МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
Навчально-науковий інститут захисту інформації
Систем інформаційного та кібернетичного захисту

До захисту
Завідувачкафедри СІКЗ
к.т.н., доцен
Шуклін Г.В.
“____”_____________2022р.

ДИПЛОМНА РОБОТА
Зі спеціальності: 125 Кібербезпека
на тему:

ОРГАНІЗАЦІЯ ПОРЯДКУ ВСТАНОВЛЕННЯ ВНУТРІШНЬО ОБ`ЄКТНОГО РЕЖИМУ НА ПІДПРИЄМСТВІ

Студент групи СЗД-41 Набоков Сергій Андрійович ________
(підпис)

Керівник
ст. викладач Гребенніков Асаді Болдгоягович ________
(підпис)

Нормконтроль ст. викл. Гребенніков Асаді Болдгоягович ________
(підпис)

Київ – 2022

МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
Навчально-науковий інститут захисту інформації
Кафедра Систем інформаційного та кібернетичного захисту

Освітньо-кваліфікаційний рівень – магістр
Спеціальність – 125 Кібербезпека

ЗАТВЕРДЖУЮ
Завідувач кафедри СІКЗ
к.т.н., доцент
_______________Шуклін Г.В.

ЗАВДАННЯ

НА ДИПЛОМНУ РОБОТУ

Студенту: НАБОКОВУ СЕРГІЮ АНДРІЙОВИЧУ

1.Тема роботи: Організація порядку встановлення внутрішньо об`єктного режиму на підприємстві

Наказ по університету від «16» лютого 2022 р. № 22.

2.Термін подання студентом закінченої дипломної роботи

3.Вихідні дані до роботи: Проаналізувати завдання, які виникають при охоронному режимі на підприємстві, а також, визначити умови, при яких виникає необхідність захисту інформації на об`єкті інформаційної діяльності. Визначити існуючі загрози захисту інформації за рахунок моніторингу та звітування про них. Оцінити виявлені загрози для створення компетентних кроків, які призведуть до мінімізації ризиків витоку конфіденційної інформації. Створити умови реакції на спробу отримання конфіденційної інформації, та здійснити документальне підтвердження даного акту.

4.**Зміст пояснювальної записки(перелік питань, які потрібно розробити):**

1. Здійснити заходи щодо можливого втручання до конфіденційної інформації на підприємстві.

2. Здійснити моніторинг можливих заходів, щодо нападу на конфіденційну інформацію на підприємстві.

3. Виявити можливі позитивні наслідки, які виникають за рахунок намагання виявити конфіденційність.

5.**Дата видачі завдання**” ” ____________2022р.

КАЛЕНДАРНИЙ ПЛАН

№	Процедура	Термін виконання	
1	Підготовка Розділу 1	-	До 04.04
2	Підготовка Розділу 2	З 04.04	До 25.04
3	Підготовка Розділу 3	З 25.04	До 06.05
4	Висновки + Презентація	З 06.05	До 13.05
5	Перевірка роботи на плагіат + Предзахист	З 16.05	До 01.06
6	Захист роботи	З 02.06	До 21.06
7	Випуск	30.06	

Студент Набоков С.А.

Керівник роботи Шуклін Г.В.

Реферат

Дипломна робота присвячена методиці організації порядку встановлення внутрішньо об`єктивного режиму захисту конфіденційної інформації на об`єкті інформаційної діяльності. Робота складається зі вступу, трьох розділів, що містять 4 малюнки, 11 таблиць, висновки та списки використаних джерел, що містять 16 найменувань. Загальний обсяг роботи становить 85 сторінок.

Об’єктом дослідження є процеси захисту конфіденційної інформації на підприємстві за рахунок організації встановлення внутрішнього режиму контроля.

Метою роботи полягає в оптимізації контролю доступу на підприємстві, що призведе до неспроможності доступу до конфіденційної інформації сторонніх осіб.

КЛЮЧОВІ СЛОВА: Контроль доступу, захист конфіденційної інформації, загрози витоку конфіденційної інформації на об'єкті інформаційної діяльності.

ЗМІСТ

Стор.

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ…………………………………….........6
ВСТУП……………………………………………………………………8
РОЗДІЛ 1. ЗАХОДИ ДЛЯ ОРГАНІЗАЦІЇ РЕЖИМУ НА ПІДПРИЄМСТВІ………………………………………………………………9
1.1 План заходів, які необхідні для підтримання……………………………9
1.2 Зміст плану об'єктного режиму для забезпечення захисту………………………………………………………….…………………20
1.3 Заходи щодо осіб, які мають відповідні обов'язки ……………………25
1.4 Звернення до зовнішніх експертів………………………………………28
1.5 Підготовка дій для ліквідації загроз………………………..…………...30
1.6 Підготовка щодо відповідних умов………..………………………………34
1.7 Страхування ризиків……………………………………………………..39
РОЗДІЛ 2. ЗАХОДИ ПО ВИЯВЛЕННЮ ТА ІДЕНТИФІКАЦІЇ ЗАГРОЗ НА ОБ`ЄКТІ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ…………………………...45
2.1Види та категорії потенційних загроз…………………………………...45
2.2Методи виявлення загроз………………………………………………50
2.3Мета дійсних загроз: контроль доступу, ліквідація та наслідки……......59
2.4 Наявність потенційних загроз в захисті об`єктів …………………………64
РОЗДІЛ 3. ДІЇ СТОРІН ПРИ РЕАЛІЗАЦІЇ ЗАГРОЗ………………………71
3.1 Структура комунікацій при загрозах……………………………………71
3.2 Початкові умови та наявність інформації сторонніми особами дані….72
3.3Дослідження та виявлення загроз: наявність інформації по кожній загрозі…..80
ВИСНОВКИ…………………………………………………………………..83
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ……………………………………….84

ВСТУП

Актуальність теми: В даний час активне використання джерела електромагнітного ресурсу, пов'язане з розробкою систем і засобів радіозв'язку та радіотехніки, а також різноманітних електронних та електромеханічних систем, призводить до значної появи додаткового електромагнітного фону, що ускладнює і так не легкий стан інтерференційної ситуації та загострення проблем електромагнітної сумісності. Особливо складна електромагнітна ситуація є у великих містах, де основними джерелами електромагнітних полів радіочастотного діапазону є телевізійні та центри радіопередач, базові станції мобільного зв’язку та величезна різноманітність інших систем і пристроїв, що випромінюють електромагнітні поля. Для оптимального розподілу радіочастотних ресурсів і уникнення колізій при спільній роботі радіоелектронних пристроїв необхідний постійний моніторинг радіоефіру, ефективно виявляючи перешкоди локального та загального характеру. З цієї точки зору необхідно використовувати високоточне вимірювальне обладнання, що дозволяє вирішити вищезазначену проблему. Одним з основних елементів такого вимірювального обладнання є антена. Значною мірою антена визначає точність вимірювань і, відповідно, достовірність їх результатів. У вимірювальні системи, що використовуються для моніторингу радіоефіру, є широкий спектр вимірювальних антен. Проте дотепер ведуться пошуки рішень щодо створення універсальної антени, яка дає змогу проводити вимірювання в дуже широкій смузі частот з мінімальними похибками. Одним із можливих рішень такої проблеми може бути створення антенної системи, що складається з кількох антен, що працюють у певних діапазонах частот, але разом перекривають весь досліджуваний радіоефірний діапазон. У цій статті пропонується та розглядається антенна система, яка може бути використана як частина вимірювального обладнання для моніторингу радіоефіру.

Розділ 1 ЗАХОДИ ДЛЯ ОРГАНІЗАЦІЇ РЕЖИМУ НА ПІДПРИЄМСТВІ

1.1 План заходів, які необхідні для підтримання

Основним завданням радіомоніторингу є вивчення радіоефіру в смузі частот, в якій працюють усі основні радіосистеми та пристрої. Під дослідженнями маються на увазі ефективне розташування випромінювача різних радіоджерел, вимірювання рівнів їх електромагнітного поля та аналіз перевантаженості радіочастотного спектру. Антена, як перший і найважливіший елемент вимірювальної техніки, повинна мати такі технічні характеристики:

- широкий діапазон робочих частот; - висока стабільність коефіцієнта посилення;
- висока стабільність форми діаграми спрямованості в основних площинах у всій смузі робочих частот;
- зручна експлуатація та уніфікація структура;

До складу вимірювального обладнання входять:

- широкодіапазонні ненаправлені антени різних додатків;
- комплекти антенних систем автоматичного пеленгування в русі, на стоянках та на стаціонарних постах;
- комплекти антенних модулів з напрямними зв'язками для ручних пеленгаторів відкритого та прихованого використання.

Як бачимо, найчастіше в вимірювальній апаратурі використовуються набори антен, кожна з яких має свій діапазон і спрямовані властивості. При моніторингу радіочастотного спектру певного діапазону необхідно використовувати антену з відповідною смугою робочих частот. Тому необхідно використовувати або універсальну широкосмугову антену, або змінювати антену при перемиканні з одного діапазону на інший. Ми розробили антенну систему, призначену для роботи у складі вимірювального обладнання для моніторингу радіоефіру. Система складається з двох антен: логарифмічної, що працює в смузі частот 80...1000 МГц, і рупорної антени, що працює в діапазоні 1...12 ГГц.

Логперіодична антена складається з двадцяти одного елемента, з проектним періодом t=0,84 і кутом a=450. Довжина збірної антенної лінії – 1,57 метра. Довжина найдовшого вібратора (одна сторона) - 0,83 метра, найкоротшого - 0,4 метра.

Проведені дослідження антени показали, що її коефіцієнт посилення в робочому діапазоні практично не змінився і становить 12 дБ, а коефіцієнт захисної дії – 18 дБ. В якості другої антени використовується вимірювальний рупор тенна П6-23А, що має такі технічні характеристики:

- діапазон частот - 1 ... 12 ГГц;
- Ефективна площа:
- на частоті до 6 ГГц - 150 см²;
- на частоті вище 6 ГГц - 130 см²;

ВЧ шлях - 50 Ом;

- Похибка ефективної площі -20%;
- КСВ - 1,5;
- антенний вхід (переріз АА) - коаксіальний;
- Вхідний опір - 50 Ом;
- рівень:
- бічні пелюстки - не більше 10 дБ;
- поперечна поляризація - не більше 20 дБ.

На малюнку 1 показана узагальнена схема системи антени. Обидві антени закріплені на загальній траверсі, яка, в свою чергу, закріплена на вертикальній щоглі. У системі можна змінювати напрям моніторингу в меридіанній (горизонтальній) площині, а також змінювати поляризацію антен. Відстань між антенами по горизонталі становить 1,5 метра, що дозволяє вирішити проблему взаємного впливу антен один на одного.

На малюнку 2 показана повна блок-схема системи, яка складається з розробленої антенної системи, системи комутації, стаціонарної системи радіоконтролю Rohde & Schwarz UMS100, з можливістю підключення портативного приймача Rohde & Schwarz PR100, антени. блок управління та термінал комп'ютера.

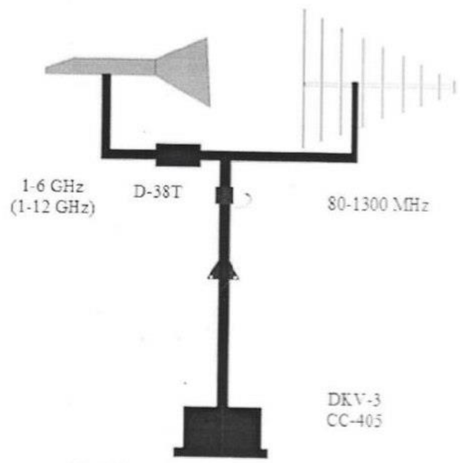


Fig.1 General scheme of the antenna system

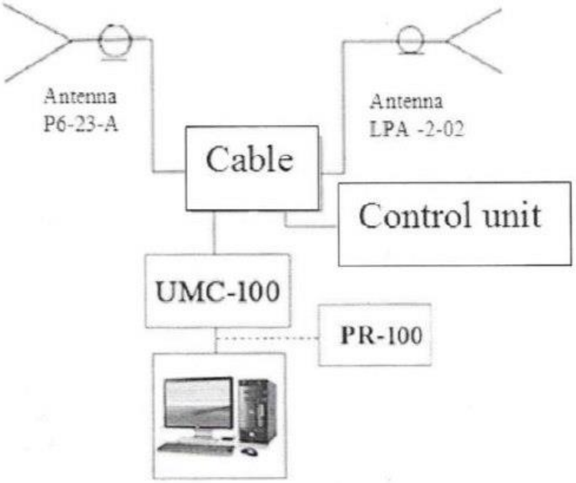


Fig. 2 Structure diagram of the antenna system

Розглянемо конструктивні особливості розробленої антенної системи.

У системі є можливість змінювати поляризацію обох антен за допомогою електродвигуна, яким можна керувати дистанційно, подаючи команди через термінал комп’ютера. Для кожної антени можна встановити власну поляризацію або однакову поляризацію для обох антен. Щогла, на якій встановлені антени, змінює своє положення за допомогою другого двигуна, яким також можна керувати дистанційно, віддаючи команди через той же комп’ютерний термінал. Таким чином, це так можна оперативно керувати напрямком моніторингу в режимі реального часу, змінюючи кут огляду антенної системи до точки приходу досліджуваного сигналу з нуля до трьохсот шістдесяти градусів. У поворотній системі використовується датчик-приймач Selsyn, який синхронно, з точністю до 0,1 градуса, задає кут повороту антен, заданий оператором на терміналі комп’ютера. Зовнішній вигляд антенної системи показаний в рис 3.

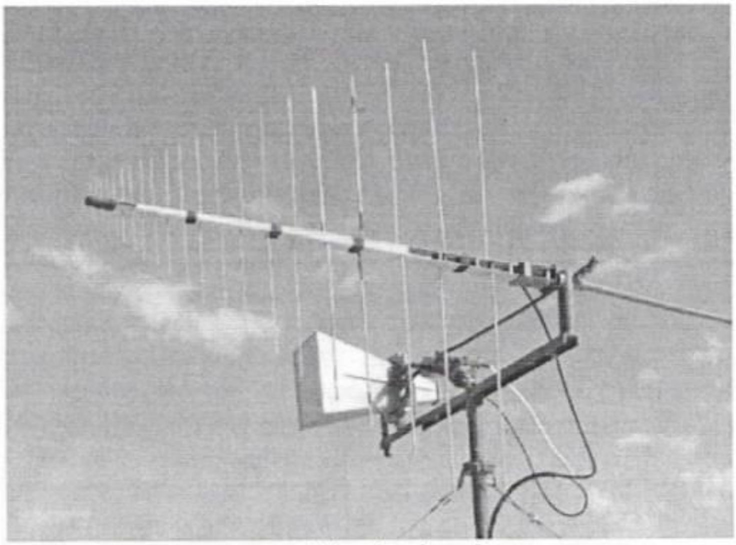
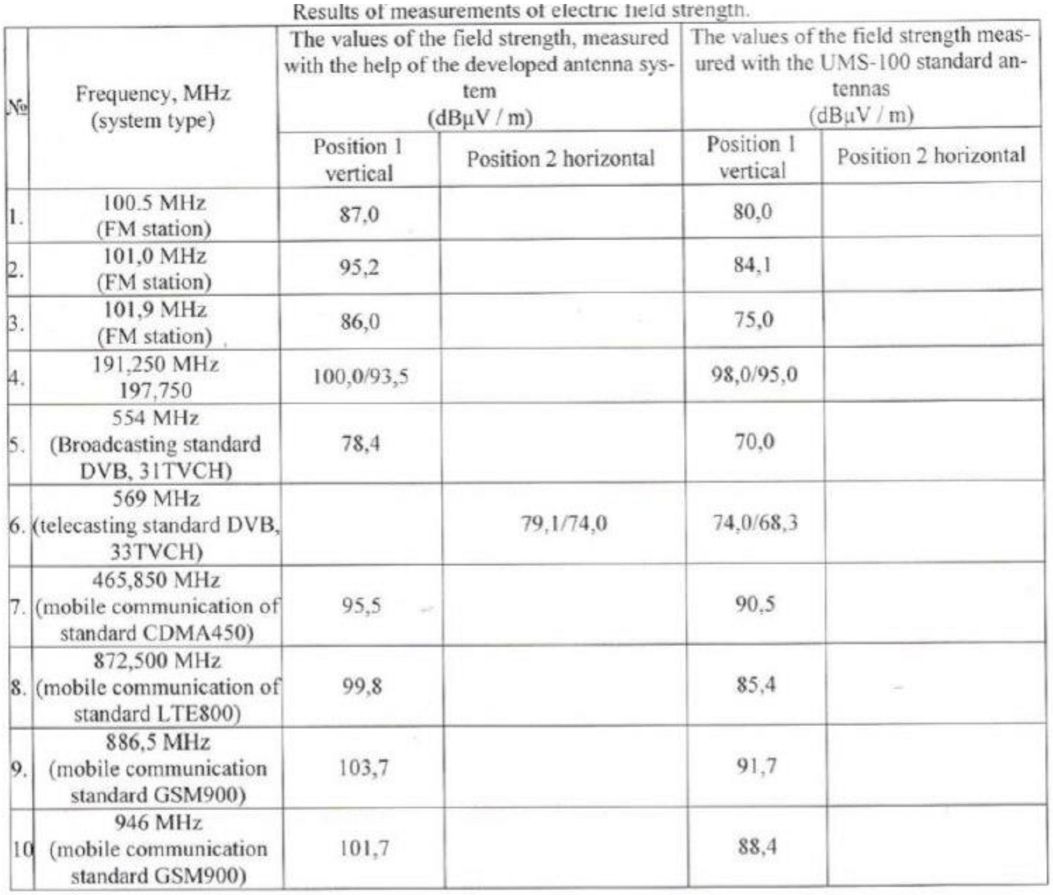


Fig.3 Appearance of the developed antenna system

За допомогою розробленої антенної системи проведено вимірювання напруженості електричного поля, створеного різними джерелами радіовипромінювання в різних регіонах Самаркандської області Республіки Узбекистан. У таблиці 1 наведено результати вимірювання, отримані за допомогою розробленої антенної системи та стандартних антен, що входять до складу вимірювального обладнання Rohde & Schwarz UMS100.

Results of measurements of electric field strength.



№	Frequency, MHz (system type)	The values of the field strength, measured with the help of the developed antenna system (dBμV / m)		The values of the field strength measured with the UMS-100 standard antennas (dBμV / m)	
		Position 1 vertical	Position 2 horizontal	Position 1 vertical	Position 2 horizontal
1.	100.5 MHz (FM station)	87,0		80,0	
2.	101,0 MHz (FM station)	95,2		84,1	
3.	101,9 MHz (FM station)	86,0		75,0	
4.	191,250 MHz 197,750	100,0/93,5		98,0/95,0	
5.	554 MHz (Broadcasting standard DVB, 31TVCH)	78,4		70,0	
6.	569 MHz (telecasting standard DVB, 33TVCH)		79,1/74,0	74,0/68,3	
7.	465,850 MHz (mobile communication of standard CDMA450)	95,5		90,5	
8.	872,500 MHz (mobile communication of standard LTE800)	99,8		85,4	
9.	886,5 MHz (mobile communication standard GSM900)	103,7		91,7	
10	946 MHz (mobile communication standard GSM900)	101,7		88,4	

Аналіз результатів вимірювань показує, що різниця між результатами, отриманими за допомогою розробленої антенної системи та стандартних антен, становить від 5 дБмкВ/м до 26 дБмкВ/м.

Наприклад:

- на частоті 465,850 МГц різниця становить 5 дБуВ/м, на частоті 100,5 МГц різниця становить 7 дБмкВ / м,
- на частоті 872,500 МГц різниця становить 14,4 дБмкВ/м,
- на частоті 2117,5 МГц різниця становить 16 дБмкВ /м,
- на частоті 2670 МГц різниця становить 13,2 дБмкВ/м,
- на частоті 1877,4 МГц різниця становить 26 дБмкВ/м.

Таким чином, можна констатувати, що розроблена антенна система дає більш точні результати, ніж при використанні стандартних антен, що входять до складу вимірювального обладнання.

Крім того, завдяки можливості дистанційного керування (у ручному або автоматичному режимах) антенною системою процес вимірювання значно спрощується, що дуже важливо для складних польових умов жарких регіонів Республіки Узбекистан.

1.2 ЗМІСТ ПЛАНУ ОБ`ЄКТНОГО РЕЖИМУ ДЛЯ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ

Осцилографи серії S

Осцилографи серії S забезпечують чудову тимчасову базу, технологічні блоки інтерфейсу та АЦП. Роздільна здатність 16 біт, низький рівень шуму, низький рівень шуму та високий рівень ENOB для чіткого уявлення про продуктивність вашого пристрою.

- 10-розрядний АЦП до 8 ГГц для додаткової роздільної здатності
- Вибір параметрів конкретної програми

Осциллографи InfiniiVision 1000 серії X

- Чотири нові моделі 2-канальних осцилографів включають збільшену пропускну здатність, збільшення пам'яті, більш високу швидкість оновлення форми сигналу, стандартну локальну мережу та можливості аналізу стандартної послідовної шини.

- Покращення, такі як аналіз послідовної шини, тепер стандартні для поточних 4-канальних моделей.

Системи збору даних DAQ970/73A

Підвищте продуктивність від 3-слотових блоків збору даних 34970/72A за допомогою DAQ970/73A, який забезпечує покращену точність вимірювання, діапазон вимірювання опору Wder і в 100 разів більшу швидкість зчитування.

-50 000 показань/с.

-9 модулів перемикача, РЧ, цифрового пристрою та модулів керування.

-USB LAN та інтерфейс GPIB.

4-портова мікрохвильова піч ECal серії 4430

Ідеально підходить для використання з РЧ збалансованими вимірювальними рішеннями Keyight.

-Швидкі калібрування, які надзвичайно повторювані та точні.

Keysight і наша дистриб'юторська мережа RIGHT Instrument. ПРАВИЛЬНА експертиза. Доставлено ПРЯМО зараз.

Keysight і наша мережа авторизованих дистриб’юторів Keysight об’єдналися, щоб забезпечити швидкий і легкий доступ до найбільшої у світі секції стандартних інструментів T&M. Це найкращий досвід вимірювань Keysight та широта продукту в обох світах у поєднанні зі швидкістю, зручністю та доставкою в той же день від наших дистриб’юторських партнерів.

Ще ніколи не було простіше відразу отримати потрібний інструмент у правильні руки.

Щоб знайти найближчого авторизованого дистриб’ютора Keysight, відвідайте його.

Програмне забезпечення PathWave BenchVue: керування. Автоматизувати. Спростити.

Програмне забезпечення Keysight PathWave BenchVue для ПК усуває багато проблем, пов’язаних із стендовим тестуванням. Зробивши його простим для підключення, керування інструментами та автоматизації тестових послідовностей, ви можете швидко пройти етап розробки тестів і отримати доступ до результатів швидше, ніж будь-коли раніше. Спеціальні програми для приладів дозволяють швидко налаштувати найбільш часто використовувані вимірювання та налаштування для кожної сім’ї приладів. Швидко створюйте власні послідовності тестів за допомогою інтегрованого додатка Test Flow, щоб автоматизувати та візуалізувати результати тестування без необхідності програмування приладу. Різноманітні потужні програми BenchVue дозволяють значно скоротити час тестування.

НОВИНКА Додатки для керування лабораторією забезпечують централізовану конфігурацію лабораторного приладу, відстежують активи та адміністup[у]ють лабораторію. Ідеально підходить для викладачів для моніторингу та контролю навчальних лабораторій.

Шукайте цей значок

у всьому каталозі, щоб ідентифікувати продукти з програмним забезпеченням BenchVue, включеним або підтримуваним.

Використовуйте програми PathWave BenchVue, щоб:

- Налаштуйте найбільш часто використовувані елементи керування та вимірювання з ваших інструментів Keysight Візуалізація кількох вимірювань одночасно.

-Легко реєструйте та експортуйте дані та зображення екрана лише за кілька кліків для пришвидшого аналізу.

- Швидко створюйте автоматизовані послідовності тестів з мінімальними знаннями про прилад.

- Централізоване керування та налаштування лабораторних станцій.

Програмне забезпечення PathWave BenchVue підтримує понад 500 інструментів Keysight, включаючи цифрові мультиметри, блоки живлення, аналізатори спектру генераторів функцій/генераторів сигналів, блоки збору даних, аналізатори мережі, осцилографи, вимірювачі потужності, датчики потужності, електронні навантаження, універсальні лічильники тощо. Шукайте BenchVue, який підтримується піктограма для сумісних продуктів Почніть прискорювати свій робочий процес сьогодні. Програми BenchVue включені в більшість продуктів у цьому каталозі. Щоб дізнатися більше, відвідайте

Дистанційно керуйте своїми настільними інструментами

Налаштуйте BenchVue для віддаленого моніторингу та керування настільними інструментами з іншого місця. Це дозволяє вчителю контролювати дистанційні лабораторії навчання/навчання, а інженери можуть дистанційно керувати системами по всьому світу.

Використання BenchVue для дистанційного керування настільними інструментами

ЗАВАНТАЖУЙТЕ ВАШ НАСТУПНИЙ СТАТУС

Програмне забезпечення Keysignt можна завантажити. Від першого моделювання до першої відправки клієнту ми надаємо інструменти, необхідні вашій команді, щоб прискорити перехід від даних до інформації до реального розуміння.

3

Навчальні рішення на основі навчальної програми та програмне забезпечення для управління лабораторією

Рішення для навчання Інтернету речей серії U3800 (loT).

- Прикладні курси серії U3800 пропонують повний готовий до навчання пакет, зосереджений на вивченні системи loT і додатків кінцевих користувачів за допомогою тематичних досліджень, практичних лабораторій і промислових завдань.

-Теми включають: автоматизація розумного дому, розумне місто, розумний автомобіль, управління катастрофами, автоматизація індустрії 4.0 та бездротовий зв’язок.

-Включає основи лоТ через бездротовий зв’язок, датчики та управління живленням, надаючи студентам практичні методи проектування та тестування з використанням передових інструментів.

Дізнайтеся більше на

U3851A РЧ мікрохвильове рішення для навчання

-РЧ мікрохвильова схема проектування, моделювання та вимірювання.

- Приносить досвід промислового проектування в клас і охоплює повний процес проектування для успішної розробки бездротових додатків 5G і loT.

- Курсове програмне забезпечення включає модульний набір прототипів із використанням модуля приймача 1,8 ГГц, лабораторні листи та завдання на основі проблем для використання з рекомендованими інструментами та програмним забезпеченням для проектування.

BV9111B Рішення для управління та контролю лабораторії BenchVue

- BenchVue Lab — це рішення для управління лабораторією на основі локальної мережі, що забезпечує централізований огляд лабораторії конфігурації приладів та відстеження активів для викладачів, які навчають лабораторій.

-Включає програми Keysight BV011XB BenchVue Lab (керування приладами, автоматизація та аналіз) і колекцію контролю освіти BV9101B BenchVue.

-Легке керування приладами, збір даних, реєстрація даних, моніторинг та створення звітів для студентів на стенді.

1.3 ЗАХОДИ ЩОДО ОСІБ, ЯКІ МАЮТЬ ВІДПОВІДНІ ОБОВ`ЯЗКИ

In recent years, there has been a growing interest in mini- and microUAVs related to the capabilities

low-cost observation and for the purposes of remote sensing of the earth's surface. For now, most UAVs use a satellite navigation system (GNSS) and an inertial navigation system (INS). However, such navigation solutions may not work in environments with weak or no GNSS signal and used in environments such as mountain/trough navigation, confined space navigation, or urban flight. 2D and 3D laser scanners can provide additional information for navigating such difficult terrain, but the disadvantage is their high cost, high weight and unsuitability for installation on mini or micro PSU aircraft. Stereoscopic video sensors are relatively lightweight and data-oriented, and the associated video processing algorithms impose significant computational requirements, which makes their real-time application problematic.

Therefore, there is a need for new motion analysis techniques for navigation in environments with weak or no GNSS signal.

The optical flow (OP) of cameras is of particular interest for research because of the simple representation of velocity. It has been observed that honeybees use optical flow for landing, airspeed regulation and obstacle avoidance. Interested in the flight pattern of insects, many developers were directed to use modified video sensors for measuring optical flow based on various robotic platforms. There are options for using optical sensors mice, for measuring the motion field, installed on the UAV, but low resolution and the impossibility of installing additional focusing optics gave unsatisfactory results in determining the optical flow.

An analysis of the modern literature on the study of optical flow has shown that both simple monocular cameras and special optical flow sensors are used to measure the optical flow. Optical flow can be used to evaluate speed, orientation and trajectory of movement after the estimated values of OP and INS passed through stochastic filters. Such OP/INS systems provide huge capabilities to support small or microUAVs in short-range navigation without relying on GNSS signal, similar to insect optical navigation system. The paper shows the possibility of using an optical sensor to estimate the UAV motion parameters. It is proposed to use texture analysis to estimate the optical flow in comparison with the standard block method. To study accuracy the work of the entire algorithm, a program was developed in the MATLAB system. Based on received given the results of translational velocity estimates, the accuracy of the proposed methods was analyzed.

Determination of motion parameters according to the optical flow data of a video camera

Various points in the space of objects are displayed by the optical system of the camera in image space at different distances from the focal plane.

However, if Since the distance between the camera and the observed scene considerably exceeds the focal length of the optical system, we can assume that the image is built in its focal plane. In this case, one can use the projective camera model, in which the image of a three-dimensional object is obtained by projecting it into the focal plane (image plane) through a single point called the optical center. Straight line perpendicular to the image plane and passing through this point is called the optical axis of the camera, and the point of intersection of the optical axis with the image plane is main point. The movement of objects in front of the camera or the movement of the camera in a stationary environment results in corresponding changes in the picture, and this measurement can be used to reconstruct the corresponding movement. The camera is moving in a static environment. The motion field is created by designing the speed on the image plane.

Point p corresponds to point P on the Earth's surface (Fig. 1). These two points are connected design equations. It is important that any point of the image can be assigned a certain vector. These vectors form the field of motion.

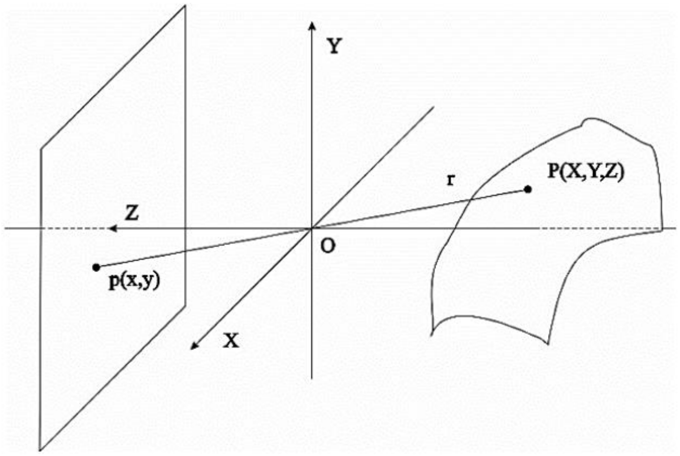


Fig. 1. Projective camera coordinate system.

Let's connect the coordinate system with the camera so that the Z axis coincides with the optical axis cameras. Let r denote the vector connecting the point O with the point P=[X,Y,Z]T, f the focal length. The projected pixel coordinates P on the image plane are determined by

$$p = \mathrm{f}\frac{\mathrm{P}}{\mathrm{Z}}.$$

In the general case, the measurement of coordinates in the photodetector is carried out in units, different from the units that specify the coordinates in the standard system. For a full description camera, it is necessary to express the coordinates of the point p in the natural units of the photodetector. In the new system, the coordinates of the projection of the point p will take the form

$$u = \frac{fX}{wZ} + u_0, \; v = \frac{fY}{hZ} + v_0.$$

where (u0, v0) are the coordinates of the main point relative to the origin of the photodetector

(in the natural coordinates of the photodetector); w and h are the scales along the ox and oy axes (for example, the distances between cells of a matrix photodetector along rows and columns).

For the subsequent presentation, we introduce a three-dimensional vector corresponding to the point P=(X,Y,Z) , and two-dimensional vector , p=(x, $y)^T$ corresponding to point p. Let us also define the vector of homogeneous internal coordinates of the camera $W = (u, v, 1)^T$. Using these notations, relations can be represented in a compact vector-matrix notation

$$ZW=AP,$$

Where $A = \begin{matrix} f/w & \mu & u0 \\ 0 & f/h & v_0 \\ 0 & 0 & 1 \end{matrix}$ - matrix of internal parameters of the camera, contains only the parameters of the optical system and photo detector of the camera.

Let OXYZ be the global coordinate system and O'X'Y'Z' the standard camera coordinate system. The transition from the OXYZ system to the O'X'Y'Z' system can be done by turning coordinate axes to the OX"Y"Z" system and subsequent offset of the origin. Then the relationship between the coordinates of the point P in the global and standard systems can be represented as

$$P' = RP + t \,,$$

where P and P′ are the vectors of spatial coordinates of the point P in the global and standard systems, respectively; R is a 3x3 matrix describing the rotation of the standard coordinate systems relative to global; t - is a three dimensional offset vector of the origin of the global system relative to the origin of the standard one.

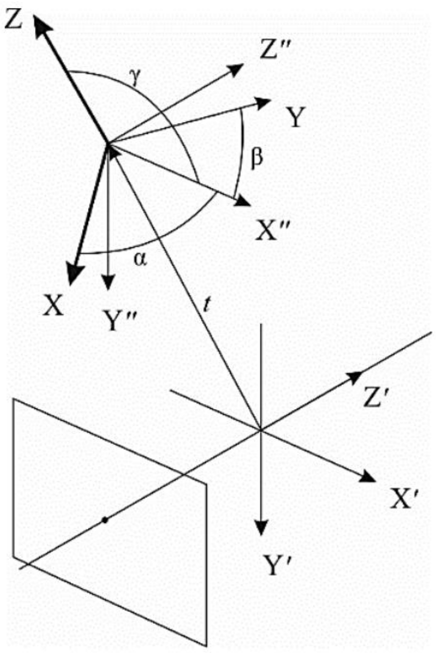


Fig.2. Transition from the global coordinate system to the standard camera coordinate system.

On fig. 2 schematically shows the coordinate transformation. Here α, β, γ are the angles formed by the OX″ axis with the OX, OY, and OZ axes, respectively. Vector $t = (t_x t_y t_z)^T$ - offset of the origin of the global coordinate system relative to the origin of the standard. For To obtain the internal parameters of the camera, as well as compensation for radial and tangential distortions, the video camera calibration procedure is performed.

The origin of coordinates in the camera image plane coincides with the main point u0=v0=0, and the coordinate units in the global system and in the camera image plane are the same (w=h=1). The motion of a rigid body can be decomposed into two components: (V) translational motion and rotational motion $(\overrightarrow{\omega)}$ around the axis passing through the origin. The speed of the point will look like:

$$V_{total} = -V - \vec{\omega}\times\mathrm{r}$$

Where $V = (V_x, V_y, V_Z)^T$ - progressive movement; $\vec{\omega} = (\omega_x, \omega_y, \omega_Z)^T$ – rotation parameters.

Taking the derivative with respect to time, we obtain the ratio between the speed P in the reference frame of the camera and the speed p in the image plane with the error function $\rho 0$.

$$\frac{flow}{\Delta t} \equiv V_{cam} = \rho_0 \cdot f \frac{ZV_{total} - V_z P}{Z^2} .$$

For the x and y components, the field of motion can be written as:

$$\dot{x} = -\frac{V_x}{Z} + x\left(\frac{V_z}{Z} + \omega_x y - \omega_y x\right) - \omega_y + \omega_z y,\ \dot{y} = -\frac{V_y}{Z} + y\left(\frac{V_z}{Z} + \omega_x y - \omega_y x\right) - \omega_z x + \omega_x$$

These equations can be written as $\dot{x} = u_t + u_r$ and $\dot{y} = v_t + v_r$.Let us divide the optical flow into translational component $(u_t + v_t)$ and rotational component $(u_r + v_r)$:

$$u_t = (-V_x + xV_z)/Z,\ \ u_r = \omega_x xy - \omega_y(x^2 + 1) + \omega_z y,$$

$$v_t = (-V_y + yV_z)/Z,\ \ v_r = \omega_x(y^2 + 1) - \omega_y xy - \omega_z x .$$

To determine the optical flow in the article [8], the method of comparison is used blocks that uses adaptively resizable and adaptive search strategy the motion vector with weighting of measurements of image blocks, where each block corresponds to a texture index.

Forward speed estimation

Let us consider three possible variants of the initial conditions for the motion of the video camera, or platforms. We use the least squares method to determine the parameters movement.

1. The distance from the camera to the surface at each point in the image is known. Let us set ourselves the goal of determining the parameters of translational motion V_x, V_y.

Let's define the smallest deviation:

$$\min_{V_x, V_y} \iint \left[\left(u - \frac{\alpha}{Z} \right)^2 + \left(v - \frac{\beta}{Z} \right)^2 \right] dxdy,$$

Where $\alpha = -V_X + xV_Z$; $\beta = -V_y + yV_Z$.

Differentiating the integrals with respect to V_X, V_y and equating the resulting equations to zero, we obtain:

$$V_x = \frac{V_z \iint xdxdy - Z \iint udxdy}{(n \cdot m)}, \quad V_y = \frac{V_z \iint ydxdy + Z \iint vdxdy}{(n \cdot m)}.$$

2. Consider the condition under which there is no translational movement along the Z axis,

$V_z = 0$. In this case, expression is simplified, and we obtain the translational motion parameters:

$$V_x = \frac{-Z \iint udxdy}{(n \cdot m)}, V_y = \frac{-Z \iint vdxdy}{(n \cdot m)}.$$

3. Next, consider the condition under which it is necessary to determine the motion parameters

V_x, V_y, V_Z with unknown Z. To consider the explicit solution, we use the expression proposed in. The least squares method consists of the following steps: first we determine the value of Z, which minimizes the integrand in each point (x, y), and then determine the value of V_x, V_y,and V_Z, which minimizes the integral.

The expression we want to minimize will take the form

$$\min_{V_x,V_y,V_z} \iint \left[\left(u - \frac{\alpha}{Z} \right)^2 + \left(v - \frac{\beta}{Z} \right)^2 \right] \left(\alpha^2 + \beta^2 \right) dxdy,$$

Where $\alpha = -V_x + xV_z$; $\beta = -V_y + yV_z$.

Denote the integral for minimization by:

$$g\left(V_x, V_y, V_z\right) = aV_x{}^2 + bV_y{}^2 + cV_z{}^2 + 2dV_xV_y + 2eV_yV_z + 2fV_zV_x,$$

Where

$a = \iint v^2 dxdy,$ $b = \iint u^2 dxdy$, $c = \iint (xv - yu)^2 dxdy$, $e = \iint u(xv - yu)dxdy$

$f = -\iint v(xv - yu)dxdy.$

To determine the speed of translational movement by the least squares method it is necessary to solve the following homogeneous system with respect to w: Gw= 0, where

$$G = \begin{pmatrix} a & d & f \\ d & b & e \\ f & e & c \end{pmatrix}.$$

Since the data contains noise, the function $g(V_x, V_y, V_Z)$ can't be set to zero for a non-zero translational speed and thus $w = (0,0,0)^T$ will be the only the right decision. Having determined the eigenvector corresponding to the own meaningλ_1, we get:

$$V_x = (b-\lambda_1)(c-\lambda_1) - f(b-\lambda_1) - d(c-\lambda_1) + e(f+d-e),$$
$$V_y = (c-\lambda_1)(a-\lambda_1) - d(c-\lambda_1) - e(a-\lambda_1) + f(d+e-f),$$
$$V_z = (a-\lambda_1)(b-\lambda_1) - e(a-\lambda_1) - f(b-\lambda_1) + d(e+f-d).$$

It should be noted that the value of λ_1 should be small with good data, and one can simply approximate the exact solution using these equations at $\lambda_1 = 0.$

Results of modeling and estimation of video camera motion parameters.

To study the accuracy of the algorithms, a program was developed in the system MATLAB. To create the effect of a UAV flight, the coordinates of the underlying surface will remain unchanged; we will change the coordinates and orientation of the camera.

Change of position and camera orientation is given by analytical equations. When running a flight simulation, the underlying surface will be displayed on the screen from a certain point of space and at certain angles, the value of which depends on the current position and camera orientation.

During the flight, the brightness of the image changes. The resulting current image is divided into 8x8 blocks and the procedure is performed

optical flow estimates. The parameters of the motion vectors (magnitude and direction) are recorded in the corresponding matrices. Depending on the problem being solved, an algorithm for analyzing motion vectors (motion fields) is chosen. Movement simulation was carried out

on eight high resolution images of the underlying surface (4412 x 4779 pixels) with different textures. For comparison, the translational velocity is calculated using texture analysis and the standard method based on equal precision measurements.

The appearance of the coordinate system modeled for the surveillance system is shown
in fig. 4. The origin of coordinates is located on the surface of the underlying surface at the selected point. The initial position of the camera is characterized by the coordinates (X, Y, Z) and orientation angles (α, β, γ).

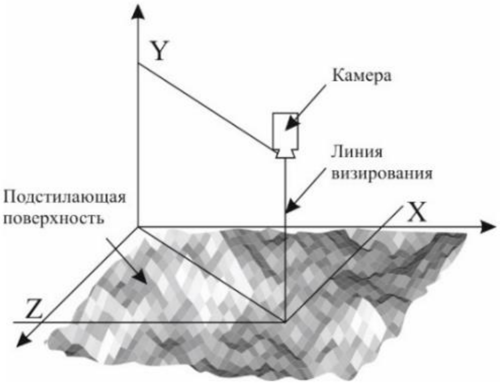


Fig. 4. Simulation of the movement of the video camera

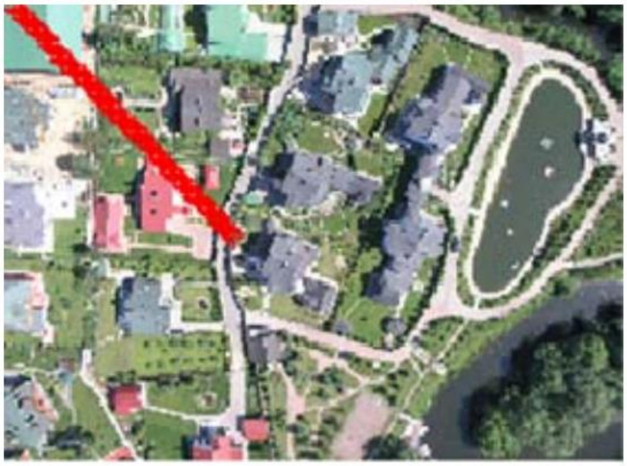


Fig. 4. Simulation of the movement of the video camera

Simulation initial data: average travel speed 16 m/s, travel height camera 100 m, camera viewing angle 90 degrees, focal length 1 mm, CCD matrix size 256x256 pixels, frame rate 30 fps. Estimation of translational speed with compensation of rotational motion, change in angular velocities Y,X,Z=[-10:10].

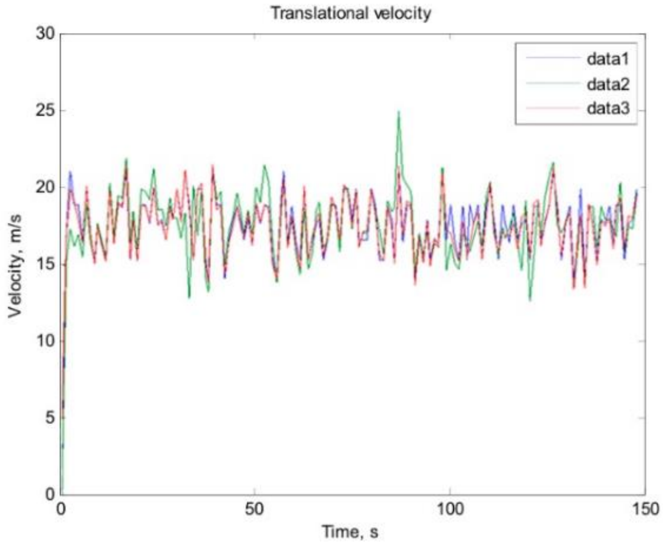


Fig. 6. Forward speed.

data1 is the true forward speed;

data2 - calculated forward speed standard method;

data3 - calculated forward speed developed by the OF method.

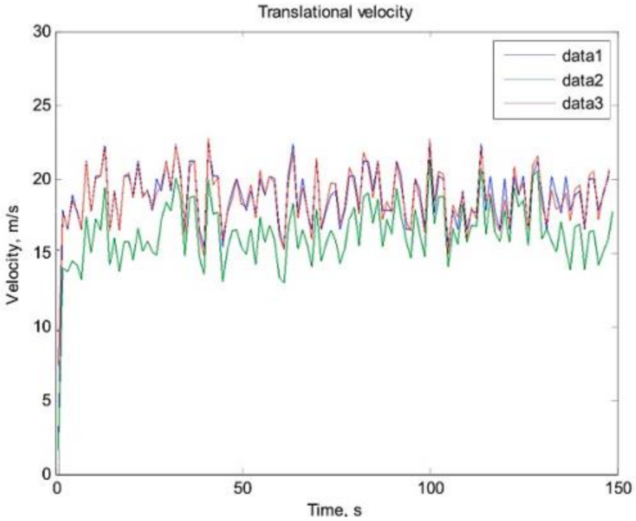


Fig. 7. Forward speed

data1 is the true forward speed;

data2 - calculated forward speed standard method;

data3 - calculated forward speed developed by the OF method.

On the basis of the obtained results of the translational velocity estimation, it is possible to analyze the accuracy of the proposed method.

For texture analysis, a parameter was proposed in that characterizes the degree of image texture according to the estimation of the covariance matrix. The analysis of the image of the underlying surface with respect to the estimate of the condition number was equal to 9.6348, which is a sign of the high texture of the entire image.

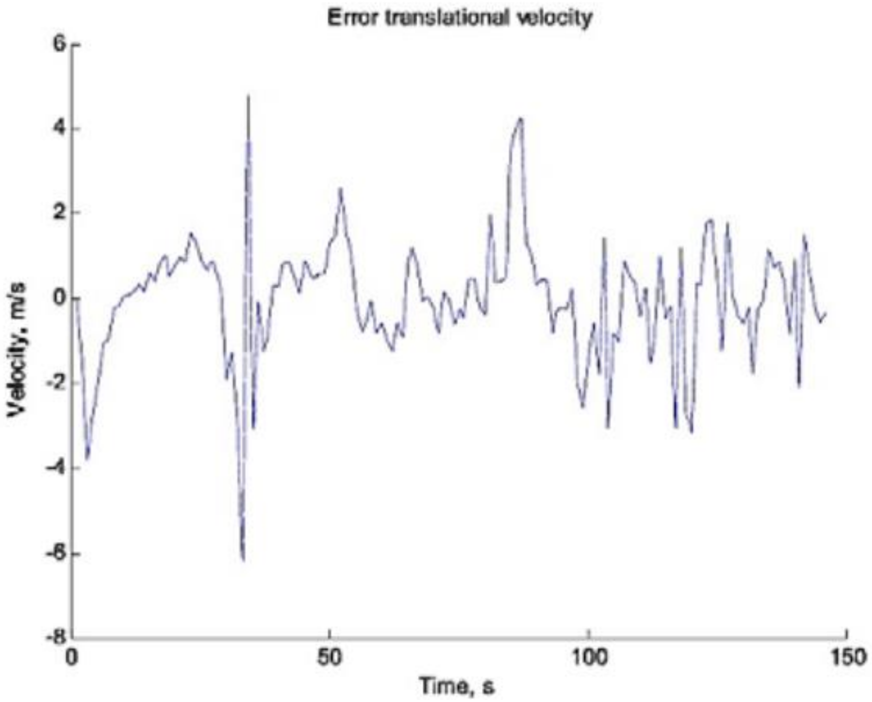


Fig.8. Errors in translational velocity estimates

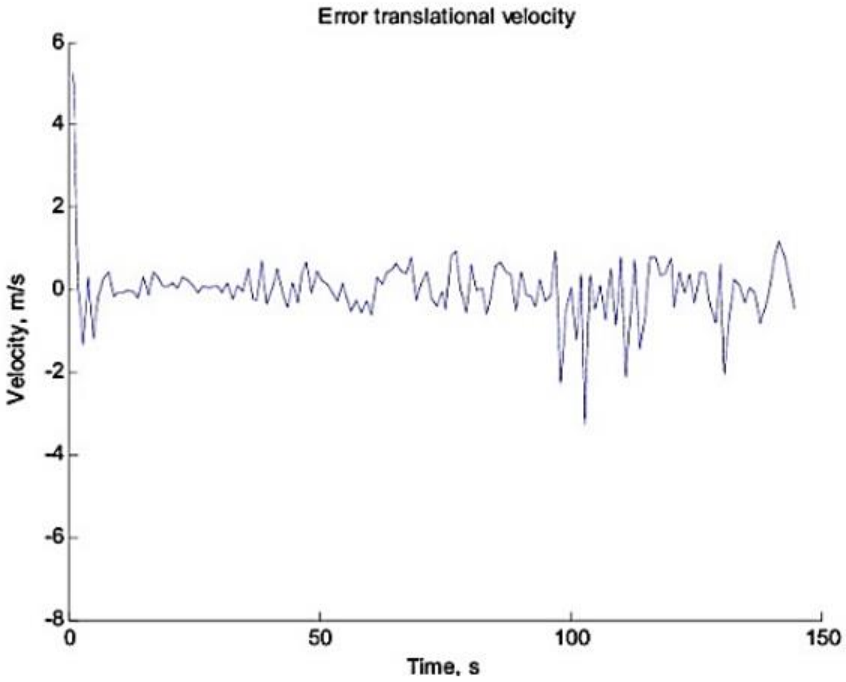


Fig. 9. Errors in translational velocity estimates developed by the OP method

For estimates based on the standard block method, the estimated mean the value of the translational velocity error was 0.154 m/s, the standard deviation of the determination error forward speed 1.4389 m/s.

The calculation of the translational velocity using the estimation of image blocks gave the following result: the average estimated value of the translational velocity error was 0.0880m/s, standard deviation of the translational velocity determination error 0.6392 m/s.

On fig. Figure 7 shows the results of velocity estimates for the image of the underlying surfaces with a weak texture index. The simulation of the motion of the video camera was carried out on a uniform texture of the water surface. Based on the received given the results of the translational velocity estimates, it is possible to estimate the accuracy of the proposed method. Texture analysis of the entire image of the underlying surface with respect to condition number estimate was 6.6203, which indicates a weak texture of the image.

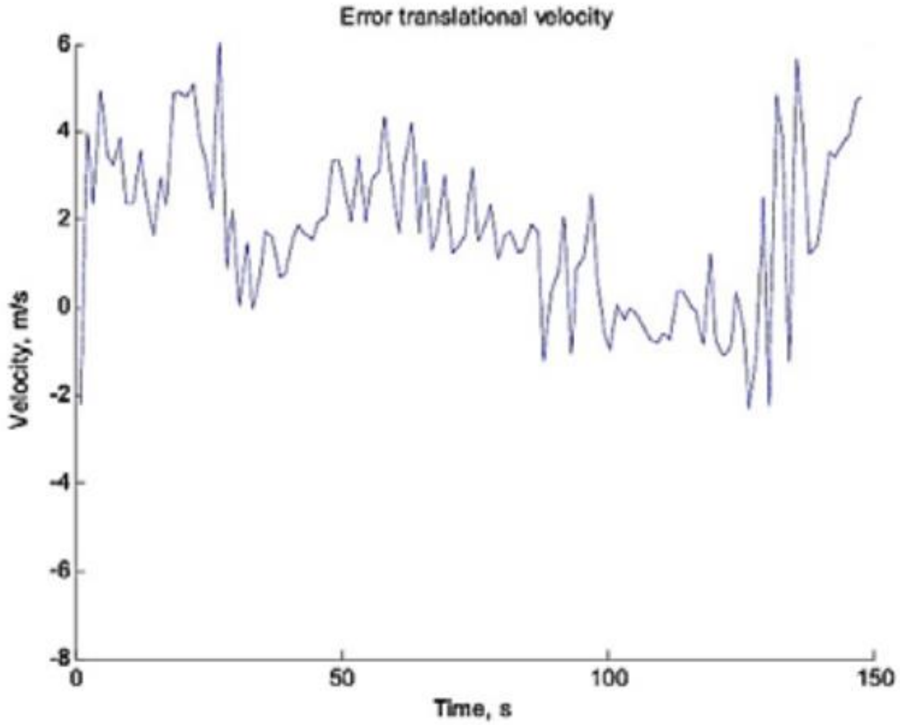


Fig. 10. Errors in translational estimates speed by the standard OP method

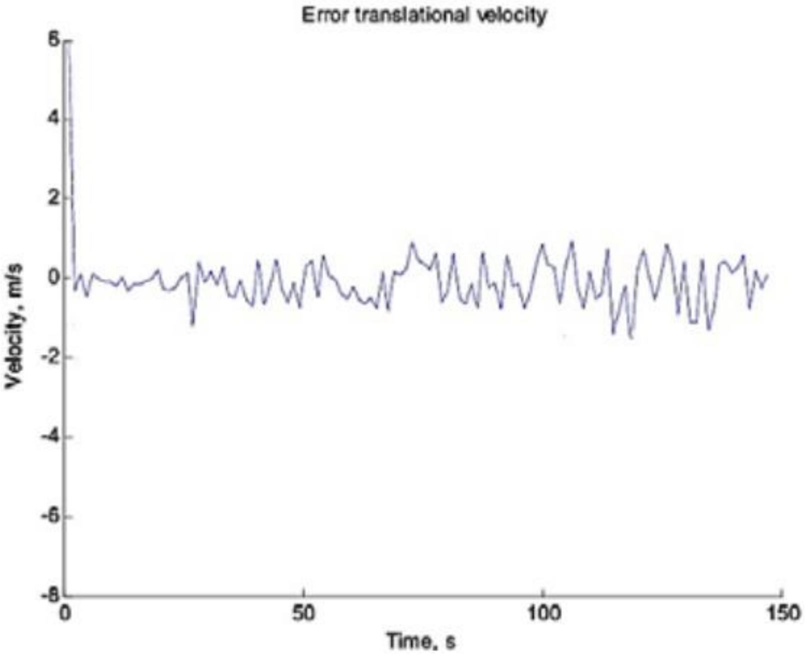


Fig. 11. Errors in translational estimates speed developed by the method O

For estimates based on the standard method, the average estimated value of the translational velocity measurement error was 2.5128 m/s, and the standard deviation of the translational velocity measurement error was 1.1727 m/s.

The translational velocity calculation using texture analysis gave the following result: the average estimated value of the translational velocity measurement error is 0.0221 m/s, and the standard deviation of the translational velocity measurement error is 0.7223 m/s. In table. Table 1 shows the results of estimates of translational motion parameters for various images of the underlying surface:

Results of estimates of translational motion parameters

Grade Options	The texture of the underlying surface							
	Topographic map	aerial photograph y ка	aerial photograph	square	Asphalt texture	texture concrete	grass texture	
texture analysis	2.7736	4.7706	9.6348	3.3554	2.5556	2.1907	3	6.6

Mat. waiting for forward speed error	0.33 m/s	1.1 m/s	1.38 m/s	0.29 m/s	0.18 m/s	0.2 m/s	0.32 m/s	2.51
RMS errors in determining the translational speed	0.6m/s	1.57 m/s	1.44 m/s	0.57 m/s	0.62 m/s	0.7 m/s	0.76 m/s	1.17
Mat. waiting for an error in determining the translational speed using the texture method	0.27 m/s	0.03 m/s	0.09 m/s	0.29 m/s	0.16 m/s	0.2 m/s	0.26 m/s	0.02
RMSD of the error in determining the translational velocity using the texture method	0.47 m/s	0.41 m/s	0.64 m/s	0.5 m/s	0.61 m/s	0.7 m/s	0.39 m/s	0.72

1.4 Зернення до зовнішніх експертів

I DEVICE OF RADIO-FREQUENCY NOISE STATIONARY "RIAC-1C".

1. General information, purpose

1.1 Stationary radio frequency noise device "PIAC-1C" is designed to protect objects from leakage of confidential information by channels of spurious electromagnetic radiation and interference by generating a noise signal.

1.2 The device includes a noise generator "RIAS-1GS" and frame soft antennas "PIAC-1AM".

1.3 Soft frame antennas "PIAC-1AM" are insulated wires with a cross section of up to 5 mm, which are placed along the perimeter of the protected object.

1.4 Up to 6 loop antennas can be connected to the output channels of the generator.

2. Specifications

2.1 The device provides suppression of emissions from low-power transmitters in the frequency band from 180 Hz to 2 GHz and above.

2.2 The quality factor of the noise signal of the device is not less than 0.8.

2.3 Spectral intensity density of the electric $E_{\text{Ш}}$ and magnetic pH components of the electromagnetic noise field (dB/μV*m^{-1}*$kHz^{-0.5}$) of the device relative to 1 μV at a distance of 1 m from the antenna:

- in the range from 0.00018 to 100 MHz not less than 65 dB
- in the range from 100 to 100 MHz not less than 70 dB
- in the range from 500 to 1200 MHz not less than 70 dB:
- in the range from 1200 to 2000 MHz, at least 70 dB.

2.4 The coefficient of interspectral correlations in the frequency band of the noise signal of the device is not more than 6 dB.

2.5 The device provides regulation of the noise signal level by at least 20 dB.

2.6 The maximum integral value of the output power of the device is not less than 10 W.

2.7 The device has a built-in system of automatic operation control and sound indication of the integrity of the emitted antennas.

2.8 The power supply of the device is carried out from the AC network with a voltage of 220 V plus 22 V minus 33 V, frequency 50±1 Hz.

2.9 Time of technical readiness of the device - no more than 5 s.

2.10 The power consumed by the device from the AC mains is not more than 20 W.

2.11 Overall dimensions of the generator - no more than 190x187x63 mm.

2.12 Mass of the generator is not more than 2 kg.

The tool generates a noise signal at a frequency at which indirect electromagnetic radiation occurs, extinguishing them. Advantages: wide range of operation, high signal quality factor, light, low standby time. Disadvantages: the size of the device, no battery for battery life, only one type of antenna, stationary.

II STATIONARY RADIO-FREQUENCY NOISE DEVICE "RIAS-1C/1"

1. General information, purpose

1.1 Stationary radio frequency noise device "RIAC-1C/1" is designed to protect objects from leakage of confidential information by channels of spurious electromagnetic radiation and interference by generating a noise signal.

1.2 The device includes a noise generator "PIAC-1GS/1" and dipole telescopic antennas "PIAC-1AD".

1.3 Telescopic dipole antennas "PIAC-1AD" are a four-legged dipole pin with a diameter of 10 mm and a length of 1225 mm.

2. Specifications

2.1 The device provides suppression of emissions from low-power transmitters in the frequency band from 180 Hz to 1 GHz and above.

2.2 The quality factor of the noise signal of the device is not less than 0.8.

2.3 The spectral density of the electric $E_{\text{Ш}}$ and magnetic pH components of the electromagnetic noise field (dB / µV * m^{-1} * $kHz^{-0.5}$) of the device relative to 1 µV at a distance of 1 m from the antenna:

- in the range from 0.00018 to 100 MHz, at least 65 dB;
- in the range from 100 to 100 MHz, not less than 70 dB;
- in the range from 500 to 1000 MHz, not less than 70 dB;

2.4 The coefficient of interspectral correlations in the frequency band of the noise signal of the device is not more than 6 dB.

2.5 The device provides regulation of the noise signal level by at least 20 dB.

2.6 The maximum integral value of the output power of the device is not less than 8 W.

2.7 The device has a built-in system of automatic operation control and sound indication of the integrity of the emitted antennas.

2.8 The power supply of the device is carried out from the AC network with a voltage of 220 V plus 22 V minus 33 V, frequency 50±1 Hz.

2.9 Time of technical readiness of the device is no more than 5 s.

2.10 The power that the device consumes from the AC mains is not more than 20 watts.

2.11 Overall dimensions of the generator - no more than 190x187x63 mm.

2.12 Mass of the generator is not more than 2 kg.

The tool generates a noise signal at a frequency at which indirect electromagnetic radiation occurs, extinguishing them. Advantages: high signal quality factor, light, low standby time. Disadvantages: the size of the device, no battery for battery life, only one type of antenna, stationary.

III DEVICE OF RADIO-FREQUENCY NOISE STATIONARY "RIAS-1C/2"

1. General information, purpose

1.1 Stationary radio frequency noise device "PIAC-1C/2" is designed to protect objects from leakage of confidential information by channels of spurious electromagnetic radiation and interference by generating a noise signal.

1.2 The device includes a noise generator "PIAC-1GS/2" and dipole telescopic antennas "PIAC-1AD".

1.3 Telescopic dipole antennas «PIAC-1AD» are a four-leg dipole pin with a diameter of 10 mm and a length of 1225 mm.

2. Specifications

2.1 The device provides suppression of emissions from low-power transmitters in the frequency band from 180 Hz to 2.5 GHz and above.

2.2 The quality factor of the noise signal of the device is not less than 0.8.

2.3 Spectral density of the electric $E_{\text{ш}}$ and magnetic pH components of the electromagnetic noise field (dB/μV*m^{-1}*kHz$^{-0.5}$) of the device relative to 1 μV at a distance of 1 m from the antenna:

- in the range from 0.00018 to 100 MHz, not less than 65 dB;
- in the range from 100 to 100 MHz not less than 70 dB;
- in the range from 500 to 1200 MHz not less than 70 dB;
- in the range from 1200 to 2500 MHz not less than 70 dB.

2.4 The coefficient of interspectral correlations in the frequency band of the noise signal of the device is not more than 6 dB.

2.5 The device provides regulation of the noise signal level by at least 20 dB.

2.6 The maximum integral value of the output power of the device is not less than 15 W.

2.7 The device has a built-in system of automatic control of functioning.

2.8 The power supply of the device is carried out from the alternating current network with a voltage of 220 8 plus 22 V minus 33 V, frequency 50±1 Hz.

2.9 The time of technical readiness of the device is no more than 5 s.

2.10 The power that the device consumes from the AC mains is not more than 20 watts.

2.11 Overall dimensions of the generator - no more than 190x187x63 mm.

2.12 Mass of the generator is not more than 2 kg.

The tool generates a noise signal at a frequency at which indirect electromagnetic radiation occurs, extinguishing them. Advantages: wide range of operation, high signal quality factor, light, low standby time. Disadvantages: the size of the device, no battery for battery life, only one type of antenna, stationary.

IV DEVICE OF RADIO-FREQUENCY NOISE MOBILE "RIAC-1M"

1. General information, purpose

1.1 Mobile radio frequency noise device “PIAC-1M. designed to protect objects from leakage of confidential information by channels of spurious electromagnetic radiation and interference by generating a noise signal.

1.2 The device includes a PIAC-1GM noise generator, PIAC-1AD internal dipole telescopic antennas (built-in) and a PIAC-1AZh rigid loop antenna.

1.3 Telescopic dipole antennas "PIAC-1AD" are a four-legged dipole pin with a diameter of 10 mm and a length of 1225 mm.

1.4 Rigid loop antenna "PLAC-1AЖ" is a circle with a diameter of 280 mm and a tube section of 10 mm.

2. Specifications

2.1 The device provides suppression of emissions from low-power transmitters in the frequency band from 180 Hz to 2 GHz above.

2.2 The quality factor of the noise signal of the device is not less than 0.8.

2.3 Spectral intensity density of the electrical $E_{ш}$ and magnetic pH components of the electromagnetic noise field (dB / μv * m^{-1} * $kHz^{-0.5}$) of the device relative to 1 μV at a distance of 1 m from the antenna:

- in the range from 0.00018 to 100 MHz, not less than 65 dB;
- in the range from 100 to 100 MHz not less than 70 dB:
- in the range from 500 to 1200 MHz not less than 70 dB;
- in the range from 1200 to 2000 MHz not less than 70 dB.

2.4 Coefficient of interspectral correlations in the frequency band of the noise signal - no more than 6dB.

2.5 The device provides regulation of the noise signal level to a value of at least 20 dB.

2.6 The maximum integral value of the output power of the device is not less than 15 W.

2.7 The device has a built-in system of automatic control of functioning.

2.8 Power supply of the device is provided from the alternating current mains with a voltage of 220 V plus 22 V minus 33 V, frequency (50:1) Hz, the accumulator and the vehicle's on-board network.

2.9 The time of technical readiness of the device is not more than 5 s.

2.10 The power that the device consumes from the AC mains is not more than 20 W.

2.11 Device devices are placed in a case.

2.12 Overall dimensions of the device are not more than 460x380x130mm.

2.13 Generator weight - no more than 2 kg.

The tool generates a noise signal at a frequency at which indirect electromagnetic radiation occurs, extinguishing them. Advantages: wide range of operation, high signal quality factor, light, low standby time. Disadvantages: the size of the device, no battery for battery life.

V COMPUTER RADIO-FREQUENCY NOISE DEVICE "RIAS-1K"

1. General information, purpose

1.1 Computer radio frequency noise device "PIAC-1K" is designed to protect objects from leakage of confidential information by channels of spurious electromagnetic radiation and interference by generating a noise signal.

1.2 The device includes a noise generator "PIAC-1ГМ", dipole telescopic antennas "PIAC-1AD" and a rigid frame antenna "PIAC-1АЖ".

1.3 Dipole telescopic antennas "PIAC-1AD" are a four-legged dipole pin with a diameter of 10 mm and a length of 1225 mm.

1.4 Rigid loop antenna "PIAC-1АЖ" is a circle with a diameter of 280 mm and a tube section of 10 mm.

2.Specifications

2.1 The device provides suppression of emissions from low-power transmitters in the frequency band from 180 Hz to 2 GHz.

2.2 The quality factor of the noise signal of the device is not less than 0.8.

2.3 Spectral intensity density of the electrical $E_{ш}$ and magnetic pH components of the electromagnetic noise field (dB/μV*m^{-1}*kHz$^{-0.5}$) of the device relative to 1 μV at a distance of 1 m from the antenna:

- in the range from 0.00018 to 100 MHz, at least 65 dB;
- in the range from 100 to 100 MHz not less than 70 dB;
- in the range from 500 to 1200 MHz not less than 70 dB;
- in the range from 1200 to 2000 MHz not less than 70 dB.

2.4 The coefficient of interspectral correlations in the frequency band of the noise signal of the device is not more than 6 dB.

2.5 The device provides regulation of the noise signal level by at least 20 dB.

2.6 The maximum integral value of the output power of the device is not less than 10 W.

2.7 The device has a built-in system of automatic control of functioning.

2.8 The power supply of the device is carried out from the power supply unit of the computer.

2.9 Time of technical readiness of the device - no more than 5 s.

2.10 The power that the device consumes from the power supply of the computer is not more than 20 watts.

2.11 The generator is placed in a free spot of the computing unit, and the antennas can be mounted either on the casing of the computing unit or in another convenient place.

2.12 Instead of dipole telescopic antennas PIAC-1AD" and rigid frame antennas "PIAC-1AЖ", active frame soft "PIAC-AM" antennas can be used, which are placed in the area where PC devices are located.

2.13 Overall dimensions of the generator - no more than 195x145x43 mm.

2.14 The mass of the generator is not more than 2 kg.

The tool generates a noise signal at a frequency at which indirect electromagnetic radiation occurs, extinguishing them. Advantages: wide range of operation, high signal quality factor, light, low standby time. Disadvantages: the size of the device, no battery for battery life, stationary tool.

VI HIGH-FREQUENCY RADIO-FREQUENCY NOISE DEVICE "RIAS-1B"

1. General information, purpose

1.1 High-frequency radio-frequency noise device "RIAC-1B" is designed to protect objects from leakage of confidential information by channels of spurious electromagnetic radiation and interference by generating a noise signal

1.2 The device includes a PIAC-1GV noise generator and PIAC-1AD telescopic dipole antennas.

1.3 Telescopic dipole antennas "PIAC-1AD" are a four-legged dipole pin with a diameter of 10 mm and a length of 1225 mm.

2. Specifications

2.1 The device provides suppression of emissions from low-power transmitters in the frequency band from 0.5 GHz to 2 GHz.

2.2 The quality factor of the noise signal of the device is not less than 0.8.

2.3 Spectral density of the electric $E_{ш}$ and magnetic pH components of the electromagnetic noise field (dB / μV*m^{-1}*kHz$^{-0,5}$) of the device relative to 1 μV at a distance of 1 m from the antenna:

-in the range from 1000 to 1500 MHz - not less than 70 dB;

-in the range from 1500 to 2000 MHz, at least 70 dB.

2.4 The coefficient of interspectral correlations in the frequency band of the noise signal of the device is not more than 6 dB.

2.5 The device provides regulation of the noise signal level by at least 20 dB.

2.6 The maximum integral value of the output power of the device is not less than 10 W.

2.7 The device has a built-in system of automatic control of functioning.

2.8 The power supply of the device is carried out from the AC network with a voltage of 220 V plus 22 V minus 33 V, frequency 50+1 Hz.

2.9 The time of technical readiness of the device is no more than 5 s.

2.10 The power that the device consumes from the AC mains is not more than 20 watts.

2.11 Overall dimensions of the generator are not more than 153x135x50mm.

2.12 Generator weight - no more than 2 kg.

The tool generates a noise signal at a frequency at which indirect electromagnetic radiation occurs, extinguishing them. Advantages: high signal quality factor, light, low standby time. Disadvantages: the size of the device, no battery for battery life, only one type of antenna, stationary.

засіб радіочастотного шуму	means of radio frequency noise	максимальне інтегральне значення	maximum integral value
витік конфіденційної інформації	leakage of confidential information	вихідна потужність	output power
побічні електромагнітні випромінювання	spurious electromagnetic radiation	система автоматичного контроля функціонування	automatic operation control system
генератор шуму	noise generator	звукова індикація цілісності	sound indication of integrity
генерація шумового сигналу	noise signal generation	час технічної готовності	time of technical readiness
мягка рамочна антена	soft frame antenna	електроживлення	power supply
вихідний канал	output channel	регуляція рівня шуму	noise level regulation
січення проводу	wire cross section	чотирьохколіний штирь	four-knee pin

придушення випромінювань	suppression of radiation	дипольні телескопічні антени	dipole telescopic antennas
малопотужні випромінювачі	low-power emitters	січення трубки	tube cross section
коефіцієнт якості шумового сигналу	noise signal quality factor	бортова мережа автомобіля	car onboard network
спектральна площина напруженості електричного і магнітного компонентів електромагнітного поля	spectral plane of the electric and magnetic components of the electromagnetic field	блок живлення комп’ютера	computer power supply
діапазон	range	ПЕОМ	PC
коефіцієнт міжспектральних корреляцій звязку	coefficient of interspectral correlations of the connection	обчислючуючий блок	computing unit
полоса частот	frequency band		

1.6 ПІДГОТОВКА ЩОДО ВІДПОВІДНИХ УМОВ

Умови	Радіотехнічні		Оптичні засоби			Акустичні засоби
	Засоби РЛР	Засоби РРТР	Засоби ОЕР в діапазоні видимих частот	Засоби ОЕР в ІК діапазоні	Лазерні засоби	Засоби акустичної розвідки
Виявлення по периметру вдень	+	+	+	–	+	+
Виявлення по периметру вночі	+	+	–	+	+	+
Виявлення в умовах існуючих завад	+	+	+	+	+	+
Виявлення БПЛА серед існуючих літальних об`єктів	–	+	–	–	–	±
Виявлення в складних метеорологічних умовах	±	+	–	–	–	–
Ідентифікація БПЛА	–	+	±	±	–	+

Розбиття одиничних та групових	+	+ (по різним каналам)	+	+	+	+ (для БПЛА різних типів)
Супроводження та виявлення траєкторії	+	+	+	+	+	+
Відстань	велика	велика	середня	середня	середня	низька

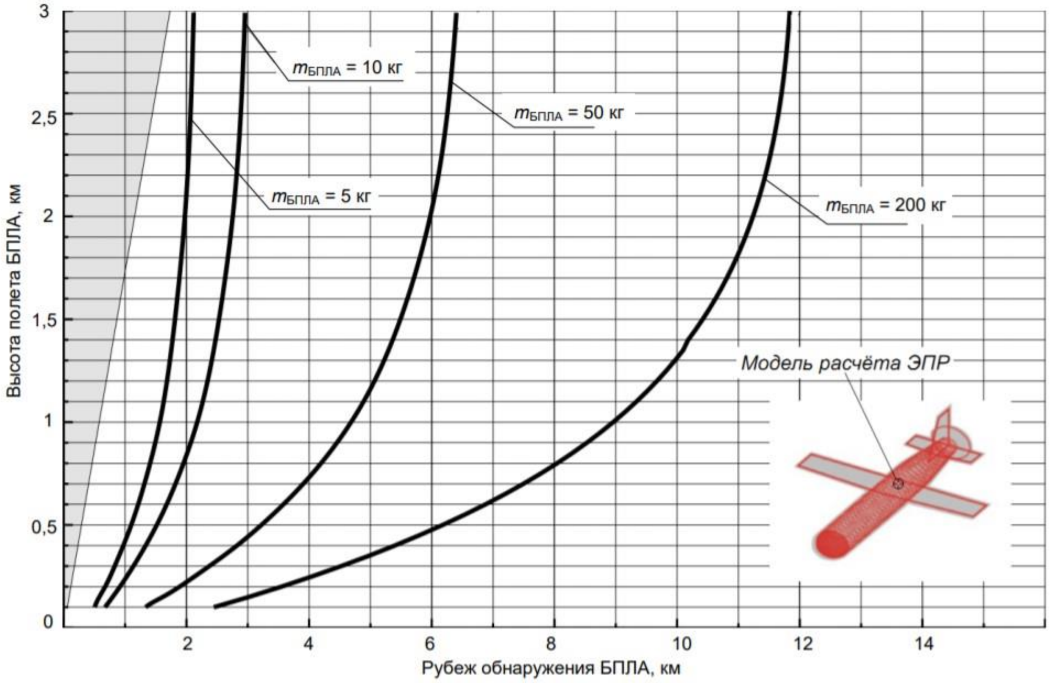


Рис. 1. Відстань для виявлення БПЛА, які мають різні властивості

1.7 СТРАХУВАННЯ РИЗИКІВ

Among the formal security models in this paper, we will consider data integrity models and the features of their application for databases.

Data integrity models

Ensuring information security is impossible without considering the concept protection of reliability and correctness of data, which is the essence of ensuring their integrity. For many, especially non-military organizations, integrity is more important than confidentiality. It is difficult to imagine a system for which integrity properties would not be important. For example, if you post information on the Internet on a Web server and your goal is to make it available to the widest range of people, then confidentiality is not required in this case. However, integrity requirements remain relevant. Numerous attacks target integrity violation. These include malicious modifications performed by viruses or other malware, application errors. However, integrity violations are not limited to deliberate attacks. user error, oversight or ineptitude are the cause of many cases of unauthorized modification of information. Events that lead to integrity violations include changing or deleting files, data in the DB, entering incorrect data, changing the configuration, errors in commands, introducing a virus and executing malicious code. Violation integrity can occur due to the actions of any user, including administrators. They can also occur due to an oversight in the security policy or due to misconfigured security controls.

Integrity should be considered from three sides [2]:

- obstruction of making changes by unauthorized subjects;
- preventing authorized entities from making unauthorized changes, such as errors;
- maintaining the internal and external consistency of objects so that their data is a correct and true reflection of the real world, and any relationships (links) with any child, equal or parent object are valid, consistent and verifiable.

Properly implemented integrity protection provides the means for authorized changes while protecting against malicious unauthorized actions (such as viruses and intrusions), as well as from errors made by authorized users (such as errors or oversights/oversights). This ensures that the data remains correct (there are no logical errors in the structure and in the data values), unchanged (identity of data to a certain standard), undistorted (no falsification of data) and saved. If a security mechanism provides integrity, it provides a high level of assurance that data, objects, and resources are not will be changed from their original protected state.

Depending on how this or that aspect of the area of data use is the most important, allocate methods and means to ensure their integrity, in sense [3]:

- correctness, undistortedness and immutability of data, based on the so-called data integrity models;
- undistorted data during transmission in communication lines and storage in information systems based on cryptography (for example, the use of such cryptographic primitives as: digital signature, cryptographic hash functions, authentication codes);
- parallel execution of transactions in client-server systems (transactions play an important role in the mechanism for ensuring the integrity of the database).

There are numerous countermeasures that can guarantee the integrity data for various possible threats [2]. Including make security easier, if there is a clear model of what needs to be protected and who and what is allowed to do [4]. Therefore, an integral part of any project to create or assess the security of IS and databases data, including, as noted in [5], is the presence of a security model. Below, in first of all, let's dwell on the analysis of some of the most well-known security models related to the aspects considered in the work - formal models of data integrity.

Clark–Wilson model

Based on the importance of data integrity, several security models, which include the models proposed by Clark with Wilson and Biba. The Clark-Wilson model [6] is descriptive. It does not contain any there were no strict mathematical expressions. The Clark–Wilson model is a framework and guide for formalizing security policies, not a specific security policy model. It highlights the importance of management approval of processes and policies security that an organization must follow [7]. Its most likely appropriate be considered as a set of practical recommendations for building an integrity system in IS.

For a better understanding of this model, we will carry out some formalization by introducing certain notation:

- S – set of subjects;

- D - a set of data in the IS (a set of objects), and $D=CDI\cup UDI$, $CDI\cap UDI=\varnothing$ where CDI (*constrained data items)* data (any data element) the integrity of which is controlled (protected by the security model); UDI (*unconstrained data items*) - data whose integrity is not controlled by the security model;

- IVP (integrity verification procedure) is a CDI integrity check procedure (a procedure that scans data elements and confirms their integrity, for example, by calculating a checksum or using the capabilities of a modern blockchain model, as shown in [8]);

- TP (transformation procedure) - a transformation procedure - a component that can initiate a transaction (sequence of operations) that transfers the system from one state to another. Conversion procedures are the only procedures that are allowed to modify CDI . Limited access to CDI through TP forms the basis of the Clark–Wilson integrity model.

The Clark-Wilson model is based, like the discretionary models of access control, on triples: “*subject – operation (transaction) that does not violate the integrity – object*”. Subjects do not have direct access to objects. Objects can only be accessed through TP .

The model distinguishes two main mechanisms that provide basic access control and integrity. Namely, a well-formed transaction preserves the integrity of the data and prevents arbitrary manipulation of these subjects. It should be noted that the concept of a well-formed transaction fits perfectly into the standard concept of transactions in traditional DBMS [9]. Separation of duties requires that each critical operation has two or more parts, each of which must be performed by a different entity or an entity with a different role.

The model consists of two sets of rules: certification (C), which is carried out by the security administrator, the system owner, the system custodian, and execution rules (E), which is carried out by the system. Execution rules correspond to application-independent security functions, and certification rules allow application-specific integrity definitions to be included in the model. It is desirable to minimize certification rules, since the certification process is complex, error prone and must be repeated after each change to the conversion procedure (program).

Somewhat paraphrased relative to the original, the rules of the Clark-Wilson model are given below:

1.Rule C1. The system must have IVPs capable of confirming the integrity of any CDI (in the original work [6] it is formulated as follows: “All IVPs must properly guarantee that all CDIs are in a valid state at the time of the IVP operation”; under the concept of “valid) state" the authors understand such a state of the system in which at any time the CDIs satisfy the requirements of integrity).

2. (C2) All TP transformation procedures must be implemented correctly, in the sense that they must not violate the integrity of the data (that is, they must put the CDI in a valid final state, given that it is in a valid state from the very beginning), and apply only to the list of CDI elements, set defined by the security administrator (ratio TP_i,(CDI_a, CDI_b, CDI_c, …)

3. (E1) The system shall control whether TP can be applied to CDI elements
in accordance with the lists specified in rule C2.

4. (E2) The system must maintain a list of allowed to specific users

TP conversion procedures indicating the admissible for each TP_i□TP and this subject (s $_j$□S) of the set of processed CDI elements (that is, triples: (S_j,TP_i,(CDI_a, CDI_b, CDI_c, …)

5. (C3) The list defined by rule E2 must meet the requirement of segregation of functional duties (including joint performance).

6. (E3) The system shall authenticate all users (each subject) attempting to perform any TP conversion procedure.

7. (C4) Each application of a TP must be recorded in a special CDI entry, a log containing information sufficient to reconstruct a complete picture of each application of that transformation procedure, and accessible only for adding information to it.

8. (C5) Any TP that accepts a UDI as input can only perform valid conversions on any possible UDI value. TP either accepts (converts to CDI) or rejects UDI . That is, special TPs can correctly handle UDIs, turning them into CDIs.

9. (E4) Only a specifically authorized entity (user, agent authorized to certify objects) may modify the lists defined in rules C3 and E2. This subject does not have the right to perform any actions if he is authorized to change the lists regulating these actions.

The role of each of the nine rules of the Clark-Wilson model in ensuring data integrity in [10] is correlated with the so-called theoretical principles of integrity control policy:

1) the correctness of transactions;

2) user authentication;

3) privilege minimization;

4) delimitation of functional duties;

5) audit of occurred events;

6) objective control;

7) managing the transfer of privileges;

8) ensuring continuous performance;

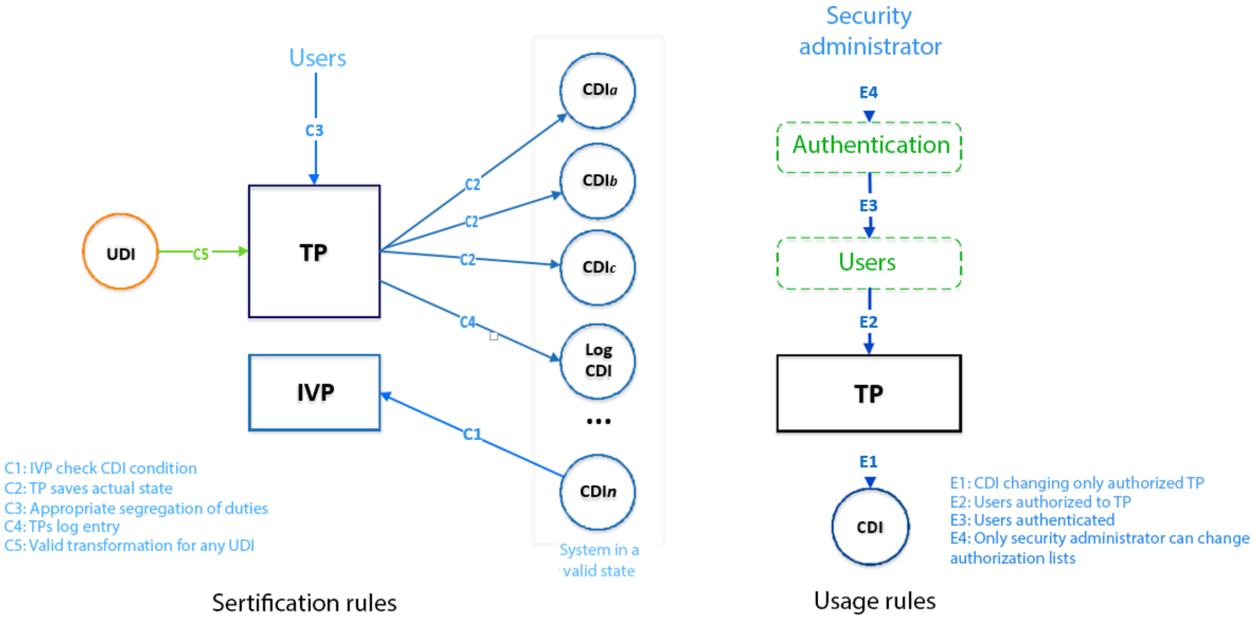
9) ease of use of protective mechanisms.

Correspondence of the rules of the Clark-Wilson model to the first six principles listed above is shown in Table. 1.

Clark–Wilson model rule	Integrity control policyprinciples
C1	1, 6
C2	1
C3	4
C4	5
C5	1
E1	3, 4
E2	1, 2, 3, 4
E3	2
E4	4

As can be seen from Table. 1, integrity control policy principles 1 (correctness of transactions) and 4 (separation of functional duties) are implemented by most of the rules of the Clark-Wilson model, which corresponds to its main idea.

On Pic. 1 shows a diagram of the application of these rules to control the operation of the system and data. UDIs represent data that exists outside the protected system. Certification rules ensure that such login credentials are properly validated. For example, rule C5 requires that well-formed TPs that convert UDI to CDI perform only validated conversions. Rules C1 and C2 require CDIs to satisfy integrity requirements in the initial state and after subsequent transformations. Rule C4 requires all transactions to be logged, as is usually the case with databases. Database logging is more to restore data after a failure, failure (for rollback - return to the previous state), and logging in the Clark-Wilson model - for auditing. Although databases can also have an audit log. Rule C3 requires an appropriate segregation of duties. Since data can only be entered in accordance with certification rules, it follows for the systems we are interested in that all data in the database must be CDI. The execution rules prevent the CDI from being modified in ways that conflict with the IVP. Rules E2–E4 refer to TP access authorization. While E1 guarantees that only well-formed certified (validated) TPs can be used to modify CDI.


Users
C3
UDI
C5
TP
C2
C2
C2
C4
CDIa
CDIb
CDIc
Log CDI
...
CDIn
C1
IVP
System in a valid state
C1: IVP check CDI condition
C2: TP saves actual state
C3: Appropriate segregation of duties
C4: TPs log entry
C5: Valid transformation for any UDI
Sertification rules
Security administrator
E4
Authentication
E3
Users
E2
TP
E1
CDI
E1: CDI changing only authorized TP
E2: Users authorized to TP
E3: Users authenticated
E4: Only security administrator can change authorization lists
Usage rules

Pic. 1. Scheme for applying the rules of the Clark-Wilson model

The main disadvantage commonly cited for the Clark–Wilson model is that IVP and related methods are not easy to implement in real computer systems [11]. For example, the main problem of implementing mechanisms for controlling the integrity of file objects is their rather strong influence on the loading of the computing resource of the system, which is due to the following reasons [12]: firstly, it may be necessary to control large amounts of information, which is associated with a significant the duration of the IVP procedure; secondly, continuous maintenance of the file object in the reference state may be required. In this regard, the question arises: what should be the frequency of starting the IVP procedure? If performed frequently, this will lead to a significant decrease in system performance, if rarely, then the effectiveness of such control may be low. Therefore, one of the main tasks in the implementation of mechanisms for controlling the integrity of file objects is the choice of principles and mechanisms for launching the CDI integrity check procedure. Another problem of the implementation of the integrity control mechanism is the control of the integrity of the controlling program itself, if the integrity control is implemented in software. All this requires a certain additional study and the adoption of appropriate decisions, depending, as a rule, on the characteristics of specific IS.

However, in the context of a DBMS, the above general drawback of the Clark-Wilson model, due to the complexity of implementing IVP and related methods, can be overcome to a large extent. So, for example, for relational DBMS, some integrity constraints are inherent in the theory: entity integrity, referential integrity. Others can be specified as static constraints using SQL (so-called declarative support for integrity constraints). Still others, as dynamic integrity constraints (the so-called procedural support for integrity constraints), which can be implemented using triggers and stored programs. All of them ensure the integrity of the CDIs that are accessed and modified by the TP transform procedures.

Thus, traditional DBMS support many of the mechanisms of the Clark-Wilson model. However, implementations based on standard SQL require some compromises. For example, the popular principle of distribution (granting) of access rights WITH GRANT OPTION (the recipient of transferred privileges is given the privilege to further transfer the received privileges, including the privilege to transfer privileges) contradicts the Clark-Wilson model (rule E4). Relevant for the DBMS also remain issues related to the mechanisms for monitoring the integrity of stored procedures, functions (as file objects). This necessitates additional research in the relevant areas.

In general, the absolute advantages of this model are its relative simplicity and ease of sharing with other security models.

РОЗДІЛ 2 ЗАХОДИ ПО ВИЯВЛЕННЮ ТА ІДЕНТИФІКАЦІЇ ЗАГРОЗ НА ОБ`ЄКТІ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

2.1 Види та категорії потенційних загроз

The Biba Model

The Biba model [13] was developed after the Bell–LaPadula model [14]. In terms of content and formal (mathematical) representation, this model is an inversion of the Bell-LaPadula mandate model, the problem of which is that it is designed to preserve confidentiality without guaranteeing data integrity.

The main elements of the Biba model:

- S – set of subjects;

- O is a set of objects, and *S* ∩ *O* = □

- □ LI = (*LI*,□□, ,□)– a lattice of integrity levels, for example:

LI = {*important* , *very important* , *crucial*}, where *important<very important<crucial*;

-RI = {modify , invoke, observe, execute} – set of access types, where modify – access

subject to modify an object (analogous to write access in the Bell-LaPadula model), invoke - access to the subject's appeal to the subject (for example, a software tool for accessing an object); observe - access of the subject to the object for reading (analogue of the read access in the model Bella - LaPadula), execute - access to execution;

- $B=\{b \subseteq S \times O \times RI\}$ – set of possible sets of current accesses in the system;
- $(i_s , i_o , i_c) \in I = LI^S \times LI^O \times LI^S$ - is a triple of functions (i_s , i_o , i_c) specifying: $i_s : S \rightarrow LI$ – the level of integrity of subjects; $i_o : O \rightarrow LI$ – object integrity level; $i_c : S \rightarrow LI$ – the current level of integrity of subjects, while for each $s \in S$ the condition $i_c (s) \leq i_s (s)$ is satisfied;

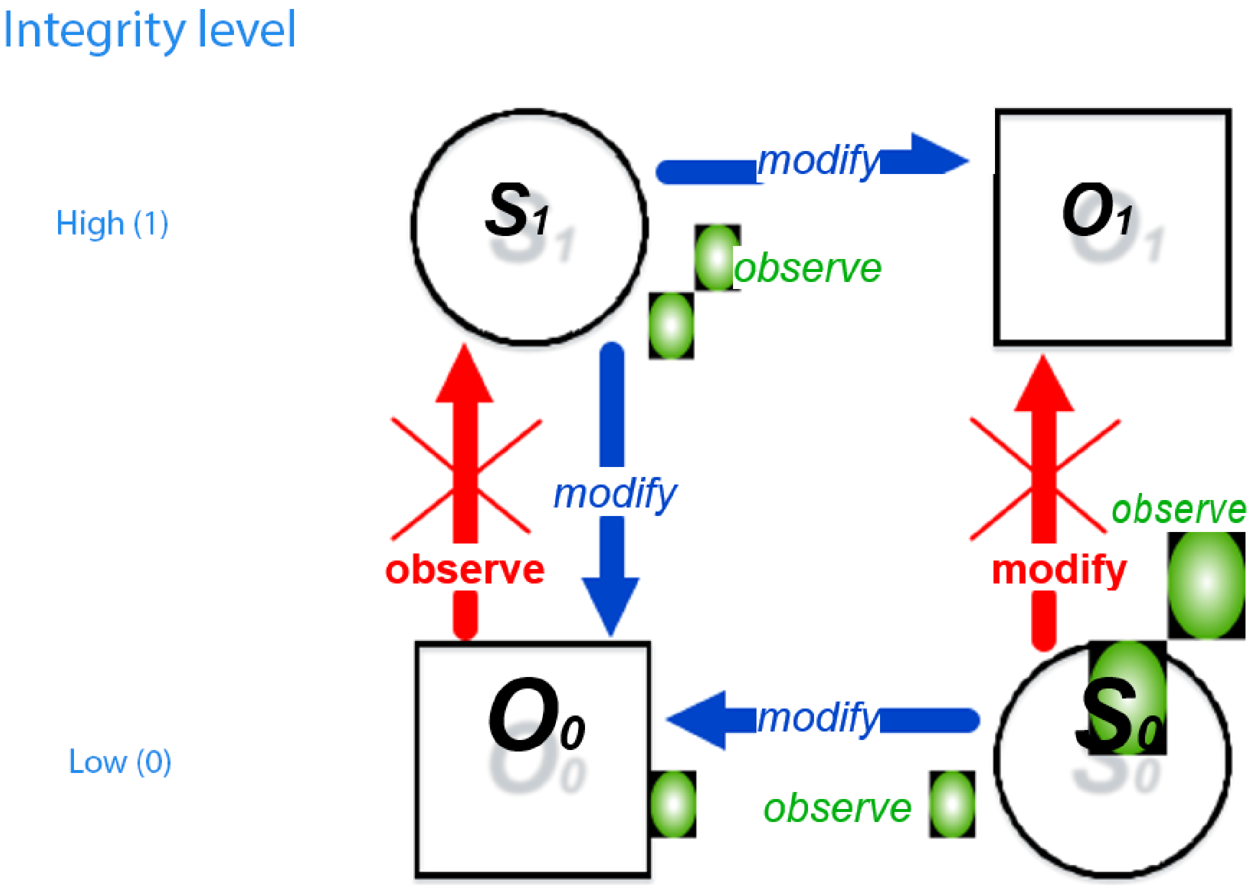
-$V = B \times I$ – set of system states.

The main properties or axioms of the Biba model (in accordance with the policy of strict integrity) can be formulated as follows:

1. The simple integrity property. The subject with the level of $i_s (s)$ can read the information contained in the object with the integrity level $i_o (o)$ if and only if the integrity level of the object io (o) prevails over the integrity level of the subject $i_s (s)$ ($i_s (s) \leq i_o (o)$); in other words, subject cannot read the object at a lower integrity level (the so-called no read-down (NRD) rule).
2. The * integrity property. A subject with an integrity level is (s) can modify the information contained in an object with an integrity level $i_o (o)$, if and only if the integrity level of the subject is (s) prevails over the integrity level of the object $i_o (o)$ ($i_o (o)$ □ $i_s (s)$); in other words, the subject cannot modify the object at a higher integrity level (the so-called no write-up (NWU) rule).
3. The invoke property indicates that subjects are allowed to invoke subjects of equal or lower level only, that is, for $\forall$ s[1], s[2] $\in$ S , s[1] can call s[2] only when i_s (s[2]) □ i_s (s[1]).

The first two properties of this model are the inverse of the two corresponding properties of the Bell-LaPadula model. Namely, the NRD rule is the exact opposite of the NRU rule of the Bell-LaPadula model, except that the Biba model uses integrity levels, and not security (confidentiality) levels, as in the Bell-LaPadula model. The NWU rule of Biba's mandated integrity model is the exact opposite of the NWD rule of the Bell-LaPadula model for the case of integrity levels rather than security.

The diagram of information flows corresponding to the Biba model in a system with two levels of integrity can be represented as follows (Pic. 2).



Pic. 2. Diagram of information flows in a system with two levels of integrity

Many criticize Biba 's model for using integrity as a measure, calling into question the legitimacy of displaying the data property "integrity" as a discretely ordered set. Indeed, in most applications, data integrity is viewed as a property (binary attribute) that is either preserved or not. Then the introduction of hierarchical levels of integrity may seem redundant. However, if integrity levels in the Biba model are considered as levels of reliability/correctness (various syntactic, semantic errors can affect the correctness of the program code in different ways, causing, for example, errors or warnings, and the corresponding information flows - as the transfer of information from a more reliable set of data to a less reliable one and vice versa, then the Biba model is a completely adequate algebraic structure.

Since the formal description of the Biba model is very close to the description of the Bell-LaPadula model, it naturally has most of the advantages and disadvantages inherent in this model.

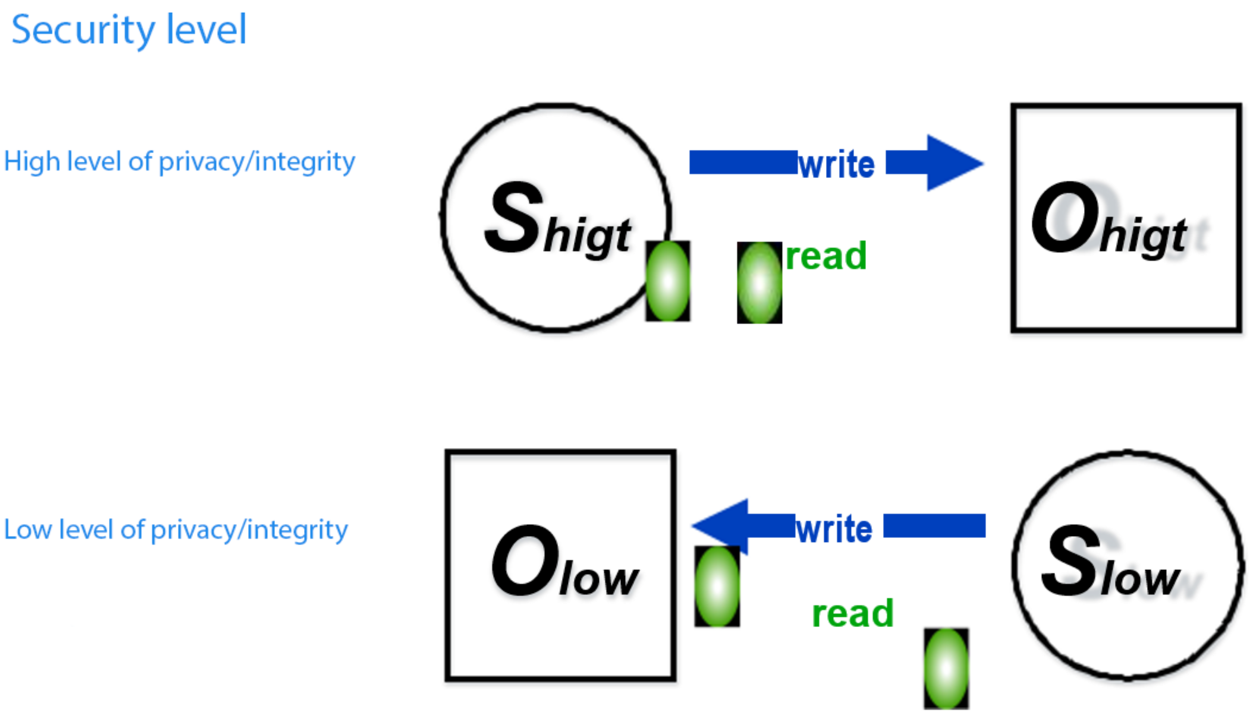
In real IS, there are rarely security systems focused solely on ensuring confidentiality or solely on ensuring the integrity of information. When building secure systems, many would like to combine both mechanisms, using various formal security models, including such as the Bell-LaPadula and Biba models. This is not an easy task. Possible options for the joint use of the Bell-LaPadula and Biba models and the complications that arise in this case are given below [3, 15, 16]:

1. Two models can be implemented in the system independently of each other. In this case, subjects S and objects O are independently assigned privacy levels and integrity levels based on two different grids. The decision on access security is made simultaneously according to the rules of both models.

It is easy to see that with this approach to organizing access, unsolvable situations are possible, for example, when according to the rules of the Bell-LaPadula model, access can be allowed, but not according to the rules of the Biba model, or vice versa.

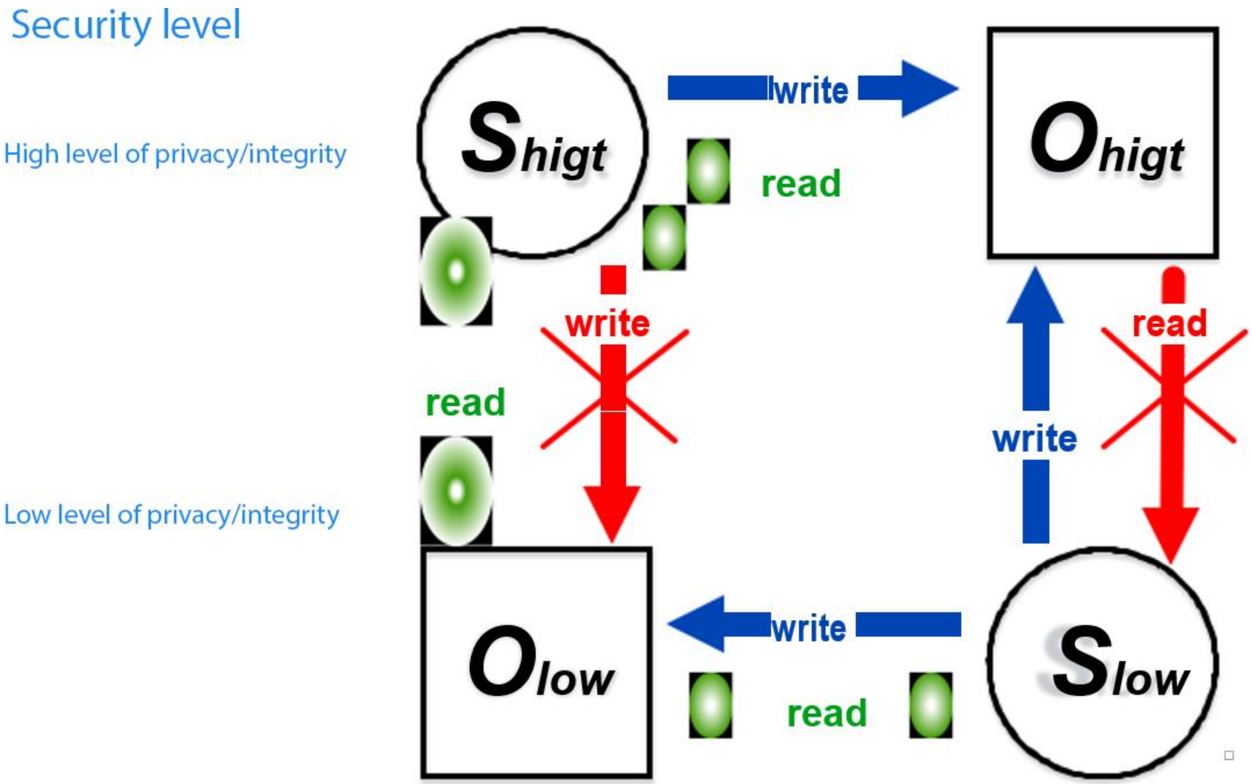
2. Logical combination of models based on one common grid of security levels (confidentiality/integrity).

In such systems, only accesses of subjects to objects within the same security level are allowed (Pic. 3).


Security level
High level of privacy/integrity
Shigt
write
read
Ohigt
Low level of privacy/integrity
Olow
write
read
Slow

Pic. 3. Joint use of the Bell-LaPadula and Biba models (access within the same security level)

3. Logical combination of models based on one common lattice, but with two security labels: confidentiality and integrity with the opposite nature of their definition. Subjects and objects with high confidentiality requirements (for example, secret data and users trusted by secrets) are located at high levels of the lattice hierarchy. Subjects and objects with high integrity requirements (for example, system software and programmers) are located at the lower levels of the lattice hierarchy (Pic. 4).



Pic. 4. Joint use of the Bell-LaPadula and Biba models (based on a single lattice with two security labels)

Despite the complexity of classifying subjects and objects of access, it is the third option that is used in modern ISs, in particular in DBMS, where a mandatory security policy is implemented [3].

Since subjects and objects with high integrity are at the bottom of the hierarchy, and components with low integrity are at the top of the hierarchy, the no read up and no write down rules mimic Biba 's mandated integrity model in the Bell-LaPadula model structure. That is, reading from the top in the hierarchy of the Bell–LaPadula model is reading from the bottom in the hierarchy of the Biba model. Similarly, the up entry in the Bell–LaPadula model is writing down in the Biba model. In practice, this allows, by placing system files (O objects), including those related to the DBMS, and administrator subjects (their processes) in the lower part of the Bell-LaPadula model hierarchy, to protect the integrity of such objects from ordinary subjects -

users (and their processes) because the no write down rule prevents them from writing to system files. In addition, if we consider execution as reading, then administrative subjects (and their processes) will not be able to execute programs outside the highest level of integrity (or the lower level of the Bell-LaPadula model hierarchy).

This scheme protects system files from Trojan horse malware because if such malware is in one of the upper levels, it will never be able to corrupt system files due to the need to execute the no write down rule. Thus, such a combination of models provides security protection for the upper levels of a certain hierarchy and integrity protection for the lower levels [16].

In conclusion, it is worth noting that the existing theoretical developments and practical implementations of IS security are based not only on the paradigm of formal security policy modeling, but also on another equally important paradigm - cryptography, aimed at solving certain problems. Moreover, these approaches, different in origin and tasks to be solved, complement each other: cryptography offers relevant methods and primitives for protecting information, providing identification, authentication, encryption, data integrity control, and formal security models provide developers of secure IP with fundamental general principles that underlie the architecture of a secure system and determine the concept of its construction [17].

It seems appropriate to conduct further research, the result of which would be some methodology for the integrated use of various security models in the design and operation of the corresponding IS and their main functional component - the database, leading to an increase in the effectiveness of their protection.

2.2 Методи виявлення загроз

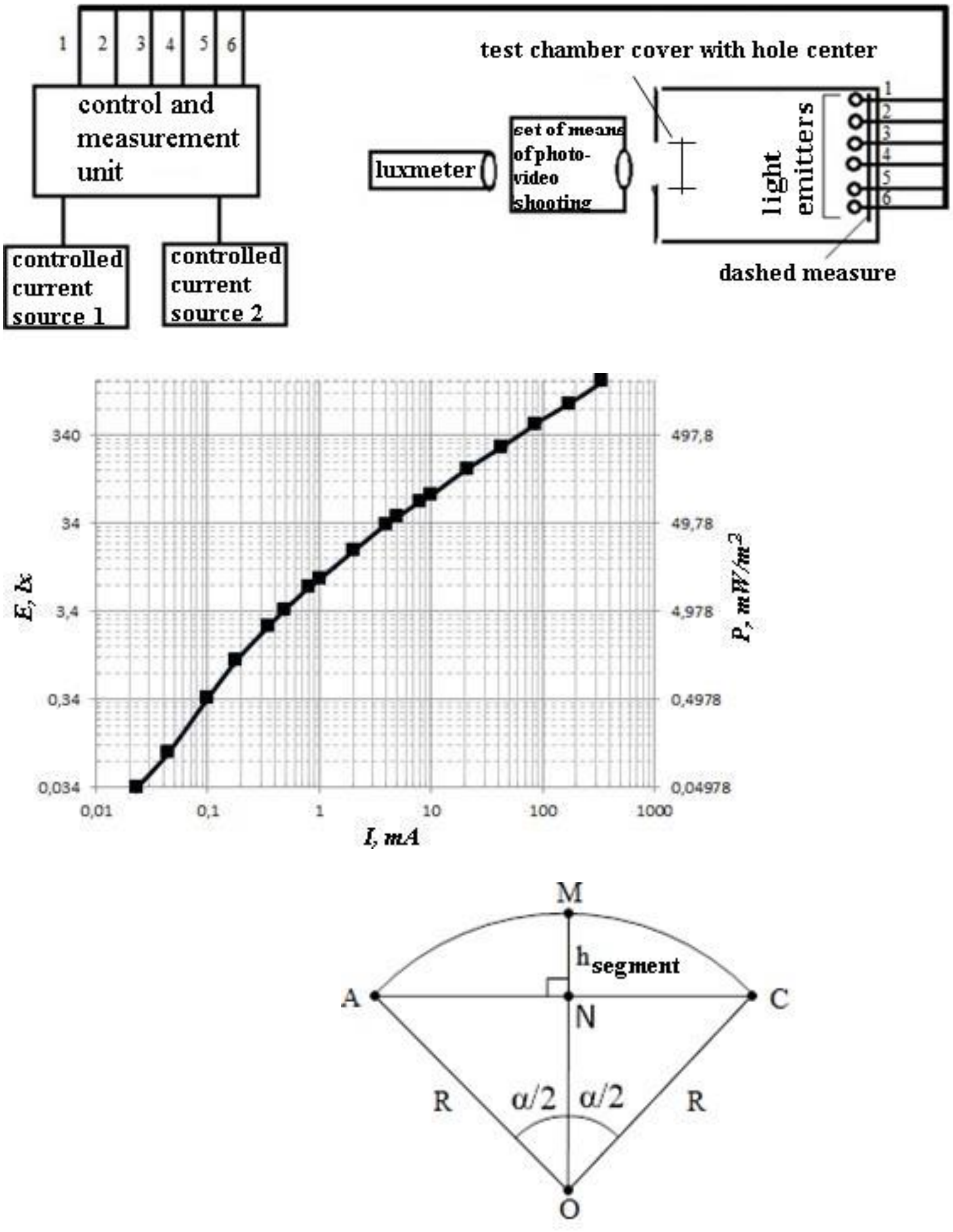


Fig. 3. Graphic explanation of the calculation

The magnitude of the power flux density (P) falling on the test chamber cover can be defined as

$$\mathrm{P} = \frac{P}{S_{ss}}$$

where S_{ss} – area of the spherical segment, the spherical surface, the cross section of which corresponds to the AMS curve (Fig. 3).

By definition

$$S_{ss} = 2\pi R \cdot h_{segment} \tag{2}$$

where R – radius of the sphere, AO = MO = CO = R (Fig. 3); $h_{segment}$ – height of the ball segment, MN = $h_{segment,}$

$$h_{segment} = MO - NO.$$

From the calculation of the triangle ANO we have

$$h_{segment} = MO - AO \cdot cos\frac{a}{2}$$

Since MO = AO = R, then:

$$h_{segment} = R - R \cdot cos\frac{a}{2},$$

$$h_{segment} = R \cdot (1 - cos\frac{a}{2}) \tag{3}$$

Substituting formula (3) into formula (2), we obtain

$$S_{ss} = 2\pi R^2 \cdot \left(1 - \cos\left(\frac{a}{2}\right)\right)$$

Therefore, the expression for calculating the power flux density P of IE emitters - band will look like

$$\mathrm{P} = \frac{P}{2\pi R^2 \cdot \left(1 - \cos\left(\frac{a}{2}\right)\right)}, [\mathrm{W/m^2}] .$$

Note: at α = 360 deg. **P** takes the form of a well-known expression for calculating the power flux density generated by an isotropic emitter: $\mathrm{P} = \frac{P}{2\pi R^2}$,[W/m^2].

Formula (1) is used to calculate the P emitters of the visible range:

$$\mathrm{P}_{oscill}(\lambda) = E_{\upsilon} \cdot \frac{1}{V(\lambda)} \cdot \frac{1}{683} = \frac{\mathrm{F}}{2\pi R^2 \cdot \left(1 - \cos\left(\frac{a}{2}\right)\right)} \cdot \frac{1}{V(\lambda)} \cdot \frac{1}{683}, [\mathrm{W/m^2}]$$

where E_v *=F/S, F* – nominal value of the intensity of the emitted light, which is known from the technical description of LEDs (Luminous Intensity); α – value of the angle at which 50% of the light energy emitted by the LED (50% Power Angle, from the technical description of LEDs);

To construct the spectral sensitivity curve, a coefficient C was determined, which is equal to the ratio of the power flux density of the reference LED with equivalent brightness, which was determined from the graph obtained in the previous step (Fig. 1) to the power flux density of the test LED.

The dependence of the coefficient C on the length and is the spectral sensitivity.

During the experiment, the spectral sensitivity of the above means of photographic intelligence and video recording was determined. The obtained results were averaged and depicted in the form of graphs, fig. 4.

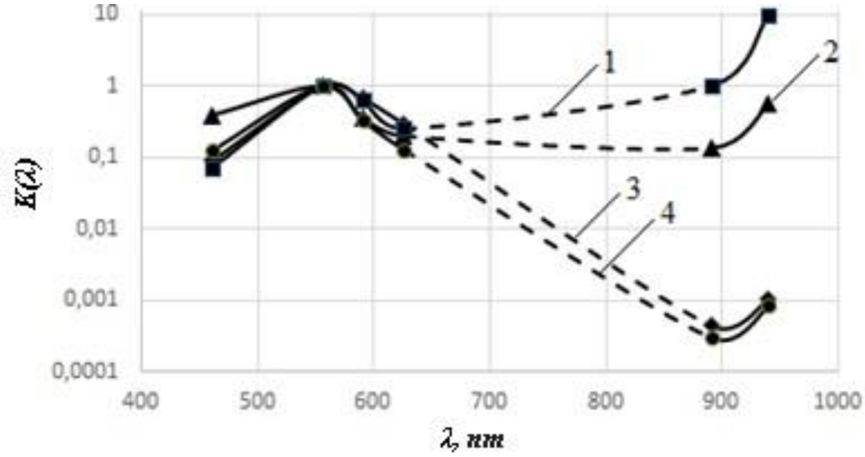


Fig. 4. Graphs of the averaged spectral sensitivity of the studied means of photographic intelligence and video: 1 – night video surveillance cameras; 2 – car DVR; 3 – mobile phone camera; 4 – digital camera

2.3 Мета дійсних загроз: контроль доступу, ліквідація та наслідки

Experimental study of the effectiveness of countering the means of photography and video by IE – illumination

After determining the spectral sensitivity of the selected receivers, an experimental study of the effectiveness of the response by the studied method was performed by determining the effective radius of the illumination spot, which creates an infrared LED.

The measurement technique involves the use of the described measuring device and a green LED. The installation is located on the surface horizontally, in front of it is the camera under study, the test field is illuminated by an artificial light source, and the ammeter is connected to a green LED.

A dashed measure with a hole in the center for the LED was prepared as a test field for measurements (Fig. 5). It is an image of lines in the form of white and black circles of different diameters, which are united by sectors. The measure step (total width of white and black lines) is 50 mm, the thickness of all lines within the sector is the same. There are 8 sectors with a line thickness: 0.5; 1; 2; 3; 4; 5; 6; 7 mm. Measurements were performed indoors without access to daylight. Canon EOS 1100D SLR Camera Selected as Test Photographic Intelligence Test Tool.

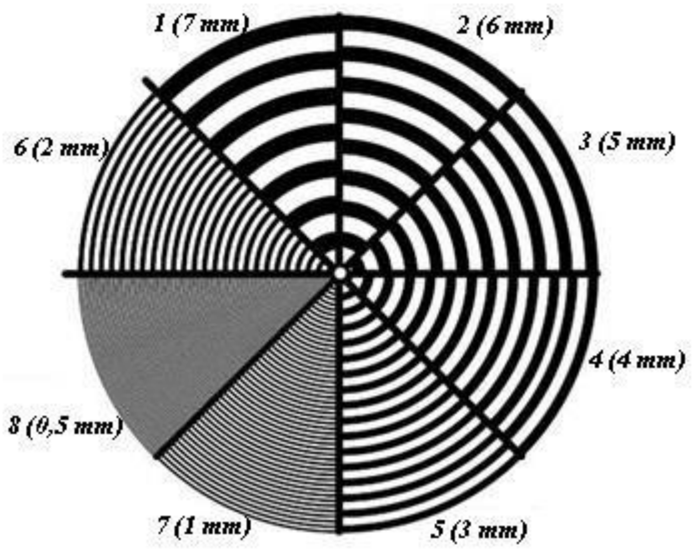


Fig. 5. Dashing measure for experimental determination of the effective radius of the illumination spot

The bar measure was placed in the test chamber of the installation so that the reference LED coincided with its center. The test camera was located at a certain distance from the test chamber, after which a series of photographs of the test field was taken with a gradual increase in the supply current of the LED to the maximum value. The images were then processed in Photoshop, which determined the radius of the spotlight in pixels, within which the camera's resolution is greater than the nominal, then recalculated to a linear measure (cm) (ie the radius of the spot created by green LED radiation and which lubricates the image of the strokes of the initially selected sector and does not allow to recognize them in the image as separate elements). The recalculation of the radius of the illumination spot was carried out according to the formulas:

$$R_{s.cm} = R_{s.rel} \cdot R_{m.cm},$$

where $R_{s.cm}$ – the magnitude of the radius of the spot of illumination, in centimeters; $R_{s.rel}$ – the radius of the illumination spot is expressed in relative magnitude; $R_{m.cm}$ – radius of the test field, in centimeters;

$$R_{s.rel} = R_{s.p.}/R_{m.p.},$$

where $R_{s.p.}$ – radius of the spot of illumination, in pixels; $R_{m.p.}$– radius of measure, in pixels.

The contrast of the test field was also determined for each value of the spot radius (and the corresponding supply current)

$$\mathrm{C} = \frac{E_i}{E_{t.f.}},$$

where E_i – total illuminance of the test field, measured by a luxmeter; $E_{t.f.}$ – initial (before turning off the green LED) illumination of the test field.

Based on the obtained results, a graph of the dependence of the effective radius of the illumination spot on the contrast is constructed (Fig. 6).

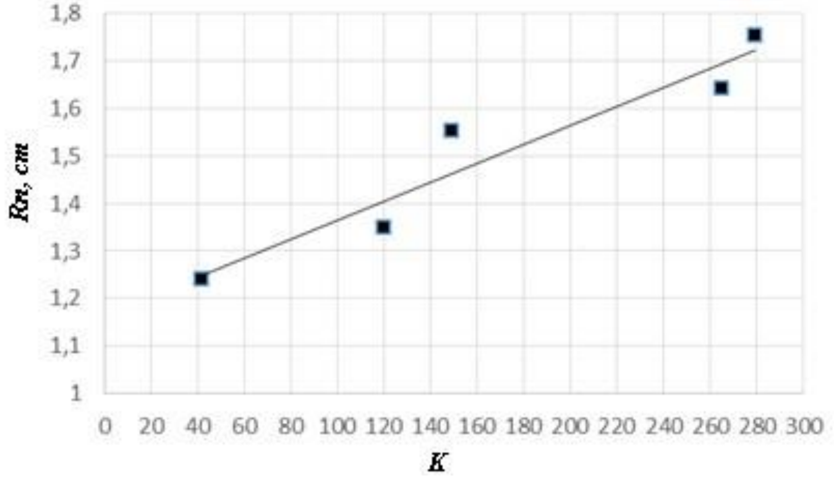


Fig. 6. Graph of the dependence of the effective radius of the spotlight on the contrast

Based on the results of the experiments, the required power of infrared LED emitters for counteraction (despair) of the studied Canon EOS 1100D camera was estimated. To do this, assume that the IE emitter must create a spot of illumination of the maximum radius provided by the green LED at the maximum supply current (see Fig. 6, R_s=17,5 cm). The required LED power values were found for different lighting conditions of the object (day, dusk, office space). It was assumed that the sensitivity of the receivers to IE light and visible ranges is the same, the wave front is flat, the power flux density does not depend on the distance, and the test field reflects all the incident light in the direction of the camera. The illumination area was calculated over a radius R.

From the technical description of the LEDs it is known that the radiated power of the green LED is 1 W, the maximum supply current of 340 mA, while emitting the power flux density P = 2,043 W/m^2 (see formula (1)).

The next step was to estimate the value of the electric power of the infrared emitter with a wavelength λ = 940 nm, which creates a power flux density, the same as that used in the experiment green LED (2,043 W/m^2).

According to the technical description of the LEDs, ie the known values of rated current I and voltage U on the LED, you can calculate the electric power of this IE - emitter:

$$P_{IE} = I \cdot U \text{ [W]}.$$

After substitution of numerical values it was received P_{IE} = 1,4 W, which corresponds to the power flux density IE light P = 1,59 W/m^2. To find electric power $P_{IE}{}^1$, at which it will radiate P = 2,043 W/m^2, assume that the value of P is proportional to the electrical power of the LED. Then, after calculating the proportion, we find the value $P_{IE}{}^1$= 1,8 W.

From the graph of the effective radius of the illumination spot on the contrast, it can be concluded that to provide a illumination spot with an area of 96 mm, the LED must create illumination that exceeds the illumination of the test field 279 times (C = 279, Fig. 6). The reflection coefficient of the test field ρ, which was determined before taking photographs of the test field, is 0.18. Using these values, we determined the value P_{dusk} – the power flux density of the counter emitter, which is necessary to illuminate the specified area at dusk (according to [4]E_v = 5 lx:

$$P_{dusk} = C \cdot \rho \cdot P_{f.t.}[\mathrm{W/m_2}],$$

where $P_{f.t.}$ – the flux density of light falling on the test field is calculated by formula (1) by value E_v and is equal to 7 mW/m^2;$\rho \cdot P_{f.t.}$– the power flux density reflected from the field under given lighting conditions.

2.5Наявність потенційних загроз в захисті об`єктів

3 At present there is a rapid progress in the creation of quantum computers to solve various computationally complex problems and for different purposes. At the same time special efforts are being made to create such a quantum computer that can solve the cryptanalysis problems of existing cryptosystems – asymmetric ciphers, key encapsulation protocols, electronic signatures. Prevention of such threats can be achieved by developing cryptographic systems that will be protected from both quantum and classical attacks, as well as be able to interact with existing protocols and communication networks. There is also a significant need for protection against attacks by third-party channels.

4 Currently, significant efforts of cryptologists are focused on the open competition NIST PQC. The main idea of the competition is to define mathematical methods on the basis of which standards for asymmetric cryptocurrencies can be developed, first of all electronic signature (ES), as well as asymmetric ciphers and key encapsulation protocols. Following the results of the second stage, the finalists of the third stage of the NIST PQC competition became three ES schemes - Crystals-Dilithium, Falcon and Rainbow. At present, a comprehensive analysis of the finalists is an important task for the entire crypto community. The vast majority of schemes that have become finalists are based on problems in the

theory of algebraic lattices. Special attention was also paid to the Rainbow ES scheme, which is based on multidimensional transformations.

5 The Rainbow EP scheme is significantly different from other NIST candidates because it is based on multidimensional transformations. It is a generalization of the structure of UOV that provides effective parameterization of the EP algorithm due to the additional algebraic structure. Rainbow's theoretical safety is based on the fact that solving a set of random multidimensional quadratic systems is an NP-complex problem. The authors of the Rainbow method claim to have achieved the EUF-CMA security model based on the use of a hash structure with a random or pseudo-random session key (salt). Very small EPs are also offered, literally only a few hundred bits (only 528 bits (66 bytes) for NIST security level I). Compared to other NIST candidates for the ES post-quantum scheme, they are much shorter. In addition, because Rainbow uses only simple operations on small finite fields, the processes of creating and verifying the signature are extremely effective [6]. In addition, the range of Rainbow parameters allows you to optimize their application in a wide range of cases. The Rainbow EP scheme has also been studied in other contexts and has some advantages, including, for example, in low-resource applications

6 It is shown that in order to guarantee the cryptographic stability of Rainbow EP, it is necessary to substantiate the requirements and build sets of system-wide parameters that provide resistance to classical and quantum attacks. In determining the requirements for the system parameters of the Rainbow NIST scheme, the competition focused on system-wide parameters that will provide 256 bits of resistance against classical and up to 128 bits against quantum cryptanalysis. These limitations, in our opinion, are due in part to the complexity of calculating system-wide parameters, as well as the significant impact of increasing them on the speed of electronic signatures. However, given the current

application of symmetric cryptocurrencies at the 512-bit stability level, we believe that it is already necessary to consider and implement on the basis of the Rainbow circuit ES with a resistance of up to 512 bits. But for this it is necessary to substantiate the basic provisions and requirements for the system-wide parameters of such lengths, as well as to build them directly. At the same time, cryptographic resistance to classical and quantum attacks of the corresponding values, as well as protection against attacks by third-party channels must be provided.

7 The purpose of this article is a preliminary analysis of existing attacks on promising electronic signature Rainbow, defining requirements for system-wide parameters to ensure cryptographic stability including at least 512 bits against classical and 256 bits against quantum cryptanalysis, as well as development and practical implementation of Rainbow algorithms 512 bits against classical and 256 bits against quantum cryptanalysis.

РОЗДІЛ 3 ДІЇ СТОРІН ПРИ РЕАЛІЗАЦІЇ ЗАГРОЗ

3.1. Структура комунікацій при загрозах

4. Let’s consider the main components of Rainbow transformations - generating system-wide parameters and cryptotransformations directly. The Rainbow ES scheme is based on multidimensional transformations. For multidimensional public key schemes, the public key is defined by a set of nonlinear multidimensional polynomials over a finite field. In general, the key of a multidimensional public key cryptosystem is a system of multidimensional quadratic polynomials with n variables and m equations:

5.

6. $$\begin{aligned} p^{(1)}(x_1,\dots,x_n) &= \sum_{i=1}^{n}\sum_{j=1}^{n} p_{ij}^{(1)}\cdot x_i x_j + \sum_{i=1}^{n} p_i^{(1)}\cdot x_i + p_0^{(1)} \\ p^{(2)}(x_1,\dots,x_n) &= \sum_{i=1}^{n}\sum_{j=1}^{n} p_{ij}^{(2)}\cdot x_i x_j + \sum_{i=1}^{n} p_i^{(2)}\cdot x_i + p_0^{(2)} \\ &\vdots \\ p^{(m)}(x_1,\dots,x_n) &= \sum_{i=1}^{n}\sum_{j=1}^{n} p_{ij}^{(m)}\cdot x_i x_j + \sum_{i=1}^{n} p_i^{(m)}\cdot x_i + p_0^{(m)} \end{aligned} \qquad (1)$$

7.

8. All coefficients and variables come from a F_q finite field with q elements. Essentially, a set of well-known polynomials

9. $$\mathrm{P}\,(x_1,\dots,x_n) = \left(p^{(1)}(x_1,\dots,x_n),\dots,p^{(m)}(x_1,\dots,x_n)\right) \qquad (2)$$

10. mathematically represents a representation F_q^n to F_q^m The message encryption or signature verification operations are to be simply evaluated $\mathrm{P}(x_1,\dots,x_n)$ using the public key. The process of decrypting encrypted text, as well as the development of EP is reduced to the implementation of the "inversion" of the representation $\mathrm{P}(x_1,\dots,x_n)$ using a secret (private) key. These components are equivalent to solving the problem of stability of MQ-transformation. The ES Rainbow scheme with u levels can be described as follows. Let F_q be a finite field with q elements, and $\upsilon_1 < \upsilon_2 < \cdots < \upsilon_u < \upsilon_{u+1} = n$ - integers. We choose $V_i = \{1,\dots,\upsilon_i\}$, $o_i = \upsilon_{i+1} - \upsilon_i$ and $O_i = \{\upsilon_i,\dots,\upsilon_{i+1}\}$, where $(i=1,\dots,u)$, so we get $|V_i| = \upsilon_i$ i $|O_i| = o_i$, where $(i=1,\dots,u)$.

11. The central display of F Rainbow consists of $m = n - \upsilon_1$ multidimensional quadratic polynomials $f^{(\upsilon_1+1)},\dots,f^{(n)}$ that look loke:

12.

13. $$f^{(k)}(\mathbf{x}) = \sum_{i,j\in V_\ell} \alpha_{ij}^{(k)} x_i x_j + \sum_{i\in V_\ell ,\, j\in O_\ell} \beta_{ij}^{(k)} x_i x_j + \sum_{i\in V_\ell \cup O_\ell} \gamma_i^{(k)} x_i + \eta^{(k)}, \qquad (3)$$

14.

15. Where $\ell \in \{1,\ldots,u\}$ - is a single integer such that $k \in O_\ell$.

16. Note that in each polynomial $f^{(k)}$ with $k \in O_\ell$ no square term $x_i x_j$, where I and j are in O_ℓ This fact was used by the authors to develop the ES. Such polynomials were called Oil-Vinegar polynomials when OV schemes were proposed.

17. To hide the structure F in the public key, it is composed of two inverse affine or linear mappings: $\mathrm{S} : \mathrm{F}^m \to \mathrm{F}^m$ та $\mathrm{T} : \mathrm{F}^n \to \mathrm{F}^n$. Therefore, the Rainbow public key has the form: n m $\mathrm{P} = \mathrm{S} \circ \mathrm{F} \circ \mathrm{T} : \mathrm{F}^n \to \mathrm{F}^m$, the secret key consists of three mappings, S, F and T and therefore allows you to invert the public key mappings

18. The following three steps are required to perform the EP for the message $\mathbf{w} \in \mathrm{F}^m$

19. 1. Calculate $\mathbf{x} = \mathrm{S}^{-1}(\mathbf{w}) \in \mathrm{F}^m$.

20. 2. Calculate previous display y with x below the central display F using the inversion algorithm, ie $\mathbf{y} = \mathrm{F}^{-1}(\mathbf{x}) \in \mathrm{F}^n$

21. 3. Calculate the signature $\mathbf{z} \in \mathrm{F}^n$, $\mathbf{z} = \mathrm{T}^{-1}(\mathbf{y})$.

22. To confirm that $\mathbf{z} \in \mathrm{F}^n$ is a valid signature for the message $\mathbf{w} \in \mathrm{F}^m$, you must calculate $\mathbf{w}' = \mathrm{P}(\mathbf{z})$. If $\mathbf{w}' = \mathbf{w}$ is satisfied, the signature is valid. Process of signature generation and verification is shown in Fig. 1.

23. Signature generation

$$\begin{tikzcd}
\mathbf{w} \in \mathrm{F}^m \arrow[r, "\mathrm{S}^{-1}"] & \mathbf{x} \in \mathrm{F}^m \arrow[r, "\mathrm{F}^{-1}"] & \mathbf{y} \in \mathrm{F}^n \arrow[r, "\mathrm{T}^{-1}"] & \mathbf{z} \in \mathrm{F}^n \arrow[lll, bend left, "\mathrm{P}"]
\end{tikzcd}$$

24.

25. Signature verification

26. Fig. 1. Rainbow signature generation and verification process

3.2. Початкові умови та наявність інформації сторонніми особами дані

4. Below are a number of attacks on the EP scheme Rainbow, namely direct attack, MinRank attack and HighRank, the UOV attack and the Rainbow Band Separation (RBS) attack.

5. Although direct and brute force attacks are signature forgery attacks that must be performed for each message separately, RBS and UOV attacks are key recovery attacks. After recovering the Rainbow secret key with one of these attacks, the cryptanalyst can generate signatures just like a legitimate user.

6. 2.1. Direct algebraic attacks are the most straightforward attacks on the multidimensional Rainbow scheme is the direct algebraic attack, in which the well-known equation $\mathrm{P}(\mathbf{z}) = \mathbf{h}$ is considered as a problem MQ. Since Rainbow is an indefinite system with n m $n \approx 1.5 \cdot m$ equations, the most effective way to solve this system is to fix n – m variables to create a deterministic system. We can expect that the resulting deterministic system has exactly one solution. In some cases, even better results are obtained when guessing additional variables before solving the system (hybrid approach). The complexity of solving such a system of m quadratic equations in m variables can be estimated using equation (4):

7. $$\text{Complexity}_{\text{direct;classical}} = \min_k \left(q^k \cdot 3 \cdot \binom{m-k+d_{reg}}{d_{reg}}^2 \cdot \binom{m-k}{2} \right) \quad (4)$$

8. multiplications in the field, where d_{reg} is the so-called degree of regularity of the system.
9. The degree of regularity of the system can be estimated as the smallest integer *d* for which the coefficient t^d in
10. $$\frac{\left(1-t^2\right)^m}{\left(1-t\right)^{m-k}} \qquad (5)$$
11. is not positive.
12. In the presence of quantum computers, the additional step of guessing the hybrid approach can be accelerated by Grover's algorithm. Using this approach, it is possible to estimate the complexity of a quantum direct attack as follows.
13. $$\text{Complexity}_{\text{direct;quantum}} = \min_k \left(q^{k/2} \cdot 3 \cdot \binom{m-k+d_{reg}}{d_{reg}}^2 \cdot \binom{m-k}{2} \right) \qquad (6)$$
14. multiplications in the field
15. 2.2. MinRank attack
16. During the MinRank attack, the cryptanalyst tries to find a linear combination of well-known polynomials of minimal rank. In the case of Rainbow, such a linear combination of rank v_2 corresponds to a linear combination of central polynomials of the first level. Thus, finding o_1 of these low-ranking linear combinations, we can identify the central polynomials of the first level and recover the equivalent secret key Rainbow.
17. To date, the most effective method of solving the MinRank problem has been proposed in. In this embodiment, the decomposition of a low-ranking Q matrix is considered on $Q = S \cdot C$, where S is $n \times r$ and C - $r \times n$ of the matrix

representing the row space of the matrix Q. The matrix is determined $C'_j = \begin{pmatrix} r_j \\ C \end{pmatrix}$ and are taken as zero r+1 minors of these C_j matrices.

18. Since the resulting system has many more equations than variables, we can solve it by linearization using the Wiedemann algorithm.
19. In particular, the number of equations in the system is given as $m \cdot \begin{pmatrix} n \\ r+1 \end{pmatrix}$, where $\begin{pmatrix} n \\ r+1 \end{pmatrix}$ this is the number of r+1 minors of the C'_j matrix. The number of variables in the system is equal to $(o_2+1)\cdot\begin{pmatrix} n \\ r \end{pmatrix}$ So if inequation
20. $$(o_2+1)\cdot\begin{pmatrix} n \\ r+1 \end{pmatrix} \geq (o_2+1)\cdot\begin{pmatrix} n \\ r \end{pmatrix} - 1 \qquad (7)$$
21. is true then it is possible to solve the system using the Wiedemann algorithm. Therefore, the complexity of solving this system is given as
22. $$\text{Complexity}_{\text{MinRank}} = 3\cdot\left(\left((o_2+1)\cdot\begin{pmatrix} n' \\ r \end{pmatrix}\right)^2 \cdot (r+1)\cdot(o_2+1)\right). \qquad (8)$$
23. Careful analysis has shown that it is not necessary to consider all n rows of the C'_j matrix to be able to solve the system. The number n' in (8) denotes the smallest number for which inequality (7) holds.

3.3. Дослідження та виявлення загроз: наявність інформації по кожній загрозі

During the MinRank attack, the cryptanalyst tries to find a linear combination of well-known polynomials of minimal rank. In the case of Rainbow, such a linear combination of rank υ_2 corresponds to a linear combination of central polynomials of the first level. Thus, finding o_1 of these low-ranking linear combinations, we can identify the central polynomials of the first level and recover the equivalent secret key Rainbow.

To date, the most effective method of solving the MinRank problem has been proposed in. In this embodiment, the decomposition of a low-ranking Q matrix is considered on $Q = S \cdot C$, where S is $n \times r$ and C - $r \times n$ of the matrix representing the row space of the matrix Q. The matrix is determined $C'_j = \begin{pmatrix} r_j \\ C \end{pmatrix}$ and are taken as zero r+1 minors of these C_j matrices.

Since the resulting system has many more equations than variables, we can solve it by linearization using the Wiedemann algorithm.

In particular, the number of equations in the system is given as $m \cdot \binom{n}{r+1}$, where $\binom{n}{r+1}$ this is the number of r+1 minors of the C'_j matrix. The number of variables in the system is equal to $(o_2+1) \cdot \binom{n}{r}$ So if inequation

$$(o_2+1) \cdot \binom{n}{r+1} \geq (o_2+1) \cdot \binom{n}{r} - 1 \tag{7}$$

is true then it is possible to solve the system using the Wiedemann algorithm. Therefore, the complexity of solving this system is given as

$$\text{Complexity}_{\text{MinRank}} = 3 \cdot \left(\left((o_2+1) \cdot \binom{n'}{r} \right)^2 \cdot (r+1) \cdot (o_2+1) \right). \tag{8}$$

Careful analysis has shown that it is not necessary to consider all n rows of the C'_j matrix to be able to solve the system. The number n' in (8) denotes the smallest number for which inequality (7) holds.

2.3. HighRank attack

The purpose of the HighRank attack is to detect (in linear representation) the variables that appear the least number of times in the central polynomials (they correspond to the Oil variables of the last Rainbow level, ie variables x_i з $i \in O_u$).

The complexity of this attack can be assessed as

$$\text{Complexity}_{\text{HighRank; classical}} = q^{o_u} \cdot \frac{n^3}{6}. \tag{9}$$

With quantum computers, you can speed up the search with the Grover algorithm. So we get

$$\text{Complexity}_{\text{HighRank; quantum}} = q^{o_u/2} \cdot \frac{n^3}{6} \tag{10}$$

multiplications in the field.

2.4. UOV attack

Since Rainbow can be considered as a continuation of the well-known Oil and Vinegar signature scheme [5], it can be attacked using all known UOV attacks [11]. You can treat Rainbow as an instance of UOV with $\upsilon = \upsilon_1 + o_1$ and $o = o_2$ The purpose of this attack is a search for a preliminary mapping of the so-called Oil subspace O of the affine transformation T, where $\mathrm{O} = \left\{ \mathbf{x} \in \mathrm{F}^n : x_1 = \cdots = x_\upsilon = 0 \right\}$.

Finding this space allows you to separate Oil from Vinegar variables and restore the private key.

The complexity of this attack can be assessed as

$$\text{Complexity}_{\text{UOV-Attack; classical}} = q^{n-2o_2-1} \cdot o_2^4 \qquad (11)$$

multiplications in the field. Using Grover's algorithm, this complexity can be reduced to

$$\text{Complexity}_{\text{UOV-Attack; quantum}} = q^{\frac{n-2o_2-1}{2}} \cdot o_2^4 \qquad (12)$$

multiplications in the field

2.5. RBS attack

The RBS attack is aimed at finding linear mappings S and T that convert well-known polynomials into polynomials of the Rainbow form. (ie values $\text{Oil} \times \text{Oil}$ must be zero) To do this, the cryptanalyst must solve several nonlinear multidimensional systems. The complexity of this step is determined by the complexity of solving the first (and largest) of these systems, which consists of $n+m-1$ quadratic equations with n variables. However, polynomials in this system are not random quadratic polynomials, but there are two groups of variables X and Y such that the polynomials are bilinear in X and Y

In particular, we get two sets of variables X and Y in the size of $|X| = n_x = \upsilon_1 + o_1$ and $|Y| = n_y = o_2$. We have $m_x = x$ polynoms which are quadratic in variables X and $m_y = n-1$ equations are bilinear in variables X and Y. Therefore, the complexity of the RBS attack can be assessed as

$$Compl_{RBS} = \min_{\alpha,\beta} 3 \cdot \mathrm{M}_{\alpha,\beta}(t,s)^2 \cdot (n_x+1) \cdot (n_y+1), \qquad (13)$$

where $\mathrm{M}_{\alpha,\beta}$ means number of members (α,β).

1. Generation of parameters for 384, 512 bits of stability

This section provides the selection (generation) of parameters for 384 and 512 bits of stability over the GF field (256). The following conditions were followed when choosing the parameters:

- the number of equations we need depends on the complexity of the direct attack and the attack on the hash function;

- the number of variables depends on the complexity of RBS, UOV and HighRank attacks.

So, if we summarize the above, we find the parameters υ_1, o_1, o_2 with q=256, ie $GF(q) = GF(256)$ possible from conditions (4) - (13). Based on this, software was developed, which was used to generate parameters υ_1, o_1 and o_2 for ES Rainbow for 384 and 512 bits of security are given in table. 1.

Table 1.

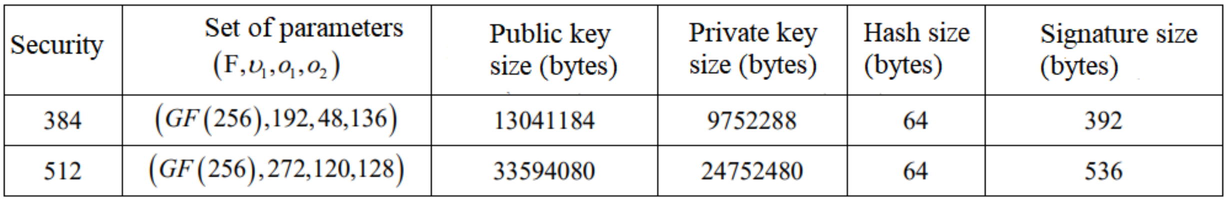
The main system-wide parameters of Rainbow for 384, 512 bits of security

Security	υ_1	o_1	o_2	$GF(q)$
384	192	48	136	$GF(256)$
512	272	120	128	$GF(256)$

With such parameters, we obtain the following sizes of keys, hashes and signatures for the three versions of Rainbow: Classic (Classic), cyclic (CZ-Rainbow), and compressed (Compressed), which are given in table. 2 - 4 respectively.

Table 2

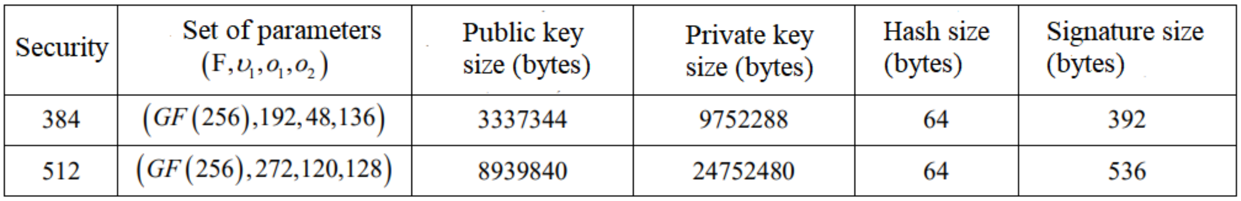
Classic Rainbow key and signature sizes



Security	Set of parameters $(\mathrm{F}, \upsilon_1, o_1, o_2)$	Public key size (bytes)	Private key size (bytes)	Hash size (bytes)	Signature size (bytes)
384	$(GF(256), 192, 48, 136)$	13041184	9752288	64	392
512	$(GF(256), 272, 120, 128)$	33594080	24752480	64	536

Table 3

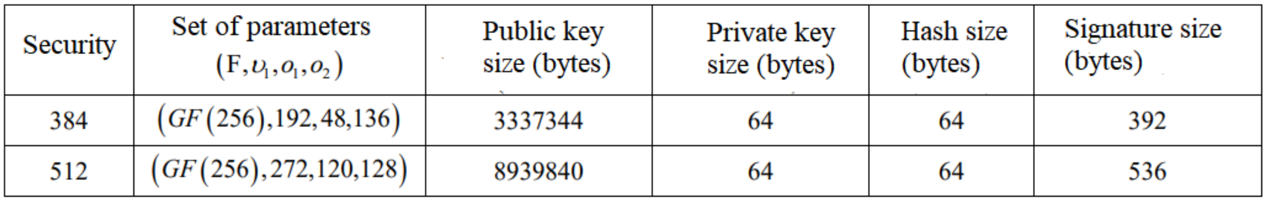
CZ-Rainbow key and signature sizes



Security	Set of parameters $(\mathrm{F}, \upsilon_1, o_1, o_2)$	Public key size (bytes)	Private key size (bytes)	Hash size (bytes)	Signature size (bytes)
384	$(GF(256), 192, 48, 136)$	3337344	9752288	64	392
512	$(GF(256), 272, 120, 128)$	8939840	24752480	64	536

Table 4

Sizes of keys and signatures Compressed Rainbow

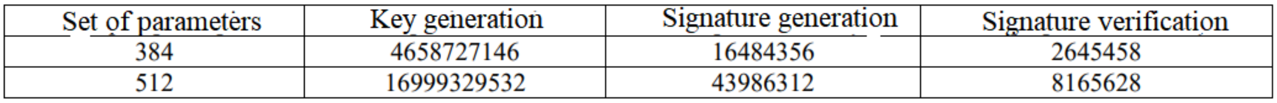


Security	Set of parameters $(\mathrm{F}, \upsilon_1, o_1, o_2)$	Public key size (bytes)	Private key size (bytes)	Hash size (bytes)	Signature size (bytes)
384	$(GF(256), 192, 48, 136)$	3337344	64	64	392
512	$(GF(256), 272, 120, 128)$	8939840	64	64	536

The performance at the specified parameters for the three versions of Rainbow, presented in CPU clock speed, is given in table. 5 - 7 respectively.

Table 5

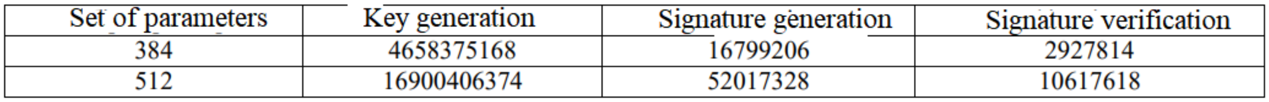
Speed Classic Rainbow



Set of parameters	Key generation	Signature generation	Signature verification
384	4658727146	16484356	2645458
512	16999329532	43986312	8165628

Table 6

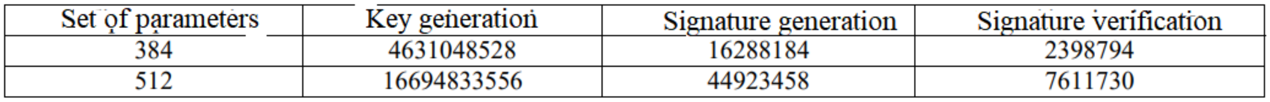
CZ-Rainbow performance



Set of parameters	Key generation	Signature generation	Signature verification
384	4658375168	16799206	2927814
512	16900406374	52017328	10617618

Table 7

Compressed Rainbow performance



Set of parameters	Key generation	Signature generation	Signature verification
384	4631048528	16288184	2398794
512	16694833556	44923458	7611730

Conclusions

1. One of the important problems of modern cryptography is the creation of standards for asymmetric cryptographic transformations of ES, which would be safe in the post-quantum period. The solution to this problem is carried out in the process of the international competition NIST USA, the task of which is to develop such a mechanism of the ES, which would be resistant to both quantum and classical attacks.

2. Crystal-Dilithium, Falcon and Rainbow became the finalists of the NIST USA competition for the ES scheme. The vast majority of schemes that have become finalists are based on problems in the theory of algebraic lattices. Special attention was also paid to the Rainbow electronic signature scheme, which is based on multidimensional transformations.

3. The Rainbow electronic signature scheme is significantly different from other NIST candidates because it is based on multidimensional transformations. It is a generalization of the UOV structure, which provides efficient parameterization due to additional algebraic structure. Rainbow's theoretical safety is based on the fact that solving a set of random multidimensional quadratic systems is an NP-difficult problem. The EUF-CMA security has been declared for the Rainbow project, which is achieved through the use of a hash structure with a random session key (salt).

4. The Rainbow ES process consists of simple operations of linear algebra, such as multiplying matrix vectors and solving linear systems over small finite fields. Also, Rainbow provides small, compared to other signatures, essentially only a few hundred bits.

5. The main disadvantage of Rainbow is the large size of public keys. Therefore, its use is recommended in systems where large public keys can be used. The dimensions of system-wide parameters and keys for the case of providing 384 and 512 security bits are given in table. 2 - 4.

6. Also from table. Figures 5 - 7 show that the verification process of CZ Rainbow EP is much slower than in the standard Rainbow scheme. However, it should be noted that this is due to the use of AES-based cryptographically secure PRNG provided by OpenSSL (which is the same as NIST) to create "fixed" parts of the public key. By using a faster streaming cipher or even generating a public key using the linear backscatter register (LFSR), this slowdown can be avoided almost completely.

7. A number of attacks on the Rainbow EP scheme were considered, namely direct attack, MinRank and HighRank attack, UOV attack and Rainbow Band Separation (RBS) attack. Although a direct attack is a signature forgery attack that must be performed for each message separately, MinRank, HighRank, UOV, and RBS attacks are key recovery attacks. After recovering the Rainbow secret key with one of these attacks, the cryptanalyst can generate signatures just like a legitimate user.

Substantiated and calculated system-wide parameters can be used to ensure increased security levels of the Rainbow EP up to and including 384 and 512 security bits, respectively, in accordance with the parameters justified in this article, namely: $\left(GF(256),192,48,136\right)$ and $\left(GF(256),272,120,128\right)$ in accordance.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. НВ БІЗНЄС (Грудень 20, 2021) Дійте так, ніби вас уже зламали. Захист бізнесу від кіберзагроз — експерт з кібербезпеки, (онлайн джерело), за посиланням: https://biz.nv.ua/ukr/bizinterview/kiberbezpeka-dlya-biznesu-v-ukrajini-poradi-eksperta-50202511.html

2. Нехай В.А (Лютий 24, 2017) ІНФОРМАЦІЙНА БЕЗПЕКА ЯК СКЛАДОВА ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВ (онлайн стаття), за посиланням: http://www.vestnik-econom.mgu.od.ua/journal/2017/24-2-2017/30.pdf

3. О. В. Криворучко (Листопад 27, 2020) КІБЕРГІГІЄНА. КІБЕРБЕЗПЕКА. БЕЗПЕКА ДЕРЖАВИ (онлайн стаття), за посиланням: https://knute.edu.ua/file/MjExMzA=/d8e24930571c0d91476be247343bb902.pdf

4. Віннікова І.І., Марчук С.В. (Червень 07, 2019) КІБЕР-РИЗИКИ ЯК ОДИН ІЗ ВИДІВ СУЧАСНИХ РИЗИКІВ У ДІЯЛЬНОСТІ МАЛОГО ТА СЕРЕДНЬОГО БІЗНЕСУ ТА УПРАВЛІННЯ НИМИ (онлайн стаття), за посиланням: https://chmnu.edu.ua/wp-content/uploads/2019/07/Vinnikova-I.I.-Marchuk-S.V..pdf

5. Телесфера (Вересень 25,2020) Кібербезпека: як захистити підприємство в епоху Індустрії X.0 (онлайн джерело), за посиланням: http://www.telesphera.net/blog/kiberbezpeka-indystrii-x-0.html

6. Лисенко І.А. (Серпень 29, 2018) Основи управління кібербезпекою (онлайн джерело), за посиланням: http://dspace.kntu.kr.ua/jspui/bitstream/123456789/8431/1/Osn_ypr_kiber.pdf

7.Василішин С. (2021) УДОСКОНАЛЕННЯ ВАЖЕЛІВ УПРАВЛІННЯ ДІДЖИТАЛІЗАЦІЙНИМИ РИЗИКАМИ ЕКОНОМІЧНОЇ БЕЗПЕКИ ТА ФОРМУВАННЯ КІБЕРБЕЗПЕКИ ОБЛІКОВОЇ СИСТЕМИ (онлайн стаття), за посиланнм: http://dspace.wunu.edu.ua/bitstream/316497/42062/1/%D0%92%D0%B0%D1%81%D0%B8%D0%BB%D1%96%D1%88%D0%B8%D0%BD.pdf

8.Гулак Г.М. (2020) МЕТОДОЛОГІЯ ЗАХИСТУ ІНФОРМАЦІЇ. АСПЕКТИ КІБЕРБЕЗПЕКИ (онлайн стаття), за посиланням: http://www.immsp.kiev.ua/postgraduate/Biblioteka_trudy/Gulak_MetodolZahystuInfOsnKiberbezp_2020.pdf

9. НКЦК (2021) Нормативно-правовий та організаційний аспекти забезпечення міжнародної кібербезпеки (онлайн стаття), за посиланням: https://www.rnbo.gov.ua/files/%D0%9D%D0%9A%D0%A6%D0%9A/28072021/Bulltn_NCK_2.pdf

10.Довгань О. (2018) КІБЕРБЕЗПЕКА ВІНФОРМАЦІЙНОМУСУСПІЛЬСТВІ (онлайн стаття), за посиланням: http://ippi.org.ua/sites/default/files/bezpeka_2018-6.pdf

11.Підгайна Є. (Липень 20, 2018) Галузі майбутнього: що відбувається в світі Cybersecurity (онлайн джерело), за посиланням: https://mind.ua/publications/20186697-galuzi-majbutnogo-shcho-vidbuvaetsya-v-sviti-cybersecurity

12.PWC (2018) Посилення цифрового середовища проти кібер-загроз (онлайн стаття), за посиланням: https://www.pwc.com/ua/uk/survey/2018/pwc-2018-gsiss-strengthening-digital-society-against-cyber-shocks-ukr.pdf

13. The Ultimate Cybersecurity Checklist for Small Businesses https://optimalidm.com/resources/blog/small-business-cyber-security-checklist/

14. MORE THAN HALF OF SMALL BUSINESSES CLOSE AFTER A CYBER ATTACK https://www.businessaustralia.com/resources/news/more-than-half-of-small-businesses-close-after-a-cyber-attack

15.Susan Morrow (Травень 27, 2021) A Beginners Guide to Cybersecurity – for Small Businesses https://vpnoverview.com/internet-safety/business/beginners-guide-cybersecurity-businesses/

16. Cybersecurity planning for any small business https://www.wellsfargo.com/biz/wells-fargo-works/planning-operations/security-fraud-protection/cybersecurity-management-plan-and-your-business/

17.НАСБУ (Березень 26, 2021)
https://academy.ssu.gov.ua/uploads/p_57_53218641.pdf

18. Раєцький А. Кібербезпека бізнесу https://legalitgroup.com/kiberbezpeka-biznesu-tse-ne-lishe-tehnichni-zahodi/

19. PQC Standardization Process: Third Round Candidate Announcement. July 22, 2020. [Electronic resource]. Access mode: https://csrc.nist.gov/News/2020/pqc-third-round-candidate-announcement.

20. Craig Gentry, Chris Peikert, Vinod Vaikuntanathan Trapdoors for hard lattices and new cryptographic constructions // Richard E. Ladner and Cynthia Dwork, editors, 40th ACM STOC, pages 197–206. ACM Press, May 2008.

21. Damien Stehlé, Ron Steinfeld Making NTRU as secure as worst-case problems over ideal lattices // Kenneth G. Paterson, editor, EUROCRYPT 2011, volume 6632 of LNCS, pages 27–47, Tallinn, Estonia, May 15–19, 2011. Springer, Heidelberg, Germany.

22. Thomas Prest Gaussian Sampling in Lattice-Based Cryptography. Theses, École Normale Supérieure, December 2015.

23. A. Kipnis, J. Patarin, L. Goubin Unbalanced Oil and Vinegar schemes // EUROCRYPT 1999, LNCS vol. 1592, pp. 206-222. Springer, 1999.

24. Rainbow Signature / Ding J. and other.2020. P. 16-22. Access mode: https://www.pqcrainbow.org/.

25. J. Ding, D. Schmidt Rainbow, a new multivariable polynomial signature scheme // ACNS 2005, LNCS vol. 3531, pp. 164-175. Springer, 2005.

26. J. Bonneau, I. Mironov Cache-Collision Timing Attacks Against AES. CHES 2006, LNCS vol. 4249, pp. 201- 215. Springer, 2006.

27. Magali Bardet, Maxime Bros, Daniel Cabarcas, Philippe Gaborit, Ray A. Perlner, Daniel Smith-Tone, JeanPierre Tillich, Javier A. Verbel Algebraic attacks for solving the Rank Decoding and MinRank problems without Groebner basis. CoRR abs/2002.08322 (2020).

28. D. Coppersmith, J. Stern, S. Vaudenay Attacks on the birational signature scheme. CRYPTO 1994, LNCS vol. 773, pp. 435-443. Springer, 1994.

29. A. Kipnis, A. Shamir Cryptanalysis of the Oil and Vinegar signature scheme. CRYPTO 1998, LNCS vol. 1462, pp. 257-266. Springer, 1998.

30. J. Ding, B.-Y. Yang, C.-H. O. Chen, M.-S. Che, C.-M. Cheng: New differential-algebraic attacks and reparametrization of Rainbow // ACNS 2008, LNCS vol. 5037, pp. 242-257. Springer, 2008.

31. J. Ding, Z. Zhang, J. Deaton, K. Schmidt, F. Visakha New attacks on lifted unbalanced oil vinegar. The 2nd NIST PQC Standardization Conference, 2019.

32. A. Kipnis, A. Shamir Cryptanalysis of the Oil and Vinegar signature scheme. CRYPTO 1998, LNCS vol. 1462, pp. 257-266. Springer, 1998.

33. A. Petzoldt, S. Bulygin, J. Buchmann Cyclic Rainbow – a Multivariate Signature Scheme with a Partially Cyclic Public Key. INDOCRYPT 2010, LNCS vol. 6498, pp. 33 – 48. Springer, 2010.

34. A. Petzoldt: Efficient Key Generation for the Rainbow Signature Scheme. PQCrypto 2020.

35. E. Thomae C. Wolf: Solving Underdetermined Systems of Multivariate Quadratic Equations Revisited. PKC 2012, LNCS vol. 7293, pp. 156-171. Springer, 2012.

36. W. Beullens, B. Preneel, A. Szepieniec, F. Vercauteren LUOV signature scheme proposal for NIST PQC project (Round 2 version), 2019.