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

До захисту
Завідувач кафедри СІКЗ
к.т.н., доцент
Шуклін Г.В.
“____”_____2023р.

АТЕСТАЦІЙНА РОБОТА
Зі спеціальності: 125 Кібербезпека
на тему:

РОЗРОБКА КОМПЛЕКСУ ЗАХИСНИХ ЗАХОДІВ ВИЯВЛЕННЯ ВТОРГНЕННЯ ТА ОПЕРАТИВНОЇ ПРОТИДІЇ ВТРАТІ ІНФОРМАЦІЇ

Студент групи СЗД-41 Жеребок Юрій Володимирович _____
(підпис)

Керівник д.т.н., проф. Ахрамович Володимир Миколайович _____
(підпис)

Нормконтроль ст. викл. Зозуля Сергій Анатолійович _____
(підпис)

Київ – 2023

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

ЗАВДАННЯ

НА ДИПЛОМНУ РОБОТУ

Студенту: Жеребку Юрію Володимировичу

1.Тема роботи: Розробка комплексу захисних заходів виявлення вторгнення та оперативної протидії втраті інформації

Наказ по університету від «24» лютого 2023 р. № 26.

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 аналіз каналів щодо можливого вторгнення до конфіденційної інформації на об`єкті інформаційної діяльності.

2.Здійснити моніторинг можливих заходів, щодо вторгнення на конфіденційну інформацію на об`єкті інформаційної діяльності.

3.Виявити можливі заходи, щодо оперативної протидії зовнішньому несанкціонованому вторгненню.

5.**Дата видачі завдання**” ” _____2023р.

КАЛЕНДАРНИЙ ПЛАН

№	Процедура	Термін виконання	
1	Підготовка Розділу 1	24.02.23	15.03.2023
2	Підготовка Розділу 2	15.03.23	17.04.23
3	Підготовка Розділу 3	17.04.23	25.05.23
4	Висновки + Презентація	25.05.23	27.05.23
5	Перевірка роботи на плагіат + Предзахист	27.05.23	01.06.23
6	Захист роботи	06.06.23	08.06.23
7	Випуск	30.06.23	

Студент Жеребок Ю.В.

Керівник роботи Ахрамович В.М.

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 70 сторінок.

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

Мета 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…….....5

ВСТУП……6

РОЗДІЛ 1. ДІЇ ДЛЯ ОРГАНІЗАЦІЇ РЕЖИМУ НА ПІДПРИЄМСТВІ……7

1.1 Список дії для організації для підтримання організації режиму……7

1.2 Список об’єктів що забезпечують режим захисту…….……11

1.3 Дії уповноважених осіб.....……25

1.4 Відомості про зовнішні прилади..……23

1.5 Теорія впливу природних і неприродних чинників……..…….....……34

1.6 Страхування ризиків та дії по запобіганню…….....35

РОЗДІЛ 2. ДІЇ ПО ВИЯВЛЕННЮ ЗАГРОЗ ТА ЇХ КЛАСИФІКАЦІЯ.....……...43

2.1Допоміжні моделі для виявлення загроз.....……...43

2.2Аналіз та знаходження загроз…….....49

2.3Цілі та мета реалізації загроз.....…….....51

2.4 Розвиток захисту та протидія появленню нових загроз ……...…53

3.4 ВИСНОВКИ…….66

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ…….67

ВСТУП

Актуальність роботи: У наш 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 радіо ефірний діапазон.

Розділ 1 ДІЇ ДЛЯ ОРГАНІЗАЦІЇ РЕЖИМУ НА ПІДПРИЄМСТВІ

1.1 Список необхідних дій для підтримання організації режиму

Головним завданням радіомоніторингу є вивчення радіоефіру в смузі частот, в якій діють 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 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.

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 а=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. 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.

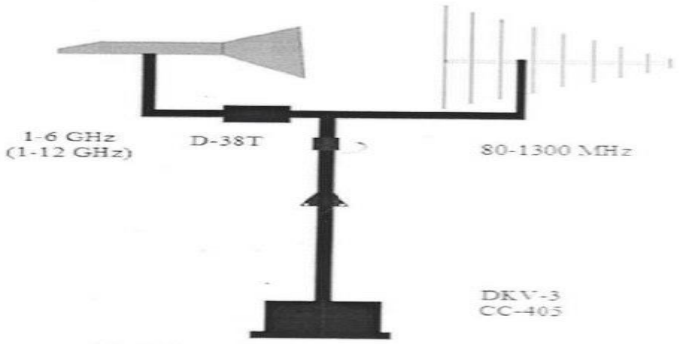


Fig.1 General scheme of the antenna system

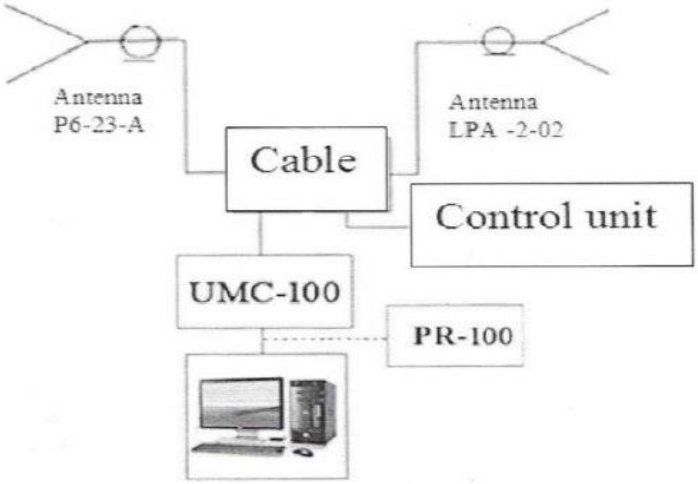


Fig. 2 Structure diagram of the antenna system

Розглянемо 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.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.

У таблиці 1 наведено результати вимірювання, отримані за допомогою розробленої антенної системи та стандартних антен, що входять до складу вимірювального обладнання Rohde & Schwarz UMS100.

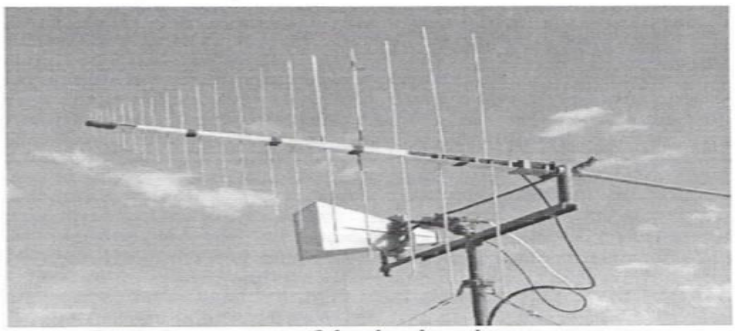


Fig.3 Appearance of the developed antenna system

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.

1.2 СПИСОК ОБ'ЄКТІВ ЩО ЗАБЕЗПЕЧУЮТЬ РЕЖИМ ЗАХИСТУ

Осцилографи серії S

Осцилографи InfiniiVision 1000 серії X

Системи збору даних DAQ970/73A

4-портова мікрохвильова піч ECal серії 4430

Програма PathWave BenchVue

Лабораторія для управління та контролю BenchVue Lab

1.3 ДІЇ УПОВНОВАЖЕНИХ ОСІБ

В останні роки зростає інтерес до міні- та мікроБПЛА, пов'язаних із можливостями малозатратні спостереження та для цілей дистанційного зондування земної поверхні. Наразі більшість БПЛА використовують супутникову навігаційну систему (GNSS) та інерціальну навігаційну систему (INS).Тому існує потреба в нових методах аналізу руху для навігації в середовищах зі слабким або відсутнім сигналом GNSS.Оптичний потік (ОП)

камер становить особливий інтерес для дослідження через просте представлення швидкості. Виявлено, що медоносні бджоли використовують оптичний потік для приземлення, регулювання швидкості та уникнення перешкод. Зацікавившись схемою польоту комах, багато розробників були спрямовані на використання модифікованих відеосенсорів для вимірювання оптичного потоку на основі різних роботизованих платформ.На основі отриманих результатів оцінки швидкості поступального руху проаналізовано точність запропонованих методів.

Визначення параметрів руху за даними оптичного потоку відеокамери Різні точки в просторі об'єктів відображаються оптичною системою камери в просторі зображення на різних відстанях від фокальної площини.

Однак, якщо відстань між камерою і спостережуваною сценою значно перевищує фокусну відстань оптичної системи, можна вважати, що зображення будується в її фокальній площині. У цьому випадку можна використовувати модель проективної камери, в якій зображення тривимірного об'єкта отримують проектуванням його на фокальну площину (площину зображення) через одну точку, яка називається оптичним центром. Пряма, перпендикулярна до площини зображення і проходить через цю точку, називається оптичною віссю фотоапарата, а точка перетину оптичної осі з площиною зображення - головною. Рух об’єктів перед камерою або рух камери в нерухомому середовищі призводить до відповідних змін у зображенні, і це вимірювання можна використовувати для реконструкції відповідного руху. Камера рухається в статичному середовищі. Поле руху створюється проектуванням швидкості на площині зображення.

Точка p відповідає точці P на поверхні Землі (рис. 1). Ці дві точки є пов’язаними рівняннями проектування. Важливо, що будь-якій точці зображення можна поставити певний вектор. Ці вектори утворюють поле руху.

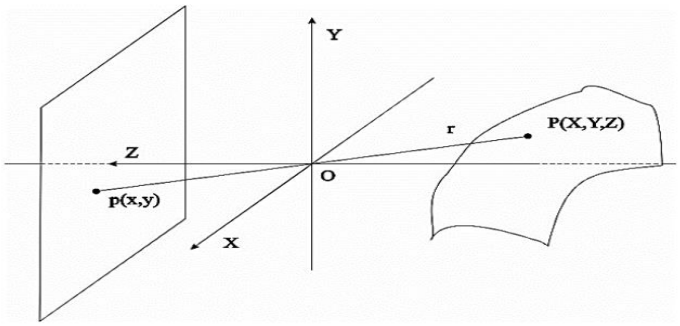


Рис. 1. Система координат проекційної камери.

Зв'яжемо систему координат з камерою так, щоб вісь Z збігалася з оптичною віссю камери. Позначимо r вектор, що сполучає точку O з точкою P=[X,Y,Z]T, f — фокусна відстань. Проекційні піксельні координати P на площині зображення визначаються

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

У загальному випадку вимірювання координат у фотоприймачі здійснюється в одиницях, відмінних від одиниць, що задають координати в стандартній системі. У новій системі координати проекції точки p матимуть вигляд

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

де (u0, v0) – координати головної точки відносно початку фотоприймача (в натуральних координатах фотоприймача); w і h — масштаби по осях ox і oy (наприклад, відстані між осередками матричного фотоприймача по рядках і стовпцях).

Для подальшого представлення введемо тривимірний вектор, що відповідає точці P=(X,Y,Z) , і двовимірний вектор , p=(x, $y)^T$ що відповідає пункту c.

Визначимо також вектор однорідних внутрішніх координат камери $W = (u, v, 1)^T$. Використовуючи ці позначення, відносини можуть бути представлені в компактній векторно-матричній нотації

$$ZW=AP,$$

Де $A = \begin{matrix} f/w & \mu & u0 \\ 0 & f/h & v_0 \\ 0 & 0 & 1 \end{matrix}$ - матриця внутрішніх параметрів камери, містить лише параметри оптичної системи та фотоприймача камери.

Нехай OXYZ — глобальна система координат, а O'X'Y'Z' — стандартна система координат камери. Перехід від системи OXYZ до системи O'X'Y'Z' можна здійснити поворотом осей координат до системи OX"Y"Z" і подальшим зміщенням початку координат. Тоді зв'язок між координатами точки P в глобальній і стандартній системах можна представити у вигляді

$$P' = RP + t,$$

де P і P′ – вектори просторових координат точки P у глобальній та стандартній системах відповідно; R – матриця 3x3, що описує поворот стандартної системи координат відносно глобальної; t - тривимірний вектор зсуву початку координат глобальної системи відносно початку стандартної.

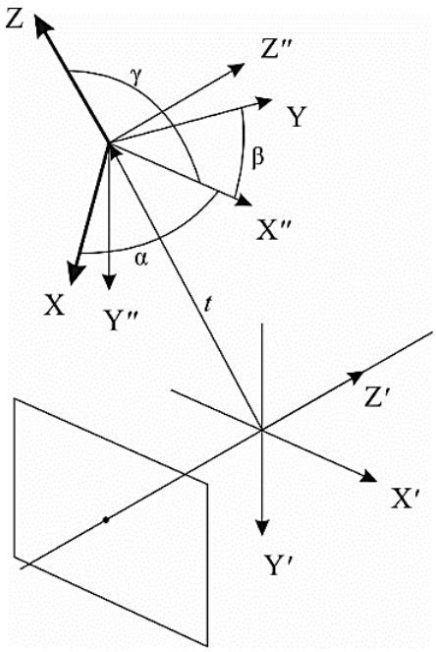


Рис.2. Перехід від глобальної системи координат до стандартної системи координат камери.

На рис. 2 схематично показано перетворення координат. Тут α, β, γ – кути, утворені віссю OX″ з осями OX, OY і OZ відповідно. Вектор t=(txtytz)T - зміщення початку глобальної системи координат відносно початку еталона. Для отримання внутрішніх параметрів камери, а також компенсації радіальних і тангенціальних спотворень виконується процедура калібрування відеокамери.

Початок координат в площині зображення камери збігається з головною точкою u0=v0=0, а одиниці координат в глобальній системі і в площині зображення камери однакові (w=h=1). Рух твердого тіла можна розкласти на дві складові: (V) поступальний рух і обертальний рух [Уравнение] навколо осі, що проходить через початок координат. Швидкість точки буде виглядати так:

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

Де,V=(Vx,Vy,VZ)T

- поступальний рух; [Уравнение] – параметри обертання.

Беручи похідну за часом, отримуємо відношення швидкості P в системі відліку камери до швидкості p в площині зображення з функцією похибок

P 0.

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

Для компонентів x і y поле руху можна записати так:

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

Ці рівняння можна записати як $\dot{x} = u_t + u_r$ і $\dot{y} = v_t + v_r$.Let us розділити оптичний потік на поступальну складову $(u_t + v_t)$ і обертальний компонент $(u_r + v_r)$:

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

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

Для визначення оптичного потоку в статті [8] використовується метод порівняння блоків, який використовує адаптивну зміну розміру та адаптивну стратегію пошуку вектора руху зі зважуванням вимірювань блоків зображення, де кожен блок відповідає індексу текстури.

Оцінка руху вперед

Розглянемо три можливі варіанти початкових умов руху відеокамери, або платформи.

1.Відома відстань від камери до поверхні в кожній точці зображення. Поставимо собі за мету визначити параметри поступального руху $V_{x,}V_y$.

Визначимо найменше відхилення:

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

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

Диференціювання інтегралів за V_X, V_y і прирівнявши отримані рівняння до нуля, отримаємо:

$$V_x = \frac{V_z \iint x dxdy - Z \iint u dxdy}{(n \cdot m)}, \quad V_y = \frac{V_z \iint y dxdy + Z \iint v dxdy}{(n \cdot m)}.$$

2. Розглянемо умову, за якої не відбувається поступального руху вздовж осі Z,

$V_z = 0$. У цьому випадку вираз спрощується, і ми отримуємо параметри поступального руху:

$$V_x = \frac{-Z \iint u dxdy}{(n \cdot m)}, V_y = \frac{-Z \iint v dxdy}{(n \cdot m)}.$$

3. Далі розглянемо умову, за якої необхідно визначити параметри руху

V_x, V_y, V_Z з невідомим Z. Щоб розглянути явне рішення, ми використовуємо вираз, запропонований у. Метод найменших квадратів складається з наступних кроків: спочатку ми визначаємо значення Z, яке мінімізує підінтегральну функцію в кожній точці (x, y), а потім визначити значення V_x, V_y,і V_Z, що мінімізує інтеграл.

Вираз, який ми хочемо мінімізувати, прийме форму

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

Де $\alpha = -V_x + xV_Z$; $\beta = -V_y + yV_Z$.

Позначимо інтеграл для мінімізації так:

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

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

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

Для визначення швидкості поступального руху методом найменших квадратів необхідно розв'язати однорідну систему за w: Gw= 0, де

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

Оскільки дані містять шум, функція $g(V_x, V_y, V_Z)$ не може бути встановлено на нуль для ненульової швидкості поступального руху і, таким чином$w = (0,0,0)^T$ буде єдино правильним рішенням. Визначивши власний вектор, відповідний власному змістуl_1, ми отримуємо:

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

Слід зазначити, що значення $l_1 = 0.$

Результати моделювання та оцінки параметрів руху відеокамери.

Для дослідження точності алгоритмів розроблено програму в системі MATLAB. Для створення ефекту польоту БПЛА координати підстилаючої поверхні залишаться незмінними; ми змінимо координати та орієнтацію камери.Під час запуску симуляції польоту підстилаюча поверхня буде відображатися на екрані з певної точки простору та під певними кутами, значення яких залежить від поточного положення та орієнтації камери. Під час

польоту змінюється яскравість зображення. Отримане поточне зображення ділиться на блоки 8x8 і виконується процедура оцінки оптичного потоку. Параметри векторів руху записуються у відповідні матриці. Залежно від задачі, що вирішується, вибирається алгоритм аналізу векторів руху (полів руху). Проводилося моделювання рухів на восьми зображеннях підстильної поверхні високої роздільної здатності (4412 x 4779 пікселів) з різними текстурами. Для порівняння швидкість поступального руху обчислюється за допомогою аналізу текстури та стандартного методу на основі вимірювань рівної точності.

Показано зовнішній вигляд системи координат, змодельованої для системи спостереження

на рис. 4. Початок координат знаходиться на поверхні підстилаючої поверхні в обраній точці. Початкове положення камери характеризується координатами (X, Y, Z) і кутами орієнтації (α, β, γ).

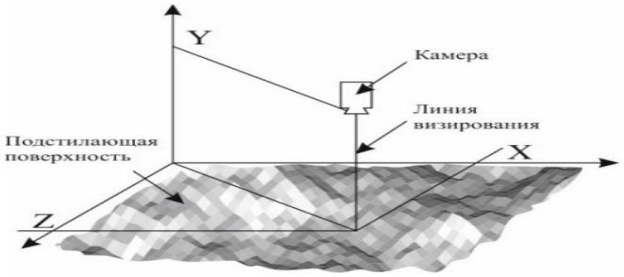


Рис. 4. Моделювання руху відеокамери

Рис. 4. Моделювання руху відеокамери

Вихідні дані моделювання: середня швидкість руху 16 м/с, висота руху камери 100 м, кут огляду камери 90 градусів, фокусна відстань 1 мм, розмір ПЗС-матриці 256x256 пікселів, частота кадрів 30 кадрів/с. Оцінка поступальної швидкості з компенсацією обертального руху, зміни кутових швидкостей Y,X,Z=[-10:10].

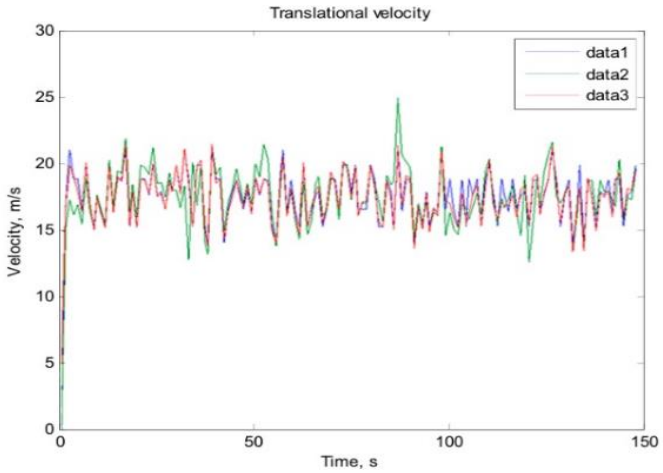


Рис. 6. Попередня швидкість.

data1 — справжня швидкість руху;

data2 - розрахована швидкість руху стандартним методом

data3 - розрахункова швидкість руху, розроблена методом OF.

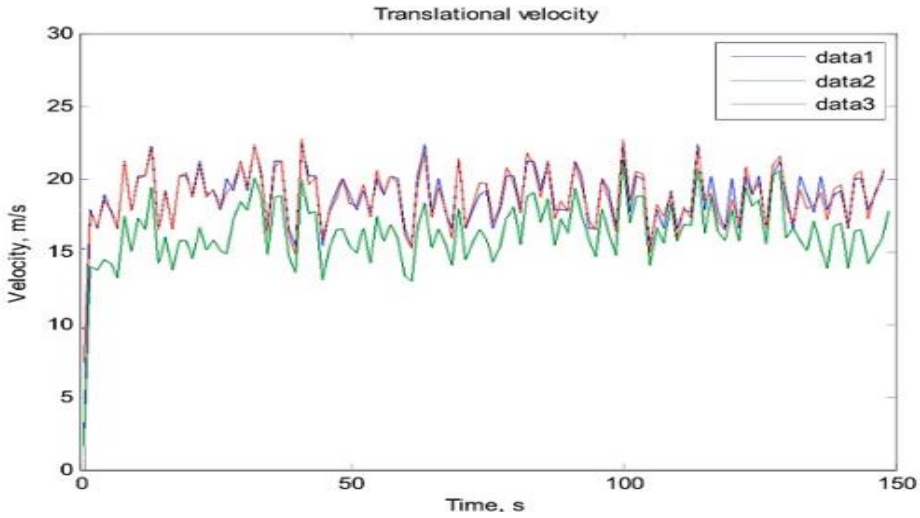


Рис. 7. Попередня швидкість

data1 — справжня швидкість руху;

data2 - розрахована швидкість руху стандартним методом;

data3 - розрахункова швидкість руху, розроблена методом OF.

На підставі отриманих результатів оцінки поступальної швидкості можна проаналізувати точність запропонованого методу.

Для аналізу текстури запропоновано параметр, який характеризує ступінь текстури зображення за оцінкою коваріаційної матриці. Аналіз зображення підстильної поверхні щодо оцінки числа умов дорівнював 9,6348, що є ознакою високої текстури всього зображення.

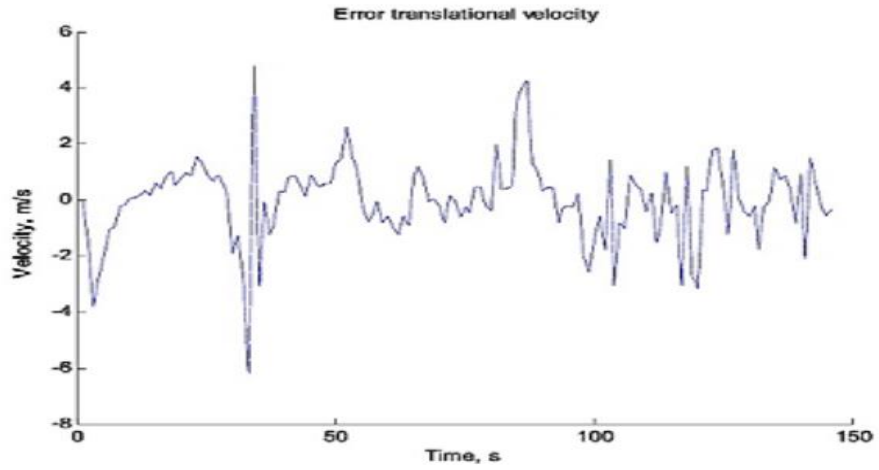


Рис.8. Помилки в оцінках поступальних швидкостей

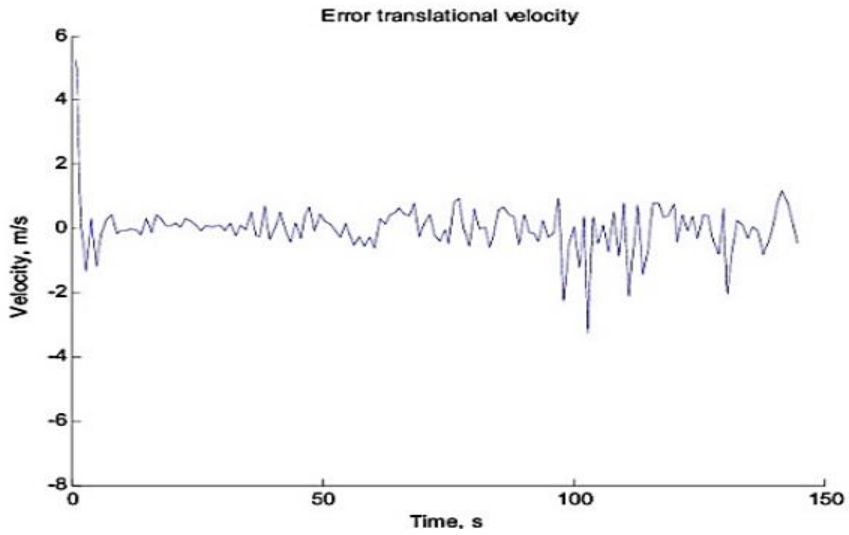


Рис. 9. Помилки в оцінках поступальних швидкостей, розроблених методом OP

Для оцінок, заснованих на стандартному блочному методі, розрахункове середнє значення похибки поступальної швидкості становило 0,154 м/с, стандартне відхилення похибки визначення швидкості прямого ходу 1,4389 м/с.

Розрахунок поступальної швидкості з використанням оцінки блоків зображення дав наступний результат: середнє розрахункове значення похибки поступальної швидкості склало 0,0880 м/с, стандартне відхилення похибки визначення поступальної швидкості 0,6392 м/с.

На рис. На рисунку 7 показані результати оцінок швидкості для зображення підстилаючих поверхонь зі слабким індексом текстури. Моделювання руху відеокамери проводилося на однорідній текстурі водної поверхні. На основі отриманих результатів оцінки поступальних швидкостей можна оцінити точність запропонованого методу. Аналіз текстури всього зображення підстильної поверхні з огляду на оцінку числа умов становив 6,6203, що вказує на слабку текстуру зображення.

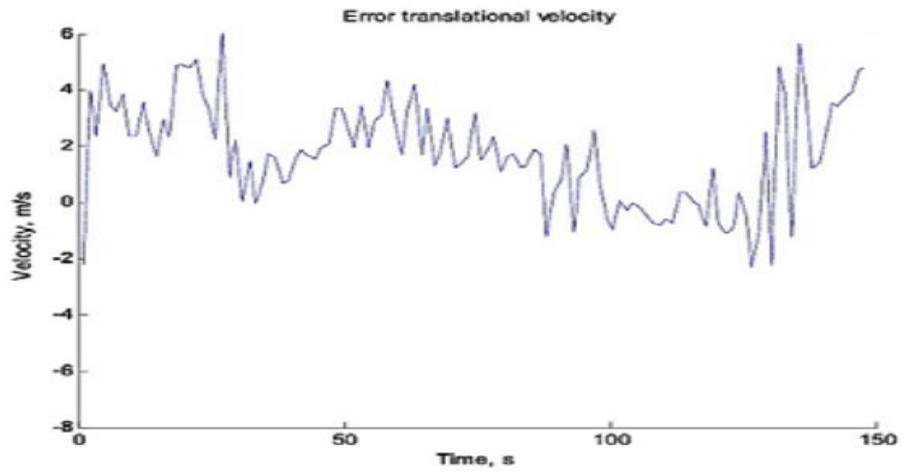


Рис. 10. Помилки трансляційних оцінок швидкості стандартним методом ОП

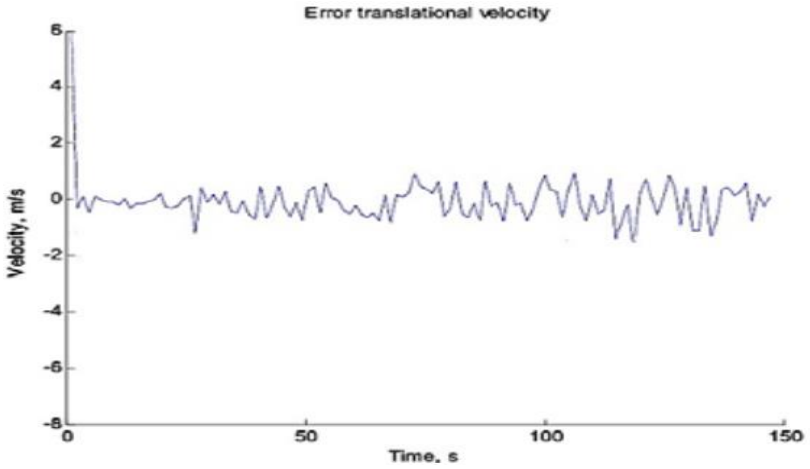


Рис. 11. Помилки трансляційних оцінок швидкості, розроблених за методом О

Для оцінок за стандартним методом середнє розрахункове значення похибки вимірювання поступальної швидкості становило 2,5128 м/с, а стандартне відхилення похибки вимірювання поступальної швидкості становило 1,1727 м/с.

Розрахунок поступальної швидкості за допомогою аналізу текстури дав наступний результат: середнє оцінене значення похибки вимірювання поступальної швидкості становить 0,0221 м/с, а стандартне відхилення похибки вимірювання поступальної швидкості становить 0,7223 м/с. У табл. У таблиці 1 наведено результати оцінок параметрів поступального руху для різних зображень підстильної поверхні:

Результати оцінок параметрів поступального руху

Варіанти оцінок	Фактура підстилаючої поверхні							
	Топографічна карта	аерофотозйомка	повітряна фотографі	площа	Текстура асфальту	текстура бетону	текстура трави	Текстура води
Текстура аналіз	2.7736	4.7706	9.6348	3.3554	2.5556	2.1907	3	6.6
мат.очікування помилки швидкості	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 помилки визначення трансляційної швидкості	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
мат. очікування помилки при визначенні швидкості поступального руху за допомогою текстури	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
СКО похибки визначення поступальної швидкості за текстурою	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 Відомості про зовнішні прилади

І ПРИЛАД РАДІОЧАСТОТНОГО ШУМУ СТАЦІОНАРНИЙ "РИАЦ-1С".

1. Загальні відомості, призначення

1.1 Стаціонарний радіочастотний перешкодовий пристрій «ПІАЦ-1С» призначений для захисту об'єктів від витоку конфіденційної інформації по каналам побічних електромагнітних випромінювань і перешкод шляхом генерації шумового сигналу.

1.2 До складу приладу входять генератор шуму "РІАС-1ГС" і каркасні м'які антени "ПІАК-1АМ".

1.3 М'які каркасні антени «ПІАК-1АМ» являють собою ізольовані проводи перерізом до 5 мм, які розміщуються по периметру об'єкта, що охороняється.

1.4 До вихідних каналів генератора можна підключити до 6 рамкових антен.

2. Технічні характеристики

2.1 Пристрій забезпечує придушення випромінювань малопотужних передавачів у смузі частот від 180 Гц до 2 ГГц і вище.

2.2 Коефіцієнт якості шумового сигналу приладу не менше 0,8.

2.3 Спектральна густина інтенсивності електричної Еш та магнітної рН складових електромагнітного шумового поля (дБ/мкВ*м-1*кГц-0,5) приладу відносно 1 мкВ на відстані 1 м від антени:

- в діапазоні від 0,00018 до 100 МГц не менше 65 дБ
- в діапазоні від 100 до 100 МГц не менше 70 дБ
- в діапазоні від 500 до 1200 МГц не менше 70 дБ:
- в діапазоні від 1200 до 2000 МГц не менше 70 дБ.

2.4 Коефіцієнт міжспектральних кореляцій у смузі частот шумового сигналу приладу не більше 6 дБ.

2.5 Пристрій забезпечує регулювання рівня шумового сигналу не менше 20 дБ.

2.6 Максимальне інтегральне значення вихідної потужності приладу не менше 10 Вт.

2.7 Прилад має вбудовану систему автоматичного контролю роботи та звукову індикацію справності випромінюваних антен.

2.8 Живлення приладу здійснюється від мережі змінного струму напругою 220 В плюс 22 В мінус 33 В частотою 50±1 Гц.

2.9 Час технічної готовності приладу - не більше 5 с.

2.10 Споживана приладом потужність від мережі змінного струму не більше 20 Вт.

2.11 Габаритні розміри генератора - не більше 190х187х63 мм.

2.12 Маса генератора не більше 2 кг.

Інструмент генерує шумовий сигнал на частоті, на якій виникають непрямі електромагнітні випромінювання, гасячи їх. Переваги: широкий діапазон роботи, висока якість сигналу, світло, малий час очікування. Недоліки: розмір пристрою, відсутність акумулятора для автономної роботи, тільки один тип антени, стаціонарна.

II СТАЦІОНАРНИЙ РАДІОЧАСТОТНИЙ ШУМОВИЙ ПРИЛАД "PIAC-1C/1"

1. Загальні відомості, призначення

1.1 Стаціонарний радіочастотний перешкодовий пристрій «РІАЦ-1С/1» призначений для захисту об'єктів від витоку конфіденційної інформації по каналам побічних електромагнітних випромінювань і перешкод шляхом генерації шумового сигналу.

1.2 До складу приладу входять генератор шуму «ПІАК-1ГС/1» та дипольні телескопічні антени «ПІАК-1АД».

1.3 Телескопічні дипольні антени «PIAC-1AD» являють собою чотирилапий дипольний штир діаметром 10 мм і довжиною 1225 мм.

2. Технічні характеристики

2.1 Пристрій забезпечує придушення випромінювання малопотужних передавачів у смузі частот від 180 Гц до 1 ГГц і вище.

2.2 Коефіцієнт якості шумового сигналу приладу не менше 0,8.

2.3 Спектральна щільність електричної Еш і магнітної рН складових електромагнітного шумового поля (дБ / мкВ * м-1 * кГц-0,5) приладу відносно 1 мкВ на відстані 1 м від антени:

- в діапазоні від 0,00018 до 100 МГц не менше 65 дБ;
- в діапазоні від 100 до 100 МГц не менше 70 дБ;
- в діапазоні від 500 до 1200 МГц не менше 70 дБ;
- в діапазоні від 1200 до 2500 МГц не менше 70 дБ.

2.4 Коефіцієнт міжспектральних кореляцій у смузі частот шумового сигналу приладу не більше 6 дБ.

2.5 Пристрій забезпечує регулювання рівня шумового сигналу не менше 20 дБ.

2.6 Максимальне інтегральне значення вихідної потужності приладу не менше 15 Вт.

2.7 Прилад має вбудовану систему автоматичного контролю функціонування.

2.8 Живлення приладу здійснюється від мережі змінного струму напругою 220 8 плюс 22 В мінус 33 В частотою 50±1 Гц.

2.9 Час технічної готовності приладу не більше 5 с.

2.10 Потужність, яку прилад споживає від мережі змінного струму не більше 20 Вт.

2.11 Габаритні розміри генератора - не більше 190х187х63 мм.

2.12 Маса генератора не більше 2 кг.

Інструмент генерує шумовий сигнал на частоті, на якій виникають непрямі електромагнітні випромінювання, гасячи їх. Переваги: широкий діапазон роботи, висока якість сигналу, світло, малий час очікування. Недоліки: розмір

пристрою, відсутність акумулятора для автономної роботи, тільки один тип антени, стаціонарна.

IV ПРИЛАД РАДІОЧАСТОТНИХ ШУМОВ МОБІЛЬНИЙ "РІАЦ-1М"

1. Загальні відомості, призначення

1.1 Пересувний радіочастотний шумовий прилад «ПІАК-1М. призначений для захисту об'єктів від витоку конфіденційної інформації по каналам побічних електромагнітних випромінювань і перешкод шляхом генерації шумового сигналу.

1.2 До складу приладу входять генератор шуму ПІАЦ-1ГМ, внутрішні дипольні телескопічні антени ПІАЦ-1АД (вбудовані) та жорстка рамкова антена ПІАЦ-1АЖ.

1.3 Телескопічні дипольні антени «PIAC-1AD» являють собою чотирилапий дипольний штир діаметром 10 мм і довжиною 1225 мм.

1.4 Жорстка рамкова антена «ПЛАК-1АЖ» являє собою коло діаметром 280 мм і перерізом труби 10 мм.

2. Технічні характеристики

2.1 Пристрій забезпечує придушення випромінювання малопотужних передавачів у смузі частот від 180 Гц до 2 ГГц вище.

2.2 Коефіцієнт якості шумового сигналу приладу не менше 0,8.

2.3 Спектральна щільність електричної Еш і магнітної рН складових електромагнітного шумового поля (дБ / мкв * м-1 * кГц-0,5) приладу відносно 1 мкВ на відстані 1 м від антени:

- в діапазоні від 0,00018 до 100 МГц не менше 65 дБ;
- в діапазоні від 100 до 100 МГц не менше 70 дБ:
- в діапазоні від 500 до 1200 МГц не менше 70 дБ;
- в діапазоні від 1200 до 2000 МГц не менше 70 дБ.

2.4 Коефіцієнт міжспектральних кореляцій в смузі частот шумового сигналу - не більше 6дБ.

2.5 Пристрій забезпечує регулювання рівня шумового сигналу до значення не менше 20 дБ. 2.6 Максимальне інтегральне значення вихідної потужності приладу не менше 15 Вт.

2.7 Прилад має вбудовану систему автоматичного контролю функціонування.

2.8 Живлення приладу здійснюється від мережі змінного струму напругою 220 В плюс 22 В мінус 33 В частотою (50:1) Гц, акумулятора та бортової мережі автомобіля.

2.9 Час технічної готовності приладу не більше 5 с.

2.10 Потужність, яку прилад споживає від мережі змінного струму, не більше 20 Вт.

2.11 Прилади приладу поміщають у футляр.

2.12 Габаритні розміри приладу не більше 460х380х130 мм.

2.13 Маса генератора - не більше 2 кг.

Інструмент генерує шумовий сигнал на частоті, на якій виникають непрямі електромагнітні випромінювання, гасячи їх. Переваги: широкий діапазон роботи, висока якість сигналу, світло, малий час очікування. Недоліки: розмір пристрою, відсутність акумулятора для автономної роботи.

V КОМП'ЮТЕРНИЙ РАДІОЧАСТОТНИЙ ШУМОВИЙ ПРИСТРІЙ "РІАС-1К"

1. Загальні відомості, призначення

1.1 Комп'ютерний радіочастотний шумовий пристрій "ПІАЦ-1К" призначений для захисту об'єктів від витоку конфіденційної інформації по каналам побічних електромагнітних випромінювань і перешкод шляхом генерації шумового сигналу.

1.2 До складу приладу входять генератор шуму «ПІАК-1ГМ», дипольні телескопічні антени «ПІАК-1АД» і жорстка каркасна антена «ПІАК-1АЖ».

1.3 Дипольні телескопічні антени «PIAC-1AD» являють собою чотирилапий дипольний штир діаметром 10 мм і довжиною 1225 мм.

1.4 Жорстка рамкова антена "ПІАК-1АЖ" являє собою коло діаметром 280 мм і перерізом труби 10 мм.

2. Технічні характеристики

2.1 Пристрій забезпечує придушення випромінювань малопотужних передавачів у смузі частот від 180 Гц до 2 ГГц.

2.2 Коефіцієнт якості шумового сигналу приладу не менше 0,8.

2.3 Спектральна густина інтенсивності електричної Еш та магнітної рН складових електромагнітного шумового поля (дБ/мкВ*м-1*кГц-0,5) приладу відносно 1 мкВ на відстані 1 м від антени:

- в діапазоні від 0,00018 до 100 МГц не менше 65 дБ;
- в діапазоні від 100 до 100 МГц не менше 70 дБ;
- в діапазоні від 500 до 1200 МГц не менше 70 дБ;
- в діапазоні від 1200 до 2000 МГц не менше 70 дБ.

2.4 Коефіцієнт міжспектральних кореляцій у смузі частот шумового сигналу приладу не більше 6 дБ.

2.5 Пристрій забезпечує регулювання рівня шумового сигналу не менше 20 дБ.

2.6 Максимальне інтегральне значення вихідної потужності приладу не менше 10 Вт.

2.7 Прилад має вбудовану систему автоматичного контролю функціонування.

2.8 Живлення пристрою здійснюється від блоку живлення комп'ютера.

2.9 Час технічної готовності приладу - не більше 5 с.

2.10 Потужність, яку споживає пристрій від блоку живлення комп'ютера не більше 20 Вт.

2.11 Генератор розміщується у вільному місці обчислювального блоку, а антени можуть бути встановлені як на корпусі обчислювального блоку, так і в іншому зручному місці.

2.12 Замість дипольних телескопічних антен PIAC-1AD" і жорсткокаркасних антен "PIAC-1АЖ" можуть використовуватися активні каркасні м'які антени "PIAC-АМ", які розміщуються в зоні розміщення пристроїв ПК.

2.13 Габаритні розміри генератора - не більше 195х145х43 мм.

2.14 Маса генератора не більше 2 кг.

Інструмент генерує шумовий сигнал на частоті, на якій виникають непрямі електромагнітні випромінювання, гасячи їх. Переваги: широкий діапазон роботи, висока якість сигналу, світло, малий час очікування. Недоліки: розмір пристрою, відсутність акумулятора для автономної роботи, стаціонарний інструмент.

VI ВИСОКОЧАСТОТНИЙ РАДІОЧАСТОТНИЙ ШУМОВИЙ ПРИЛАД "PIAC-1Б"

1. Загальні відомості, призначення

1.1 Пристрій високочастотний радіочастотний перешкод "PIAЦ-1Б" призначений для захисту об'єктів від витоку конфіденційної інформації по каналам побічних електромагнітних випромінювань і перешкод шляхом генерації шумового сигналу.

1.2 До складу пристрою входять генератор шуму PIAC-1GV і телескопічні дипольні антени PIAC-1AD.

1.3 Телескопічні дипольні антени «PIAC-1AD» являють собою чотирилапий дипольний штир діаметром 10 мм і довжиною 1225 мм.

2. Технічні характеристики

2.1 Пристрій забезпечує придушення випромінювання малопотужних передавачів в діапазоні частот від 0,5 ГГц до 2 ГГц.

2.2 Коефіцієнт якості шумового сигналу приладу не менше 0,8.

2.3 Спектральна густина електричної Еш та магнітної рН складових електромагнітного шумового поля (дБ/мкВ*м-1*кГц-0,5) приладу відносно 1 мкВ на відстані 1 м від антени:

-в діапазоні від 1000 до 1500 МГц - не менше 70 дБ;

- в діапазоні від 1500 до 2000 МГц не менше 70 дБ.

2.4 Коефіцієнт міжспектральних кореляцій у смузі частот шумового сигналу приладу не більше 6 дБ.

2.5 Пристрій забезпечує регулювання рівня шумового сигналу не менше 20 дБ.

2.6 Максимальне інтегральне значення вихідної потужності приладу не менше 10 Вт.

2.7 Прилад має вбудовану систему автоматичного контролю функціонування.

2.8 Живлення приладу здійснюється від мережі змінного струму напругою 220 В плюс 22 В мінус 33 В частотою 50+1 Гц.

2.9 Час технічної готовності приладу не більше 5 с.

2.10 Потужність, яку прилад споживає від мережі змінного струму не більше 20 Вт.

2.11 Габаритні розміри генератора не більше 153х135х50 мм.

2.12 Маса генератора - не більше 2 кг.

Інструмент генерує шумовий сигнал на частоті, на якій виникають непрямі електромагнітні випромінювання, гасячи їх. Переваги: висока якість сигналу, світло, малий час очікування. Недоліки: розмір пристрою, відсутність акумулятора для автономної роботи, тільки один тип антени, стаціонарна.

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	spectral plane of the electric and	блок живлення комп’ютера	computer power supply

напруженості електричного і магнітного компонентів електромагнітного поля	magnetic components of the electromagnetic field		
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 ТЕОРІЯ ВПЛИВУ ПРИРОДНИХ І НЕПРИРОДНИХ ЧИННИКІВ

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

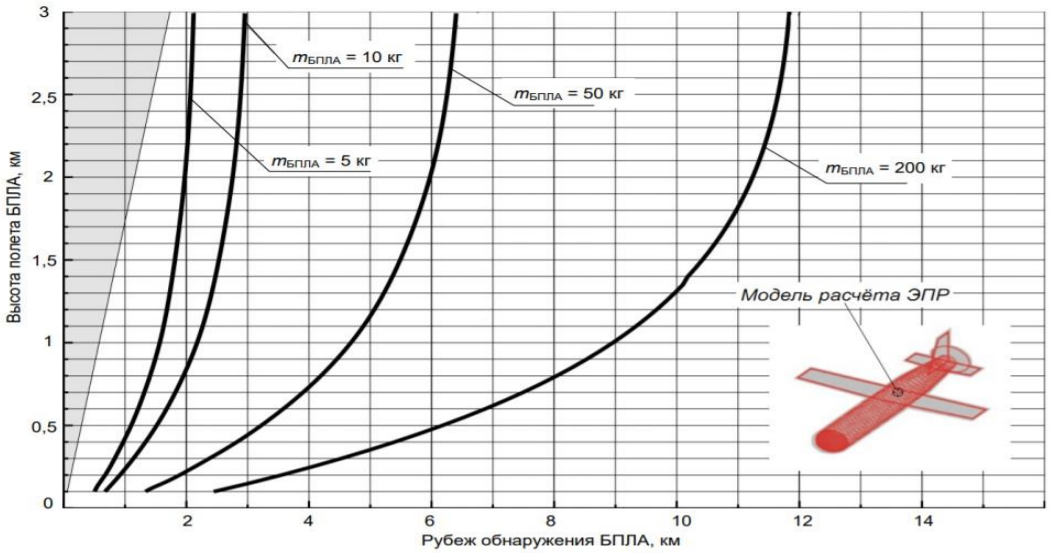


Рис. 1. Відстань для виявлення БПЛА, які мають різні властивості

1.7 СТРАХУВАННЯ РИЗИКІВ ТА ДІЇ ПО ЗАПОБІГАННЮ

Важко уявити систему, для якої властивості цілісності не були б важливими. Проте вимоги доброчесності залишаються актуальними.Численні атаки спрямовані на порушення цілісності. До них відносяться зловмисні модифікації, здійснені вірусами чи іншими зловмисними програмами, помилки програми. Однак порушення цілісності не обмежуються навмисними атаками. помилки користувача, недогляд або некомпетентність є причиною багатьох випадків неавторизованої зміни інформації. П Порушення цілісності може статися через дії будь-якого користувача, в тому числі і адміністратора. Вони також можуть виникати через недогляд у політиці безпеки або через неправильно налаштовані елементи керування безпекою.Належним чином реалізований захист цілісності забезпечує засоби для авторизованих змін, одночасно захищаючи від зловмисних несанкціонованих дій, а також від помилок авторизованих користувачів. Це гарантує, що дані залишаються правильними, незмінними і збереженими. Якщо механізм безпеки забезпечує цілісність, він

забезпечує високий рівень гарантії того, що дані, об’єкти та ресурси не будуть змінені з початкового захищеного стану.

Залежно від того, наскільки той чи інший аспект сфери використання даних є найбільш важливим, виділяють методи і засоби забезпечення їх цілісності, в сенсі [3]:

- правильність і незмінність даних, що базуються на так званих моделях цілісності даних;
- неспотворені дані при передачі в лініях зв'язку та зберіганні в інформаційних системах на основі криптографії (наприклад, використання таких криптографічних примітивів, як: цифровий підпис, криптографічні хеш-функції, коди автентифікації);
- паралельне виконання транзакцій у клієнт-серверних системах (транзакції відіграють важливу роль у механізмі забезпечення цілісності бази даних).

Існують численні контрзаходи, які можуть гарантувати цілісність даних для різних можливих загроз [2]. У тому числі полегшити безпеку, якщо є чітка модель того, що потрібно захищати, а також кому і що дозволено робити [4]. Тому невід’ємною частиною будь-якого проекту зі створення або оцінки безпеки ІБ та баз даних, у тому числі, як зазначено в [5], є наявність моделі безпеки. Нижче, перш за все, зупинимося на аналізі деяких найбільш відомих моделей безпеки, пов'язаних з розглянутими в роботі аспектами - формальних моделей цілісності даних.

Модель Кларка-Вілсона

Через важливість цілісності данних, розроблено кілька моделей безпеки, які включають моделі, запропоновані Кларком з Вілсоном і Бібою. Модель Кларка-Вілсона [6] є описовою. Він не містить ніяких, не було строгих математичних виразів. Модель Кларка-Вілсона є основою та посібником для

формалізації політики безпеки, а не конкретною моделлю політики безпеки. Це підкреслює важливість схвалення керівництвом процесів і політик безпеки, яких повинна дотримуватися організація [7]. Його, швидше за все, доцільно розглядати як набір практичних рекомендацій щодо побудови системи цілісності в ІБ.

Для кращого розуміння цієї моделі виконаємо деяку формалізацію, ввівши певні позначення:

- S – множина предметів;
- D - набір даних в IS (набір об'єктів), а D=CDI∪UDI, CDI∩UDI = Æ де CDI (обмежені елементи даних) дані (будь-який елемент даних), цілісність яких контролюється (захищена модель безпеки); UDI (unconstrained data items) - дані, цілісність яких не контролюється моделлю безпеки;
- IVP (integrity verification procedure) – це процедура перевірки цілісності CDI (процедура, яка сканує елементи даних і підтверджує їх цілісність, наприклад, шляхом обчислення контрольної суми або використання можливостей сучасної моделі блокчейну, як показано в [8]);
- TP (transformation procedure) - процедура трансформації - компонент, який може ініціювати транзакцію (послідовність операцій), що переводить систему з одного стану в інший. Процедури перетворення є єдиними процедурами, яким дозволено змінювати CDI. Обмежений доступ до CDI через TP є основою моделі цілісності Кларка–Вілсона.

Модель Кларка-Вілсона базується, як і дискреційні моделі контролю доступу, на трійках: «суб’єкт – операція (транзакція), що не порушує цілісність – об’єкт». Суб'єкти не мають прямого доступу до об'єктів. Доступ до об'єктів можливий лише через TP.

Модель розрізняє два основні механізми, які забезпечують базовий контроль доступу та цілісність. А саме, добре сформована транзакція зберігає цілісність

даних і запобігає довільним маніпуляціям цими суб’єктами. Слід зазначити, що концепція добре сформованої транзакції ідеально вписується в стандартну концепцію транзакцій традиційної СУБД [9]. Розподіл обов'язків вимагає, щоб кожна критична операція складалася з двох або більше частин, кожна з яких повинна виконуватися іншою організацією або організацією з іншою роллю.

Модель складається з двох наборів правил: сертифікація (С), яка виконується адміністратором безпеки, власником системи, зберігачем системи, і правила виконання (Е), які виконує система. Правила виконання відповідають функціям безпеки, незалежним від програми, а правила сертифікації дозволяють включати в модель визначення цілісності для конкретної програми. Бажано звести до мінімуму правила сертифікації, оскільки процес сертифікації є складним, схильним до помилок і його необхідно повторювати після кожної зміни процедури (програми) перетворення.

Правила моделі Кларка-Вілсона, дещо перефразовані відносно оригіналу, наведені нижче:

1.Правило С1. Система повинна мати IVP, здатні підтвердити цілісність будь-якого CDI (в оригінальній роботі [6] це сформульовано так: «Усі IVP повинні належним чином гарантувати, що всі CDI знаходяться в дійсному стані під час операції IVP»; під поняттям «дійсний) стан» автори розуміють такий стан системи, при якому в будь-який момент часу CDI задовольняють вимогам цілісності).

2.(С2) Усі процедури перетворення TP повинні бути реалізовані правильно, у тому сенсі, що вони не повинні порушувати цілісність даних (тобто вони повинні переводити CDI у дійсний кінцевий стан, враховуючи, що він знаходиться в дійсному стані із самого початку) і застосовувати лише до списку елементів CDI, встановленого адміністратором безпеки (співвідношення TPi, (CDIa, CDIb, CDIc, …)

3.(E1) Система повинна контролювати, чи можна застосовувати TP до елементів CDI відповідно до списків, зазначених у правилі C2.

4.(E2) Система повинна підтримувати список дозволених для конкретних користувачів

Процедури перетворення TP із зазначенням допустимого для кожного TPi□TP і цього предмета (s j□S) набору оброблених елементів CDI (тобто трійок: (Sj,TPi,(CDIa, CDIb, CDIc, …)

5.(C3) Список, визначений правилом E2, повинен відповідати вимозі розподілу функціональних обов'язків (включаючи спільне виконання).

6.(E3) Система повинна автентифікувати всіх користувачів (кожного суб’єкта), які намагаються виконати будь-яку процедуру перетворення TP.

7. (C4) Кожне застосування TP має бути записане в спеціальний запис CDI, журнал, що містить інформацію, достатню для відновлення повної картини кожного застосування цієї процедури перетворення, і доступний лише для додавання інформації до нього.

8.(C5) Будь-який TP, який приймає UDI як вхідні дані, може виконувати дійсні перетворення лише для будь-якого можливого значення UDI. TP або приймає (перетворює на CDI), або відхиляє UDI. Тобто спеціальні ТП можуть коректно обробляти UDI, перетворюючи їх на CDI.

9.(E4) Лише спеціально уповноважена особа (користувач, агент, уповноважений сертифікувати об’єкти) може змінювати списки, визначені в правилах C3 та E2. Цей суб'єкт не має права вчиняти будь-які дії, якщо він уповноважений змінювати переліки, що регламентують ці дії.

Роль кожного з дев’яти правил моделі Кларка-Вілсона в забезпеченні цілісності даних у [10] співвідноситься з так званими теоретичними принципами політики контролю цілісності:

1) правильність здійснення операцій;

2) аутентифікація користувача;

3) мінімізація привілеїв;

4) розмежування функціональних обов'язків;

5) аудит подій, що відбулися;

6) об'єктивний контроль;

7) управління передачею пільг;

8) забезпечення безперервної продуктивності;

9) зручність використання захисних механізмів.

Відповідність правил моделі Кларка-Вілсона першим шести принципам, перерахованим вище, показано в табл. 1.

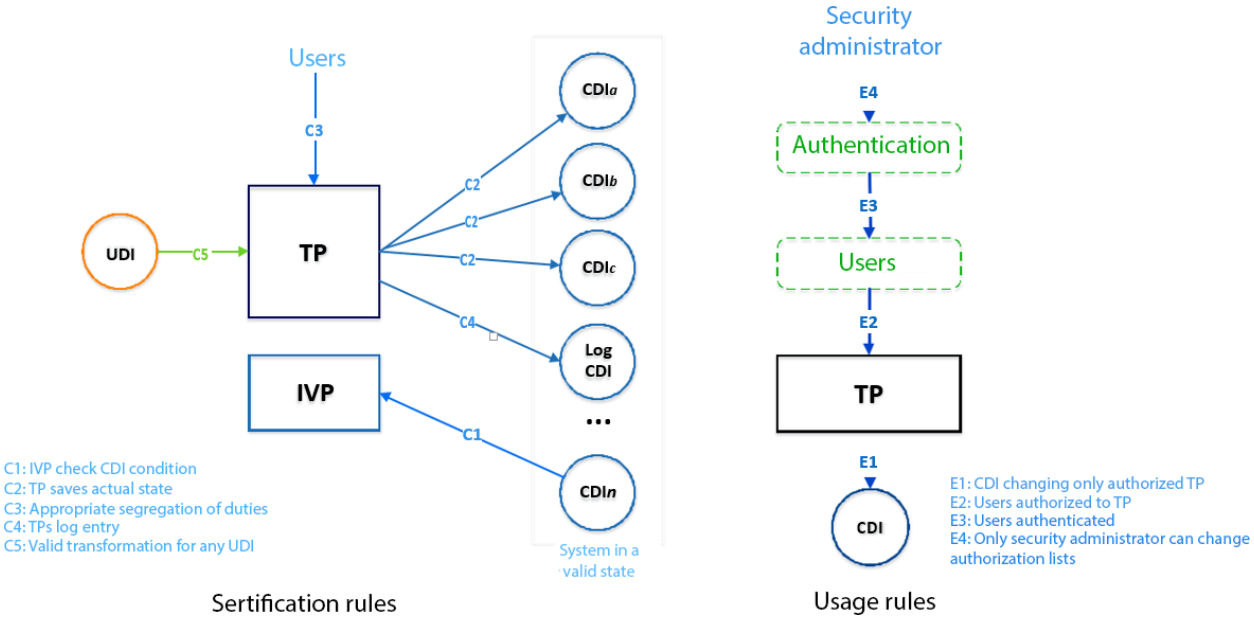
Правило моделі Кларка–Вілсона	Принципи політики контролю доброчесності
C1	1, 6
C2	1
C3	4
C4	5
C5	1
E1	3, 4
E2	1, 2, 3, 4
E3	2
E4	4

Як видно з табл. 1, принципи політики контролю доброчесності 1 (коректність транзакцій) і 4 (розподіл функціональних обов'язків) реалізуються більшістю правил моделі Кларка-Вілсона, що відповідає її основній ідеї.

На рис. 1 показана схема застосування цих правил для контролю роботи системи та даних. UDI представляють дані, які існують поза захищеною

системою. Правила сертифікації гарантують належну перевірку таких облікових даних для входу. Наприклад, правило C5 вимагає, щоб правильно сформовані TP, які перетворюють UDI на CDI, виконували лише перевірені перетворення. Правила C1 і C2 вимагають від CDI відповідати вимогам цілісності в початковому стані та після наступних перетворень. Правило C4 вимагає, щоб усі транзакції реєструвалися, як це зазвичай буває з базами даних. Логування бази даних більше для відновлення даних після збою, збою (для відкату - повернення до попереднього стану), а логування в моделі Кларка-Вілсона - для аудиту. Хоча бази даних також можуть мати журнал аудиту. Правило C3 вимагає відповідного розподілу обов'язків. Оскільки дані можна вводити лише відповідно до правил сертифікації, для систем, які нас цікавлять, усі дані в базі даних повинні бути CDI.

Правила виконання запобігають зміні CDI у спосіб, який суперечить IVP. Правила E2–E4 стосуються авторизації доступу до TP. У той час як E1 гарантує, що лише добре сформовані сертифіковані (підтверджені) TP можуть використовуватися для зміни CDI.



Мал. 1. Схема застосування правил моделі Кларка-Вілсона

Основним недоліком моделі Кларка–Вілсона є те, що IVP і пов’язані з ним методи непросто реалізувати в реальних комп’ютерних системах [11]. Наприклад, основною проблемою реалізації механізмів контролю цілісності файлових об’єктів є їх досить сильний вплив на завантаження обчислювального ресурсу системи, що зумовлено наступними причинами [12]: по-перше, може знадобитися контролювати великі обсяги інформації, що пов’язано зі значною тривалістю процедури IVP; по-друге, може знадобитися постійна підтримка файлового об'єкта в еталонному стані. У зв'язку з цим виникає питання: з якою частотою слід починати процедуру IVP? Якщо виконувати його часто, це призведе до значного зниження продуктивності системи, якщо рідко, то ефективність такого контролю може бути низькою. Тому одним із основних завдань при реалізації механізмів контролю цілісності файлових об’єктів є вибір принципів і механізмів запуску процедури перевірки цілісності CDI. Іншою проблемою реалізації механізму контролю цілісності є контроль цілісності самої керуючої програми, якщо контроль цілісності реалізовано програмно. Усе це потребує певного додаткового вивчення та прийняття відповідних рішень залежно, як правило, від характеристик конкретної ІС.

Однак у контексті СУБД можна значною мірою подолати зазначений вище загальний недолік моделі Кларка-Вілсона, пов’язаний зі складністю реалізації IVP і пов’язаних методів. Так, наприклад, для реляційної СУБД деякі обмеження цілісності закладені в теорії: цілісність сутності, посилальна цілісність. Інші можуть бути визначені як статичні обмеження за допомогою SQL (так звана декларативна підтримка обмежень цілісності). Ще інші, як динамічні обмеження цілісності (так звана процедурна підтримка обмежень цілісності), які можуть бути

реалізовані за допомогою тригерів і збережених програм. Усі вони забезпечують цілісність CDI, до яких звертаються та змінюють процедури перетворення TP.

Таким чином, традиційні СУБД підтримують багато механізмів моделі Кларка-Вілсона. Однак реалізації на основі стандартного SQL вимагають певних компромісів. Наприклад, популярний принцип розподілу (надання) прав доступу WITH GRANT OPTION (одержувачу переданих привілеїв надається привілей на подальшу передачу отриманих привілеїв, включаючи привілей на передачу привілеїв) суперечить моделі Кларка-Вілсона (правило E4).). Актуальними для СУБД також залишаються питання, пов'язані з механізмами контролю цілісності збережених процедур, функцій (як файлових об'єктів). Це зумовлює необхідність проведення додаткових досліджень у відповідних напрямках.Загалом, абсолютними перевагами цієї моделі є її відносна простота та легкість спільного використання з іншими моделями безпеки.

РОЗДІЛ 2 ДІЇ ПО ВИЯВЛЕННЮ ЗАГРОЗ ТА ЇХ КЛАСИФІКАЦІЯ

2.1 Допоміжні моделі для виявлення загроз

Модель Біба

Модель Біба [13] була розроблена після моделі Белла–ЛаПадули [14]. З точки зору змісту та формального (математичного) представлення, ця модель є інверсією мандатної моделі Белла-ЛаПадули, проблема якої полягає в тому, що вона розроблена для збереження конфіденційності без гарантії цілісності даних.

Основні елементи моделі Biba:

- S – множина предметів;

- O – множина об’єктів, S ∩ O = □

- □ LI = (*LI*,□□, ,□)– решітка рівнів цілісності:

LI = {важливий, дуже важливий, вирішальний}, де важливий<дуже важливий<вирішальний;

-RI = {модифікувати, викликати, спостерігати, виконувати} – набір типів доступу, де модифікувати – доступ

Bella - LaPadula), execute - доступ до виконання;

- B={b ⊆S x O x RI} – множина можливих наборів поточних доступів у системі;

- (is , io , ic) ∈ I = LIS x LIO x LIS - це трійка функцій (is , io , ic), що визначає: is : S → LI –

рівень цілісності суб'єктів; io : O → LI – рівень цілісності об’єкта; ic : S → LI –

поточний рівень цілісності суб’єктів, при цьому для кожного s ∈ S виконується умова ic (s) ≤ is (s);

-V = B x I – множина станів системи.

Основні властивості або аксіоми моделі Біба (відповідно до політики суворої цілісності) можна сформулювати наступним чином:

1. Проста властивість цілісності. Суб'єкт з рівнем is (s) може зчитувати інформацію, що міститься в об'єкті з рівнем цілісності io (o), тоді і тільки тоді, коли рівень цілісності об'єкта io (o) переважає над рівнем цілісності суб'єкта is (s) (is (s) ≤ io (o)); іншими словами, суб'єкт не може прочитати об'єкт на нижчому рівні цілісності (так зване правило без читання (NRD)).

2. Властивість * цілісності. Суб’єкт із рівнем цілісності (s) може змінювати інформацію, що міститься в об’єкті з рівнем цілісності io (o), якщо і тільки якщо рівень цілісності суб’єкта (s) переважає над рівнем цілісності об’єкта io (o) (io (o) □ is (s)); іншими словами, суб’єкт не може модифікувати об’єкт на вищому рівні цілісності (так зване правило без запису (NWU)).

3.Властивість invoke вказує, що суб'єктам дозволено викликати суб'єкти лише рівного або нижчого рівня, тобто для ∀ s[1], s[2] ∈ S, s[1] може викликати s[2] лише тоді, коли є (s[2]) □ є (s[1]).

Перші дві властивості цієї моделі є зворотними до двох відповідних властивостей моделі Белла-ЛаПадули. А саме, правило NRD є прямою протилежністю правила NRU моделі Белла-ЛаПадули, за винятком того, що модель Біба використовує рівні цілісності, а не рівні безпеки (конфіденційності), як у моделі Белла-ЛаПадули. Правило NWU мандатної моделі цілісності Biba є прямою протилежністю правила NWD моделі Белла-ЛаПадули для випадків рівнів цілісності, а не безпеки.

Діаграму інформаційних потоків, що відповідає моделі Біба в системі з двома рівнями цілісності, можна представити наступним чином (рис. 2).

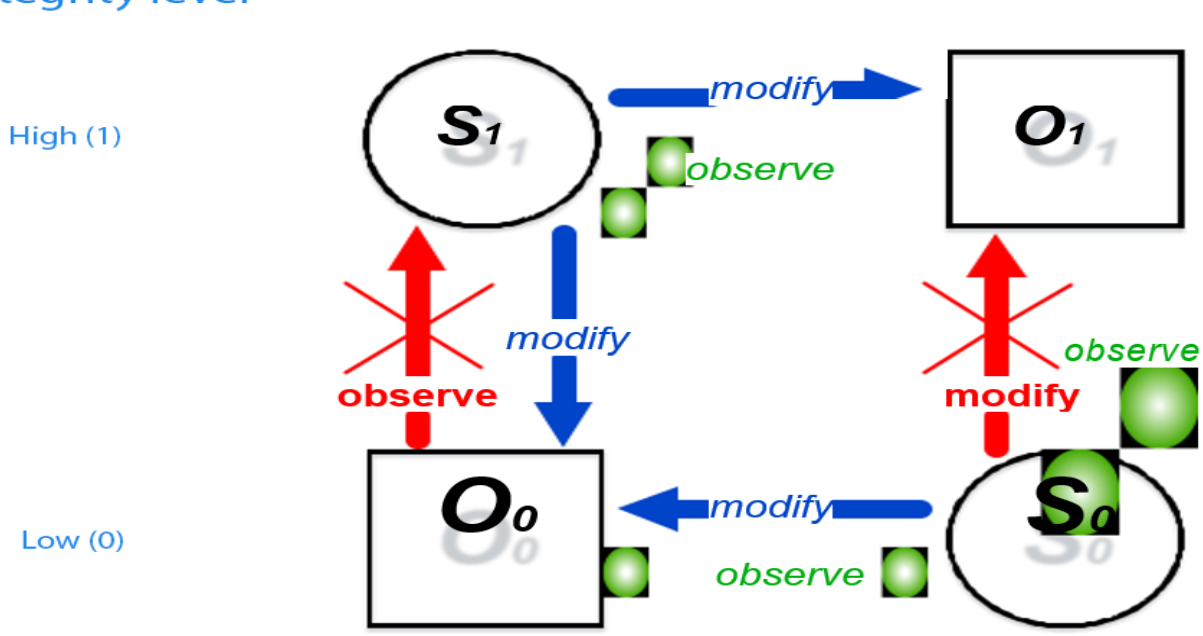


Рис. 2. Діаграма інформаційних потоків у системі з двома рівнями цілісності

У реальних ІБ рідко існують системи безпеки, орієнтовані виключно на забезпечення конфіденційності або виключно на забезпечення цілісності інформації. При створенні захищених систем багато хто хотів би поєднати

обидва механізми, використовуючи різні формальні моделі безпеки, в тому числі такі як моделі Белла-ЛаПадули та Біба. Це непросте завдання. Нижче наведено можливі варіанти спільного використання моделей Белла-ЛаПадули та Біба та ускладнення, які при цьому виникають [3, 15, 16]:

1. Дві моделі можуть бути реалізовані в системі незалежно одна від одної. У цьому випадку суб'єктам S і об'єктам O незалежно призначаються рівні конфіденційності та рівні цілісності на основі двох різних сіток. Рішення про безпеку доступу приймається одночасно за правилами обох моделей.

2. Логічне поєднання моделей на основі однієї загальної сітки рівнів безпеки (конфіденційність/цілісність).

У таких системах дозволено лише доступ суб'єктів до об'єктів одного рівня безпеки (рис. 3).

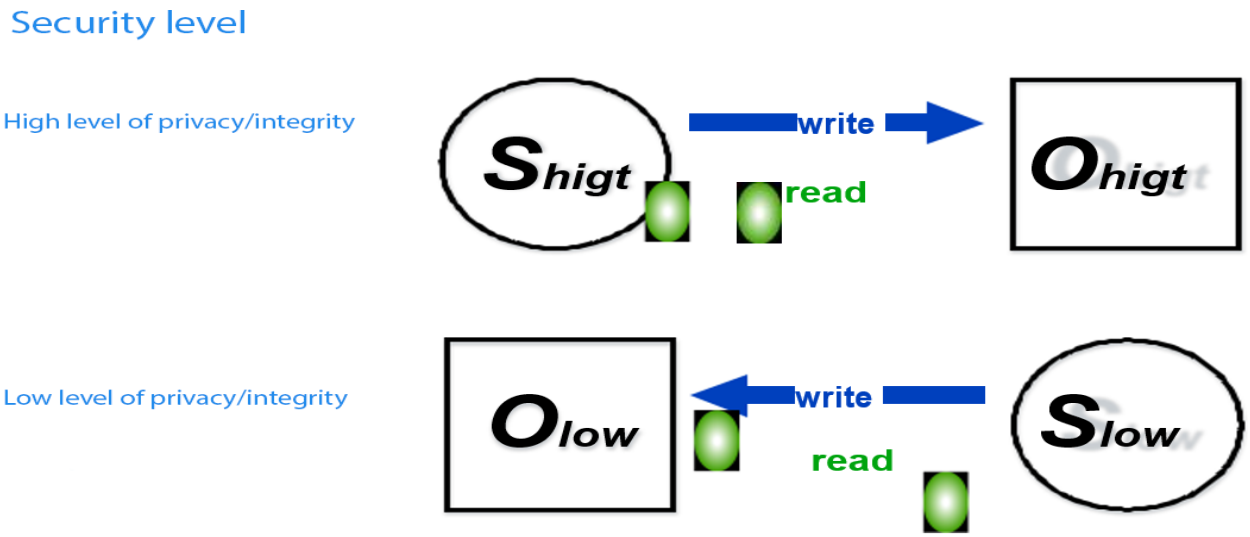


Рис. 3. Спільне використання моделей Bell-LaPadula і Biba (доступ в межах одного рівня безпеки)

3.Логічне поєднання моделей на основі однієї загальної решітки, але з двома мітками безпеки: конфіденційності та цілісності з протилежним характером їх визначення. Суб'єкти та об'єкти з високими вимогами до конфіденційності (наприклад, секретні дані та користувачі, яким довіряють секрети),

розташовані на високих рівнях ієрархії решітки. Суб'єкти та об'єкти з високими вимогами до цілісності (наприклад, системне програмне забезпечення та програмісти) розташовані на нижніх рівнях ієрархії решітки (рис. 4).

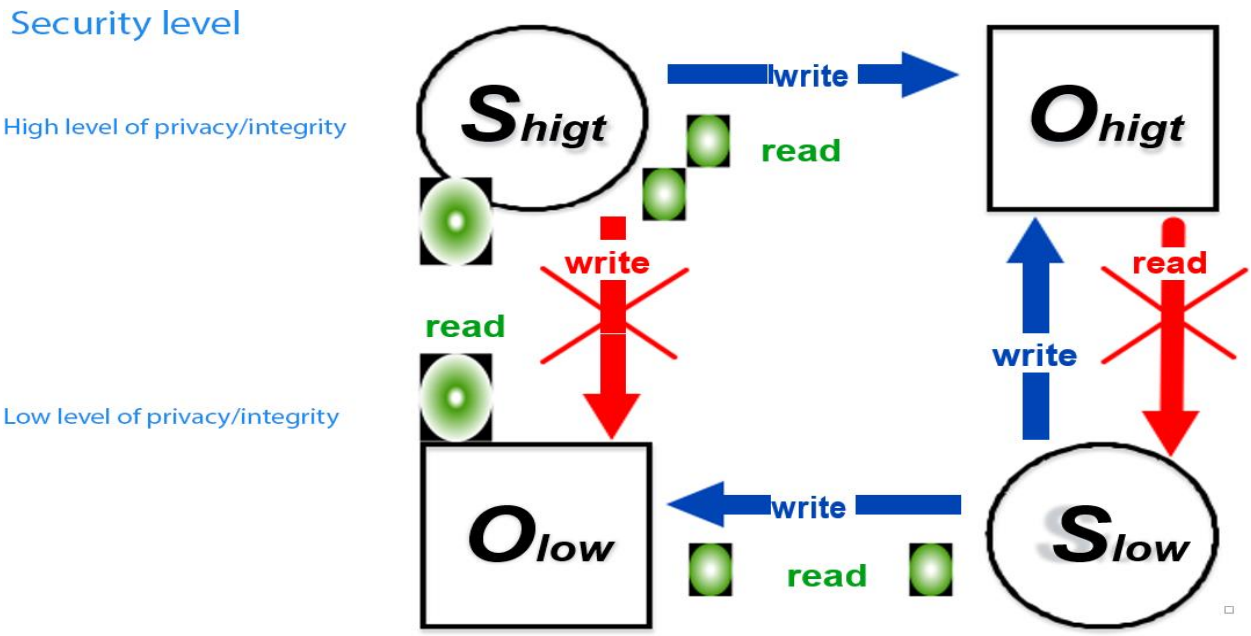


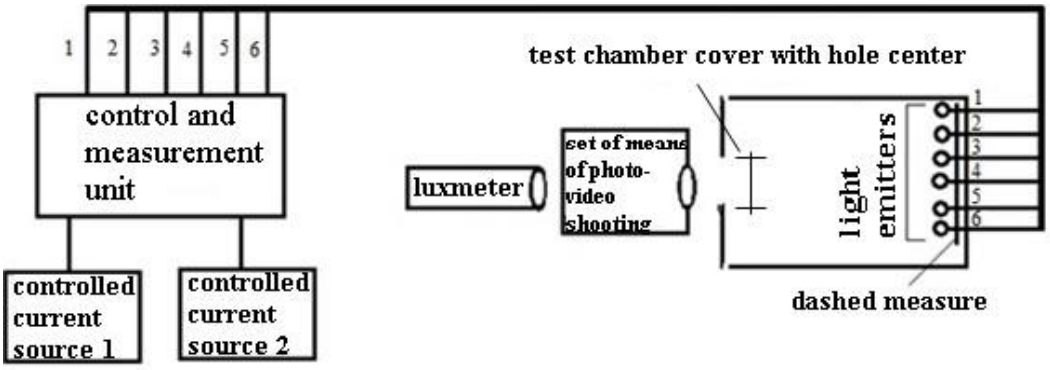
Рис. 4. Спільне використання моделей Bell-LaPadula і Biba (на основі однієї решітки з двома захисними мітками) Незважаючи на складність класифікації суб'єктів та об'єктів доступу, саме третій варіант використовується в сучасних ІС, зокрема в СУБД, де реалізована обов'язкова політика безпеки [3].

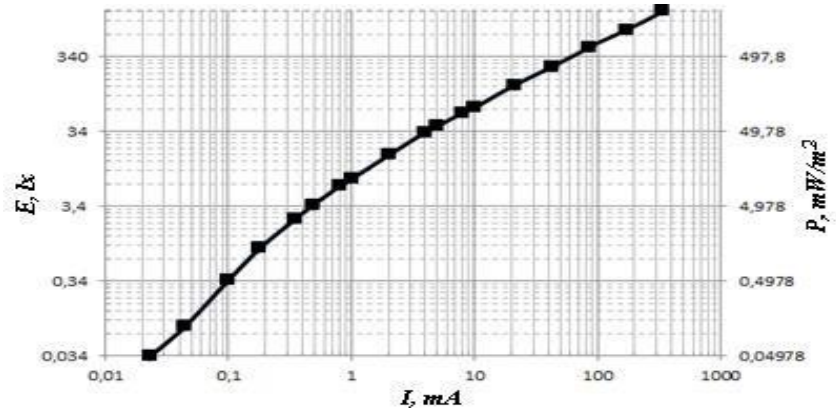
Оскільки суб'єкти та об'єкти з високою цілісністю знаходяться в нижній частині ієрархії, а компоненти з низькою цілісністю – у верхній частині ієрархії, правила заборони читання та запису імітують обов'язкову модель цілісності Біби в моделі Белла-ЛаПадули структура. Тобто читання зверху в ієрархії моделі Белла–ЛаПадули є читанням знизу в ієрархії моделі Біба. Подібним чином запис угору в моделі Белла–ЛаПадули є записом у моделі Біби. На практиці це дозволяє шляхом розміщення системних файлів (об'єктів О), у тому числі пов'язаних із СУБД, і суб'єктів адміністратора (їх процесів) у нижній частині ієрархії моделі Белла-ЛаПадули захистити цілісність таких

об’єктів від звичайних. суб'єкти - користувачі (та їхні процеси), оскільки правило заборони запису забороняє їм записувати в системні файли. Крім того, якщо ми розглядаємо виконання як читання, то адміністративні суб’єкти (і їхні процеси) не зможуть виконувати програми за межами найвищого рівня цілісності (або нижчого рівня ієрархії моделі Белла-ЛаПадули).Ця схема захищає системні файли від зловмисного програмного забезпечення троянського коня, оскільки якщо таке зловмисне програмне забезпечення знаходиться на одному з верхніх рівнів, воно ніколи не зможе пошкодити системні файли через необхідність виконання правила заборони запису. Таким чином, така комбінація моделей забезпечує захист безпеки для верхніх рівнів певної ієрархії та захист цілісності для нижніх рівнів [16].

Підсумовуючи, варто зазначити, що існуючі теоретичні розробки та практичні реалізації безпеки ІБ базуються не лише на парадигмі формального моделювання політики безпеки, а й на іншій не менш важливій парадигмі – криптографії, спрямованій на вирішення певних завдань. Більше того, ці підходи, різні за походженням і завданнями, що вирішуються, доповнюють один одного: криптографія пропонує відповідні методи та примітиви для захисту інформації, забезпечення ідентифікації, автентифікації, шифрування, контролю цілісності даних, а формальні моделі безпеки забезпечують розробникам захищеної ІР фундаментальну інформацію. загальні принципи, що лежать в основі архітектури захищеної системи та визначають концепцію її побудови [17].Видається доцільним проведення подальших досліджень, результатом яких стане певна методологія комплексного використання різних моделей безпеки при проектуванні та функціонуванні відповідних ІС та їх основної функціональної складової – бази даних, що призведе до підвищення ефективності їх захист

2.2 Аналіз та знаходження загроз





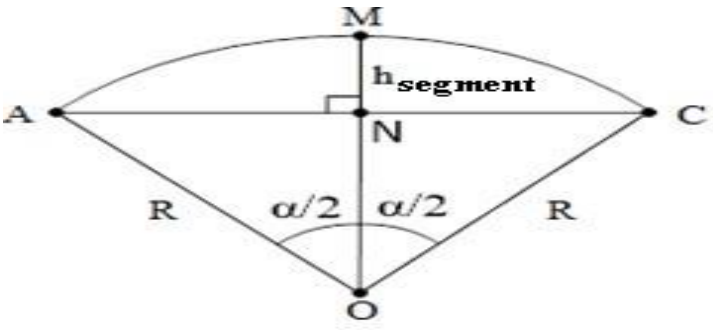


Рис. 3. Графічне пояснення розрахунку

Величина щільності потоку потужності (P), що падає на кришку випробувальної камери, може бути визначена як

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

де □□□ – площа сферичного сегмента, сферичної поверхні, переріз якої відповідає кривій AMS (рис. 3).

За визначенням

$$S_{ss} = 2\pi R \cdot h_{segment} \quad (2)$$

де R – радіус сфери, AO = MO = CO = R (Fig. 3); $h_{segment}$ – висота кульового сегмента, MN = $h_{segment}$,

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

З обчислення трикутника AHO маємо

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

Оскільки MO = AO = R, тоді:

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

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

Підставляючи формулу (3) у формулу (2), отримуємо

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

Тому вираз для розрахунку густини потоку потужності P випромінювачів IE – смуга матиме вигляд

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

Примітка: при α = 360 град. P приймає форму добре відомого виразу для обчислення щільності потоку потужності, створеної ізотропним випромінювачем: $\mathrm{P} = \frac{P}{2\pi R^2}$,[W/m^2].

Для розрахунку P випромінювачів видимого діапазону використовується формула (1):

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

де Ev =F/S, F – номінальне значення інтенсивності випромінюваного світла, яке відомо з технічного опису світлодіодів (Luminous Intensity); α – значення кута, під яким світлодіод випромінює 50% світлової енергії (50% Power Angle, з технічного опису світлодіодів);

Для побудови кривої спектральної чутливості було визначено коефіцієнт С, який дорівнює відношенню густини потоку потужності еталонного світлодіода з еквівалентною яскравістю, визначеного за графіком, отриманим на попередньому кроці (рис. 1), до щільність потоку потужності тестового світлодіода.

Залежність коефіцієнта С від довжини і є спектральною чутливістю.

В ході експерименту визначено спектральну чутливість вищезазначених засобів фоторозвідки та відеозапису. Отримані результати усереднювали та зображали у вигляді графіків, рис. 4.

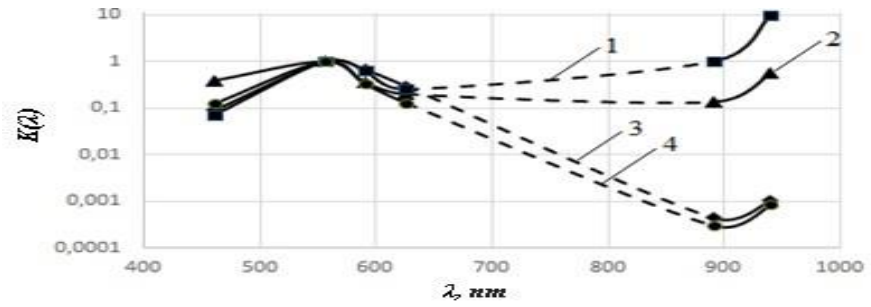


Рис. 4. Графіки усередненої спектральної чутливості досліджуваних засобів фоторозвідки та відео: 1 – камери нічного відеоспостереження; 2 – автомобільний відеореєстратор; 3 – камера мобільного телефону; 4 – цифровий фотоапарат

2.3 Цілі та мета реалізації загроз

Експериментальне дослідження ефективності протидії засобів Після визначення спектральної чутливості обраних приймачів було проведено експериментальне дослідження ефективності відгуку досліджуваним методом шляхом визначення ефективного радіуса плями освітлення, яку створює інфрачервоний світлодіод.

Методика вимірювання передбачає використання описаного вимірювального приладу і зеленого світлодіода. Установка розташована на поверхні горизонтально, перед нею знаходиться досліджувана камера, досліджуване поле освітлюється штучним джерелом світла, амперметр підключений до зеленого світлодіода.

Як тестове поле для вимірювань було підготовлено пунктирну мірку з отвором у центрі для світлодіода (рис. 5). Це зображення ліній у вигляді білих і чорних кіл різного діаметру, які об'єднані секторами. Крок мірки (сумарна ширина білих і чорних ліній) 50 мм, товщина всіх ліній всередині сектора однакова. Є 8 секторів з товщиною лінії: 0,5; 1; 2; 3; 4; 5; 6; 7 мм. Вимірювання проводили в приміщенні без доступу денного світла. Дзеркальна фотокамера Canon EOS 1100D обрана як тестовий інструмент для тестування фотографічного інтелекту.

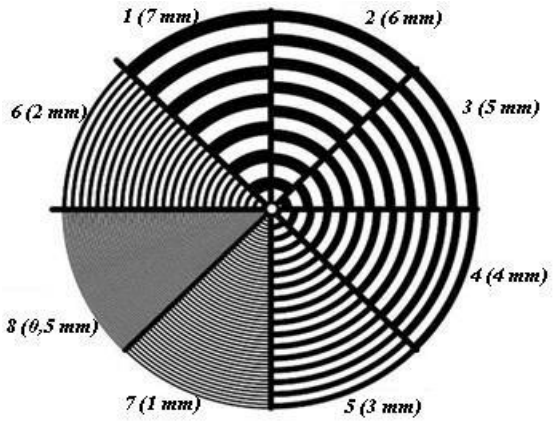


Рис. 5. Штрихова міра для експериментального визначення ефективного радіуса плями освітлення

Стержневу міру розташовували в випробувальній камері установки так, щоб еталонний світлодіод збігався з її центром. Тестова камера розташовувалася на певній відстані від тестової камери, після чого була зроблена серія фотографій тестового поля з поступовим збільшенням струму живлення світлодіода до максимального значення. Потім зображення було оброблено у Photoshop, який визначив радіус прожектора в пікселях, у межах якого роздільна здатність камери є більшою за номінальну, а потім перераховано до лінійної міри (см) (тобто радіус плями, створеної зеленим світлодіодним випромінюванням і який змащує зображення штрихів спочатку виділеного сектора і не дозволяє розпізнати їх на зображенні як окремі елементи). Перерахунок радіуса плями освітлення проводили за формулами:

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

де $R_{s.cm}$ – величина радіуса плями освітлення, в сантиметрах; $R_{s.rel}$ – t Радіус плями освітлення виражається відносною величиною; $R_{m.cm}$ – радіус досліджуваного поля, сантиметри;

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

де $R_{s.p.}$ – радіус плями освітлення, в пікселях; $R_{m.p.}$– радіус вимірювання, у пікселях.

Контраст тестового поля також визначався для кожного значення радіуса плями (і відповідного струму живлення)

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

де E_i – загальна освітленість досліджуваного поля, виміряна люксметром; $E_{t.f.}$ – початкове (до вимкнення зеленого світлодіода) освітлення тестового поля.

За отриманими результатами побудовано графік залежності ефективного радіуса плями освітлення від контрасту (рис. 6).

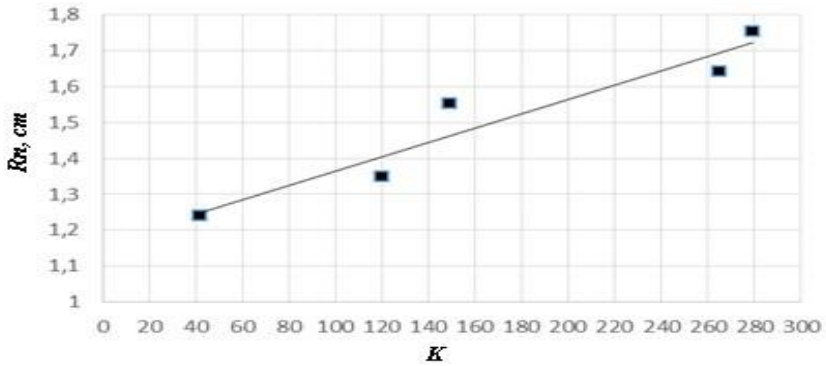


Рис. 6. Графік залежності ефективного радіуса прожектора від контрасту

За результатами експериментів оцінено необхідну потужність інфрачервоних світлодіодних випромінювачів для протидії (розпачу) досліджуваної камери Canon EOS 1100D. Для цього припустимо, що випромінювач ІЕ повинен створити пляму освітлення максимального радіуса, який забезпечує зелений світлодіод при максимальному струмі живлення (див. рис. 6, Rs=17,5 см). Знайдено необхідні значення потужності світлодіодів для різних умов освітлення об’єкта (день,

сутінки, офісне приміщення). Передбачалося, що чутливість приймачів до ІЕ світлового і видимого діапазонів однакова, фронт хвилі плоский, щільність потоку потужності не залежить від відстані, а тестове поле відбиває все падаюче світло в напрямку камера. Площа освітлення розраховувалась по радіусу R.

З технічного опису світлодіодів відомо, що випромінювана потужність зеленого світлодіода становить 1 Вт, максимальний струм живлення 340 мА, при щільності потоку потужності випромінювання P = 2,043 Вт/м2 (див. формулу (1)).

Наступним кроком була оцінка величини електричної потужності інфрачервоного випромінювача з а

довжина хвилі λ = 940 нм, що створює щільність потоку потужності, таку ж, як використовувався в експерименті зелений світлодіод (2,043 Вт/м2).

Відповідно до технічного опису світлодіода, тобто відомих значень номінального струму I і напруги U на світлодіоді, можна розрахувати електричну потужність даного ІЕ - випромінювача:

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

Після підстановки числових значень було отримано □□□ = 1,4 Вт, що відповідає щільності потоку потужності ІЕ світла P = 1,59 Вт/м2. Щоб знайти електричну потужність □□□1, при якій він буде випромінювати P = 2043 Вт/м2, припустимо, що значення P пропорційне електричній потужності світлодіода. Потім, обчисливши пропорцію, знаходимо значення □□□1= 1,8 Вт.

З графіка залежності ефективного радіуса плями освітлення на контрасті можна зробити висновок, що для забезпечення плями освітлення площею 96 мм світлодіод повинен створювати освітленість, що перевищує освітленість досліджуваного поля в 279 разів (C = 279, рис. 6). Коефіцієнт відбиття пробного поля ρ, визначений перед фотографуванням пробного поля, становить 0,18. За цими значеннями визначили величину P□□□□ – густину потоку потужності зустрічного випромінювача, яка необхідна для освітлення зазначеної ділянки в сутінках (згідно [4]Ev = 5 лк:

$$P_{dusk} = C \cdot \rho \cdot P_{f.t.} \text{[W/m2]},$$

де $P_{f.t.}$ – густина потоку світла, що падає на дослідне поле, розраховується за формулою (1) за величиною Ev і дорівнює 7 мВт/м2; f_0□ · P□.□.– густина потоку потужності, відбитої від поля за заданих умов освітлення.

2.4 Розвиток захисту від загроз та протидія появленню нових загроз

3 В даний час спостерігається швидкий прогрес у створенні квантових комп'ютерів для вирішення різноманітних обчислювально складних завдань і для різних цілей. Водночас докладаються спеціальні зусилля для створення такого квантового комп’ютера, який зможе вирішити проблеми криптоаналізу існуючих криптосистем – асиметричних шифрів, протоколів інкапсуляції ключів, електронних підписів. Запобігання таким загрозам можна досягти шляхом розробки криптографічних систем, які будуть захищені як від квантових, так і від класичних атак, а також зможуть взаємодіяти з існуючими протоколами та мережами зв’язку. Також існує значна потреба в захисті від атак сторонніх каналів.

4 Зараз значні зусилля криптологів зосереджені на відкритому конкурсі NIST PQC. Основна ідея конкурсу полягає у визначенні математичних методів, на основі яких можна розробити стандарти для асиметричних криптовалют, насамперед електронного підпису (ЕП), а також асиметричних шифрів і протоколів інкапсуляції ключів. За підсумками другого етапу фіналістами третього етапу конкурсу NIST PQC стали три схеми EC - Crystals-Dilithium, Falcon і Rainbow. Наразі комплексний аналіз фіналістів є важливим завданням для всього криптоспільноти. Переважна більшість схем, які стали фіналістами, засновані на задачах теорії алгебраїчних решіток. Також особливу увагу було приділено схемі Rainbow ES, яка базується на багатовимірних перетвореннях.

5 Схема Rainbow EP значно відрізняється від інших кандидатів NIST, оскільки вона заснована на багатовимірних перетвореннях. Він є узагальненням структури УОВ, що забезпечує ефективну параметризацію алгоритму ЕП за рахунок додаткової алгебраїчної структури. Теоретична

безпека Rainbow базується на тому факті, що розв’язання набору випадкових багатовимірних квадратичних систем є NP-комплексною проблемою. Автори методу Rainbow стверджують, що досягли моделі безпеки EUF-CMA, заснованої на використанні хеш-структури з випадковим або псевдовипадковим сеансовим ключем (salt). Також пропонуються дуже маленькі EP, буквально лише кілька сотень біт (лише 528 біт (66 байт) для рівня безпеки NIST I). Порівняно з іншими кандидатами NIST для постквантової схеми ES, вони набагато коротші. Крім того, оскільки Rainbow використовує лише прості операції над малими скінченними полями, процеси створення та перевірки підпису надзвичайно ефективні [6]. Крім того, діапазон параметрів Rainbow дозволяє оптимізувати їх застосування в широкому діапазоні випадків. Схема Rainbow EP також вивчалася в інших контекстах і має деякі переваги, в тому числі, наприклад, у програмах з низьким ресурсом

6 Показано, що для забезпечення криптографічної стійкості Rainbow EP необхідно обґрунтувати вимоги та побудувати набори загальносистемних параметрів, які забезпечують стійкість до класичних та квантових атак. Визначаючи вимоги до системних параметрів схеми Rainbow NIST, конкурс зосереджувався на загальносистемних параметрах, які забезпечуватимуть 256 біт стійкості проти класичного та до 128 біт проти квантового криптоаналізу. Ці обмеження, на нашу думку, зумовлені частково складністю обчислення загальносистемних параметрів, а також значним впливом їх збільшення на швидкість електронного підпису. Однак, враховуючи поточне застосування симетричних криптовалют на рівні 512-бітної стабільності, ми вважаємо, що вже необхідно розглядати та реалізовувати на базі схеми Rainbow ES зі стійкістю до 512 біт. Але для цього необхідно обґрунтувати основні положення та вимоги до

загальносистемних параметрів таких довжин, а також безпосередньо їх побудувати. При цьому повинна бути забезпечена криптографічна стійкість до класичних і квантових атак відповідного значення, а також захист від атак сторонніми каналами.

7 Метою цієї статті є попередній аналіз існуючих атак на перспективний електронний підпис Rainbow, визначення вимог до загальносистемних параметрів для забезпечення криптографічної стабільності, включаючи щонайменше 512 біт проти класичного та 256 біт проти квантового криптоаналізу, а також розробка та практичне впровадження алгоритмів Rainbow 512 біт проти класичного та 256 біт проти квантового криптоаналізу.

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.