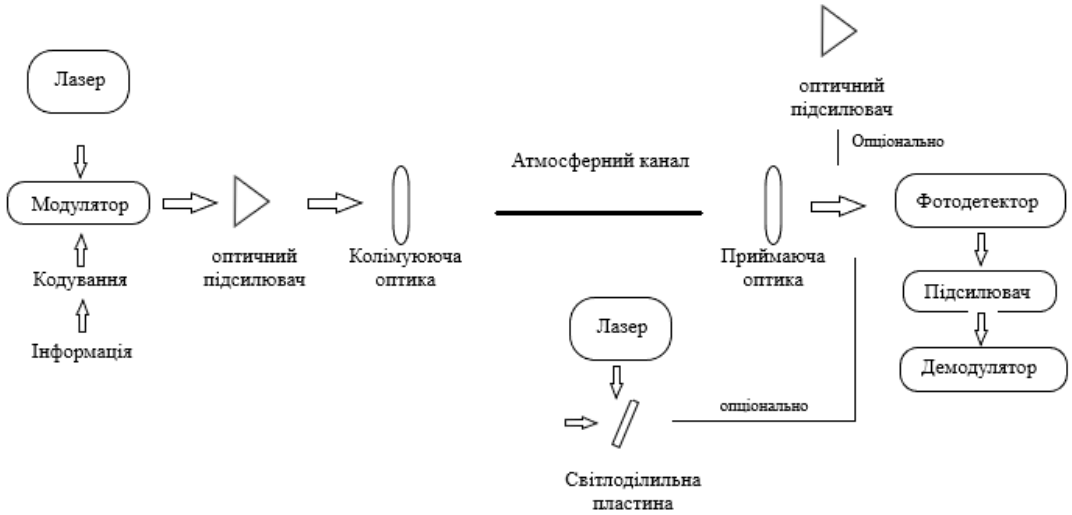


Рис. 1. Схема приймально-передавального обладнання

Некогерентні системи є більш розповсюдженими, зважаючи на більш просту конструкцію та нижчу вартість. Приймальна апаратура некогерентних систем містить оптичний фільтр, фокусувальну оптику та фотодетектор. Струм з фотоприймача підсилюється операційним підсилювачем з низьким шумом, а також використовується низькочастотний фільтр для обмеження рівнів теплового і фонових шумів. В якості фотоприймачів найбільшого розповсюдження набули *Si, InGaA*s, *Ge* фотодіоди, завдяки високій квантовій ефективності та високій швидкісті спрацювання. Вибір матеріалу фотодіодів залежить від спектрального діапазону, на 850 нм використовують *Si* фотодіоди, що мають найбільшу чутливість, водночас на 1550 нм застосовують *InGaAs* діоди. З огляду на тип фотодіодів перевага надається

P-i-N, а також лавинним фотодіодам. Перший тип фотодіодів прийнятний для побудови систем обмеженої дальності (декілька км). Такі обмеження зумовлені рівнями теплового шуму. Для систем зі значною дальністю передавання даних пріоритетним стає використання лавинних фотодіодів завдяки високій чутливості. Недоліком таких фотодіодів є значні показники шуму, котрі доцільно враховувати під час проєктування електричних схем підсилення та оптимізації відношення сигнал/шум.

У деяких роботах для підвищення чутливості систем на 1550 нм пропонувалось застосування оптичних підсилювачів, зокрема, на основі ербієвих волокон і напівпровідникових оптичних підсилювачів [22, 23]. Слід зазначити, що використання таких пристроїв значно ускладнює приймальну систему. Крім того, додатково виникають проблеми, пов'язані із юстуванням оптичних елементів з оптичним волокном, а також наявністю додаткового шуму спонтанної емісії, що може значно погіршити показники приймача. Втім, якщо показники системи переважно обмежені електронним шумом, використання оптичних підсилювачів може бути доцільним.

Вплив на канал передавання даних

Передавання оптичного сигналу в атмосфері пов'язано з впливом низки чинників, здебільшого, втратами, що спричинені геометрією променю, юстуванням оптичних елементів, атмосферним поглинанням, впливом турбулентних потоків на згасання, зовнішніми шумами.

1. Втрати, пов'язані з юстуванням оптики та механічними впливами.

Суттєвий вплив на оптичну потужність, що реєструється, чинить розходження оптичного променю. Водночас на хід оптичного променю можуть суттєво впливати атмосферні вихори, особливо на значних відстанях передавання даних [24]. Під час застосування в міській забудові вібрації можуть позначатися на юстуванні оптичних елементів, враховуючи досить малу діаграму спрямованості, а також вузьке поле зору оптики для приймання. Для простих систем, які працюють на малих відстанях і не устатковані системами трекінгу, простим рішенням є збільшення діаграми спрямованості передавача. Крім того, для компенсації цих впливів було запропоновано використання просторових частково когерентних Гаусових променів, геометричної оптимізації променю, а також використання джерел з перебудовою довжини хвилі, насамперед квантово-каскадних лазерів [25 – 27]. Однак системи, що застосовуються для передавання даних на значні відстані, повинні бути устатковані системою трекінгу та корекції для їхньої ефективного функціонування. В декількох роботах було проведено дослідження впливу помилок юстування на роботу таких систем, отримано аналітичні вирази для бітових помилок, а також вплив цих чинників на системи, що застосовують кодування сигналу [28 – 30].

2. Згасання оптичного сигналу в атмосферному каналі.

Існує три основні чинники, що вливають на згасання оптичного сигналу в атмосфері: поглинання, розсіювання і вплив атмосферної турбулентності на розповсюдження оптичного сигналу.

Поглинання оптичного випромінювання можна описати законом Бугера–Ламберта:

$$I = I_0 e^{-\alpha CL}, \qquad (1)$$

де I – інтенсивність, яка реєструється; I_0 – інтенсивність на виході; α – коефіцієнт поглинання; C – концентрація; L – довжина оптичної траси.

Атмосферне поглинання, перш за все, спричинено наявністю деяких газів, присутніх в атмосфері, насамперед, водяної пари, метану, оксиду азоту, кисню, азоту, двоокису вуглецю. Спектр поглинання для цих компонентів показано на рис. 2 [31].

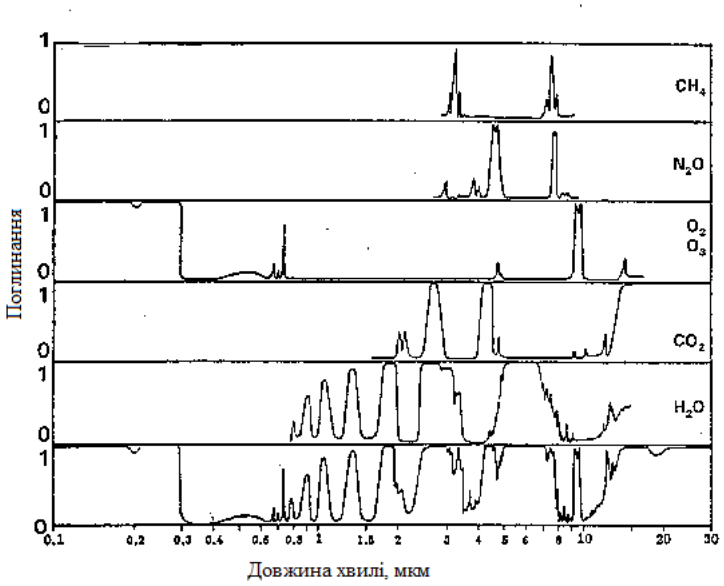


Рис. 2. Спектр поглинання атмосферних газів

Ці гази мають сильні лінії поглинання в *ІЧ*-області спектру та видимій області спектру зі значно меншою інтенсивністю [18]. Наприклад, метан має сильні лінії поглинання в ближній *ІЧ*-області на смугах з центрами 890 нм, 1650 нм, 2,3 мкм, 3,36 мкм. Зважаючи на це, іноді може бути важливим вибір лазерного джерела (робочої довжини хвилі), особливо на наддовгих оптичних трасах, де навіть незначні концентрації можуть значно впливати на згасання оптичного сигналу. У цілому, на найбільш розповсюджених довжинах хвиль, які застосовуються в системах з відкритими оптичними трасами, а саме 850 і 1550 нм, оптичний атмосферний канал можна вважати оптично прозорим [32].

Значно більший вплив на оптичний сигнал чинить розсіювання. Для оцінки розсіювання можна враховувати параметр характеристичного розміру:

$$x_0 = 2\pi r / \lambda\,, \tag{2}$$

де r – радіус частки; λ – довжина хвилі випромінювання.

Зазвичай цей параметр у ближній ІЧ-області перевищує одиницю. Так, для $x_0 = 1$ можна використати теорію Мі і неселективне розсіювання в залежності від розмірів розсіювальних часточок [32, 33]:

$$\beta_{мі} = \frac{3{,}91}{V}\left(\frac{0{,}55 мкм}{\lambda}\right)^a, дБ / км\,, \tag{3}$$

де V – відстань; λ – довжина хвилі випромінювання; a – розмір частки;

$$\beta_{несел.} = \pi a^2 N_a Q_{розс.}(a/\lambda) \tag{4}$$

де a – розмір частки; λ – довжина хвилі випромінювання; N_a – розподіл розсіювальних часток (см$^{-3}$); $Q_{розс.}$ – коефіцієнт розсіяння (як правило, дорівнює ~2).

Переважний вклад у розсіювання вносять краплі води в повітрі. З практичної точки зору під час дощу і легкого снігу вплив на оптичний сигнал не дуже великий і зрідка перевищує згасання 3 дБ/км [34]. Коефіцієнт розсіювання значно зростає, коли розмір крапель стає співставним з довжиною хвилі, як у випадку туману. Експериментально встановлено, що саме туман є домінантним чинником згасання оптичного сигналу, що може становити до 90 % втрат на відстанях вже 50м. Вплив цього чинника майже не залежить від довжини хвилі в

ближній ІЧ-області спектру. Іншим чинником, залежним від довжини хвилі зі значно меншим впливом, є розсіяння на частках смогу [35]. З огляду на це, в місцях з частими опадами і туманами може бути доцільним впровадження систем, які функціонують у видимому діапазоні.

3. Вплив турбулентності.

В ясний день, коли ефекти поглинання і розсіювання майже не мають впливу на оптичний сигнал, присутній інший вагомий чинник – згасання оптичного сигналу внаслідок турбулентності оптичних мас. Неоднорідності температури і тиску уздовж оптичної траси, що викликані нагрівом від сонячного світла і вітром, впливають на показник заломлення. Ці неоднорідності (турбулентності) викликають випадкові флуктуації амплітуди і фази оптичного сигналу. Це може суттєво впливати на роботу систем передавання даних з відкритими оптичними трасами, особливо на великих відстанях передавання.

Однак серед цих видів спотворень власне спотворення інтенсивності є найбільш значним. Воно відоме як сцинтиляційний вплив. Вплив атмосферної турбулентності стає найбільш показовим опівдні або опівночі через максимальну різницю температур, створювану в цей час, хоча ефект турбулентності погіршує якість оптичного сигналу протягом усього дня. Втрата атмосферної турбулентності, викликана сцинтиляцією, згідно з [32]:

$$\rho(L) = 2 \times \sqrt{23{,}17 \times k^{7/6} \times \times C_n^2 \times L^{11/6}}, дБ, \quad (5)$$

де k – хвильове число; L – довжина оптичної траси; C_n^2 – структурний параметр заломлення.

Структурний параметр заломлення є досить складним показником, який залежить від географічного місцезнаходження, висоти над рівнем моря, часу дня і в середньому становить 10^{-17}–10^{-13} м$^{-2/3}$ [36].

Загалом врахування турбулентностей на передавання оптичного сигналу і моделювання цього процесу є доволі складною і нетривіальною задачею. Більш детально ознайомитись з цією тематикою можна в роботах [37 – 39].

Слід також відмітити дослідження впливу форми пучка на якість передавання сигналу за умов турбулентності. Встановлено, що для значних відстаней передавання даних добре себе рекомендує кільцевий розподіл, водночас, за малих відстаней найкраща робота спостерігається для косинусоїдально-гаусівського розподілу інтенсивності [40, 41].

Методи покращення характеристик оптичних систем передавання даних

Найбільшою проблемою під час реалізації передавання даних відкритою оптичною трасою є згасання сигналу внаслідок атмосферних турбуленцій. У теперішній час існує низка методик, які застосовуються для компенсації цього чинника. Серед них, насамперед, можна виділити просторове розділення, розділення передавання сигналів, використання систем з декількома виходами/входами.

Просторове розділення може бути впроваджене шляхом використання декількох діафрагм приймача, використання декількох променів для передавання сигналу, або поєднання обох методів.

Найпростіше рішення для мінімізації впливу турбулентного згасання – використання великої діафрагми приймальної оптики. Цей метод називається апертурним усередненням, він є ефективним, якщо діафрагма приймальної оптики є більшою за кореляційну довжину згасання $\sqrt{\lambda L}$, де λ і L – довжина хвилі і довжина оптичної траси [42]. Метод усереднення за апертурою досить добре вивчений і широко застосовується у системах із відкритими оптичними трасами. Він показує значне зниження рівня впливу синциляції при середніх і великих довжинах оптичних трас. Також зниження згасання може бути досягнуто при використанні декількох малих діафрагм. Кожна приймальна діафрагма матиме менше апертурне усереднення, але поєднаний сигнал з декількох діафрагм матиме деякий ступень просторово-

го розділення. Загалом системи з декількома діафрагмами показують значно ліпші результати роботи, ніж з однією, при однаковому ефективному розмірі діафрагми. Системи з однією великою діафрагмою набули більшого розповсюдження внаслідок простоти реалізації, водночас, системи з декількома використовуються в умовах значних турбулентностей повітря. Ще одним недоліком систем з декількома діафрагмами є необхідність використання фотодіода з великою активною областю і пов'язану з цим понижену швидкість передавання даних.

Простішим методом реалізації розділення сигналу є тривіальна передача одного і того сигналу декількома окремими променями. Цей метод також показує досить непогану ефективність і дозволяє, наприклад, за типових умов, отримати підвищення рівня сигнал/шум під час використання двох і трьох променів на 5 і 7,5 дБ порівняно з системами, що використовують лише один промінь [43]. Також можливе застосування декількох джерел випромінювання, що працюють на різних довжинах хвиль.

Окрім методів розділення, ефект впливу турбулентності може бути мінімізований з використанням адаптивної оптики [44]. Цей метод включає використання сенсорів хвильового фронту і деформованих дзеркал для компенсації впливу турбулентностей. Слід відзначити, що використання цього методу на сьогодні досить ускладнене, а ефективне застосування можливе на невеликих оптичних трасах.

Висновки

Розроблення і впровадження новітніх систем оптичного передавання даних відкритими трасами є досить складною і нетривіальною задачею. Проте впровадження таких систем відкриває широкі перспективи для побудови інформаційних мереж наступного покоління, що задовольнятимуть широке коло сучасних телекомунікаційних потреб. Оптичні технології в майбутньому зможуть замінити деякі технології бездротового передавання даних, і, в деяких випадках, стати їхнім доповненням. На теперішній час широко застосовуються системи з швидкостями передавання даних понад 10 Гбіт/с, і наявна тенденція до їхнього збільшення. Переваги оптичного каналу можуть також дати сильний поштовх для розгортання високошвидкісних мереж у місцях де ВОЛЗ і безпровідні мережі радіозв'язку побудувати проблематично. Інший перспективний напрямок розширення каналів передавання даних між супутниками в космосі і приймальною апаратурою на землі. Також характерною особливістю є відсутність інтерференції між інформаційними каналами, що притаманна радіозв'язку. Таким чином, впровадження таких систем є перспективним для побудови локальних мереж високої щільності, а також забезпечення передавання даних між транспортними засобами.

Для систем із відкритими оптичними трасами обмежувальним чинником, насамперед, є вплив турбулентних потоків повітря на розповсюдження оптичного сигналу. На даний момент ведуться активні роботи з вивчення, моделювання та розроблення методів мінімізації цього чинника. Тут треба відмітити роботи щодо вивчення форми пучка і досить успішних методик просторового розділення, використання багатоканальних систем і методів адаптивної оптики.

Список літератури:

1. D. Phillipson. Alexander Graham Bell | The Canadian Encyclopedia // Thecanadianencyclopedia.ca, Jul. 28, 2010. https://www.thecanadianencyclopedia.ca/en/article/alexander-graham-bell

2. H. Henniger. An introduction to free-space opticalcommunications // Journal of Radio Engineering. 2010. Vol. 19, no. 2. P. 203–212.

3. D. L. Begley. Free-space laser communications: a historical perspective // The 15th Annual Meeting of the IEEE Lasers and Electro-Optics Society. Glasgow, UK, 2002. Vol.2. P. 391–392. doi: 10.1109/LEOS.2002.1159343.

4. W. S. Rabinovich et al. Free-space optical communications research and demonstrations at the US Naval Research Laboratory. 2015. Vol. 54, no. 31. P. F189–F189. doi: https://doi.org/10.1364/ao.54.00f189.

5. A. Biswas and W. H. Farr. Detectors for ground based reception of laser communication from Mars. Lasers and electro-optics society // The 17th Annual Meeting of the IEEE Lasers and Electro-Optics Society. 2004. Vol. 1. P. 74–75. 7-11 November 2004.

6. T. Jono et al. Demonstrations of ARTEMIS-OICETS Inter-Satellite Laser Communications // 24th AIAA International Communications Satellite Systems Conference, Jun. 2006, doi: https://doi.org/10.2514/6.2006-5461.

7. R. Lange and B. Smutny. Homodyne BPSK-based optical inter-satellite communication links // Proceedings of SPIE, the International Society for Optical Engineering/Proceedings of SPIE, Feb. 2007. doi: https://doi.org/10.1117/12.698646.

8. H. Le Minh, D. C. O'Brien, G. Faulkner, M. Wolf, L. Grobe, J. Lui, and O. Bouchet. A 1.25 Gbit/s indoor optical wireless demonstrator // IEEE Photonics Technology Letters. 2010. Vol. 22, no. 21. P. 1598–1600.

9. H. Elgala, R. Mesleh, and H. Haas, "Indoor optical wireless communication: potential and state-of-the-art // IEEE Communications Magazine. Sep. 2011. Vol. 49, no. 9. P. 56–62. doi: https://doi.org/10.1109/mcom.2011.6011734.

10. N. Barnwell, T. Ritz, S. Parry, M. Clark, P. Serra, and J. W. Conklin. The Miniature Optical Communication Transceiver–A Compact, Power-Efficient Lasercom System for Deep Space Nanosatellites // Aerospace. Dec. 2018. Vol. 6, no. 1. P. 2. doi: https://doi.org/10.3390/aerospace6010002.

11. S. M. Walsh et al. Demonstration of 100 Gbps coherent free-space optical communications at LEO tracking rates // Scientific Reports. Oct. 2022. Vol. 12, no. 1. P. 18345. doi: https://doi.org/10.1038/s41598-022-22027-0.

12. Jürgen Jahns, Sing H. Lee. Optical Computing Hardware // Elsevier eBooks, Jan. 1994. doi: https://doi.org/10.1016/c2013-0-07396-3.

13. F. R. Gfeller and U. Bapst. Wireless in-house data communication via diffuse infrared radiation // Proceedings of the IEEE. Nov. 1979. Vol. 67. P. 1474–1486.

14. J. M. Kahn and J. R. Barry. Wireless infrared communications // Proceedings of the IEEE. Feb. 1997. Vol. 85, no. 2. P. 265–298. https://doi.org/10.1109/5.554222

15. M. Sichitiu and M. Kihl. Inter-vehicle communication systems: a survey // IEEE Communications Surveys & Tutorials. 2008. Vol. 10, no. 2. P. 88–105. doi: https://doi.org/10.1109/comst.2008.4564481.

16. Vincent. Optical satellite networks // Journal of Lightwave Technology. 2003. Vol. 21, no. 11. P. 2811–2827. doi: https://doi.org/10.1109/jlt.2003.819534.

17. E. Ciaramella, Y. Arimoto, G. Contestabile, M. Presi, A. D'Errico, A. Guarino, and M. Matsumoto. 1.28-Tb/s (32x40 Gb/s) free-space optical WDM transmission system // IEEE Photonics Technology Letters. Aug. 2009. Vol. 21, no. 16. P. 1121–1123.

18. HITRANonline, www.hitran.org. https://www.hitran.org/ (accessed Jun. 22, 2024).

19. S. Bloom, E. Korevaar, J. Schuster, and H. Willebrand. Understanding the performance of free-space optics // Journal of Optical Networking. June 2003. Vol. 2, no. 6. P. 178–200.

20. Zhengyuan Xu and B. M. Sadler. Ultraviolet Communications: Potential and State-Of-The-Art // IEEE Communications Magazine. May 2008. Vol. 46, no. 5. P. 67–73. doi: https://doi.org/10.1109/mcom.2008.4511651.

21. G. Li. Recent advances in coherent optical communication // Advances in Optics and Photonics. Feb. 2009. Vol. 1, no. 2. P. 279. doi: https://doi.org/10.1364/aop.1.000279.

22. M. Razavi and J. H. Shapiro. Wireless optical communications via diversity reception and optical preamplification // IEEE Transactions on Wireless Communications. May 2005. Vol. 4, no. 3. P. 975–983. doi: https://doi.org/10.1109/twc.2005.847102.

23. A. O. Aladeloba, A. J. Phillips, and M. S. Woolfson. Improved bit error rate evaluation for optically pre-amplified free-space optical communication systems in turbulent atmosphere // IET Optoelectronics. 2012. Vol. 6, no. 1. P. 26. doi: https://doi.org/10.1049/iet-opt.2010.0100.

24. F. Dios, Juan Antonio Rubio, A. Rodríguez, and A. Comerón. Scintillation and beam-wander analysis in an optical ground station-satellite uplink // Applied optics. Jul. 2004. Vol. 43, no. 19. P. 3866–3866. doi: https://doi.org/10.1364/ao.43.003866.

25. I. E. Lee, Z. Ghassemlooy, W. P. Ng, and M.-A. Khalighi. Joint optimization of a partially coherent Gaussian beam for free-space optical communication over turbulent channels with pointing errors // Optics Letters. Jan. 2013. Vol. 38, no. 3. P. 350. doi: https://doi.org/10.1364/ol.38.000350.

26. H. Sandalidis. Optimization Models for Misalignment Fading Mitigation in Optical Wireless Links // IEEE Communications Letters. May 2008. Vol. 12, no. 5. P. 395–397. doi: https://doi.org/10.1109/lcomm.2008.071788.

27. X. Liu. Free-space optics optimization models for building sway and atmospheric interference using variable wavelength // IEEE Transactions on Communications. Feb. 2009. Vol. 57, no. 2. P. 492–498. doi: https://doi.org/10.1109/tcomm.2009.02.070089.

28. S. Arnon.Effects of atmospheric turbulence and building sway on optical wireless-communication systems // Optics Letters. Jan. 2003. Vol. 28, no. 2. P. 129. doi: https://doi.org/10.1364/ol.28.000129.

29. H. G. Sandalidis, T. A. Tsiftsis, and G. K. Karagiannidis. Optical Wireless Communications With Heterodyne Detection Over Turbulence Channels With Pointing Errors // Journal of Lightwave Technology. Oct. 2009. Vol. 27, no. 20. P. 4440–4445. doi: https://doi.org/10.1109/jlt.2009.2024169.

30. H. G. Sandalidis. Coded Free-Space Optical Links over Strong Turbulence and Misalignment Fading Channels // IEEE Transactions on Communications. Mar. 2011. Vol. 59, no. 3. P. 669–674. doi: https://doi.org/10.1109/tcomm.2011.121410.090318.

31. R. M. Goody and G. D. Robinson. Radiation in the troposphere and lower stratosphere // Quarterly Journal of the Royal Meteorological Society. Apr. 1951. Vol. 77, no. 332. P. 151–187. doi: https://doi.org/10.1002/qj.49707733203.

32. J. Mohale, M. R. Handura, T. O. Olwal, and C. N. Nyirenda. Feasibility study of free-space optical communication for South Africa // Optical Engineering. May 2016. Vol. 55, no. 5. P. 056108. doi: https://doi.org/10.1117/1.oe.55.5.056108.

33. H. A. Fadhil et al. Optimization of free space optics parameters // An optimum solution for bad weather conditions. Oct. 2013. Vol. 124, no. 19. P. 3969–3973. doi: https://doi.org/10.1016/j.ijleo.2012.11.059.

34. S. S. Muhammad. Characterization of fog attenuation in terrestrial free space optical links // Optical Engineering. Jun. 2007. Vol. 46, no. 6. P. 066001. doi: https://doi.org/10.1117/1.2749502.

35. Heinz Willebrand and B. S. Ghuman. Free space optics : enabling optical connectivity in today's networks. Indianapolis, Ind. : Sams, 2002.

36. L. C. Andrews, R. L. Phillips, and C. Y. Hopen. Aperture averaging of optical scintillations: power fluctuations and the temporal spectrum // Waves in Random Media. Jan. 2000 Jan. 2000. Vol. 10, no. 1. P. 53–70. doi: https://doi.org/10.1088/0959-7174/10/1/305.

37. Tatarskii V. I. Wave propagation in a turbulent medium. Mineola, New York : Dover Publications, Inc, 2017.

38. X. M. Zhu and J. M. Kahn. Free-space optical communication through atomospheric turbulence channels // IEEE Transactions on Communications. Aug. 2002. Vol. 50, no. 8. P. 1293–1300.

39. N. D. Chatzidiamantis, H. G. Sandalidis, G. K. Karagiannidis, S. A. Kotsopoulos, and Michail Matthaiou. New results on turbulence modeling for free-space optical systems // CiteSeer X (The Pennsylvania State University), Apr. 2010, doi: https://doi.org/10.1109/ictel.2010.5478872.

40. S. A. Arpali, H. T. Eyyuboğlu, and Y. Baykal. Bit error rates for general beams // Applied Optics. Nov. 2008. Vol. 47, no. 32. P. 5971. doi: https://doi.org/10.1364/ao.47.005971.

41. Hamza Gerçekcioğlu, Yahya Baykal, and Cem Nakiboğlu. Annular beam scintillations in strong turbulence // Journal of the Optical Society of America. Jul. 2010. Vol. 27, no. 8. P. 1834–1834. doi: https://doi.org/10.1364/josaa.27.001834.

42. Frida Strömqvist Vetelino, C. Young, L. Andrews, and Jaume Recolons. Aperture averaging effects on the probability density of irradiance fluctuations in moderate-to-strong turbulence // Applied optics. Mar. 2007. Vol. 46, no 11. P. 2099–2099. doi: https://doi.org/10.1364/ao.46.002099.

43. S. Navidpour, M. Uysal, and M. Kavehrad. BER Performance of Free-Space Optical Transmission with Spatial Diversity // IEEE Transactions on Wireless Communications. Aug. 2007. Vol. 6, no. 8. P. 2813–2819. doi: https://doi.org/10.1109/twc.2007.06109.

44. R. K. Tyson. Bit-error rate for free-space adaptive optics laser communications // Journal of the Optical Society of America A. Apr. 2002. Vol. 19, no. 4. P. 753. doi: https://doi.org/10.1364/josaa.19.000753.

Надійшла до редколегії 22. 01.2025

Відомості про авторів:

Кухтін Сергій Михайлович – канд. фіз.-мат. наук, Харківський національний університет радіоелектроніки, ст. викладач кафедри фізичних основ електронної техніки; Україна; e-mail: serhii.kukhtin@nure.ua; ORCID: https://orcid.org/0000-0001-8335-5373

Євгенія Петрівна Федоренко – Харківський національний університет радіоелектроніки, доцент кафедри фізичних основ електронної техніки; Україна; e-mail: yevheniia.fedorenko@nure.ua; ORCID: https://orcid.org/0009-0004-6394-0216

УДК 621.3729(75) **DOI:10.30837/rt.2025.1.220.15**

О.Д. МЕНЯЙЛО, канд. техн. наук, О.В. ГРИГОР'ЄВА

АНАЛІЗ ШУМОВИХ КОМПОНЕНТІВ ДІОДНИХ АВТОГЕНЕРАТОРІВ НВЧ

Вступ

Останнім часом при проєктуванні автогенераторів НВЧ підвищився інтерес до використання діодів з так званим негативним опором. Серед найбільш розповсюджених діодних генераторів є такі, як генератори на тунельних діодах, генератори на діодах Ганна та лавино-пролітних діодах, що працюють в режимах IMPATT або TRAPATT. Цим автогенераторам властивий певний рівень паразитних флуктуацій. Особливо цей недолік присутній у генераторах на лавино-пролітних діодах.

Робота присвячена як теоретичному, так і практичному дослідженню флуктуаційних компонентів діодних автогенераторів. Проведені дослідження свідчать про узгодженість теоретичних висновків з практичними результатами. Висновки, що витікають з провідних досліджень, можуть бути використані при проєктуванні діодних генераторів НВЧ з заданими флуктуаційними характеристиками.

Механізм формування флуктуаційних компонентів діодних автогенераторів

Шумові флуктуації діодних автогенераторів НВЧ в основному складаються з двох компонентів: флуктуації основної частоти (високочастотний шум) і флуктуації, що зумовлені низькочастотною модуляцією (низькочастотний шум).

З метою теоретичного аналізу впливу низькочастотних та високочастотних джерел шумових флуктуацій розглянемо модель, діодного автогенератора, яка враховує обидві ці шумові компоненти. Одна з таких можливих моделей наведена на рис. 1.

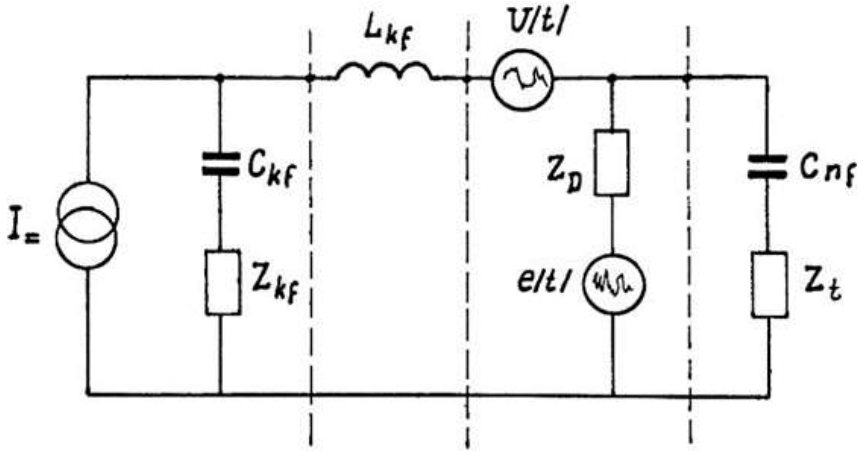


Рис. 1. Схема моделі автогенератора з урахуванням
його шумових флуктуаційних компонентів

На еквівалентній схемі (рис. 1) генератор напруги *e(t)* презентує високочастотну, флуктуаційну компоненту шуму і під'єднується послідовно з комплексним опором діода Z_D. Модуляційний шум, що виникає в результаті флуктуацій постійного струму δI, може бути представлений генератором напруги U(t), підключеним послідовно до ланцюга живлення. Таке представлення генератора дозволяє роздільно враховувати флуктуації, що породжені, як флуктуаціями струму джерела живлення, так і високочастотними флуктуаціями, джерелом яких є фізичні процеси в напівпровіднику діода. Фільтр, що складається з ємності C_{kf} та індуктивності L_{kf} служить для розділу високочастотної та низькочастотної частин генератора.

Комплексний опір Z_{kf}, в свою чергу, презентує вхідний опір джерела живлення автогенератора. Ланцюг C_{nf} та Z_t моделює елементи розділу навантаження та коливальної системи і комплексне навантаження діодного генератора.

У випадку обмежених флуктуацій, високочастотна напруга e(t), що представляє собою високочастотну флуктуаційну компоненту шуму, може бути визначена як

$$e(t) = \mathrm{Re}\,[n(t)\exp j\omega t] = \mathrm{Re}\,\{[e_c(t) + je_s(t))]\exp j\omega t\},$$

де $e_c(t)$ та $e_s(t)$ – синусоїдальні та косинусоїдальні компоненти шумової функції n(t).

Зазначимо, що компоненти $e_c(t)$ та $e_s(t)$ являються функціями, що відносно повільно змінюються та характеризуються відповідними спектрами $S_{ee}(\omega)$ та $S_{ss}(\omega)$.

Модуляційні флуктуації, в свою чергу, можуть бути описані флуктуацією постійного струму $\delta_I(t)$, що відповідає певному спектру потужності $S_{II}(\omega)$.

Механізм формування флуктуаційних компонентів діодного автогенератора можна проілюструвати наступним чином (рис. 2).

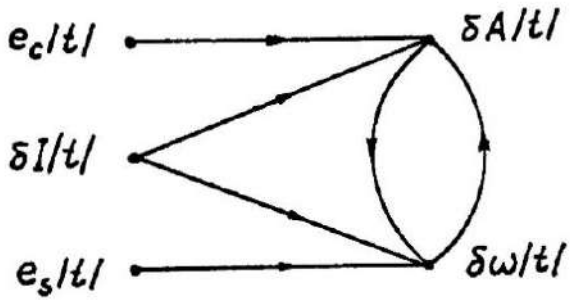


Рис. 2. Схема механізму формування флуктуаційних компонентів автогенератора

Згідно з таким механізмом косинусоїдальна компонента флуктуаційного шуму викликає флуктуацію амплітуди, а це призводить, завдяки нелінійності системи, до наступного відхилення частоти; в той час, як синусоїдальна компонента флуктуаційного шуму викликає коливання частоти, що, в свою чергу, призводить до коливання амплітуди через елементи генератора, які залежать від частоти.

Таким чином, модуляційний шум може безпосередньо спричиняти компоненти шуму, як амплітудно модульовані, так і частото модульовані.

Експериментальне дослідження флуктуаційних компонентів автогенераторів

Для експериментального дослідження флуктуаційних компонентів було вибрано генератор на лавино-пролітному діоді як приклад діодного автогенератора, що має досить великий рівень власних шумів. На рис. 3 і 4 представлені результати досліджень амплітудно-модульованих та частото-модульованих шумових компонентів автогенератора на лавино-пролітному діоді в залежності від добротності його коливальної системи.

Звертає на себе увагу, як і слід було передбачити за результатами теоретичного аналізу, експоненційний характер цих залежностей, що є природньо. По мірі наближення до несучої частоти амплітуда коливань повинна збільшуватися, а по мірі віддалення від несучої частоти рівень флуктуаційних компонентів зменшується та дещо стабілізується.

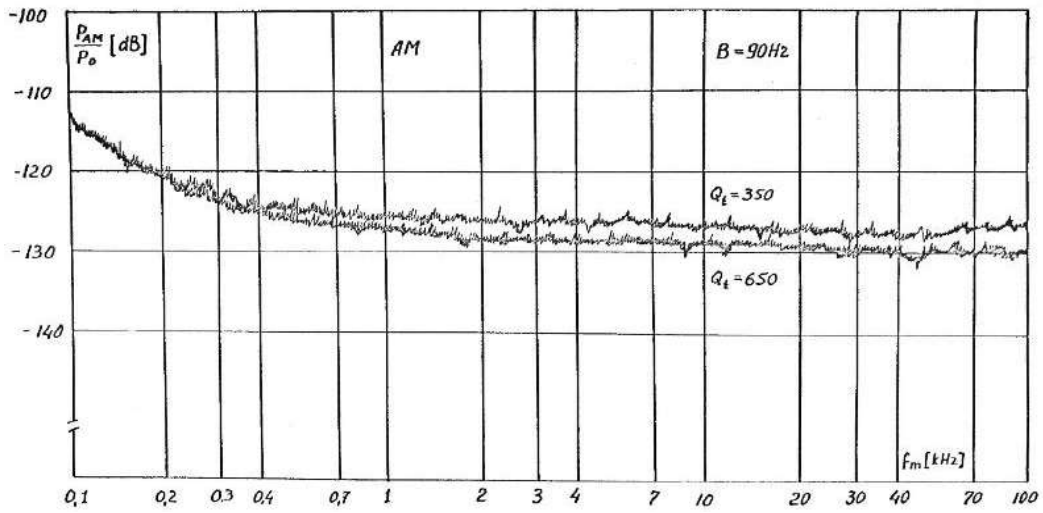


Рис. 3. Результати досліджень амплітудно-модульованих шумових компонентів автогенератора в залежності від добротності його коливальної системи

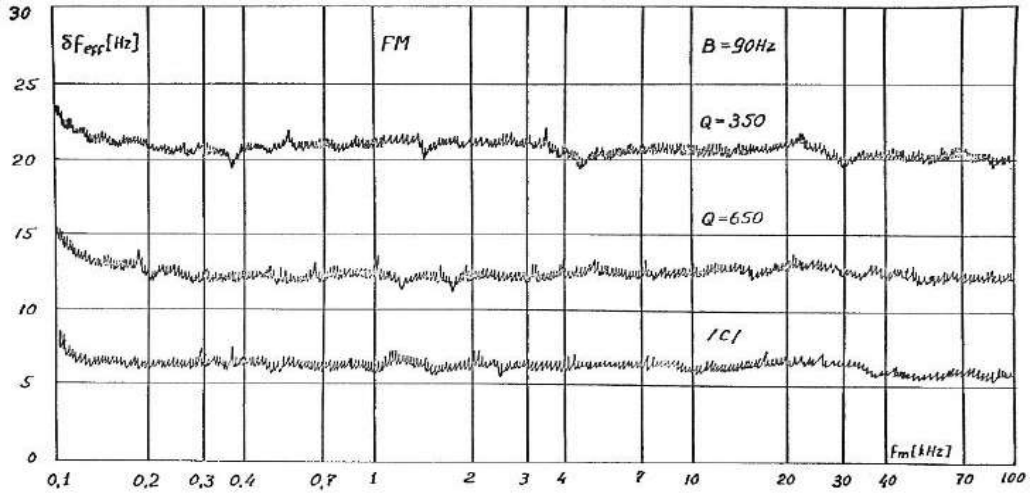


Рис. 4. Результати досліджень частото-модульованих шумових компонентів автогенератора в залежності від добротності його коливальної системи

Експериментальні данні свідчать про те, що добротність коливальної системи генератора більше впливає на частото-модульовану шумову компоненту ніж на амплітудно-модульовану компоненту.

Результати досліджень свідчать, також, що частото-модульовані шумові компоненти при певній величині струму живлення досягають свого мінімуму. Цей факт демонструє крива, зображена на рис. 5. Для автогенератора, що досліджувався, цей мінімум знаходився в діапазоні від 90 мА до 95 мА.

У той же час, залежність амплітудо-модульованих компонентів шуму від постійного струму живлення значно слабша, що дає можливість, при подальшому аналізі, нею знехтувати.

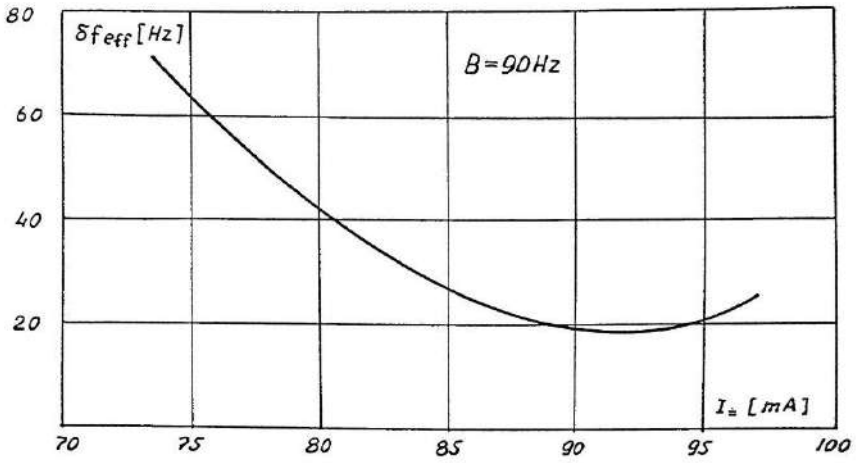


Рис. 5. Залежність частото-модульованих шумових компонентів
від струму живлення автогенератора

В якості прикладу на рис. 6 наведено вид типових спектрів частото-модульованих компонентів автогенератора на лавино-пролітному діоді фірми Hewlett Packard, зроблений з екрана аналізатора спектру.

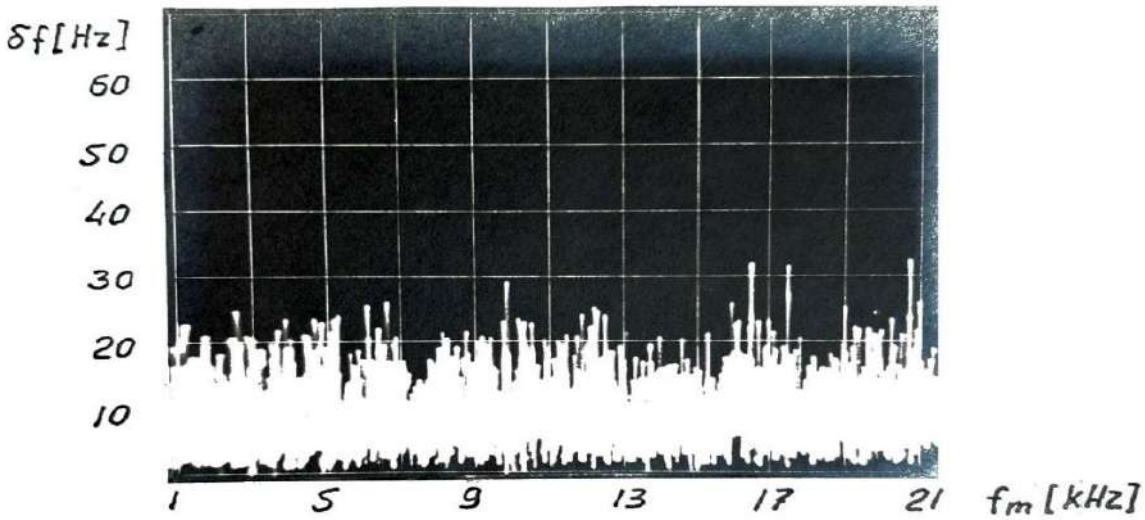


Рис. 6. Вид експериментального частото-модульованого спектру компонентів
генератора на лавино-пролітному діоді

Як свідчать дані, представлені на рис. 6, в діапазоні частот від 1 до 21 кГц флуктуаційні відхилення частоти носять рівномірний характер та знаходяться в межах від 0 до 20 Гц.

Висновки

Результати проведеного теоретичного та практичного аналізу свідчать про наступне:

– серед флуктуаційних компонентів діодних автогенераторів доцільно виділяти низькочастотні та високочастотні компоненти – модуляційні та флуктуаційні;

– у разі невеликих відхилень від несучої, модуляційні флуктуації, при відповідному вхідному опорі джерела живлення, можна зробити досить малими;

– високочастотні флуктуації визначаються трьома основними параметрами: безпосередньо, флуктуаціями струму діода, нелінійністю активної та пасивної частин лавинного діода,

частотною залежністю навантаження. Враховуючи ці три параметри, можна звести флуктуації до мінімуму, або відповідним чином впливати на них;

– в загальному випадку частото-модульований шум генератора на лавино-пролітному діоді більш значний ніж амплітудно модульований шум.

Список літератури:

1. Prager H.J., Chang K.K.N, Weisbrod J. A Theoryfor the High-Efficiency Mode of Oscillationin Avalanche Diode // Proc. IBBE, 55, 586, 1967.
2. Chang K.K.N., RCA Rev, 30, 3. 1969.
3. T.Misawaю Multiple uniform lagger approximationin analysis of negativ resistance in p-n junction in breakdown // IEEE Tran. ElectronDevices vol. ED-14 1967. pp. 795-808.
4. T.Misawa. Negative Resistance in p-n JunctionsUnder AvalancheBreakdown Conditions, pts.I and II // IEEE Trans. Electron Devices, vol. ED-13 pp 137-151. Jan. 1966.
5. М. Бондаренко. Мікроелектроніка НВЧ. Ч. 2. Напівпровідникові елементи та пристрої НВЧ : навч. посіб. для студ. спец. 153 «Мікро- та наносистемна техніка», 171 «Електроніка». Харків, 2019.
6. Осадчук О.В. Математичне моделювання генератора НВЧ на основі транзисторної структури з від‘ємним опором / О.В. Осадчук, А.О. Семенов // Вісник Хмельн. нац. ун-ту, 2005.
7. Super Low Noise InGaAs HEMT MGF431×G. Technical description/ Mitsubishi Semiconductor as of Apr.' 98. P. 1238–1239. 96. Low Noise Pseudomorphic HEMT in a Surface Mount Plastic Package // Aqilent Technologies. Innovating the HP Way. 2001. P. 145–147. №4, Ч.1, Т.2. С. 256–259.
8. Патент на корисну модель 7411 Україна, МКИ Н 03 В 7/00. Генератор з електричним регулюванням частоти генерації / В.С. Осадчук, О.В. Осадчук, А.О. Семенов (Україна). №20041210199; Заявлено 13.12.2004; Опубл. 15.06.2005, Бюл. №6. 2 с.
9. Яненко О.П. Моделювання нормованих спотворень монохроматичних сигналів НВЧ генераторів / О.П. Яненко, Д.М. Ясінський // Вісник, НТУУ «КПІ». Сер. Радіотехніка радіоапаратобудування.
10. Лукин К.А., Максимов П.П. Динаміка двочастотних лавино-генераторних діодів мікрохвильового діапазону // Радіофізика та електроніка. 2015. Т. 6(20), № 4. С. 54–61.
11. Коцержинський, Б.О. Фазові шуми малошумлячих транзисторних НВЧ генераторів // Вісник НТУУ «КПІ». Радіотехніка, радіоапаратобудування: збірник наукових праць. 2009. № 39. С. 88–90.

Надійшла до редколегії 04.01.2025

Відомості про авторів:

Меняйло Олександр Дмитрович – канд. техн. наук, доцент, Харківський національний університет радіоелектроніки, доцент кафедри проєктування та експлуатації електронних апаратів, Україна; e-mail: oleksandr.meniailo@nure.ua; ORCID: https://orcid.org/0000-0002-3760-0523

Григор'єва Ольга Володимирівна – Харківський національний університет радіоелектроніки, старший викладач кафедри проєктування та експлуатації електронних апаратів, Україна; e-mail: olha.hryhorieva@nure.ua; ORCID: https://orcid.org/0000-0002-5759-8897

УДК 621.391 **DOI:10.30837/rt.2025.1.220.16**

М.А. ШТОМПЕЛЬ, д-р техн. наук

МЕТОД ДЕКОДУВАННЯ ПОСЛІДОВНИХ АЛГЕБРАЇЧНИХ КАСКАДНИХ ЗГОРТКОВИХ КОДІВ ДЛЯ СИСТЕМ МОБІЛЬНОГО ЗВ'ЯЗКУ

Вступ

Розвиток технологій радіозв'язку дозволяє впроваджувати новітні електронні комунікаційні послуги, що висувають жорсткі вимоги до якості передавання даних. Наприклад, радіотехнології п'ятого покоління застосовуються у таких сценаріях: розширений мобільний широкосмуговий доступ, надзвичайно надійні комунікації з низькою затримкою обробки даних, масивні комунікації машинного типу. В рамках розширеного мобільного широкосмугового доступу користувачі отримують послуги віртуальної та доповненої реальності, мультимедійний контент, що вимагає значної швидкості обробки даних та підвищеної пропускної спроможності мобільної мережі. Для надання електронних послуг, критичних до затримки та достовірності даних, застосовуються граничні обчислення, логічні сегменти мережі, покращені методи обробки інформації. Послуги міжмашинної взаємодії та впровадження Інтернету речей обумовлюють застосування енергоефективного мережевого та кінцевого обладнання з низькою обчислювальною складністю та підтримкою механізмів високонадійного низькошвидкісного передавання даних [1–3].

Для вирішення цих завдань у сучасних радіотехнологіях використовуються завадостійкі кодові конструкції. Застосування методів завадостійкого кодування дозволяє покращити такі ключові показники мереж мобільного зв'язку: надійність, продуктивність, затримка, покриття, спектральна ефективність, енергетична ефективність. Зокрема, у радіотехнологіях нового покоління підтримуються коди з малою щільністю перевірок на парність у каналах передавання даних та полярні коди у каналах управління [4, 5]. Відомо, що каскадні кодові конструкції дозволяють підвищити ефективність та надійність передавання даних, тому актуальною задачею є впровадження даних кодів у новітні системи мобільного зв'язку та пошук ефективних методів декодування.

Аналіз принципів побудови та декодування каскадних кодових конструкцій

Каскадні кодові конструкції формуються шляхом поєднання за різними принципами декількох кодів. У загальному випадку метою формування каскадних кодів є підвищення коригувальної здатності кодової конструкції та можливість регулювання ефективності декодування складових кодів [6].

Наприклад, турбокоди, що застосовуються у системах мобільного зв'язку третього та четвертого поколінь, є прикладом паралельно з'єднаних рекурсивних згорткових кодів із застосуванням перемежувача. Довгі турбо коди досягають максимуму пропускної здатності для деяких моделей каналу зв'язку та значно перевершують за ефективністю алгебраїчні блокові коди [7]. Типове декодування даних кодів засновано на пошуку максимуму апостеріорної імовірності шляхом ітеративного обміну м'якою інформацією між двома складовими декодерами. Кожна ітерація декодування складається з двох фаз. На першій фазі визначається зовнішня інформація на основі сигналу, прийнятого з каналу зв'язку. На наступній фазі перемежовані елементи зовнішньої інформації використовуються як апріорні імовірності та обчислюється зовнішня інформація на позиціях перевірочних символів другого коду у прийнятій послідовності. Таким чином, другим декодером знаходиться рішення щодо інформаційних символів з використанням апостеріорних імовірностей. На наступних ітераціях декодування перший декодер використовує інформацію, отриману від другого декодеру, у якості апріорних імовірностей для знаходження власного рішення. Декодування завершується при досягненні максимальної кількості ітерацій [8]. Слід зазначити, що вибір типу перемежувача

значно впливає на забезпечення декореляції інформації, якою обмінюються складові декодери, та гарантування псевдовипадкості коротких турбо кодів [9].

З іншого боку, сучасні технології радіозв'язку використовують послідовні каскадні кодові конструкції, складовими яких можуть виступати коди різних класів [10]. Фактично дані конструкції формуються шляхом добутку окремих кодів та додатково можуть містити перемежувач для забезпечення більшої випадковості. Прикладом даного підходу є класична каскадна схема, в якій на зовнішній ступені застосовується код Ріда–Соломона, а внутрішня ступень виконана на основі нерекурсивного випадкового згорткового коду. Декодування даної кодової конструкції здійснюється послідовно незалежними типовими декодерами для цих кодів: декодер Берлекемпа–Мессі – для коду Ріда–Соломона, декодер Вітербі – для згорткового коду [11]. Таким чином, декодування послідовних каскадних кодових конструкцій можна реалізувати незалежно, що дозволяє знизити обчислювальну складність його реалізації та доволі легко змінювати компонентні коди. У більш загальному випадку, у якості складових кодів можуть застосовуватись ідентичні блокові коди (алгебраїчні блокові коди, коди з малою щільністю перевірок на парність тощо) або згорткові коди (алгебраїчні, випадкові, нерекурсивні, рекурсивні тощо). При цьому бажано, щоб зовнішній код мав велику мінімальну кодову відстань для виправлення максимальної кількості помилок у прийнятій послідовності. Для декодування таких послідовних каскадних кодових конструкцій застосовуються різноманітні декодери на основі обчислення апостеріорних імовірностей, врахування надійності прийнятих символів, алгоритму Чейза тощо [12].

Синтез послідовних алгебраїчних каскадних згорткових кодів

За результатами проведеного аналізу у роботі розглядається можливість застосування алгебраїчних каскадних кодів у системах мобільного зв'язку нового покоління. Для побудови пропонується послідовна схема, в якій зовнішня ступень реалізується на базі недвійкового блокового коду Ріда–Соломона, внутрішня ступень – з використанням нерекурсивного алгебраїчного згорткового коду. Між даними ступенями використовується блоковий перемежувач.

Недвійковий (N,K,D) код Ріда–Соломона над полем $GF(2^m)$ дозволяє виправляти до $t=\lfloor D-1/2 \rfloor$ помилок у символах, кожен з яких містить m біт [10]. Даний код має такі параметри: довжина інформаційного повідомлення K, довжина кодового слова N, мінімальна кодова відстань D, швидкість коду $R=K/N$. Отже, код Ріда–Соломона має гарні можливості для виправлення групових помилок. Крім того, дані коди є блоковими кодами максимальної довжини, тобто вони мають найбільшу мінімальну кодову відстань $D=N-K+1$ для заданих параметрів N та K. Ці коди відносяться до класу циклічних кодів, що дозволяє задати деякий недвійковий (N,K,D) код Ріда–Соломона породжувальним багаточленом

$$g(x)=(x-\alpha)(x-\alpha^2)...(x-\alpha^{2t}), \tag{1}$$

де α – примітивний елемент у полі $GF(2^m)$, що визначається примітивним багаточленом $p(x)$ степені m.

Породжувальний багаточлен (1) має $(N-K)$ послідовних коренів α, α^2, …, α^{N-K}, що можна представити у циклічній формі наступним чином:

$$g(x)=g_0+g_1x+...+g_{N-K}x^{N-K}, \tag{2}$$

де $g_i \in GF(2^m)$, $i \in [0, N-K]$ – недвійковий символ у полі $GF(2^m)$.

Тоді породжувальна матриця даного коду дорівнює

$$G=\begin{pmatrix} g_0 & g_1 & \cdots & g_{N-K} & 0 & 0 & 0 \\ 0 & g_0 & g_1 & \cdots & g_{N-K} & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & g_0 & g_1 & \cdots & g_{N-K} \end{pmatrix}. \quad (3)$$

У загальному випадку побудова (n_0, k_0, ν) нерекурсивного алгебраїчного згорткового коду здійснюється з використанням породжувального багаточлену деякого недвійкового блокового коду. Даний код має наступні параметри: довжина інформаційного кадру k_0, довжина кодового кадру n_0, довжина кодового обмеження ν, кодова швидкість $R_0 = k_0 / n_0$. Відомо, що для гарантування максимальної корегувальної здатності необхідно застосовувати породжувальний багаточлен (2) коду Ріда–Соломона як блокового коду максимальної довжини [13]. У даній роботі для формування (n_0, k_0, ν) нерекурсивного алгебраїчного згорткового коду та зовнішнього коду Ріда–Соломона використовуються еквівалентні породжувальні матриці (3). Для отримання алгебраїчного згорткового коду кінцевої довжини застосовується усічення кодової послідовності. В результаті даного підходу на основі множення інформаційного блоку довжини k на породжувальну матрицю (3) формується кодовий блок довжиною $n = kn_0$ з урахуванням останніх ν інформаційних бітів.

Метод декодування послідовних алгебраїчних каскадних згорткових кодів

Нехай інформація у системі мобільного зв'язку передається через канал з адитивним білим гаусовим шумом (АБГШ) із застосуванням двійкової фазової модуляції. Позначимо інформаційне повідомлення, що надходить на зовнішній кодер, як $U = (U_0, U_1, ..., U_{K-1})$ та кодове слово коду Ріда–Соломона як $C = (C_0, C_1, ..., C_{N-1})$. Блоковий перемежувач застосовує до даного кодового блоку перестановку $\Pi(C)$. Отримана перемежована послідовність виступає інформаційним блоком для внутрішнього кодеру $u = \Pi(C)$, на основі якого формується кодовий блок алгебраїчного згорткового коду $c = (c_0, c_1, ..., c_{n-1})$. Передбачається, що $N = k$ та блоковий перемежувач має довжину k. Далі кодовий блок перетворюється у фазомодульований сигнал та передається через канал з АБГШ. На приймальній стороні прийнята послідовність $r = (r_0, r_1, ..., r_{n-1})$ надходить на внутрішній декодер, який формує оцінку кодового блоку $c' = (c'_0, c'_1, ..., c'_{n-1})$ алгебраїчного згорткового коду. Після цього застосовується зворотна перестановка $R' = \Pi^{-1}(c')$ для формування прийнятого вектору для зовнішнього декодеру та знаходиться оцінка кодового слова $C' = (C'_0, C'_1, ..., C'_{N-1})$ коду Ріда–Соломону. Після цього визначається відповідне інформаційне повідомлення $U' = (U'_0, U'_1, ..., U'_{K-1})$.

Для підвищення ефективності декодування прийнятої послідовності з використанням послідовних алгебраїчних каскадних згорткових кодів пропонується на внутрішній ступені використати декодер на основі впорядкованих статистик, що має ряд переваг порівняно з алгоритмом Вітербі [14, 15]. На зовнішній ступені застосовується алгебраїчний декодер на основі алгоритму Берлекемпа–Мессі. Запропонований підхід складається з наступних етапів.

Етап 1. Декодування внутрішнього коду ((n_0, k_0, ν) нерекурсивного алгебраїчного згорткового коду) за впорядкованими статистиками.

К р о к 1.1. Знаходження найбільш надійного базису шляхом формування модифікованих прийнятої послідовності та породжувальної матриці, оцінки кодового блоку відповідно:

$$r'' = \pi_2(\pi_1(r')), \quad G'' = \pi_2(\pi_1(G)), \quad c'' = \pi_2(\pi_1(c')) = (c''_B c''_P), \quad (4)$$

де π_1 – перестановка за зменшенням надійності елементів ($|r_i'| \geq |r_j'|, i < j$); π_2 – перестановка для гарантування лінійної незалежності перших k стовпців матриці $G' = \pi_1(G)$ у систематичній формі; c_B'' – найбільш надійний базис; c_P'' – перевірочна частина кодового блоку.

К р о к 1.2. Визначення найбільш імовірної тестової оцінки кодового блоку:

$$c_b'' = c_e'' \text{ при} \min(d_\omega(c_e'', c'')),$$

де c_e'' – тестовий кодовий блок, що дорівнює $c_e'' = (c_B'' + e)G''$; e – тестовий вектор помилок з набору векторів ваги Хемінга ω; $d_\omega(c_e'', c'')$ – зважена вага Хемінга між тестовим кодовим блоком c_e'' та прийнятою оцінкою кодового блоку, отриманою згідно з (4):

$$d_\omega(c_e'', c'') = \sum_{i=0}^{n-1} |r_i|, c_{e,i}'' \neq c_i''.$$

К р о к 1.3. Формування оцінки кодового блоку $c_b = \pi_1^{-1}(\pi_2^{-1}(c_b''))$.

Для підвищення імовірності знаходження вірної оцінки кодового блоку алгебраїчного згорткового коду необхідно збільшувати набір тестових векторів шляхом використання більшої ваги Хемінга ω, що визначає степінь декодування за впорядкованими статистиками [14]. Слід зазначити, що це призводить до зростання обчислювальної складності та затримки декодування.

Етап 2. Зворотна перестановка оцінки кодового блоку c_b алгебраїчного згорткового коду у блоковому перемежувачі $R' = \Pi^{-1}(c_b)$.

Етап 3. Алгебраїчне декодування зовнішнього коду ((N, K, D) коду Ріда–Соломона).

К р о к 3.1. Визначення синдрому прийнятого вектору R':

$$S(x) = S_0 + S_1 x + ... + S_{N-K-1} x^{N-K-1},$$

де $S_i \in GF(2^m)$, $i \in [0, N-K-1]$ – недвійковий символ у полі $GF(2^m)$.

К р о к 3.2. Обчислення ключового виразу на базі алгоритму Берлекемпа–Мессі:

$$\Lambda(x) \cdot S(x) \equiv \Omega(x) (\text{mod}\, x^{N-K}),$$

де $\Lambda(x)$, $\deg(\Lambda(x)) \leq t$ – багаточлен локатору помилок; $\Omega(x)$, $\deg(\Omega(x)) < t (\leq N-K-t)$ – багаточлен значень помилок.

К р о к 3.3. Знаходження позицій помилок шляхом обчислення коренів $\Lambda(x)$ та обчислення значень помилок на основі $\Lambda(x)$ та $\Omega(x)$ на базі пошуку Ченя та процедури Форні.

Якщо кількість символьних помилок у прийнятій послідовності менше t, даний алгебраїчний декодер здатний виправити усі помилки. У противному випадку, в залежності від розподілу та кількості помилок декодер здійснює відмову від декодування або формує кодове слово відмінне від переданого.

Висновки

1. Показано, що побудова послідовних каскадних кодових конструкцій для систем мобільного зв'язку може здійснюватися на базі різних компонентних кодів та відповідних декодерів. Це надає змогу регулювати характеристики даних кодових конструкцій в залежності від наявних вимог та параметрів каналу зв'язку.

2. Запропонована послідовна алгебраїчна каскадна схема кодування, що складається з недвійкового блокового коду Ріда–Соломона, нерекурсивного алгебраїчного згорткового

коду та блокового перемежувача. Відмінною особливістю даної схеми є застосування алгебраїчного згорткового коду з максимально досяжною корегувальною здатністю.

3. Розроблено метод декодування послідовних алгебраїчних каскадних згорткових кодів на базі декодеру на основі впорядкованих статистик та алгебраїчного декодеру на основі алгоритму Берлекемпа–Мессі. Даний метод дозволяє регулювати ефективність декодування на кожному етапі шляхом зміни параметрів окремих декодерів.

Список літератури:

1. G. Pocovi, T. Kolding and K. I. Pedersen. On the Cost of Achieving Downlink Ultra-Reliable Low-Latency Communications in 5G Networks // IEEE Access. 2022. Vol. 10. P. 29506–29513. doi: 10.1109/ACCESS.2022.3158361.

2. A. M. Aslam, R. Chaudhary, A. Bhardwaj, I. Budhiraja, N. Kumar and S. Zeadally. Metaverse for 6G and Beyond: The Next Revolution and Deployment Challenges // IEEE Internet of Things Magazine. March 2023. Vol. 6, no. 1. P. 32–39. doi: 10.1109/IOTM.001.2200248.

3. H. Zhang and W. Tong. Channel Coding for 6G Extreme Connectivity–Requirements, Capabilities, and Fundamental Tradeoffs // IEEE BITS the Information Theory Magazine. March 2023. Vol. 3, no. 1. P. 54–66. doi: 10.1109/MBITS.2023.3322978.

4. M. Geiselhart, F. Krieg, J. Clausius, D. Tandler and S. ten Brink. 6G: A Welcome Chance to Unify Channel Coding? // IEEE BITS the Information Theory Magazine. March 2023. Vol 3, no. 1. P. 67–80. doi: 10.1109/MBITS.2023.3322974.

5. M. Rowshan, M. Qiu, Y. Xie, X. Gu and J. Yuan. Channel Coding Toward 6G: Technical Overview and Outlook // IEEE Open Journal of the Communications Society. 2024. Vol. 5. P. 2585–2685. doi: 10.1109/OJCOMS.2024.3390000.

6. M. M. Azeem, R. Abozariba and A. T. Asyhari. Exploiting Short Block and Concatenated Codes for Reliable Communications Within the Coexistence of 5G-NR-U and WiFi // IEEE Transactions on Vehicular Technology. Feb. 2023. Vol. 72, no. 2. P. 1893–1908. doi: 10.1109/TVT.2022.3208933.

7. J. Wang and Z. Wang. Research on Parallel Turbo Encoding and Decoding Technology // 2024 IEEE 6th Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC), Chongqing, China, 2024. P. 1378–1381. doi: 10.1109/IMCEC59810.2024.10575400.

8. F. Namadchi, M. Shirvanimoghaddam and H. El Gamal. A Parallel Concatenated Coding Scheme and List-Based Decoding Algorithm for URLLC // 2024 IEEE Wireless Communications and Networking Conference (WCNC), Dubai, United Arab Emirates, 2024. P. 1–6. doi: 10.1109/WCNC57260.2024.10570864.

9. K. Ackah Bohulu and C. Han. Interleaver Design for Turbo Codes Based on Complete Knowledge of Low-Weight Codewords of RSC Codes // 2023 IEEE Wireless Communications and Networking Conference (WCNC), Glasgow, United Kingdom, 2023. P. 1–6. doi: 10.1109/WCNC55385.2023.10118656.

10. A. Y. Sukmadji and F. R. Kschischang. Performance-Complexity-Latency Trade-Offs of Concatenated RS-BCH Codes // IEEE Transactions on Communications. July 2024. Vol. 72, no. 7. P. 3829–3841. doi: 10.1109/TCOMM.2024.3369731.

11. X. Guo, W. Zhang, H. Wang, J. Zhao and Y. Liu. High-Performance Soft Decision Decoding for Compound Channel Using RS-SPC Concatenated Codes // IEEE Communications Letters. June 2023. Vol. 27, no. 6. P. 1481–1485. doi: 10.1109/LCOMM.2023.3266896.

12. X. Liu, W. Zhang, Y. Chang and Y. Liu. A Novel Concatenation Decoding of Reed-Solomon Codes With SPC Product Codes // IEEE Signal Processing Letters. 2023. Vol. 30. P. 808–812. doi: 10.1109/LSP.2023.3291653.

13. S. Panchenko et al. Analysis of Efficiency of the Bioinspired Method for Decoding Algebraic Convolutional Codes // Eastern-European Journal of Enterprise Technologies. Mar. 2019. Vol. 2, no. 4 (98). P. 22–30, https://doi.org/10.15587/1729-4061.2019.160753.

14. M. Shirvanimoghaddam et al. Short Block-Length Codes for Ultra-Reliable Low Latency Communications // IEEE Communications Magazine. February 2019. Vol. 57, no. 2. P. 130–137. doi: 10.1109/MCOM.2018.1800181.

15. C. Yue, M. Shirvanimoghaddam, B. Vucetic and Y. Li. A Revisit to Ordered Statistics Decoding: Distance Distribution and Decoding Rules // IEEE Transactions on Information Theory. July 2021. Vol. 67, no. 7. P. 4288–4337. doi: 10.1109/TIT.2021.3078575.

Надійшла до редколегії 28.01.2025

Відомості про автора:

Штомпель Микола Анатолійович – д-р техн. наук, професор, Український державний університет залізничного транспорту, професор кафедри транспортного зв'язку; Україна; e-mail: shtompel.mykola@kart.edu.ua, ORCID: https://orcid.org/0000-0003-3132-8335

ABSTRACTS РЕФЕРАТИ

SYSTEMS AND METHODS OF INFORMATION PROTECTION
СИСТЕМИ І МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ

UDC 004.056.55

Using a fixed point instead of a floating point to implement the Falcon electronic signature0 / *O.G. Kachko, I.D. Gorbenko, S.O. Kandii* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2025. №220. P. 7 – 17.

The article examines the efficiency of using fixed-point arithmetic in cryptographic algorithms, particularly for key generation and digital signature formation. A modification of the key generation algorithm is proposed, allowing the use of a unified scale for all stages of cryptographic operations. The proposed approach simplifies the implementation of algorithms while maintaining high performance and eliminates the need for different data representation formats. A universal library was developed to support operations with arbitrary scales, enabling key operations such as multiplication, division, root extraction, and exponentiation. Special attention was given to the implementation of multiplication and division, which are the most resource-intensive operations. Multiplication is implemented using the Karatsuba algorithm, while division is based on bitwise long division. For operations involving secret keys, the requirement for time-independent execution was addressed to ensure cryptographic resistance. Complex multiplication was identified as the most resource-intensive operation due to its multi-step calculations, including multiple multiplication and division steps. Experimental studies on the performance of the algorithms were conducted on random data sets with overflow prevention and minimization of random factors influencing execution time. The results showed that the minimum execution time values for fixed-point arithmetic outperform the corresponding values for emulated floating-point mode. However, the average and maximum execution times for fixed-point arithmetic are inferior to those of floating-point emulation in most cases, which is attributed to an increase in reduce_error-type errors. These errors significantly impact key generation, as they are detected at the final stage of the operation, requiring its re-execution. The obtained results demonstrate the potential of using fixed-point arithmetic in cryptographic algorithms with optimal scale selection. This approach enhances computational efficiency and ensures time-independent execution of operations, which is critical for working with secret data. The presented findings can be utilized for further improvement of cryptographic algorithms and their implementation in resource-constrained environments.

Key words: Falcon; floating point emulation; fixed point; software implementation; lattice cryptography

3 tabl. 5 fig. Ref: 8 items.

УДК 004.056.55

Застосування фіксованої точки замість плаваючої для реалізації електронного підпису алгоритму Falcon / *О.Г. Качко, І.Д. Горбенко, С.О. Кандій* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2025. Вип. 220. С. 7 – 17.

Досліджено ефективність використання фіксованої точки у криптографічних алгоритмах, зокрема для генерації ключів та формування електронного підпису. Розглянуто модифікацію алгоритму генерації ключів, яка дозволяє використовувати єдиний масштаб для всіх етапів криптографічних операцій. Запропонований підхід забезпечує зручність реалізації алгоритмів, зберігаючи високу продуктивність, та дозволяє уникнути необхідності використання різних форматів представлення даних. Розроблено універсальну бібліотеку для роботи з довільним масштабом даних, що підтримує ключові операції множення, ділення, обчислення кореня та експоненти. Особливу увагу приділено реалізації множення та ділення, які є найресурсоємнішими операціями. Множення реалізоване з використанням алгоритму Карацуби, а ділення – на основі побітового ділення в стовпчик. Для роботи з секретними ключами враховано вимогу незалежності від часу виконання операцій, що є важливим для забезпечення криптографічної стійкості. Операція комплексного множення виявилася найбільш ресурсоємною через використання багатоступеневих обчислень, включаючи операції множення та ділення. Експериментальні дослідження продуктивності алгоритмів проводилися на випадкових наборах даних із запобіганням переповненню та мінімізацією впливу випадкових факторів на час виконання. Далі наведені результати при порівнянні середніх значень. Застосування фіксованої точки для операцій розгортання ключів забезпечило прискорення в 2,3 рази, обчислення електронного підпису в 3,7 разів в порівнянні з режимом емуляції. Водночас при генерації ключів застосування фіксованої точки для n = 512 забезпечило прискорення в 1,5 рази, а для n = 1024 – уповільнення на 22. Це пов’язано зі зростанням помилок типу reduce_error. Збільшення таких помилок суттєво впливає на операцію генерації ключів, оскільки вони визначаються наприкінці операції, що потребує її повторного виконання. Отримані результати демонструють перспективність використання фіксованої точки у криптографічних алгоритмах за умови оптимального вибору масштабу. Такий підхід дозволяє підвищити продуктивність обчислень та забезпечити незалежність від часу виконання операцій, що є критично важливим для роботи із секретними даними. Представлені результати можуть бути використані для подальшого вдосконалення криптографічних алгоритмів і їх впровадження у середовищах із обмеженими ресурсами.

Ключові слова: Falcon; емуляція плаваючої точки; фіксована точка; єдиний масштаб; програмна реалізація; криптографія на решітках.

Табл. 3. Іл. 5. Бібліогр.: 8 назв.

UDC 004.05

The Reasonability of using artificial intelligence capabilities to ensure enterprise cybersecurity based on the concept of zero trust / *V.V. Borodavka, V.I. Yesin* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2025. №220. P. 18 – 39.

Modern enterprises face increasingly complex cybersecurity challenges, which require new approaches to digital asset protection. To ensure modern enterprise cybersecurity, a complex approach is needed, including adaptive and intelligent protection mechanisms that can withstand modern threats. The traditional perimeter-based protection model is not able to provide an adequate level of protection, as modern attacks are becoming increasingly sophisticated and enterprise infrastructure is undergoing significant changes due to the expansion of the attack surface, the use of cloud technologies and remote access. In this regard, an increasing number of organizations are focusing on the concept of zero trust, which is based on the principle of "never trust, always verify" and allows for secure access to their corporate resources anytime and anywhere, as well as their efficient functioning regardless of where they are located. Implementation of the zero-trust architecture involves the usage of modern methods and technologies, including artificial intelligence. The use of artificial intelligence technologies makes it possible to effectively detect threats, identify anomalies in systems and networks, automate access control, and dynamically monitor user behavior. This paper focuses on analyzing the role of artificial intelligence in ensuring cybersecurity of enterprises in the context of the zero-trust architecture. The paper aims to determine the possibilities of using artificial intelligence technologies to increase the level of protection of information systems and identify cyber threats within the framework of the zero trust architecture. The paper briefly describes the conceptual architecture of zero trust, its main logical components and approaches to integrating artificial intelligence into them. The analysis of existing approaches leads to the conclusion that the combination of artificial intelligence and the principles of zero trust contributes to the creation of a flexible and adaptive protection system capable of detecting, analyzing and neutralizing threats in real time, increasing resilience of an enterprise to cyber threats. In addition, the paper discusses the challenges associated with integrating artificial intelligence into the zero-trust architecture. In particular, it raises the issues of adapting outdated systems, creating mechanisms and recommendations for the gradual implementation of the zero-trust architecture and training staff to work effectively in the new environment, the need to standardize data and ensure consistency in security automation processes.

Key words: zero trust; zero trust architecture; zero trust architecture deployment models; information security; cybersecurity.

1 tabl. 5 fig. Ref: 49 items.

УДК 004.05

Доцільність використання можливостей штучного інтелекту для забезпечення кібербезпеки підприємства, яка ґрунтується на концепції нульової довіри / *В.В. Бородавка, В.І. Єсін* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2025. Вип. 220. С. 18 – 39.

Сучасні підприємства стикаються з усе складнішими викликами у сфері кібербезпеки, що вимагає нових підходів до захисту цифрових активів. Для забезпечення кібербезпеки сучасного підприємства необхідний комплексний підхід, що включає адаптивні та інтелектуальні механізми захисту, здатні протистояти сучасним загрозам. Традиційна модель захисту на основі периметра не спроможна забезпечити належний рівень захисту, оскільки сучасні атаки стають дедалі складнішими, а інфраструктура підприємств зазнає значних змін у зв'язку з розширенням поверхні атак, використанням хмарних технологій та віддаленого доступу. У зв'язку з цим все більше організацій звертають увагу на концепцію нульової довіри, яка ґрунтується на принципі «ніколи не довіряй, завжди перевіряй» та дозволяє забезпечити безпечний доступ у будь-який час і в будь-якому місці до власних корпоративних ресурсів, а також їхнє ефективне функціонування незалежно від того, де вони розташовані. Реалізація архітектури нульової довіри передбачає впровадження сучасних методів і технологій, серед яких важливе місце займає штучний інтелект. Використання технологій штучного інтелекту дає змогу ефективно виявляти загрози, ідентифікувати аномальні дії в системах та мережі, автоматизувати керування доступом та здійснювати динамічний контроль поведінки користувачів. Стаття націлена на аналіз ролі штучного інтелекту в забезпеченні кібербезпеки підприємств у контексті архітектури нульової довіри. Мета роботи – визначити можливості застосування технологій штучного інтелекту для підвищення рівня захисту інформаційних систем та ідентифікації кіберзагроз у рамках архітектури нульової довіри. У стислому викладі розглядаються концептуальна архітектура нульової довіри, її основні логічні компоненти та підходи до інтеграції штучного інтелекту в них. Аналіз існуючих підходів дозволяє зробити висновок, що поєднання штучного інтелекту та принципів нульової довіри сприяє створенню гнучкої та адаптивної системи захисту, здатної в реальному часі виявляти, аналізувати та нейтралізувати загрози, підвищуючи стійкість підприємства до кіберзагроз. Крім того, у роботі розглядаються виклики, пов'язані з інтеграцією штучного інтелекту до архітектури нульової довіри. Зокрема, порушуються питання адаптації застарілих систем, створення механізмів та рекомендацій для поступового впровадження архітектури нульової довіри та навчання персоналу для ефективної роботи в нових умовах, необхідності стандартизації даних та забезпечення узгодженості процесів автоматизації безпеки.

Ключові слова: нульова довіра; архітектура нульової довіри; штучний інтелект; машинне навчання; інформаційна безпека; кібербезпека.

Табл. 1. Іл. 5. Бібліогр.: 49 назв.

UDC 004.8

Study of the current state and prospects of artificial intelligence in cybersecurity / *Yu.L. Golikov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2025. №220. P. 40 – 49.

In the modern world, with the development of new technologies, artificial intelligence (AI) in cybersecurity has become an integral component. Therefore, studying its advantages, risks, and potential use cases is a highly relevant research topic. In current digital environment, where cyber threats are becoming increasingly sophisticated, the implementation of AI technologies significantly enhances the effectiveness of security systems by enabling automated threat detection and response. In this study the main applications of AI in cybersecurity were examined, including threat detection, malware analysis, cryptographic security enhancement, phishing protection, and attack prediction. One of the key aspects is the integration of AI into Security Information and Event Management (SIEM) systems, which analyze vast amounts of data and help to detect anomalies. Such systems reduce the workload on security teams and improve the accuracy and speed of threat response. Special attention is given to the analysis of modern AI-powered antivirus solutions, particularly Microsoft Defender for Endpoint and Darktrace. These solutions are based on behavioral analysis algorithms and machine learning, allowing for more effective detection of complex threats and incident prevention. Microsoft Defender provide a high level of endpoint protection. Meanwhile, Darktrace utilizes self-learning models to analyze network traffic, enabling the detection of zero-day threats and internal risks within organizations. The study also learns the major risks associated with the use of AI in cybercrime. AI is increasingly leveraged by malicious actors to automate attacks, significantly increasing their effectiveness and making detection more challenging. The primary AI-based cyber threats discussed include Data Poisoning attacks, Evasion Attacks, Prompt Injection Attacks, and AI-based social engineering. To mitigate these risks, the development of robust AI models resistant to adversarial attacks, increased algorithm transparency, and implementation of the International AI regulation standards is recommended, including NIST. Additionally, raising awareness among users and cybersecurity specialists is crucial, as the human factor remains one of the most significant vulnerabilities in security systems. In conclusion, it is said that AI is a key factor in the advancement of cybersecurity, offering significant improvements in protecting information and critical systems. However, without proper regulation and protective measures, AI can become a powerful tool for cybercriminals, posing new security challenges in the digital age. Striking a balance between innovation, ethical standards, and security will be essential in shaping the future strategy for the effective use of AI.

Key words: artificial intelligence; cybersecurity; machine learning; SIEM; IDS; AI-based antivirus.

1 tabl. 2 fig. Ref: 27 items.

УДК 004.8

Дослідження поточного стану та перспективи застосування штучного інтелекту в кібербезпеці / *Ю.Л. Голіков* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2025. Вип. 220. С. 40 – 49.

В сучасному світі з розвитком нових технологій, штучний інтелекту (ШІ) у сфері кібербезпеки є невід'ємною складовою, тому вивчення його переваг, ризиків та можливі сценарії використання є актуальною темою дослідження. В сучасному цифровому середовищі, де кіберзагрози стають дедалі складнішими, впровадження технологій ШІ значно підвищує ефективність систем захисту, дозволяючи автоматизувати виявлення та реагування на атаки. Тому було розглянуто основні напрями застосування ШІ в кібербезпеці, зокрема виявлення загроз, аналіз шкідливого програмного забезпечення, посилення криптографії, захист від фішингових атак та прогнозування атак. Одним із ключових аспектів є інтеграція ШІ в системи управління інформаційною безпекою (SIEM), які аналізують величезні обсяги даних та допомагають виявляти аномалії. Такі системи значно знижують навантаження на команди безпеки та підвищують точність і швидкість реагування. Окрему увагу приділено аналізу сучасних антивірусних рішень, що використовують штучний інтелект, а саме Microsoft Defender for Endpoint та Darktrace. Вони базуються на алгоритмах поведінкового аналізу та машинного навчання, що дозволяє ефективніше виявляти складні загрози та запобігати інцидентам. Microsoft Defender забезпечує високий рівень захисту кінцевих точок. Натомість Darktrace використовує самонавчальні моделі для аналізу мережевого трафіку, що дозволяє виявляти загрози нульового дня та внутрішні загрози в організаціях. Розглянуто основні ризики, пов'язані із використанням ШІ у кіберзлочинності. ШІ активно застосовується зловмисниками для автоматизації атак, що значно підвищує їхню ефективність і складність виявлення. Розглянуто основні типи загроз на основі ШІ, а саме такі атаки, як атаки отруєння даних, атаки ухилення, атаки швидкого впровадження та соціальна інженерія на основі ШІ. Для зменшення ризиків пропонується розробка стійких моделей ШІ, що менше піддаються атакам, підвищення прозорості алгоритмів, а також впровадження міжнародних стандартів регулювання ШІ, чим активно займаються великі команди дослідників, серед яких і NIST. Рекомендується підвищення обізнаності користувачів та спеціалістів з кібербезпеки, оскільки людський фактор залишається однією з найбільших вразливостей систем. Наголошується, що штучний інтелект є ключовим фактором розвитку кібербезпеки, який може значно покращити захист інформації та критичних систем. Водночас, без належного регулювання та захисних заходів, ШІ може стати потужним інструментом для зловмисників, що створює нові виклики для безпеки в цифрову епоху. Баланс між інноваціями, етичними нормами та безпекою стане ключовим фактором у формуванні стратегії ефективного використання ШІ у майбутньому.

Ключові слова: штучний інтелект; кібербезпека; машинне навчання; SIEM; IDS; антивірус на основі ШІ.

Табл. 1. Іл. 2. Бібліогр.: 27 назв.

UDC 681.3.07 (3.06)

Classification of attacks and cyber security requirements for the QRNG web resource / *D.M. Morhul, O.P. Nariezhnii, T.O. Hrinenko* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2025. №220. P. 50 – 57.

Web services of quantum random number generators (QRNG) open new opportunities for enhancing the resilience of cryptographic systems due to their ability to generate true random numbers based on quantum effects. Unlike pseudo-random number generators (PRNG), the QRNG ensures a high level of unpredictability in output data, making them critical components in modern security systems. However, their implementation is accompanied by significant challenges, particularly due to potential attacks at the software level and during integration with hardware infrastructure.

At the software level, major threats include attacks on cryptographic libraries, substitution or manipulation of runtime output data, and side-channel attacks exploiting information leaks from physical number generation processes. At the hardware level, risks arise from equipment defects, failures in integration processes, or improper operation of the QRNG in combination with other systems.

This study provides a classification of the main types of attacks on QRNG web services, presents an analysis of existing attacks, and introduces modern approaches to their prevention. Among the key solutions are the certification of the QRNG during development and deployment, multi-factor verification of output data to ensure unpredictability, and the use of monitoring systems with artificial intelligence algorithms for anomaly detection. Special attention is given to hybrid protection methods that combine the QRNG with quantum key distribution (QKD) and post-quantum cryptographic algorithms, allowing for the mitigation of risks from both classical and quantum attacks.

Thus, a comprehensive combination of software and hardware security methods will enhance the reliability of QRNG and their resilience to modern threats. Further research should focus on the implementation of unified standards for QRNG and the optimization of their integration into existing cryptographic systems.

Key words: attack; cybersecurity; extractor; quantum cryptography; AI monitoring system; Quantum Random Number Generator.

1 tabl. Ref: 9 items.

УДК 681.3.07 (3.06)

Класифікація атак та вимоги кібербезпеки до веб-ресурсу QRNG / *Д.М. Моргуль, О.П. Нарєжній, Т.О. Гріненко* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2025. Вип. 220. С. 50 – 57.

Веб сервіси квантових генераторів випадкових чисел (Quantum Random Number Generator, QRNG) відкривають нові можливості для забезпечення стійкості криптографічних систем завдяки їхній здатності генерувати справжні випадкові числа на основі квантових ефектів. На відміну від генераторів псевдовипадкових чисел (Pseudo Random Number Generator, PRNG), QRNG забезпечують високу непередбачуваність вихідних даних, що робить їх критичними компонентами у сучасних системах безпеки. Однак їх впровадження супроводжується значними викликами, зокрема через потенційні атаки на програмному рівні та на рівні інтеграції з апаратною інфраструктурою.

На програмному рівні основні загрози включають атаки на криптографічні бібліотеки, підміну або маніпуляцію вихідними даними середовища виконання, а також атаки через бічні канали, які експлуатують витоки інформації з фізичних процесів генерації чисел. На апаратному рівні виникають ризики, пов'язані з дефектами обладнання, збоєм у процесах інтеграції або некоректною роботою QRNG у поєднанні з іншими системами.

У роботі надано класифікацію основних типів атак на веб-сервіси QRNG, результати аналізу існуючих атак та представлено сучасні підходи щодо їх запобігання. Серед ключових рішень відокремлюються: сертифікація QRNG на етапі розробки й використання, мультифакторна перевірка вихідних даних для забезпечення їх непередбачуваності та використання систем моніторингу з алгоритмами штучного інтелекту для виявлення аномалій. Приділено увагу гібридним методам захисту, які поєднують QRNG із квантовою ключовою дистрибуцією (Quantum Key Distribution, QKD) та постквантовими криптографічними алгоритмами, що дозволяє мінімізувати ризики як класичних, так і квантових атак.

Таким чином, комплексне поєднання програмних і апаратних методів забезпечення безпеки дозволить підвищити надійність QRNG та їх стійкість до сучасних загроз. Подальші дослідження мають бути зосереджені на впровадженні уніфікованих стандартів для QRNG та оптимізації їх інтеграції в існуючі криптографічні системи.

Ключові слова: атака; кібербезпека; екстрактор; квантова криптографія; AI система моніторингу; Quantum Random Number Generator.

Табл. 1. Бібліогр.: 9 назв.

UDC 621.317.76.089.68:621.373.82

Models and methods for protecting an autonomous differential correction system for global navigation satellite systems against cyber threats / *O.A. Snieosikov, O.P. Nariezhnii, T.O. Hrinenko* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2025. №220. P. 58 –74.

Ensuring stable, accurate, and secure satellite navigation requires not only investment in cybersecurity systems for Global Navigation Satellite Systems (GNSS), but also continuous research into emerging cyber threats, as well as finding effective methods to neutralize them, particularly in the post-quantum era. Among the key protection mechanisms, the following should be highlighted: secure signal transmission protocols that prevent data interception and tampering;

authentication mechanisms that enable the identification of legitimate satellite signals; anti-spoofing technologies that detect and neutralize attempts to manipulate navigation data; and protection technologies for the information and communication systems of autonomous differential correction systems to ensure the confidentiality, integrity, and availability of GNSS data.

The research results obtained in this work and the proposed security measures may serve as a foundation for the development of a national system for coordinate, time, and navigation support in Ukraine. The adoption of appropriate legislation and standards will help to ensure the cyber resilience of navigation systems and support their integration into the European satellite infrastructure.

Key words: GPS jamming; GNSS; information and communication system; QRNG; cyberattack; cybersecurity; GPS; Differential GNSS; GPS spoofing; IDS; IPS.

6 fig. Ref: 44 items.

УДК 621.317.76.089.68:621.373.82

Моделі та методи захисту від кіберзагроз автономної системи диференціальної корекції глобальних навігаційних супутникових систем / *О.А. Снєосіков, О.П. Нарєжній, Т.О. Гріненко* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2025. Вип. 220. С. 58 – 74.

Забезпечення стабільної, точної та безпечної супутникової навігації вимагає не лише інвестування у системи кібербезпеки глобальних навігаційних супутникових систем (Global Navigation Satellite Systems, GNSS), а й постійного дослідження та вивчення нових кіберзагроз, а також пошуку ефективних методів їх нейтралізації, зокрема у постквантовий період. Серед ключових механізмів захисту слід виділити: захищені протоколи передачі сигналів, що запобігають перехопленню та підробці даних; механізми автентифікації, які дозволяють ідентифікувати легітимні супутникові сигнали; антиспуфінгові технології, що виявляють та нейтралізують спроби маніпуляції навігаційними даними; технології захисту інформаційно-комунікаційних систем автономних систем диференціальної корекції для забезпечення конфіденційності, цілісності та доступності GNSS даних.

Отримані у роботі результати дослідження та запропоновані заходи безпеки можуть бути використані як основа для реалізації національної системи координатно-часового та навігаційного забезпечення України. Впровадження відповідного законодавчого регулювання та стандартів дозволить забезпечити кіберстійкість навігаційних систем та інтегрувати їх у європейську супутникову інфраструктуру.

Ключові слова: глушіння сигналу; глобальна навігаційна супутникова система; інформаційно-комунікаційна система; квантовий генератор випадкових чисел; кібератака; кібербезпека; система глобального позиціонування; система диференціальної корекції; спуфінг сигнал; система виявлення вторгнень; система запобігання вторгненням.

Іл. 6. Бібліогр.: 44 назв.

UDC 621.373.8+621.391+681.88

Targeted interference to laser acoustic reconnaissance / *V.I. Zabolotnyi, N.O. Kholiev, V.S. Dovgal* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2025. №220. P. 75 – 81.

Methods of laser acoustic reconnaissance (LAR) of information disclosed at information activity objects (IAOs) are constantly being improved. Complexes of measures and means of protection against technical channels of information leakage (TCIL) of this nature are being developed and applied, which emphasizes the relevance of research on the topic of this work.

The elements of the technical channel of information leakage are quantitatively analyzed: the parameters of window glass oscillation, the features of the operating principle of interference-type LAR, the lateral characteristics of the laser emission beam, and it is proposed to use them to create a targeting frequency band and direction of propagation of lateral emissions of the LAR beam by using corner reflectors in the infrared spectrum of optical vibrations.

Key words: protection of voiced information; laser acoustic reconnaissance; targeted interference.

4 fig. Ref: 5 items.

УДК 621.373.8+621.391+681.88

Прицільні перешкоди лазерним засобам акустичної розвідки / *В.І. Заболотний, Н.О. Холев, В.С. Довгаль* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2025. Вип. 220. С. 75 – 81.

Постійно удосконалюються методи лазерних засобів акустичної розвідки (ЛЗАР) інформації, що озвучується на об’єктах інформаційної діяльності (ОІД). Розвиваються і застосовуються комплекси заходів і засобів захисту від технічного каналу витоку інформації (ТКВІ) цієї природи, що підкреслює актуальність досліджень за темою роботи.

Кількісно проаналізовано елементи технічного каналу витоку інформації: параметри коливання шибки вікна, особливості принципу дії ЛЗАР інтерференційного типу, бічні характеристики променя випромінювання лазеру, запропоновано використовувати для створення прицільних по смузі частот і напряму поширення бічних випромінювань променя ЛЗАР за рахунок використання кутикових відбивачів в інфрачервоному діапазоні оптичних коливань.

Ключові слова: захист інформації, що озвучується; лазерний засіб акустичної розвідки; прицільна перешкода

Іл. 4. Бібліогр.: 5 назв.

UDC 004.056.5

Research and classification of the main types of attacks on artificial intelligence systems in cybersecurity / *Yu.L. Golikov, Ye.V. Ostrianska* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2025. №220. P. 82 – 91.

The modern development of artificial intelligence (AI) and machine learning (ML) opens up new opportunities in the field of cybersecurity, but at the same time creates serious challenges in the form of intelligent cyberattacks. The study is devoted to the analysis and classification of ways to use AI for malicious purposes and the study of effective methods to counter such threats. In particular, the article covers the main types of attacks using ML technologies, which demonstrate how attackers can manipulate machine learning algorithms, undermine trust in data, and bypass protection systems. Special attention is paid to the mechanisms of data poisoning attacks, as they are considered the most influential in machine learning, which involve introducing malicious data into the process of training models, which leads to distortion of results and undermines the effectiveness of security algorithms. Evasion attacks are also considered, in which attackers create unique data samples that can remain invisible to traditional threat detection systems. Privacy attacks are analyzed as a way to obtain confidential information from ML models, which can be used to steal user data. Abuse attacks demonstrate how attackers can use AI tools to automate attacks, scale phishing campaigns, and analyze vulnerabilities in defense systems. The relevance of the study is due to the fact that traditional approaches to cyber defense are no longer able to effectively counter threats that adapt and evolve due to machine learning. The article emphasizes the critical importance of researching defense methods, in particular, building reliable machine learning systems that have built-in mechanisms for detecting anomalies and adapting to new threats. One of the key approaches is federated learning, which allows training models without centralized data storage, reducing the risk of information leakage. The development of deep learning in the field of cyber defense is also considered, which allows analyzing behavioral patterns of threats in real time. The combination of technological measures with human control remains an important aspect, since, despite the power of AI tools, the human factor remains key in the process of ensuring cybersecurity. Thus, the article demonstrates the balance between the opportunities and threats of AI in the field of cybersecurity, emphasizing the need for further research in the direction of resilient ML models that can effectively resist attacks. Without proper regulation and control, AI can become not only a defender, but also a tool for attackers, which requires the development of new security strategies and international regulation in the field of cybersecurity.

Key words: artificial intelligence; cyberattacks; machine learning; cybersecurity; federated learning.

1 tabl. 2 fig. Ref: 25 items.

УДК 004.056.5

Дослідження та класифікація основних типів атак на системи штучного інтелекту в кібербезпеці / *Ю.Л. Голіков, Є.В. Острянська* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2025. Вип. 220. С. 82 – 91.

Сучасний розвиток штучного інтелекту (ШІ) та машинного навчання (ML) відкриває нові можливості у сфері кібербезпеки, проте водночас створює серйозні виклики у вигляді інтелектуальних кібератак. Дослідження присвячене аналізу та класифікації способів використання ШІ у зловмисних цілях та вивченню ефективних методів протидії таким загрозам. Зокрема, стаття охоплює основні види атак, що використовують технології ML, які демонструють, як зловмисники можуть маніпулювати алгоритмами машинного навчання, підривати довіру до даних та обходити системи захисту. Окрему увагу приділено механізмам атак отруєння даних, так як вони вважаються найбільш небезпечними при машинному навчанні, які передбачають внесення шкідливих даних у процес навчання моделей, що призводить до викривлення результатів та підриву ефективності алгоритмів безпеки. Також розглядаються атаки проникнення, у яких атакуючі створюють унікальні зразки даних, що можуть залишатися невидимими для традиційних систем виявлення загроз. Атаки на конфіденційність аналізуються як спосіб отримання конфіденційної інформації з ML-моделей, що може використовуватися для викрадення даних користувачів. Атаки зловживання демонструють, як зловмисники можуть використовувати ШІ-інструменти для автоматизації атак, масштабування фішингових кампаній та аналізу слабких місць захисних систем. Актуальність дослідження зумовлена тим, що традиційні підходи до кіберзахисту вже не здатні ефективно протистояти загрозам, які адаптуються та еволюціонують завдяки машинному навчанню. Стаття наголошує на критичній важливості дослідження методів захисту, зокрема побудови надійних систем машинного навчання, що мають вбудовані механізми виявлення аномалій та адаптацію до нових загроз. Одним із ключових підходів є федеративне навчання, яке дозволяє тренувати моделі без централізованого зберігання даних, зменшуючи ризик витоку інформації. Також розглянуто розвиток глибокого навчання у сфері кіберзахисту, що дозволяє аналізувати поведінкові патерни загроз у режимі реального часу. Важливим аспектом залишається поєднання технологічних заходів із людським контролем, оскільки, незважаючи на потужність ШІ-інструментів, людський фактор залишається ключовим у процесі забезпечення кібербезпеки. Отже, стаття демонструє баланс між можливостями та загрозами ШІ у сфері кібербезпеки, підкреслюючи необхідність подальших досліджень у напрямку стійких ML-моделей, які можуть ефективно протистояти атакам. Без належного регулювання та контролю ШІ може стати не лише захисником, а й інструментом зловмисників, що вимагає розробки нових стратегій безпеки та міжнародного врегулювання у сфері кіберзахисту.

Ключові слова: штучний інтелект; кібератаки; машинне навчання; кібербезпека; федеративне навчання.

Табл. 1. Іл. 2. Бібліогр.: 25 назв.

UDC 621.391:519.2

Analysis of the limitations of quantum computing in cryptoanalysis problems / *Y.V. Kotukh, G.Z. Khalimov, M.V.Korobchynskyi, I.Y.Dzhura* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2025. №220. P. 92– 101.

The NISQ era is a transitional phase in the development of quantum computing with a limited number of qubits and high noise levels. In response to the limitations, specialized algorithms have been developed, such as the variational quantum eigenvalue algorithm (VQE) for modeling molecular structures, and QAOA for solving combinatorial optimization problems. To reduce the impact of noise on the calculations, effective strategies are used: randomized compilation (RC) and zero-noise extrapolation (ZNE). Hybrid quantum-classical approaches are also being developed that combine quantum generation with classical optimization and processing methods. Potential areas of application of NISQ technologies include the optimization of logistics problems, financial modeling, and supply chain optimization. In cryptography, NISQ devices stimulate the development of quantum-resistant encryption algorithms. The main challenges remain the limited scalability of systems and the problem of noise in quantum computing. The search for new architectures, including topological qubits and "glass" chips for a more stable environment, continues. An important trend is the gradual transition to the era of fully fault-tolerant quantum computers (FTQC), expected in the period 2025-2029. Unlike NISQ, which focuses on noise reduction methods, FTQC implements full quantum error correction (QEC). Quantum computing has transformed from an academic discipline into a field with a clear commercial strategy. Despite current limitations, existing achievements open up real opportunities for the applied use of quantum computing in cryptography. The analysis of mathematical criteria of different eras of quantum computing development has implications for solving cryptanalytic problems, transforming the understanding of the time frames and methodological approaches to overcoming cryptographic protection of classical cryptosystems.

Key words: quantum computer; postquantum cryptography; cryptanalysis; NISQ; EFTQC; FTQC.

Tab. 5. Ref: 16 items.

УДК 004.056.55

Аналіз обмежень квантових обчислень у задачах криптоаналізу / *Є.В. Котух, Г.З. Халімов, М.В. Коробчинський, І.Є. Джура* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2025. Вип. 220. С. 92– 101.

NISQ-ера є перехідною фазою розвитку квантових обчислень з обмеженою кількістю кубітів та високим рівнем шуму. У відповідь на обмеження розроблено спеціалізовані алгоритми, як-от варіаційний квантовий алгоритм знаходження власних значень (VQE) для моделювання молекулярних структур, та QAOA для вирішення комбінаторних оптимізаційних задач. Для зменшення впливу шуму на обчислення використовуються ефективні стратегії: рандомізована компіляція (RC) та екстраполяція до нульового шуму (ZNE). Також розвиваються гібридні квантово-класичні підходи, що поєднують квантову генерацію з класичними методами оптимізації та обробки результатів. Потенційні сфери застосування NISQ-технологій охоплюють оптимізацію логістичних задач, фінансове моделювання та оптимізацію ланцюгів постачання. У криптографії NISQ-пристрої стимулюють розвиток квантово-стійких алгоритмів шифрування. Головними викликами залишаються обмежена масштабованість систем та проблема шуму в квантових обчисленнях. Триває пошук нових архітектур, включаючи топологічні кубіти та "скляні" чіпи для стабільнішого середовища. Важливою тенденцією є поступовий перехід до ери квантових комп'ютерів із повноцінною толерантністю до помилок (FTQC), які очікуються в період 2025-2029 рр. На відміну від NISQ, що фокусуються на методах зниження шуму, FTQC впроваджує повноцінну квантову корекцію помилок (QEC). Квантові обчислення перетворились із академічної дисципліни на сферу з чіткою комерційною стратегією. Незважаючи на поточні обмеження, наявні досягнення відкривають реальні можливості для прикладного використання квантових обчислень у криптографії. Аналіз математичних критеріїв різних епох розвитку квантових обчислень має наслідки для вирішення криптоаналітичних задач, трансформуючи розуміння часових рамок та методологічних підходів до подолання криптографічного захисту класичних криптосистем.

Ключові слова: квантовий комп’ютер; постквантова криптографія; крипто аналіз; NISQ; EFTQC; FTQC.

Табл. 5. Бібліогр.: 11 назв.

AUTOMATION AND ROBOTICS
АВТОМАТИЗАЦІЯ ТА РОБОТОТЕХНІКА

UDC 004.932

Automated information and visualization system for optical control of ultra thin microcables / *I.Sh. Nevlyudov, O.M. Listratenko, I.V. Borschov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2025. №220. P. 102 – 111.

The paper highlights the analyzed types of critical and minor defects in flexible Al-Pi microcables and developed their systematization. A thorough and detailed study of methods for detecting defects, obtaining and processing information was conducted, it allowed us to select optimal approaches for automated optical inspection. A structural diagram of an optical inspection system (OIS) has been developed, it provides effective detection of defects in flexible ultrathin microcables used in sensor modules and digital track detector calorimeters. The technical support and equipment of the OIS workplace were also provided, including modern means of optical analysis and computer data processing.

The OIS, an automated optical inspection system, was created, it can be used in production and it has a wide range of functions and characteristics making it possible to detect effectively various surface defects while ensuring high

quality and reliability of flexible ultrathin Al-Pi microcables. In the process of work, modern methods for improving the accuracy and speed of optical control of the developed and tested system were analyzed, they allowed us to identify promising areas for further improvement of the system.

Key words: optical inspection system; structural diagram; workplace; ultra thin microcables.

1 tabl. 4 fig. Ref: 7 items.

УДК 004.932

Автоматизована інформаційно-вимірювальна система оптичного контролю гнучких надтонких мікрокабелів / *І.Ш. Невлюдов, О.М. Лістратенко, І.В. Борщов* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2025. Вип. 220. С. 102 – 111.

Виконано аналіз видів критичних та малозначних дефектів гнучких Al-Pi мікрокабелів та розроблено їх систематизацію. Проведено детальне дослідження методів виявлення дефектів, отримання та обробки інформації, що дозволило вибрати оптимальні підходи для автоматизованого оптичного контролю. Розроблено структурну схему інформаційно-вимірювальної системи (ІВС) оптичного контролю, яка забезпечує ефективне виявлення дефектів у гнучких надтонких мікрокабелів, що застосовуються у сенсорних модулях та цифрових трекових детекторних калориметрах. Виконано технічне забезпечення та оснащення робочого місця ІВС, що включає сучасні засоби оптичного аналізу та комп'ютерної обробки даних.

Створено ІВС автоматизованого оптичного контролю, що може використовуватися на виробництві і має широкий набір функцій та характеристик, які дозволяють ефективно виявляти різноманітні поверхневі дефекти при забезпеченні високої якості та надійності гнучких надтонких Al-Pi мікрокабелів.

Проаналізовано сучасні методи покращення точності та швидкості оптичного контролю системи, що була розроблена та протестована, що дозволило визначити перспективні напрямки її подальшого вдосконалення.

Ключові слова: інформаційно-вимірювальна система оптичного контролю; структурна схема; робоче місце; надтонкі мікрокабелі.

Табл. 1. Іл. 4. Бібліогр.: 7 назв.

RADIO ELECTRONIC SYSTEMS
РАДІОЕЛЕКТРОННІ СИСТЕМИ

UDC 621.396.96

Methods for acoustic sounding of the atmosphere using antenna arrays / *V.M. Kartashov, R.O. Bobnev* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2025. №220. P. 112 – 119.

Acoustic sounding systems (AS) of the atmosphere – sodars provide information on the state of processes occurring in the lower layers of the atmosphere. They allow measuring vertical profiles of wind speed and direction, turbulence parameters. The information obtained is used in applied tasks to ensure takeoff and landing of aircraft, study of atmospheric processes. However, the effectiveness of existing acoustic means is insufficient and there are practical needs for the development of appropriate promising methods of sounding and signal processing, which will be implemented when building specific stations.

The recent development of effective piezoelectric acoustic emitters has provided the possibility of creating acoustic antennas for sodars in the form of antenna arrays, which has had a significant impact on the structure of the acoustic locator and allows expanding significantly its potential capabilities. However, the use of acoustic antenna arrays in sodars has a number of features, so it is necessary to conduct additional research to analyze the potential capabilities of emerging sodars.

The article considers methods for remote sensing of the atmosphere by sodars with an antenna array when performing simultaneous sensing in several directions. Adequate mathematical models of acoustic signals and methods of multi-channel sensing have been developed, mathematical computer modeling of sensing processes has been performed. The proposed method has been analyzed when performing simultaneous sensing of the atmosphere in several directions at one frequency, as well as when using different frequencies of sensing signals in different directions. The implementation of the considered methods in practice will ensure increased efficiency and reduced time for measuring atmospheric characteristics.

Mathematical modeling of methods for adaptive spatial selectivity of acoustic locators with an adaptive antenna array has been performed, their significant potential capabilities have been shown. The implementation of such methods in practice will allow increasing significantly the noise immunity of acoustic locators, especially when they operate in difficult interference conditions, for example, in airport conditions.

Key words: acoustic sounding of the atmosphere; sodar; method; acoustic antenna array; synthesis; sounding signal; radiation pattern; optimality criterion.

5 fig. Ref: 21 items.

УДК 621.396.96

Методи акустичного зондування атмосфери з використанням антенних решіток / *В.М. Карташов, Р.О. Бобнєв* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2025. Вип. 220. С. 112 – 119.

Системи акустичного зондування (АЗ) атмосфери – содари забезпечують отримання інформації про стан процесів, що відбуваються в нижніх шарах атмосфери. Вони дозволяють вимірювати вертикальні профілі швидкості і напрямку вітру, параметрів турбулентності. Отримана інформація використовується в прикладних за-

дачах для забезпечення зльоту та посадки літальних апаратів, вивчення атмосферних процесів. Проте ефективність існуючих акустичних засобів є недостатньою і існують потреби практики з розробки відповідних перспективних методів зондування та обробки сигналів, що реалізуватимуться при побудові конкретних станцій.

Розробка ефективних п'єзоелектричних акустичних випромінювачів забезпечила можливість створення акустичних антен содарів у вигляді антенних решіток, що значно вплинуло на структуру акустичного локатора і надає змогу суттєво розширити його потенційні можливості. Однак використання акустичних антенних решіток у содарах має і низку особливостей, тому необхідно провести додаткові дослідження з метою аналізу потенційних можливостей содарів, що відкриваються.

В статті розглянуто методи дистанційного зондування атмосфери содарами з антенною решіткою при виконанні одночасного зондування у декількох напрямках. Розроблено адекватні математичні моделі акустичних сигналів і методів багатоканального зондування, виконано математичне комп'ютерне моделювання процесів зондування. Проаналізовано запропонований метод при виконанні одночасного зондування атмосфери в декількох напрямках на одній частоті, а також при використанні різних частот зондувальних сигналів у різних напрямках. Реалізація розглянутих методів на практиці забезпечить підвищення оперативності та скорочення часу вимірювання характеристик атмосфери.

Виконано математичне моделювання методів адаптивної просторової вибірковості акустичних локаторів з адаптивною антенною решіткою, показано їхні значні потенційні можливості. Реалізація таких методів на практиці дасть змогу суттєво підвищити завадозахищеність акустичних локаторів, особливо за їхньої роботи в умовах складної завадової обстановки, наприклад в умовах аеропорту.

Ключові слова: акустичне зондування атмосфери; содар; метод; акустична антенна решітка; синтез; зондувальний сигнал; діаграма спрямованості; критерій оптимальності.

Іл. 5. Бібліогр.: 21 назв.

UDC 621.39:534.87]:004.056.5

Features of detecting acousto-electromagnetic information leakage channels / *A.M. Oleynikov, Yu.V. Lykov, Y.S. Pavlenko* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2025. №220. P. 120 – 127.

The article highlights the features of the formation and detection of acousto-electromagnetic information leakage channels caused by acousto-electric transformations in technical devices. These channels present a significant threat to information security, as they convert acoustic oscillations into electrical or electromagnetic signals that may carry confidential information.

The primary focus is on the classification of acousto-electric and acousto-magnetic channels, which are divided into direct and modulation channels. Direct channels arise from the direct interaction of acoustic waves with sensitive device elements, such as piezoelectric elements, speakers, or transformers. Modulation channels are formed when acoustic influence changes the parameters of high-frequency generator signals, creating hazardous modulations.

The physical processes underlying acousto-electric and acousto-magnetic transformations are examined. Acoustic waves alter the electrical parameters of sensitive elements such as inductance, capacitance, or electromagnetic permeability. This leads to the generation of signals that can be detected in power networks or transmission lines.

The article describes methods for detecting acousto-electromagnetic channels. For direct channels, a setup including an acoustic generator, a sound wave emitter, and a spectrum analyzer that records output electrical signals is used. For modulation channels, an analysis of high-frequency signals modulated by acoustic waves is applied.

A comprehensive set of measures to neutralize acousto-electromagnetic channels is proposed. These measures include shielding technical devices to protect against acoustic waves, using noise-absorbing materials, optimizing device designs to reduce their sensitivity to acoustic influences, and monitoring the acoustic environment using spectrum analyzers. Masking signals in rooms with high-security requirements are also an effective measure.

Key words: acousto-electric channels; signal modulation; information leakage; data protection; piezoelectric effect.

4 fig. Ref: 12 items.

УДК 621.39:534.87]:004.056.5

Особливості виявлення акустоелектромагнітних каналів витоку інформації / *А.М. Олейніков, Ю.В. Ликов, Я.С. Павленко* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2025. Вип. 220. С. 120 – 127.

Висвітлено особливості формування та виявлення акустоелектромагнітних каналів витоку інформації, які виникають через акустоелектричні перетворення у технічних пристроях. Зазначені канали є значною загрозою для інформаційної безпеки, оскільки перетворюють акустичні коливання на електричні або електромагнітні сигнали, що можуть нести конфіденційну інформацію.

Основна увага приділена класифікації акустоелектричних і акустомагнітних каналів, які поділяються на прямі та модуляційні. Прямі канали утворюються внаслідок безпосередньої взаємодії акустичних хвиль із чутливими елементами пристроїв, такими як п’єзоелементи, гучномовці чи трансформатори. Модуляційні канали виникають тоді, коли акустичний вплив змінює параметри сигналів високочастотних генераторів, створюючи небезпечні модуляції.

Розглянуто фізичні процеси, що лежать в основі акустоелектричних та акустомагнітних перетворень. Акустичні хвилі змінюють електричні параметри чутливих елементів, таких як індуктивність, ємність або

електромагнітна проникність. Це викликає появу сигналів, які можуть бути виявлені у мережах живлення або передавальних лініях.

Описано методики виявлення акустоелектромагнітних каналів. Для прямих каналів використовується схема з акустичним генератором, випромінювачем звукових хвиль і спектроаналізатором, який фіксує вихідні електричні сигнали. Для модуляційних каналів застосовується аналіз високочастотних сигналів, модульованих акустичними хвилями.

Запропоновано комплекс заходів для нейтралізації акустоелектромагнітних каналів. Вони включають екранування технічних засобів для захисту від акустичних хвиль, використання шумозаглушувальних матеріалів, оптимізацію конструкцій пристроїв для зниження їх чутливості до акустичних впливів, а також моніторинг акустичного середовища за допомогою спектроаналізаторів. Маскувальні сигнали у приміщеннях із високими вимогами до безпеки також є дієвим заходом.

Ключові слова: акустоелектричні канали; модуляція сигналів; виток інформації; захист даних; п'єзоелектричний ефект.

Іл. 4. Бібліогр.: 12 назв.

UDC 621.396; 550.388

Improvement of ionospheric sounding modes in the incoherent scatter technique / *L.Ya. Emelyanov, V.O. Pulyayev, N.O. Kuzmenko, D.A. Dziubanov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2025. №220. P. 128 – 135.

Improvement of the modes of high-frequency radio waves pulsed radiation, reception and processing of received signals incoherently scattered by ionospheric plasma, implemented using incoherent scatter radars intended for remote sensing of near-Earth space are exemplified. An analysis of some modes of radio pulse sounding was carried out, namely the mode using a long radio pulse intended for the upper ionosphere study, and a mode for the lower ionosphere study, when the sounding signal was emitted in the form of two short elements, the distance between which varied depending on the radar scan number. The advantages and disadvantages of these modes are shown. Options for using radio pulses of a more complex structure are proposed due to the optimal coding of a larger number of elements taking into account the nature of scattering in the ionospheric plasma. The results of the search for multi-element coded signals for the study of the lower and upper altitude ranges are presented, providing the calculation of the ordinates of the scattered signal autocorrelation function with high resolution both in space and time. The hardware implementation of sounding modes using these signals is presented. In particular, a block diagram of the incoherent scatter radar is presented for working with signals of opposite circular polarizations, which uses for this purpose-controlled phase shifters of the transmitter excitation system, orthogonal antenna vibrators and ring bridge of the receiving-feeder path. The change in the parameters of the high-frequency filling of the sounding radio signal is carried out according to the signals of the radar control system. In general, this makes it possible to transmit and receive signals with various coding options for their elements, most suitable for specific conditions, and to use modes in which the direction of circular rotation of the plane of polarization of the radio wave changes. A multi-channel computing device is proposed for calculating the autocorrelation function of the incoherent scatter signal when using such coded signals.

Key words: incoherent scatter technique; radar signals; sounding modes; signal coding, processing.

6 fig. Ref: 15 items.

УДК 621.396; 550.388

Удосконалення режимів зондування іоносфери у методі некогерентного розсіяння / *Л.Я. Ємельянов, В.О. Пуляєв, Н.О. Кузьменко, Д.А. Дзюбанов* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2025. Вип. 220. С. 128 – 135.

Наведено приклади удосконалення режимів імпульсного випромінювання високочастотних радіохвиль, приймання та обробки прийнятих сигналів, некогерентно розсіяних іоносферною плазмою, які реалізуються за допомогою радарів некогерентного розсіяння, призначених для дистанційного зондування навколоземного космічного простору. Проаналізовано режими радіоімпульсного зондування, а саме режиму з використанням довгого радіоімпульсу, призначеного для дослідження верхнього висотного діапазону іоносфери, і режиму для дослідження нижньої іоносфери, коли випромінюється зондувальний сигнал у вигляді двох коротких елементів, відстань між якими змінюється в залежності від номеру радіолокаційної розгортки. Показано переваги та недоліки цих режимів. Запропоновано варіанти використання радіоімпульсів більш складної структури завдяки оптимальному кодуванню більшої кількості елементів з урахуванням характеру розсіяння в іоносферній плазмі. Наведено результати пошуку багатоелементних кодованих сигналів для дослідження нижнього і верхнього висотних діапазонів, які забезпечують розрахунок ординат автокореляційної функції сигналу розсіяння з високою роздільною здатністю як у просторі, так і у часі. Представлено апаратурну реалізацію режимів зондування цих сигналів, зокрема структурну схему радара некогерентного розсіяння для роботи з сигналами протилежної кругової поляризації, яка використовує для цього керовані фазообертачі системи збудження передавача, ортогональні антенні вібратори та кільцевий міст приймально-фідерного тракту. Зміна параметрів високочастотного заповнення радіосигналу зондування здійснюється за сигналами системи керування радара. В цілому, це дає можливість передавати і приймати сигнали з різними варіантами кодування їх елементів, найбільш придатними для конкретних умов, та використовувати режими, в яких змінюється напрямок кругового обертання площини

поляризації радіохвилі. Запропоновано багатоканальний обчислювальний пристрій для розрахунку автокореляційної функції сигналу розсіяння при використанні таких кодованих сигналів.

Ключові слова: метод некогерентного розсіяння; радіолокаційні сигнали; режими зондування; кодування, обробка сигналів.

Іл. 6. Бібліогр.: 15 назв.

PHYSICS OF DEVICES, ELEMENTS AND SYSTEMS
ФІЗИКА ПРИЛАДІВ, ЕЛЕМЕНТІВ І СИСТЕМ

UDC 621.396.6

Trends in the development of wireless laser energy transmission / *D.V. Sokirkaiev, A.A. Zarudny* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2025. №220. P. 136 – 145.

The article reviews and analyzes the current state of laser energy transfer (LET) systems and their development prospects. The key components of the system, including laser emitters and high-performance optoelectronic converters (OCs), as well as the influence of the transmission medium on the system efficiency are considered.

Particular attention is paid to the optimization of each module of the OET to improve the efficiency of the entire system. The influence of laser radiation characteristics, DUT materials, temperature, and transmission conditions on the system efficiency is described. Modern achievements in the creation of multi-junction LETs using GaAs and other innovative materials are analyzed. Examples of practical applications of solar cells in aviation, space and military industries, including power supply of UAVs, spacecraft, as well as use in space solar power plants (SSPS) are considered.

The main technical limitations of modern LPS systems, which hinder the increase in overall efficiency to the level of 20-25 %, are highlighted. Possible directions for further research, such as the improvement of materials, laser cooling systems, and the adaptation of the LPE design to specific operating conditions, are presented.

LET is considered a promising technology that can change the approach to wireless energy supply in conditions where other methods are inefficient or dangerous. It is expected that in the future, due to further development of technologies, the efficiency of LEP systems will exceed 30%.

Key words: laser energy transmission; wireless energy; laser; optoelectronic converters; GaAs.

2 tabl. 2 fig. Ref: 44 items.

УДК 621.396.6

Тенденції розвитку бездротової лазерної передачі енергії / *Д.В. Сокіркаєв, О.А. Зарудний* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2025. Вип. 220. С. 136 – 145.

Проведено огляд та аналіз сучасного стану систем лазерної передачі енергії (ЛПЕ) та їх перспектив розвитку. Розглянуто ключові компоненти системи, включаючи лазерні випромінювачі та високоефективні оптично-електронні перетворювачі (ОЕП), а також вплив середовища передачі на ефективність роботи системи.

Особливу увагу приділено оптимізації кожного модуля ЛПЕ для підвищення ефективності всієї системи. Описано вплив характеристик лазерного випромінювання, матеріалів ОЕП, температури та умов передачі на ККД системи. Проаналізовано сучасні досягнення у створенні багатоперехідних ОЕП з використанням GaAs та інших інноваційних матеріалів. Розглянуто приклади практичного застосування ЛПЕ в авіації, космічній та військовій галузях, включаючи живлення БПЛА, космічних апаратів, а також використання в космічних сонячних електростанціях (SSPS).

Висвітлено основні технічні обмеження сучасних систем ЛПЕ, які стримують підвищення загальної ефективності до рівня 20–25 %. Наведено можливі напрями для подальших досліджень, такі як удосконалення матеріалів, систем охолодження лазерів, та адаптація дизайну ОЕП до специфічних умов роботи.

ЛПЕ розглядається як перспективна технологія, здатна змінити підхід до бездротового постачання енергії в умовах, де інші методи є неефективними або небезпечними. Очікується, що у майбутньому, завдяки подальшому розвитку технологій, ефективність систем ЛПЕ перевищить 30 %.

Ключові слова: лазерна передача енергії; бездротова енергетика; оптично-електронні перетворювачі; GaAs; космічні сонячні електростанції; БПЛА.

Табл. 2. Іл. 2. Бібліогр.: 44 назв.

UDC 621.372

Features of constructing data transmission systems over free-space optical routes / *S.M. Kukhtin, E.P. Fedorenko* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2025. №220. P. 146 – 155.

This paper provides an overview related to the current state of free-space optics systems, areas of their application and advantages compared to wireless radio-frequency systems. A review related to development history of such systems is also provided. Principles of transmitting/receiving equipment development, including common schemes, radiation sources, detectors and other basic components of these systems are covered in this paper. Analysis of the atmospheric conditions effect on optical signal transmission, such as atmospheric absorption, scattering and turbulence has been studied. The most common methods used to improve the efficiency of free-space optics systems are also considered in this paper.

Key words: optics; laser; telecommunications; data; atmosphere; link; turbulence.

2 fig. Ref: 44 items.

УДК 621.372

Особливості побудови систем передавання даних відкритими оптичними трасами / *С.М. Кухтін, Є.П. Федоренко* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2025. Вип. 220. С. 146 – 155.

Проведено огляд сучасного стану систем передачі даних відкритими оптичними трасами, сфер їхнього застосування, а також переваги у порівнянні з існуючими безпровідними системами із застосуванням радіоканалу. Проведено історичний огляд їхнього розвитку. Розглянуто особливості побудови приймально-передавального обладнання, включно з розповсюдженими схемами, джерелами і приймачами оптичного випромінювання, а також іншими основними компонентами таких систем. Проведено аналіз впливу атмосферних умов на передачу оптичних сигналів, а саме, особливості атмосферного поглинання, розсіювання і впливу атмосферних турбулентностей на розповсюдження оптичного сигналу. Проаналізовано найбільш поширені методи підвищення ефективності систем передавання даних відкритим оптичним каналом.

Ключові слова: оптика; лазер; телекомунікації; дані; атмосфера; траса; турбулентність.

Іл. 2. Бібліогр.: 44 назв.

UDC 621.3729(75)

Analysis of noise components of microwave diode oscillators / *O.D. Meniailo, O.V. Grigorieva* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2025. №220. P. 156 – 160.

The work deals with theoretical and practical study of fluctuation components of diode oscillators.

The mechanism of formation of fluctuation components of diode oscillators is considered.

An experimental study of fluctuation components of oscillators is carried out. A generator on an avalanche-transit diode was chosen as an example of a diode autogenerator with a fairly high level of its own noise.

According to the results of research into amplitude-modulated and frequency-modulated noise components of an oscillator on an avalanche-flying diode depending on the quality factor of its oscillatory system, the exponential nature of these dependencies, predicted by the results of theoretical analysis, is observed,

The conducted studies indicate the consistency of theoretical conclusions with practical results.

The conclusions of the research can be used in the design of microwave diode generators with specified fluctuation characteristics.

Key words: diode oscillators; fluctuation components; experimental research; frequency-modulated noise; amplitude-modulated noise.

6 fig. Ref: 11 items.

УДК 621.3729(75)

Аналіз шумових компонентів діодних автогенераторів НВЧ / *О.Д. Меняйло, О.В. Григор'єва* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2025. Вип. 220. С. 156 – 160.

Робота присвячена теоретичному і практичному дослідженню флуктуаційних компонентів діодних автогенераторів.

Розглянуто механізм формування флуктуаційних компонентів діодних генераторів.

Проведено експериментальне дослідження флуктуаційних компонентів автогенераторів. В якості прикладу діодного автогенератора, що має досить великий рівень власних шумів, вибрано генератор на лавино-пролітному діоді.

За результатами досліджень амплітудно-модульованих та частото-модульованих шумових компонентів автогенератора на лавино-пролітному діоді в залежності від добротності його коливальної системи спостерігається експоненційний характер цих залежностей, що передбачалось за результатами теоретичного аналізу.

Проведені дослідження свідчать про узгодженість теоретичних висновків з практичними результатами. Висновки можуть бути використані при проєктуванні діодних генераторів НВЧ з заданими флуктуаційними характеристиками.

Ключові слова: діодні автогенератори; флуктуаційні компоненти; експериментальне дослідження; частото-модульований шум; амплітудно модульований шум.

Іл. 6. Бібліогр.: 11 назв.

ELECTRONIC COMMUNICATIONS
ЕЛЕКТРОННІ КОМУНІКАЦІЇ

UDC 621.391

Method for decoding sequential algebraic cascade convolutional codes for mobile communication systems / *M.A. Shtompel* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2025. №220. P. 161 – 165.

The development of radio communication technologies allows the introduction of the latest electronic communication services that impose strict requirements on the quality of data transmission. To increase the efficiency and reliability of data transmission in these electronic communications systems, it is advisable to use parallel and sequential cascade code structures. It is shown that the construction of sequential cascade code structures for mobile communication systems can be carried out on the basis of various component codes and corresponding decoders. This makes it possible to adjust the characteristics of these codes depending on the existing requirements and parameters of the communication channel.

A sequential algebraic cascade coding scheme is proposed, where the outer stage is implemented based on a non-binary Reed-Solomon block code, and the inner stage is implemented using a non-recursive algebraic convolutional code. A block interleaver is used between these stages. A distinctive feature of this scheme is the use of an algebraic convolutional code with the maximum achievable correction capability. This is achieved by constructing this code based on the generator polynomial of the Reed-Solomon code.

A method for decoding sequential algebraic cascade convolutional codes based on a combination of two decoders has been developed. At the first stage, the internal code is decoded using ordered statistics. Within this stage, the most reliable basis is initially found based on the reliability of the symbols of the received sequence. Test error vectors of a given Hamming weight are added to the found basis, resulting in a set of test code blocks. The search for the estimate of the transmitted code block is carried out on the basis of minimizing the weighted Hamming weight between the formed code blocks and the accepted estimate of the code block. At the next stage, the accepted vector for the outer code is formed by inversely permuting the found estimate of the code block in the block interleaver. At the final stage, algebraic decoding of the Reed-Solomon code occurs based on the Berlekamp-Massey algorithm.

Key words: algebraic; cascade; convolutional; code; decoding; mobile; communication.

Ref: 15 items.

УДК 621.391

Метод декодування послідовних алгебраїчних каскадних згорткових кодів для систем мобільного зв'язку / *М.А. Штомпель* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2025. Вип. 220. С. 161 – 165.

Розвиток технологій радіозв'язку дозволяє впроваджувати новітні електронні комунікаційні послуги, що висувають жорсткі вимоги до якості передавання даних. Для підвищення ефективності та надійності передавання даних у цих системах електронних комунікацій доцільно використовувати паралельні та послідовні каскадні кодові конструкції. Показано, що побудова послідовних каскадних кодових конструкцій для систем мобільного зв'язку може здійснюватися на базі різних компонентних кодів та відповідних декодерів. Це надає можливість регулювати характеристики даних кодів в залежності від наявних вимог та параметрів каналу зв'язку.

Запропонована послідовна алгебраїчна каскадна схема кодування, в якій зовнішня ступень реалізується на базі недвійкового блокового коду Ріда–Соломона, внутрішня ступень – з використанням нерекурсивного алгебраїчного згорткового коду. Між даними ступенями використовується блоковий перемежувач. Відмінною особливістю даної схеми є застосування алгебраїчного згорткового коду з максимально досяжною коригувальною здатністю. Це досягається шляхом побудови даного коду на основі породжувального багаточлену коду Ріда–Соломона.

Розроблено метод декодування послідовних алгебраїчних каскадних згорткових кодів на базі комбінування двох декодерів. На першому етапі виконується декодування внутрішнього коду за впорядкованими статистиками. В рамках даного етапу спочатку знаходиться найбільш надійний базис на основі надійності символів прийнятої послідовності. До знайденого базису додаються тестові вектори помилок заданої ваги Хемінга, в результаті чого формується набір тестових кодових блоків. Пошук оцінки переданого кодового блоку здійснюється на основі мінімізації зваженої ваги Хемінга між сформованими кодовими блоками та прийнятою оцінкою кодового блоку. На наступному етапі формується прийнятий вектор для зовнішнього коду шляхом зворотної перестановки знайденої оцінки кодового блоку у блоковому перемежувачі. На завершальному етапі відбувається алгебраїчне декодування коду Ріда–Соломона на основі алгоритму Берлекемпа–Мессі.

Ключові слова: алгебраїчний; каскадний; згортковий; код; декодування; мобільний; зв'язок.

Бібліогр.: 15 назв.

COLLECTION OF SCIENTIFIC PAPERS
RADIOTEKHNIKA
Issue 220
In English and Ukrainian

ЗБІРНИК НАУКОВИХ ПРАЦЬ
РАДІОТЕХНІКА
Випуск 220
Англійською та українською мовами

Коректор Л.І. Сащенко

.

Підп. до друку 11.04.2025. Формат 60x90/8. Папір офсет. Гарнітура Таймс. Друк. ризограф.
Ум. друк. арк**.** 11,04. Обл.-вид. арк. 10,3 Тираж 300 прим. Зам. № 173. Ціна договір.

Харківський національний університет радіоелектроніки (ХНУРЕ)
Просп. Науки, 14, Харків, 61166.

Оригінал-макет підготовлено і збірник надруковано у ПФ „Колегіум”,
Свідоцтво про внесення суб’єкта видавничої діяльності до Державного реєстру видавців.
Сер. ДК №1722 від 23.03.2004.