МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ "ЛЬВІВСЬКА ПОЛІТЕХНІКА"

Кваліфікаційна наукова праця
на правах рукопису

КУТЕНЬ РОМАН БОГДАНОВИЧ

УДК 621.394/.396.019.3

ДИСЕРТАЦІЯ

ПОКРАЩЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ ПРИ ПЕРЕДАЧІ БЕЗДРОТОВИМИ СИСТЕМАМИ

125 Кібербезпека та захист інформації
(шифр і назва спеціальності)

12 Інформаційні технології
(галузь знань)

Подається на здобуття наукового ступеня доктора філософії

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ /Кутень Роман Богданович/

Науковий керівник:
Пархуць Любомир Теодорович,
доктор технічних наук, професор

Львів – 2024

АНОТАЦІЯ

Кутень Р. Б. Покращення захисту інформації при передачі бездротовими системами. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 125 "Кібербезпека" (12 – Інформаційні технології). – Національний університет "Львівська політехніка", – Львів, 2024.

Дана дисертаційна робота присвячена вирішенню актуальної науково-прикладної задачі – підвищення стабільності, захищеності і відмовостійкості процесу передавання інформації у бездротових системах та забезпечення достатнього рівня прихованості та захищеності параметрів сигналу, а також задачі забезпечення можливості роботи засобів бездротового зв'язку та керування в умовах активного електромагнітного протиборства (в тому числі із застосуванням засобів радіоелектронної боротьби).

Забезпечення захисту інформації в інформаційних та кіберфізичних системах залишається однією із найсерйозніших проблем і важливим завданням у сфері інформаційної безпеки. За сучасного розвитку комунікаційних технологій особливо гостро ця проблема постає в контексті використання бездротових систем зв'язку на основі радіохвиль. Оскільки передача здійснюється відкритим радіоефіром, то будь-хто, хто має відповідне обладнання, має можливість отримати доступ до передаваного сигналу і до приймально-передавального тракту загалом. За наявності необхідних навичок та техніки зловмисник може перешкоджати роботі бездротової системи, виводити з ладу канали зв'язку, викрадати дані, підробляти дані, тощо.

За останні роки проведено багато досліджень в галузі забезпечення захисту систем бездротового зв'язку та забезпечення його завадостійкості. Чимало робіт присвячені підвищенню дальності роботи систем бездротового зв'язку. Розроблено великий спектр криптографічних систем і протоколів обміну даними, розроблені протоколи та методи для забезпечення надійності зв'язку в

умовах випадкових завад, розділення каналів зв'язку для багатокористувацького доступу. Багато досліджень присвячено захисту власне фізичного рівня передавання інформації, тобто маскування за допомогою шумових сигналів із широким спектром і хаотичною структурою, маскування за допомогою псевдовипадкового переналаштування робочої несучої частоти.

У даній роботі основна увага зосереджується на питаннях захисту бездротових систем зв'язку, які через широкомасштабне російське вторгнення в Україну почали масово використовуватись збройними силами України для належного покриття комунікаційних потреб.

Однією з таких систем, які найкритичніше потребують захисту, є системи зв'язку та керування безпілотними апаратами, зокрема безпілотними літальними апаратами (БПЛА) або так званими "дронами". Їхня роль у воєнних конфліктах стає чим далі важливішою і спектр застосування дронів за останній час значно розширився: якщо колись це була тільки розвідка і нагляд, то тепер існують апарати, які вміють наносити безпосереднє вогневе ураження ("БПЛА-камікадзе"), здійснювати скиди засобів ураження, здійснювати доставку провізії та боєприпасів наземним підрозділам і навіть проводити дистанційне мінування інженерними засобами.

Проведені дослідження включають аналіз можливостей застосування існуючих засобів захисту інформації при передачі бездротовими каналами у сучасних малогабаритних безпілотних авіаційних комплексах, а також розробку нових моделей захисту, які розраховані на застосування безпосередньо у інформаційних та кіберфізичних системах, що здатні до самостійного переміщення.

Об’єктом дослідження є захищеність каналів бездротового зв’язку, зокрема бездротових каналів керування, відслідковування телеметрії та іншого обміну даними з безпілотними засобами (у тому числі БПЛА подвійного та військового призначення).

Предметом дослідження є методи забезпечення маскування сеансу передачі, приховування частот несучих сигналів, шифрування даних, які

передаються бездротовими мережами, автентифікації приймача-передавача, методи забезпечення цілісності даних та підвищення їх стійкості до завад, у тому числі навмисно створених засобами просторового зашумлення та радіоелектронної боротьби (РЕБ).

У першому розділі "**Основні відомості щодо передавання інформації у інформаційних системах та мережах**" проведено огляд вітчизняної та зарубіжної наукової літератури. На основі чого було проаналізовано аспекти застосування інформаційних мереж для обміну і передавання даних, використовувані в них технології і проаналізовано їх поточне використання в цивільній та військовій сферах.

Визначено, що інформаційні технології та бездротові системи зайняли провідне місце у багатьох сферах діяльності: від повсякденних побутових потреб аж до військових застосувань. На використанні бездротових технологій базуються такі сучасні системи як: системи зв'язку, засоби ведення підприємницької діяльності, бізнесу, логістика та транспортні технології, енергетика, системи "розумне місто", "розумний будинок", банківські системи, тощо. Одним із виявлених аспектів також є те, що високий розвиток технологій бездротового зв'язку, зменшення габаритів пристроїв доступу до радіоефіру стали ключовими факторами, які сприяли розвитку невеликих вбудованих систем та зокрема, безпілотних пристроїв, що є передовим напрямком розробок в більшості галузей сучасних технологій.

Аналогічні тенденції спостерігаються і для систем зв'язку військового призначення. У теперішніх реаліях проведення бойових дій та із досвіду АТО і ООС видно, що основою систем зв'язку військового призначення стали саме бездротові системи, які працюють із використанням радіохвиль, оскільки радіозв’язок дає перевагу у мобільності швидкості розгортання тощо. По аналогії із розвитком цивільних систем спостерігаємо також розвиток використання і застосування безпілотних пристроїв для виконання військових завдань в сучасних збройних конфліктах. Зокрема в захисті територіальної цілісності України безпілотні комплекси застосовуються для розвідки,

спостереження, коригування роботи артилерії, для нанесення ураження (безпілотник-камікадзе), для скидання боєприпасів (так звані "бомбери") та для налагодження і покращення основної системи зв'язку (безпілотники-ретранслятори).

Основною проблемою, виявленою в ході аналітичного огляду, є те, що через широкий масштаб російського вторгнення і велика протяжність лінії фронту породили величезні запити на системи зв'язку та системи безпілотних пристроїв зі сторони збройних сил України. Потужностей виробництва і наявних засобів у Міноборони недостатньо, тому це спричинило використання у військовій сфері засобів зв'язку цивільного походження, зокрема, використання для безпілотних операцій безпілотників цивільного походження та призначених для хобі польотів. Така проблема вимагає негайного реагування і забезпечення можливості впровадження належних засобів захисту для таких пристроїв.

У другому розділі "**Проблематика захисту інформації при передаванні бездротовими системами**" детально розглянуто існуючі підходи до проблеми захисту інформації при передачі її у бездротових системах. Базуючись на попередніх результатах досліджень із першого розділу, основний аналіз всіх можливих засобів і концепцій захисту інформації в каналах зв'язку проводився в контексті можливості та способів їх застосування у безпілотних авіаційних системах, зокрема, системах цивільного походження, які почали широко використовуватися у військових цілях.

Визначено основні потреби у захисті пристроїв цивільного походження, які диктуються їхнім військовим використанням: потенційно такі засоби не мають здатності до надійного функціонування, тобто є потреба забезпечення функціонування пристроїв в умовах туману, дощу, снігу, сильних поривів вітру, тощо. Такі пристрої потребують впровадження або розробки нових надійних систем шифрування та кодування каналів, оскільки базових засобів для військового користування є недостатньо. Цивільні бездротові системи і пристрої в принципі не розраховані на роботу в умовах використання

противником засобів радіо-електронної розвідки, радіо-електронної боротьби, радіо-пеленгаційних станцій, пристроїв придушення тощо.

Проведено аналіз структури моделі системи функціонування відкритих систем OSI. Це дало можливість при подальшому аналізі додатків і застосунків, використовуваних на тому чи іншому рівні моделі взаємодії, зробити певне ранжирування методів та засобів захисту інформації при її передаванні, відповідно до рівня функціонування того чи іншого методу.

Незважаючи на те, що існує велика кількість сучасних підходів до забезпечення захисту інформації при передачі бездротовими системами, огляд та аналіз сучасних досліджень і публікацій, проведений у даному розділі, вказує на гостру необхідність модифікації існуючих засобів та розроблення принципово нових методів для запобігання перехопленню інформації, придушення каналів зв'язку на найнижчих рівнях моделі OSI, зокрема на фізичному та канальних рівнях, які можна буде використовувати у безпілотних пристроях із дистанційним бездротовим керуванням (які зазвичай є автономними засобами із живленням від акумулятора). Таку потребу диктує той факт, що більшість запропонованих сучасних методів захисту, поряд із своєю високою ефективністю і високим рівнем захисту, вимагає досить високих ресурсозатрат. Це стосується як і обсягу обчислень і об'єму необхідної пам'яті, так і фізичних габаритів тих чи інших застосунків для забезпечення захисту маскування чи приховування передачі інформації.

У третьому розділі "**Покращення захищеності бездротових систем керування та зв’язку в контексті БПЛА**" запропоновано та науково обґрунтовано нову ідею для покращення стійкості та захищеності каналу зв'язку безпілотного пристрою перед засобами РЕБ. Запропоновані та розроблені методи покращення існуючих методів та засобів захисту. Запропоновані методики мають вагоме значення в питаннях захисту інформації в системах зв'язку і керування безпілотних пристроїв.

Перш за все, для реалізації кожного з методів було додатково проведено попередній аналіз використовуваних в тому чи іншому апараті схемотехнічних

рішень, після чого усі розроблювані методи опиралися на результати цього аналізу. Механізм роботи запропонованих методів був вибудуваний так, щоб максимально забезпечити практичну реалізацію кожного методу захисту за рахунок власних можливостей базових компонентів безпілотного апарату.

Це дозволило впровадити максимально ефективні засоби захисту інформації як для передачі відеосигналу від БПЛА, так і для забезпечення підвищення доступності апарату (забезпечення збереження працездатності каналів зв'язку в умовах активного використання засобів РЕБ).

Запропоновано підхід до реалізації заходів захисту на основі використання вбудованої системи, яка являє собою додатково встановлений мікроконтролер. Мікроконтролер функціонує в режимі "менторства" і втручається лише у випадку позаштатної ситуації або увімкнення відповідного алгоритму реалізації засобу захисту. Втручання його полягає виключно у адаптивному керуванні налаштуваннями існуючих елементів БПЛА.

Для забезпечення конфіденційності відеоканалу безпілотника за основу взято метод частотного переналаштування, який було адаптовано для використання у безпілотному малогабаритному пристрою, а також покращено рівень ресурсозатрат шляхом його реалізації через керування параметрами VTX за допомогою мікроконтролера через протокол SmartAudio.

Додатково для захисту конфіденційності вперше було запропоновано використати як метод захисту менеджмент потужності сигналу, який полягає у адаптивному збільшенні/зменшенні потужності передачі відео, в залежності від віддалення/зближення безпілотника до пульта керування відповідно. Це дає змогу мінімізувати можливість перехоплення сигналу противником шляхом зменшення відношення сигнал/шум у місці його розташування.

Запропонований нами підхід до імплементації кожного методу захисту дозволив повною мірою забезпечити реалізацію принципу "оптимальний рівень захисту за оптимального рівня затрат". Завдяки такому підходу, описана у розділі практична реалізація не вимагає перепрограмування БПЛА, заміни його компонентів чи інших суттєвих змін основних його складових, що дає змогу

впровадити запропоновані системи захисту навіть у вже функціонуючі БПЛА шляхом модернізації, яка може бути проведена навіть у польових умовах.

На основі розробленої теоретичної концепції, запропонований метод "аварійного відновлення зв'язку", який складається із двох фаз (пасивна та активна). Під час пасивної фази мікроконтролером за допомогою збору відповідних метрик здійснюється обчислення і збереження у пам’яті пройденого маршруту та визначення стану зв’язку системи керування (норма чи втрата зв’язку). При виявленні на пасивній фазі ознак втрати зв’язку, застосовується активна фаза, яка полягає у негайному поверненні безпілотника у зворотному напрямку згідно записаного у пам’ять маршруту.

Окрім забезпечення безпосереднього захисту безпілотника, на якому він реалізований, цей метод дозволяє також захистити і інші пристрої, які не є обладнані такою системою захисту. Для цього було запропоновано і описано методику "зондування" оперативного простору захищеним БПЛА і фіксування небезпечних зон на топографічній схемі. Маючи вибірку безпечних маршрутів, можна відправляти на завдання незахищені БПЛА виключно за умовно безпечними маршрутами.

У четвертому розділі "**Експериментальні дослідженння запропонованих методів покращення захисту інформації у бездротових системах**" проведено практичну реалізацію та експериментальне випробування ефективності та точності запропонованих методів захисту. Досліджувалась також сама концепція захисту "оптимальний захист за оптимального рівня затрат" шляхом перевірки працездатності реалізованих на базі мікроконтролера методів захисту. Алгоритмічна реалізація пропонованих методів захисту відбувалася із максимальним використанням механізму переривань мікроконтролера з метою зниження рівня енергоспоживання до мінімально можливого.

Запропоновані і реалізовані нами методи захисту загалом показали свою ефективність для реалізації у безпілотних авіаційних системах. Зокрема система менеджменту потужності, за результатами проведеного дослідження, працює згідно заданого алгоритму і вимагає мінімальних енергозатрат. Результати

роботи системи менеджменту потужності показали, що запропоновані нами співвідношення рівнів потужності можна значно змістити у напрямку збільшення відстані роботи за одного і того ж рівня потужності передавача, оскільки якість відео була стабільно високою аж до моменту зміни потужності сигналу на вищу.

Запропонована реалізація частотного переналаштування за результатами експериментів дала позитивні результати, які частково перевершили очікування. Зокрема, реальний мінімальний період зміни частоти вдалося зменшити майже 2-а рази (80мс проти 150мс). Другий позитивний аспект: експерименти показали, що використаний для дослідження відеопередавач, при застосуванні протоколу smart audio, можна перемикати на частоти, які не входять у стандартну таблицю каналів, а також на частоти, які взагалі не входять в діапазон, визначений стандартом. Діапазон роботи відеопередавача можна встановити в межах від 5 ГГц до 6 ГГц, що дає додаткову значну перевагу для захисту системи відео.

Запропонований метод "аварійного відновлення зв'язку" досліджувався шляхом тестування алгоритму відслідковування та збереження траєкторії польоту, за якою в активній фазі повертатиметься безпілотник. Запропонована множина отримуваних від БПЛА метрик, які можна використати для збереження маршруту. В результаті проведених тестових польотів і оцінки точності відстеження траєкторії визначено, що найбільш ефективним набором метрик є комбінація із акселерометра та гіроскопа (з фіксуванням значень за всіма трьома осями). За необхідності скорочення розміру даних і обсягу обчислень можна записувати покази гіроскопа лише за віссю рискання, експерименти показали, що при цьому точність знижується не суттєво (похибка прямолінійного польоту зросла із 0,833% лише до 1,267%).

Використання інших розглянутих метрик, на жаль, не рекомендується, оскільки результати експерименту показали їхню недостатню високу точність та низьку надійність. Загалом, результати проведених нами експериментів приводять до позитивного висновку щодо використання запропонованих

методів захисту, поряд з цим залишилися деякі відкриті питання, які в майбутньому потребуватимуть подальшого дослідження.

У **висновках** до роботи описано основні здобуті результати та заключення, які випливають із результатів проведених наукових та експериментальних досліджень. Представлено основні отримані показники характеристик роботи запропонованих та реалізованих систем захисту. Наведено порівняльну оцінку можливостей використання різних наборів метрик для засобу аварійного відновлення зв'язку із обґрунтуванням вибору найбільш оптимального набору на основі кількісних показників їхньої точності.

У **додатках** до дисертаційної роботи подано список наукових публікацій автора та акти впровадження результатів дисертаційного дослідження.

Ключові слова: бездротові системи, інформаційні мережі, доступність, канал зв’язку, антенні пристрої, безпілотні апарати, радіоелектронна боротьба, радіоелектронна розвідка, кодування, легковагове шифрування, приймально-передавальний тракт, переналаштування частоти, відновлення зв’язку.

SUMMARY

Kuten R. B. Improving Information Protection during Transmission in Wireless Systems. – Qualifying scientific work in manuscript form.

Dissertation for the degree of Doctor of Philosophy in specialty 125 "Cybersecurity" (12 – Information Technologies). – Lviv Polytechnic National University, Lviv, 2024.

This dissertation work is dedicated to the solution of an actual scientific and applied problem – increasing the stability, security and fault tolerance of the information transmission process in wireless systems and ensuring a sufficient level of signal parameters' concealment and security, as well as the problem of ensuring the possibility of wireless communication and control in conditions of active electromagnetic confrontation (including with the use of means of radio-electronic warfare).

Ensuring the protection of information in information and cyber-physical systems remains one of the most serious problems and an important task in the field of information security. With the modern development of communication technologies, this problem is particularly acute in the context of the use of wireless communication systems based on radio waves. Since the transmission is carried out over the open radio air, anyone with the appropriate equipment has the opportunity to access the transmitted signal and the receiving-transmitting path in general. With the necessary skills and equipment, an attacker can interfere with the operation of a wireless system, disable communication channels, steal data, forge data, etc.

In recent years, a lot of research has been carried out in the field of ensuring the protection of wireless communication systems and ensuring its immunity to interference. Many works are devoted to increasing the range of wireless communication systems. A wide range of cryptographic systems and data exchange protocols have been developed, protocols and methods have been developed to ensure the reliability of communication in conditions of random interference, separation of communication channels for multi-user access. Many studies are

devoted to the protection of the actual physical level of information transmission, that is, masking with the help of noise signals with a wide spectrum and chaotic structure, masking with the help of pseudorandom reconfiguration of the operating carrier frequency.

The main focus is on the protection of wireless communication systems, which, due to the large-scale Russian invasion of Ukraine, began to be massively used by the armed forces of Ukraine to adequately cover communication needs.

One of the systems most critically in need of protection is the communication and control systems of unmanned aerial vehicles, particularly unmanned aerial vehicles (UAVs) or so-called "drones". Their role in military conflicts is becoming more and more important, and the range of use of drones has recently expanded significantly: if once it was only reconnaissance and surveillance, now there are devices that can inflict direct fire damage ("kamikaze UAVs"), drop assets damage, deliver supplies and ammunition to ground units, and even carry out remote mining by engineering means.

The conducted research includes the analysis of the possibilities of using existing means of information protection during transmission via wireless channels in modern small-sized unmanned aircraft complexes, as well as the development of new protection models that are designed for use directly in information and cyber-physical systems capable of independent movement.

The **object of the research** is the security of wireless communication channels, in particular, wireless control channels, telemetry tracking and other data exchange with unmanned vehicles (including dual purpose and military UAVs).

The **subject of research** are methods of masking the transmission session, hiding the frequencies of carrier signals, encryption of data transmitted by wireless networks, authentication of the receiver-transmitter, methods of ensuring data integrity and increasing their resistance to interference, including intentionally created means of spatial noise and radio-electronic warfare (REB).

In the first chapter **"Basic information on information transmission in information systems and networks"** a review of domestic and foreign scientific

literature was conducted. On the basis of which, aspects of the use of information networks for data exchange and transmission, the technologies used in them, and their current use in civil and military spheres were analyzed.

It has been determined that information technology and wireless systems have taken a leading place in many areas of activity: from everyday household needs to military applications. Such modern systems are based on the use of wireless technologies as: communication systems, means of conducting entrepreneurial activity, business, logistics and transport technologies, energy, "smart city", "smart house" systems, banking systems, etc. One of the revealed aspects is also the fact that the high development of wireless communication technologies, the reduction of the dimensions of radio access devices became the key factors that contributed to the development of small embedded systems and, in particular, unmanned devices, which are the leading direction of development in most branches of modern technology.

Similar trends are observed for military communication systems. In the current realities of conducting military operations and from the experience of the ATO and OOS, it is clear that wireless systems that work with the use of radio waves have become the basis of military communication systems, since radio communication gives an advantage in terms of mobility, speed of deployment, etc. By analogy with the development of civil systems, we are also observing the development of the use and application of unmanned devices for the performance of military tasks in modern armed conflicts. In particular, in the protection of the territorial integrity of Ukraine, unmanned complexes are used for reconnaissance, surveillance, adjusting the work of artillery, for inflicting damage (kamikaze drone), for dropping ammunition (so-called "bombers") and for setting up and improving the main communication system (drones- repeaters).

The main problem identified during the analytical review is that due to the wide scale of the Russian invasion and the long length of the front line, huge requests for communication systems and systems of unmanned devices have been generated by the armed forces of Ukraine. The production capacities and available means of the Ministry of Defense are not enough, so this has caused the use of civilian means of

communication in the military sphere, in particular, the use of civilian drones and hobby flights for unmanned operations. Such a problem requires an immediate response and ensuring the possibility of implementing appropriate protection measures for such devices.

In the second chapter **"Problems of information protection during transmission by wireless systems"** existing approaches to the problem of information protection during transmission in wireless systems are discussed in detail. Based on the preliminary results of research from the first chapter, the main analysis of all possible means and concepts of information protection in communication channels was carried out in the context of the possibility and methods of their application in unmanned aircraft systems, in particular, systems of civilian origin, which began to be widely used for military purposes.

The main needs for the protection of devices of civilian origin, which are dictated by their military use, have been determined: potentially, such devices do not have the ability to function reliably, that is, there is a need to ensure the functioning of devices in conditions of fog, rain, snow, strong gusts of wind, etc. Such devices require the introduction or development of new reliable encryption and channel coding systems, as the basic means for military use are insufficient. Civilian wireless systems and devices, in principle, are not designed to work in the conditions of the enemy's use of radio-electronic intelligence, radio-electronic warfare, radio direction-finding stations, suppression devices, etc.

An analysis of the structure of the model of the operating system of OSI open systems was carried out. This made it possible during further analysis of applications and applications used at one or another level of the interaction model to make a certain ranking of methods and means of protecting information during its transmission, according to the level of functioning of one or another method.

Despite the fact that there are a large number of modern approaches to ensuring the protection of information during transmission by wireless systems, the review and analysis of modern research and publications conducted in this section indicates an urgent need to modify existing means and develop fundamentally new methods to

prevent information interception, suppression communication links at the lowest layers of the OSI model, particularly at the physical and link layers, which will be used in unmanned wireless remote control devices (which are typically self-contained battery-powered vehicles). This need is dictated by the fact that most of the proposed modern methods of protection, along with their high efficiency and high level of protection, require quite high resource costs. This applies both to the amount of calculations and the amount of required memory, as well as to the physical dimensions of certain applications to ensure the protection of masking or concealment of information transmission.

In the third chapter **"Improving the security of wireless control and communication systems in the context of UAVs"**, a new idea for improving the stability and security of the communication channel of an unmanned device against EW devices is proposed and scientifically substantiated. Methods for improving existing methods and means of protection are proposed and developed. The proposed methods are of great importance in matters of information protection in communication systems and control of unmanned devices.

First of all, for the implementation of each of the methods, a preliminary analysis of the schematic solutions used in this or that device was additionally carried out, after which all the developed methods were based on the results of this analysis. The mechanism of operation of the proposed methods was built in such a way as to ensure the practical implementation of each method of protection due to the inherent capabilities of the basic components of the unmanned aerial vehicle.

This made it possible to implement the most effective means of information protection both for the transmission of video signals from UAVs and to ensure increased availability of the device (ensuring the maintenance of the functionality of communication channels in conditions of active use of EW devices).

An approach to the implementation of protection measures based on the use of a built-in system, which is an additionally installed microcontroller, is proposed. The microcontroller functions in the "mentoring" mode and intervenes only in the case of an emergency situation or the activation of the corresponding algorithm for

implementing the protection tool. Its intervention consists solely in the adaptive management of the settings of the existing elements of the UAV.

To ensure the privacy of the drone's video channel, the basis is taken of the frequency reconfiguration method, which has been adapted for use in an unmanned small-sized device, and also improved the level of resource consumption by implementing it through the control of VTX parameters using a microcontroller through the SmartAudio protocol. In addition, for the protection of privacy, it was proposed for the first time to use signal power management as a protection method, which consists in adaptively increasing/decreasing the power of video transmission, depending on the distance/approach of the drone to the control panel, respectively. This minimizes the possibility of enemy interception of the signal by reducing the signal-to-noise ratio at its location.

The approach proposed by us to the implementation of each method of protection made it possible to fully ensure the implementation of the principle "optimal level of protection at the optimal level of costs." Thanks to this approach, the practical implementation described in the section does not require reprogramming the UAV, replacing its components or other significant changes to its main components, which makes it possible to implement the proposed protection systems even in already functioning UAVs through modernization, which can be carried out even in field conditions.

On the basis of the developed theoretical concept, the method of "emergency restoration of communication" is proposed, which consists of two phases (passive and active). During the passive phase, the microcontroller calculates and stores the traveled route in memory and determines the communication status of the control system (normal or loss of communication) using the collection of relevant metrics. When signs of loss of communication are detected in the passive phase, the active phase is used, which consists in the immediate return of the drone in the reverse direction according to the route recorded in the memory. In addition to providing direct protection of the drone on which it is implemented, this method also allows you to protect other devices that are not equipped with such a protection system. For

this purpose, the technique of "probing" the operative space by a protected UAV and fixing dangerous zones on the topographical scheme was proposed and described. Having a sample of safe routes, it is possible to send unprotected UAVs on missions exclusively along conditionally safe routes.

In the fourth chapter **"Experimental studies of the proposed methods of improving information protection in wireless systems"** the practical implementation and experimental testing of the effectiveness and accuracy of the proposed protection methods were carried out. The very concept of protection "optimal protection at the optimal level of costs" was also studied by checking the performance of protection methods implemented on the basis of a microcontroller. The algorithmic implementation of the proposed protection methods took place with the maximum use of the microcontroller interrupt mechanism in order to reduce the level of energy consumption to the minimum possible.

The protection methods proposed and implemented by us have generally shown their effectiveness for implementation in unmanned aircraft systems. In particular, the power management system, according to the results of the conducted research, works according to the given algorithm and requires minimal energy consumption. The results of the power management system showed that the ratio of power levels proposed by us can be significantly shifted in the direction of increasing the operating distance at the same transmitter power level, since the video quality was consistently high until the signal power was changed to a higher one.

The proposed implementation of frequency reconfiguration based on the results of experiments gave positive results that partially exceeded expectations. In particular, it was possible to reduce the real minimum frequency change period by almost 2 times (80ms versus 150ms). The experiments showed that the video transmitter used for the study, when applying the smart audio protocol, can be switched to frequencies that are not included in the standard channel table, as well as to frequencies that are not included at all in the range defined by the standard. The operating range of the video transmitter can be set between 5 GHz and 6 GHz, which provides an additional significant advantage for the protection of the video system.

The proposed method of "emergency recovery of communication" was investigated by testing the algorithm of tracking and saving the flight trajectory by which the drone will return in the active phase. A set of metrics received from the UAV that can be used to save the route is proposed. As a result of conducted test flights and evaluation of the accuracy of trajectory tracking, it was determined that the most effective set of metrics is a combination of an accelerometer and a gyroscope (with values fixed on all three axes). If it is necessary to reduce the size of the data and the volume of calculations, it is possible to record gyroscope readings only along the yaw axis, experiments have shown that the accuracy does not decrease significantly (the error of straight flight increased from 0.833% to only 1.267%).

Unfortunately, the use of other considered metrics is not recommended, as the results of the experiment showed their insufficient high accuracy and low reliability. In general, the results of our experiments lead to a positive conclusion regarding the use of the proposed protection methods, along with this there are some open questions that will require further research in the future.

The **conclusions** to the work describe the main results obtained and conclusions that follow from the results of scientific and experimental research. The main obtained performance indicators of the proposed and implemented protection systems are presented. A comparative assessment of the possibilities of using different sets of metrics for the means of emergency communication restoration with justification of the choice of the most optimal set based on quantitative indicators of their accuracy is given.

The **appendices** to the dissertation contain a list of the author's scientific publications and acts of implementation of the results of the dissertation research.

Key words: wireless systems, information networks, availability, communication channel, antenna devices, unmanned aerial vehicles, radio electronic warfare, radio electronic intelligence, coding, lightweight encryption, reception-transmission path, frequency reconfiguration, communication restoration.

Список публікацій здобувача:

Наукові праці, в яких опубліковано наукові результати дисертації:

1. Кутень Р. Застосування частотного переналаштування для захисту безпілотних літальних апаратів // Social Development and Security. – 2024. – Vol. 14, No. 2. – P. 64-73. DOI: 10.33445/sds.2024.14.2.7.
2. Кутень Р., Ахмедова А. Підвищення рівня захищеності та життєздатності безпілотних авіаційних пристроїв // Безпека інформації. – 2024. – Т. 30, № 1. – С. 88-94. DOI: 10.18372/2225-5036.30.18609.
3. Кутень Р.Б., Синявський О.Ю. Методи і засоби забезпечення стабільності та захисту радіозв’язку в умовах складної електромагнітної обстановки. Комп’ютерні системи та мережі. 2024. №1(6). – С. 99-107. DOI: 10.23939/csn2024.01.099.

Наукові праці, які засвідчують апробацію матеріалів дисертації:

4. Дудикевич В. Б., Микитин Г. В., Кутень Р. Б., Галунець М. О. До питання безпеки безпровідних мереж на основі моделі OSI // Сучасні методи, інформаційне, програмне та технічне забезпечення систем керування організаційно-технічними та технологічними комплексами : мат-ли VIII Міжн. н.-т. Internet-конф. (Київ, 26 листопада). – 2021.
5. Дудикевич В. Б., Микитин Г. В., Кутень Р. Б., Галунець М. О. Шифрування повідомлень в безпровідних мережах на основі алгоритму "Калина" // Інформаційна безпека та інформаційні технології : збірник тез доповідей V Всеукраїнської н.-практ. конф. молодих учених, студентів і курсантів (Львів, 26 листопада). – 2021.
6. Dudykevych V., Mykytyn G., Kuten R., Halunets M. The security features of wireless networks of intellectual transport system // Захист інформації і безпека інформаційних систем : матеріали VIII Міжнародної науково-технічної конференції, 11-12 листопада, 2021, Львів. – 2021.
7. Дудикевич В. Б., Микитин Г. В., Галунець М. О., Кутень Р. Б. Кіберфізична система "розумний дім": структура – загрози – безпека //

Інформаційна безпека та інформаційні технології : збірник тез доповідей IV Міжнародної науково-практичної конференції, ІБІТ 2022, м. Львів, 30 листопада 2022 року. – 2022.

8. Дудикевич В., Собчук І., Ракобовчук Л., Кутень Р. Легковаговагове шифрування для захисту даних RFID-міток // Захист інформації і безпека інформаційних систем: матеріали V Міжнар. наук.-техн. конф. – 2016.

Інші публікації, що додатково відображають результати дисертації:

9. Дудикевич В. Б., Микитин Г. В., Галунець М. О., Кутень Р. Б., Ракочий В. І. Елементи безпеки провідних мереж на основі витої пари // Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення : збірник тез доповідей Міжнародної наукової інтернет-конференції (Тернопіль, 6-7 квітня 2022 р.). – 2022.
10. Дудикевич В.Б., Микитин Г.В., Галунець М.О., Кутень Р.Б., Васильєв Д.В., Бабенцов Г.А. Багаторівневий захист технологій функціонування інтелектуальних обєктів. Досягнення та перспективи інформаційних систем і технологій : мат-ли XXI Всеукр. н.-т. конф. молодих вчених, аспірантів та студентів (Одеса, 21-22 квітня). – 2022.
11. Дудикевич В.Б., Микитин Г.В., Кутень Р.Б., Сидорик Д.О. Комплексна модель безпеки інтелектуальної кіберфізичної транспортної системи // Інформаційна безпека та інформаційні технології : збірник тез доповідей VI Всеукр. н.-практ. конф. молодих учених, студентів і курсантів, (м. Львів, 30 листопада). – 2023.
12. Дудикевич В.Б., Микитин Г.В., Галунець М.О., Кутень Р.Б. Безпека комунікаційного середовища кіберфізичної системи інтелектуального моніторингу повітря // Сучасні методи, інформаційне, програмне та технічне забезпечення систем керування організаційно-технічними та технологічними комплексами : матеріали IX Міжнародної науково-технічної Internet-конференції (Київ, 25 листопада 2022 р.). – 2022.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ

БПА – безпілотний апарат

БПЛА – безпілотний літальний апарат

РЕБ – радіо-електронна боротьба

РЕР – радіо-електронна розвідка

ПЗ – програмне забезпечення

VTX – радіопередавач відеосигналу

FPV – (First Person View) вигляд від першої особи

ЗС – Збройні Сили

ГУР – Головне управління розвідки

МК – мікроконтролер

ІС – інформаційна система

КФС – кіберфізична система

ЛБЗ – лінія бойового зіткнення

UART – послідовний порт передачі даних

RX – вивід для прийому даних

TX – вивід для передавання даних

SA – протокол "Smart Audio", для управління передавачем відео

СОУ – Сили Оборони України

ВСТУП

Актуальність теми. У сучасному світі, де інформація є одним з найважливіших ресурсів, ми спостерігаємо стрімкий розвиток інформаційно-комунікаційних технологій, який в свою чергу значно збільшує обсяги даних, що передаються тими чи іншими мережами і появи нових телекомунікаційних послуг. Це викликає потребу у зростанні кількості, продуктивності та швидкодії засобів і пристроїв телекомунікаційних систем. Особливий розвиток спостерігаємо в галузі бездротових технологій. [1,2]

У зв’язку розвитком технологій та збільшенням трафіку даних, зростає також зацікавленість зі сторони зловмисників у перешкоджанні роботи бездротових систем, виведення з ладу каналів зв’язку, викрадення даних із них, тощо. Через це захист інформації стає критично важливим завданням. Особливо це стосується інформації з обмеженим доступом, передавання якої вимагає високого рівня захищеності.

Бездротові системи та мережі використовують в широкому спектрі застосувань, від домашніх мереж до промислових систем. Радіозв'язок є життєво важливим для безлічі застосувань, включаючи мобільний зв'язок, бездротові мережі, військові комунікації, канали керування безпілотними апаратами (БПА) військового призначення та багато іншого. Однак, збереження надійного з'єднання в умовах низького рівня сигнал/шум, активної протидії противника, наявності природних перешкод чи завад є великим викликом, особливо у випадку штучного створення шумових завад кваліфікованим зловмисником.

Особливо критичною є потреба стабільного завадостійкого зв’язку в теперішній час, коли технології набувають все більшого значення у бойових діях та відіграють дуже важливу роль у захисті територіальної цілісності нашої держави. Насамперед, це стосується використання на полі бою чи для розвідки безпілотних літальних апаратів (БПЛА або "дронів"), роль яких у воєнних конфліктах стає все важливішою та їхній вплив на стратегію і тактику ведення

бою лише зростає.

За останні роки було проведено багато досліджень у галузі забезпечення захисту бездротового зв’язку, забезпечення його завадостійкості, підвищення дальності зв’язку. Розроблено криптографічні системи та протоколи обміну даними, запропоновано підходи до забезпечення надійності зв’язку, розділення каналів зв’язку для багатокористувацького доступу до середовища передачі та багато інших досліджень, висвітлених у відповідних роботах та матеріалах наукових досліджень, що були проаналізовані та опрацьовані в ході написання даної наукової роботи [3-11]. Проте проблематику покращення захисту передавання інформації із обмеженим доступом, зокрема маскування факту такої передачі, забезпечення кращої відмовостійкості каналу зв’язку порівняно з існуючими на сьогодні рішеннями, не можна вважати вирішеною, тому підняті у роботі питання надалі є актуальними та потребують вирішення.

Чимала кількість рішень, які покликані забезпечити захист та відмовостійкість передачі інформації в умовах складної електромагнітної обстановки чи активного протиборства зі сторони зловмисника, передбачає використання значних ресурсів для їхньої реалізації, є доступними лише для відносно великих та потужних обчислювальних систем. Вони не придатні для реалізації у невеликих автономних пристроях, вбудованих системах, які мають обмеження по рівню продуктивності процесорів чи вимірювальних засобів, допустимих потужностях сигналу, обсягу запам’ятовувальних пристроїв, тощо, до яких впевнено можна віднести приведені для прикладу раніше "дрони".

Тому, у цій роботі детально розглянуто питання надійності функціонування і захисту бездротових систем та мереж, що використовуються в тому числі для керування безпілотними апаратами, отримання даних телеметрії таких апаратів, зображень їх бортових камер, значень певних вимірів, чи будь-якої іншої необхідної нам інформації із них. Причиною такого вибору є те, що такі апарати стають все більш поширеними в різних галузях, включаючи військову сферу, сільське господарство, рятувальні операції та інше. Відповідно, захист інформації, що передається через бездротові мережі для керування цими

апаратами, отримання з них даних на відстані є важливим аспектом їх експлуатації. Враховуючи ці аспекти можна впевнено підсумувати, що питання та задачі щодо захисту бездротових систем, зокрема систем керування і зв'язку БПЛА, які підняті і опрацьовані у даній роботі ***є актуальними науково-прикладними задачами.***

Зв'язок роботи із науковими програмами, планами і темами.

Дисертаційні дослідження виконувались у відповідності до наукового напряму кафедри захисту інформації Національного університету "Львівська політехніка": – "Дослідження систем технічного захисту інформації, каналів зв'язку та комп'ютерних мереж, фізичного захисту інформації та криптографії", в межах кафедральної науково-дослідної роботи: "Розроблення та удосконалення методів і засобів захисту інформації для протидії несанкціонованому доступу в інформаційно-комунікаційних мережах" (шифр ЗІ-7) (№ держреєстрації 0119U101690).

Мета і задачі дослідження

Метою дисертаційної роботи є підвищення стабільності та відмовостійкості процесу передавання інформації у бездротових системах, забезпечення достатнього рівня прихованості та захищеності параметрів сигналу, забезпечення можливості роботи засобів зв'язку та керування безпілотними апаратами в умовах активного електромагнітного протиборства (в тому числі зі застосуванням засобів радіоелектронної боротьби).

Відповідно, для досягнення цієї мети в роботі поставлено та вирішено такі **завдання:**

1. Провести аналіз сучасного застосування інформаційних систем, та впровадження бездротових технологій у їхньому функціонуванні.
2. Провести аналіз і виділити системи та застосунки із найбільш критичною залежністю від стану функціонування бездротової системи зв'язку.

3. Провести порівняльний аналіз сучасних підходів до забезпечення захисту бездротових каналів зв’язку та надати оцінку можливості їх впровадження у автономні безпілотні системи.
4. Здійснити вдосконалення існуючих підходів та методик щодо оцінки захищеності інформаційних та кіберфізичних систем для забезпечення можливості застосування їх моделей та концепцій до систем, здатних самостійно переміщуватися у просторі.
5. Провести детальне дослідження можливостей сучасних схемотехнічних рішень, які використовуються у БПА, в контексті можливості використання їх власних функцій для реалізації методів та систем захисту.
6. Розробити моделі і алгоритми для захисту бездротових систем безпілотних пристроїв із врахуванням активного використання цивільних засобів у бойових умовах згідно концепції "оптимальний захист за оптимальних затрат".
7. Провести експериментальні дослідження для випробування та оцінки ефективності розроблених методів на реальній моделі.

Об’єкт дослідження. Захищеність каналів безпровідного зв’язку, зокрема безпровідних каналів керування, відслідковування телеметрії чи іншого обміну даними з безпілотними засобами (у тому числі БПЛА подвійного чи військового призначення).

Предмет дослідження. Методи забезпечення маскування сеансу передачі, приховування частот несучих сигналів, шифрування даних у безпровідних мережах, автентифікації приймача-передавача, методи забезпечення цілісності та підвищення стійкості передаваних даних до завад, у тому числі навмисно створених засобами просторового зашумлення та радіоелектронної боротьби (РЕБ).

Методи дослідження. Для вирішення поставлених завдань, дослідження процесів, моделей, систем передавання, оброблення, кодування та шифрування

даних, моделювання пропонованих систем керування використовувалися методи теорії сигналів та процесів, математичного аналізу, чисельні методи, методи теорії інформації та кодування, елементи теорії електродинаміки та поширення електромагнітних хвиль, статистичного аналізу, математичне моделювання.

Наукова новизна отриманих результатів.

– вперше запропоновано критерій просторової стійкості, який визначає здатність дистанційно керованого пристрою до самостійного просторового переміщення;
– вперше розроблено математичну модель критерію просторової стійкості та обґрунтовано доцільність його використання при дослідженні захищеності інформаційних та кіберфізичних систем;
– отримали подальший розвиток існуючі методики оцінки стану захищеності бездротових систем керування, шляхом врахування до результатів їхнього оцінювання результату оцінки за запропонованим критерієм просторової стійкості;
– розроблено метод "аварійного відновлення зв'язку", який ґрунтується на відстеженні залежності якості зв’язку від просторового переміщення та автономному поверненні керованого пристрою до точки останнього стабільного зв’язку за інерційними даними маршруту, що дозволило значно підвищити ефективність протидії систем керування і зв’язку до засобів РЕБ та зменшити затрати на реалізацію засобів захисту пристрою;
– розроблено методику захисту інформації у бездротових системах, яка основана на мінімізації потужності передавача інформації достатньої для зв'язку з пунктом керування. Дана методика, на відміну від існуючих, забезпечує захищеність даних від перехоплення засобами розвідки противника;
– вдосконалено та адаптовано до роботи у малопотужних автономних системах із симплексним зв’язком методи захисту інформації із

використанням псевдовипадкового переналаштування несучої частоти передавача, що дозволило підвищити їх захищеність перед засобами розвідки без зниження швидкодії інформаційної системи;

Практичне значення отриманих результатів.

1. Використання запропонованого підходу до реалізації систем захисту у малих автономних системах, за принципом "нагляд->аналіз->керування" дозволив впровадити високоефективні методи захисту, не впливаючи на ефективність та швидкодію пристрою у штатних умовах.
2. Застосування методів захисту на базі мікроконтролера, описаних і випробуваних у роботі, не вимагає великих фінансових затрат і ресурсу самого пристрою, завдяки чому ціна пристрою змінюється не суттєво.
3. Розроблені методи захисту можуть бути впроваджені у вже існуючий і функціонуючий пристрій з мінімальною зміною його конфігурації, що дозволяє здійснити такий апгрейд фактично у польових умовах.
4. Реалізація запропонованого методу аварійного відновлення зв’язку дозволить значно підвищити "живучість" безпілотників, особливо в умовах їхнього бойового застосування.
5. Завдяки застосуванню методу "аварійного відновлення зв’язку" отримано можливість "зондування" оперативного простору апаратом без його втрати, що дозволило емпірично визначити зони просторової стійкості, згідно пропонованої концепції. Завдяки цьому отримано можливість скласти топографічну схему "безпечних" маршрутів для апаратів, не обладнаних такою системою захисту

Апробація результатів дисертації.

Основні результати дисертаційного дослідження були представлені та обговорені на наукових семінарах кафедри захисту інформації НУ"ЛП" та на 8-ми міжнародних науково-технічних конференціях, серед яких:

– VIII Міжнародна науково-технічна Internet-конференція "Сучасні методи,

інформаційне, програмне та технічне забезпечення систем керування організаційно-технічними та технологічними комплексами" (Київ, 26 листопада 2021 року).

– V Всеукраїнська науково-практична конференція молодих учених, студентів і курсантів "Інформаційна безпека та інформаційні технології" (Львів, 26 листопада 2021 р.).
– VIII Міжнародна науково-технічна конференція "Захист інформації і безпека інформаційних систем" (11-12 листопада, 2021, Львів.).
– Міжнародна наукова інтернет-конференція "Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення" (Тернопіль, 6-7 квітня 2022 р.).
– XXI Всеукраїнська науково-технічна конференція молодих вчених, аспірантів та студентів "Досягнення та перспективи інформаційних систем і технологій" (Одеса, 21-22 квітня 2022 р.).
– IV Міжнародна науково-практична конференція "Інформаційна безпека та інформаційні технології" (м. Львів, 30 листопада 2022 р.).
– IX Міжнародна науково-технічна Internet-конференція "Сучасні методи, інформаційне, програмне та технічне забезпечення систем керування організаційно-технічними та технологічними комплексами" (Київ, 25 листопада 2022 р.).
– VI Всеукраїнська науково практична конференція молодих учених, студентів і курсантів "Інформаційна безпека та інформаційні технології" (м. Львів, 30 листопада 2023 р.).

Структура і обсяг дисертації. Дисертація складається із вступу, чотирьох розділів, висновків, бібліографічного списку використаних джерел, що містить у собі 97 пунктів найменувань. Загальний обсяг роботи 188 сторінок, серед них 38 рисунків, 10 таблиць, 2 додатки на 4 сторінках.

РОЗДІЛ 1. ОСНОВНІ ВІДОМОСТІ ЩОДО ПЕРЕДАВАННЯ ІНФОРМАЦІЇ У ІНФОРМАЦІЙНИХ СИСТЕМАХ ТА МЕРЕЖАХ

Інформаційні системи сучасного світу стають все складнішими та розгалуженими, сприяючи зручній та швидкій передачі даних у реальному часі. Разом з цим зростає і важливість забезпечення безпеки та конфіденційності цих даних, особливо коли йдеться про інформацію з обмеженим доступом. Забезпечення конфіденційності та цілісності даних у таких мережах є завданням, яке вимагає комплексного підходу та використання сучасних технологій кібербезпеки.

Інформаційна мережа –це сукупність територіально розрізнених кінцевих систем, об'єднаних телекомунікаційною мережею, за допомогою якої забезпечується взаємодія прикладних процесів, активізованих у кінцевих системах, та їх колективний доступ до ресурсів мережі. Передавання інформації в інформаційній мережі розуміється як процес обміну даними між різними кінцевими системами, що включають комп'ютери, мобільні пристрої, сервери та інші пристрої, які мають доступ до мережі. Цей процес забезпечується за допомогою телекомунікаційних технологій, які дозволяють передавати дані через мережу з використанням різних протоколів та каналів зв'язку. [12]

Передача цієї інформації в мережі може відбуватися в різних формах, таких як передача файлів, відправлення електронної пошти, стрімінг мультимедійного вмісту, відеоконференції тощо. Важливою частиною цього процесу є забезпечення безпеки та конфіденційності передаваних даних, а також забезпечення високої надійності таких каналів зв'язку, що вимагає використання шифрування, аутентифікації та інших заходів кібербезпеки. Для обміну інформацією з обмеженим доступом в інформаційних системах необхідне впровадження спеціальних заходів та технологій, що забезпечують найвищий рівень конфіденційності та цілісності при передачі цих даних.

1.1. Застосування інформаційних мереж у цивільних системах та

комунікаціях

Інформаційні мережі у цивільних системах та комунікаціях забезпечують інтеграцію та обмін даними між різними суб'єктами: від урядових установ і комерційних підприємств до приватних громадян. Вони сприяють покращенню організації робочих процесів, забезпечують доступ до різноманітних сервісів та ресурсів, полегшують взаємодію між людьми та автоматизують багато повсякденних операцій. [13]

Світові тенденції розвитку інформаційних технологій характеризуються зростанням їх технічної досконалості й інтелектуальної наповнюваності за рахунок створення в телекомунікаційних мережах високоінтелектуальних серверів із широким спектром інформаційних послуг, використання цифрової передачі аудіо- і відеоінформації, зростанням рівня використання оптичних систем і пакетних принципів передачі даних. Особливо актуальним і поширеним зараз є розвиток бездротового зв’язку, який характеризується розгортанням широкосмугових радіосистем, вдосконаленням і розширенням протоколів стільникових та супутникових каналів зв`язку. [14]

Цивільні інформаційні мережі використовуються у багатьох галузях, таких як:

Транспорт: моніторинг та управління транспортними потоками, системи навігації та контролю руху транспортних засобів.

Транспортна галузь використовує інформаційні мережі для різних цілей, що сприяє покращенню ефективності та безпеки транспортних систем [15]. Основні застосування цих мереж у транспорті включають моніторинг та управління транспортними потоками, системи навігації та контролю руху транспортних засобів.

Моніторинг транспортних потоків: Інформаційні мережі дозволяють збирати дані про рух транспорту на дорогах, залізницях, водних шляхах та в повітряному просторі. Ці дані можуть включати інформацію про кількість транспортних засобів, їх швидкість, розташування та інші параметри, що дозволяє ефективно використовувати дорожні мережі та розвивати плани

розвитку інфраструктури.

Управління транспортними потоками: На основі зібраних даних інформаційні мережі дозволяють регулювати рух транспорту, включаючи сигналізацію світлофорів, координацію роботи громадського транспорту, оптимізацію маршрутів для уникнення заторів та забезпечення швидкого переміщення пасажирів та вантажів.

Системи навігації: Інформаційні мережі використовуються для створення систем навігації, які допомагають водіям, пілотам та іншим учасникам транспортних процесів знаходити оптимальні маршрути, уникати перешкод та забезпечувати безпеку руху.

Контроль руху транспортних засобів: Інформаційні мережі використовуються для встановлення систем контролю за рухом транспортних засобів, включаючи системи відеоспостереження, системи реєстрації швидкості руху, системи виявлення аварій та інші технології, що сприяють підвищенню безпеки на дорогах та в інших місцях транспортного руху.

Виробники транспортних засобів розробляють нові технології для того, щоб вони ставали безпечнішими, пересування було зручнішим та завдавало менше стресу. Передові технології все частіше застосовуються до великих систем громадського транспорту та поширення для пасажирів інформації про прибуття поїздів та автобусів.

Частина цих технологій застосовується для поліпшення ефективності руху транспорту та відповідних комерційних операцій як ланки кола постачання. Ці технології відомі під назвою як інтелектуальні транспортні системи (ITC). ITC допомагають зробити транспортну систему безпечнішою, ефективнішою та надійнішою, а також зменшують її вплив на довколишнє середовище.

ITC – це суміш комп’ютерної сфери, телекомунікацій та інформаційних технологій разом із знаннями у транспортному і автомобільному секторах. Ключові ITC технології з’являються на основі головних напрацювань у цих секторах, що також тягне за собою і розвиток відповідних моделей забезпечення безпеки ITC [16]. Відтак, ITC можна визначити також як

застосування комп'ютерних, комунікаційних та інформаційних технологій для ефективного управління транспортними мережами та засобами у реальному часі.

Медицина: електронні медичні картки, телемедицина, системи моніторингу пацієнтів.

Застосування інформаційних мереж у медичній галузі є надзвичайно важливою складовою сучасного медичного обслуговування, яка має значний вплив на якість та ефективність надання медичних послуг. За допомогою інформаційних технологій у медицині досягнуті величезні успіхи в галузі діагностики, лікування та моніторингу пацієнтів. Розвиток цих технологій дозволяє зберігати, обробляти та передавати великі обсяги медичної інформації з високою швидкістю та точністю, що сприяє швидшому та більш точному прийняттю медичних рішень.

Електронні медичні картки: Це цифрові версії медичних карток пацієнтів, які зберігаються в електронній формі та доступні медичному персоналу у будь-який момент. Це дозволяє зберігати та обмінюватися медичною інформацією ефективно та безпечно, що полегшує діагностику, лікування та моніторинг пацієнтів.

Телемедицина: це використання інформаційних технологій для проведення медичних консультацій та діагностики на віддаленій основі. За допомогою телемедицини лікарі можуть віддалено надавати консультації пацієнтам, а також вести моніторинг за їхнім станом на відстані.

Системи моніторингу пацієнтів: Інформаційні мережі використовуються для розробки систем моніторингу пацієнтів, які дозволяють в реальному часі відслідковувати важливі медичні показники, такі як серцевий ритм, тиск, рівень кисню тощо. Ці дані можуть передаватися безпосередньо до медичних систем або зберігатися в хмарних сервісах для подальшого аналізу та використання.

Освіта: дистанційне навчання, використання онлайн-ресурсів та інтерактивних платформ.

З розвитком інформаційних мереж, розвивався і рівень освіти. Сьогодні усі

освітні заклади використовують інформаційні мережі для навчання, поширення інформації та зберігання даних.

Прикладом існує побудована Національна науково-освітня інформаційна мережа України. Вона була необхідним етапом подальшого розвитку сфер науки і освіти. Вона має значне інтелектуальне наповнення, вміщує бази даних і знань із різних напрямів освіти і науки, системи пошуку інформації, електронні бібліотеки, забезпечує віддалене користування потужними обчислювальними ресурсами, забезпечує роботу в режимі віртуальних освітніх та наукових лабораторій, здійснює мультисервісну обробку інформації (графічну, відео- та аудіоінформацію) [17].

Енергетика: моніторинг та керування енергетичними мережами, системи енергоефективності.

Сучасні технології інформаційних мереж мають значний потенціал для застосування в енергетичному секторі, сприяючи покращенню ефективності та управління енергетичними мережами. Моніторинг та керування енергетичними мережами є ключовими аспектами, які дозволяють забезпечити стабільність, надійність і оптимальну роботу систем енергопостачання.

Системи моніторингу дозволяють отримувати в реальному часі дані про стан енергетичних мереж, включаючи рівень споживання енергії, навантаження на мережі, стан електроустаткування та інші параметри. Ці дані допомагають операторам енергосистем приймати обґрунтовані рішення щодо оптимізації режиму роботи мережі, уникнення аварій та збільшення загальної ефективності системи [18].

Керування енергетичними мережами здійснюється за допомогою розумних систем автоматизації, які базуються на аналізі великих обсягів даних та використанні прогностичних моделей. Це дозволяє оптимізувати роботу енергетичних систем, розподіляти навантаження між різними джерелами енергії, підтримувати стабільність мережі в умовах змінних навантажень та впроваджувати енергоефективні технології.

Громадська безпека: відеоспостереження, системи реагування на

надзвичайні ситуації.

Відеоспостереження є ефективним інструментом для виявлення порушень громадського порядку, запобігання злочинам та забезпечення загальної безпеки. Сучасні системи відеоспостереження базуються на використанні високоякісних камер, які забезпечують чітке зображення та великий кут охоплення об'єкта спостереження. Застосування аналітичних алгоритмів дозволяє автоматично виявляти підозрілі або небезпечні ситуації, що допомагає оперативно реагувати на потенційні загрози. Системи реагування на надзвичайні ситуації включають в себе комплекс заходів та технологій, спрямованих на швидке та ефективне управління кризовими ситуаціями. Зразком таких систем можуть бути системи виявлення лісових пожеж чи, наприклад, інтелектуальна кіберфізична система моніторингу якості повітря [19].

Це може включати в себе автоматизовані системи сповіщення про небезпеку, системи віддаленого керування надзвичайними службами, системи евакуації та надзвичайних комунікацій [18, 20] .

Побут: інформаційні мережі зайняли важливу роль і у побутовому застосуванні, особливо в контексті системи "розумний дім".

Система "розумний дім" використовує інформаційні мережі для забезпечення автоматизації та контролю за різними аспектами домашнього життя. Її структура може включати управління освітленням, опаленням, кондиціонуванням повітря, безпекою та іншими системами. Завдяки чому система "розумний дім" може збирати дані з різних датчиків, аналізувати ці дані та використати їх для автоматичного контролю за системами дому [21] . Наприклад, автоматично вимкнути освітлення, коли в домі немає людей, або включити систему опалення, при зниженні температури.

Як бачимо, інформаційні системи задіяні без перебільшень у всіх сферах людської діяльності і варто зазначити, що розвиток бездротових технологій відіграє тут ключову роль, адже такі системи не вимагають прокладання кабелів, працюють через радіоканал просто у відкритому просторі і забезпечують наявність зв’язку, керування чи навігації навіть у віддалених і

складно доступних регіонах.

Бездротові системи значно полегшують доступ до повсякденних міських та домашніх мереж та застосунків. Майже кожному із нас зараз відомі значення таких термінів як Wi-Fi, Bluetooth, GPS, NFC, RFID, тощо. Тому саме бездротові системи будуть основним об’єктом подальших досліджень.

1.2. Структура та технології бездротових інформаційних систем та мереж

На сьогоднішній день така галузь телекомунікаційної індустрії обладнання і послуг як бездротові системи передачі інформації (БСПІ) розвивається особливо швидко. Швидке впровадження, вдосконалення і постійна адаптація до найбільш різноманітних задач бездротових технологій ініціює кардинальні перетворення в соціальній архітектурі суспільства, парадигмах державного управління, а також в механізмах економічної активності. Вони також впливають на стратегічні напрямки оборонної політики та повсякденні ритуали громадян. Згідно із прогнозами Міжнародного союзу електрозв’язку за умови активного використання бездротових технологій, очікується, що кількість пристроїв, що підключені до мережі, у найближчому майбутньому перевищить кількість підключених користувачів більш ніж у 6 разів (25,5 млрд. підключених пристроїв, проти 4 млрд. підключених користувачів) [22].

При цьому, на ринку пропонується досить широкий спектр обладнання безпровідного доступу, від найпростішого обладнання для організації локального безпровідного інтерфейсу (Bluetooth, Home RF, UWB) до обладнання для доступу в глобальні мережі і побудови безпровідних комп'ютерних мереж (Wi-Fi, WiMAX, DECT, GSM) [23, 24] .

Бездротова інформаційна мережа (БІМ) може складатися з різних компонентів, які взаємодіють між собою для забезпечення безперервного бездротового зв'язку між пристроями (Рис.1.1).

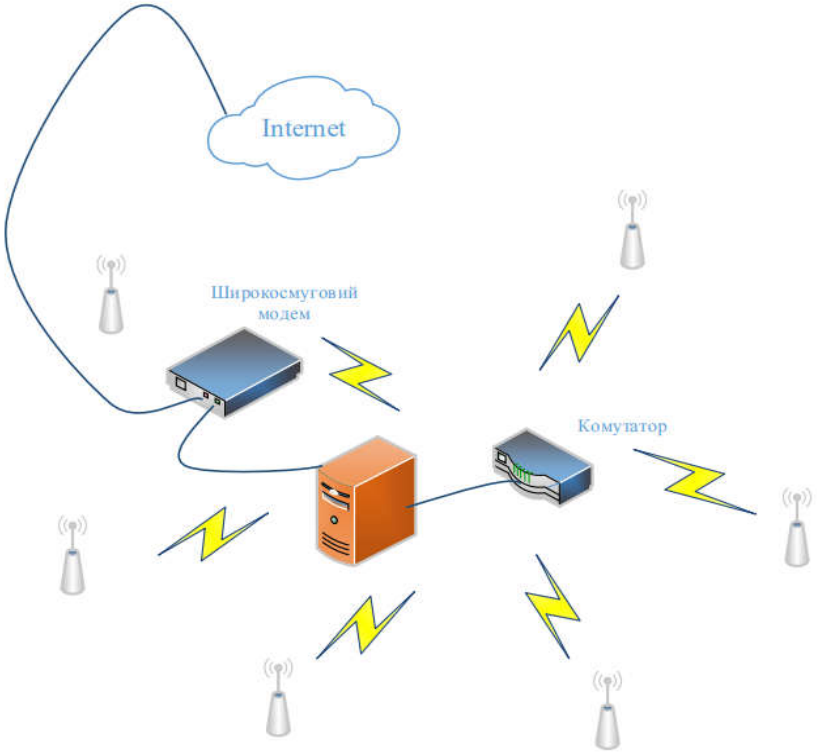


Рисунок 1.1. Типова структура бездротової інформаційної системи

Основні складові структури бездротової мережі включають у себе [25]:

1. Пристрої: Це комп'ютери, ноутбуки, смартфони, планшети, IoT-пристрої, датчики та інші пристрої, які мають можливість бездротового зв'язку.

2. Точки доступу (Access Points): Це пристрої, які створюють "покриття" безпровідної мережі і забезпечують з'єднання між бездротовими пристроями та провідною мережею. Точки доступу можуть бути обладнані пристроями зв’язку із різними стандартами бездротового зв'язку, такими як Wi-Fi, Bluetooth, Zigbee тощо.

3. Мережеві інтерфейси: Це бездротові карти (Wi-Fi, Bluetooth тощо) у пристроях, які дозволяють їм підключатися до бездротової мережі.

4. Мережеве програмне забезпечення: Це програмне забезпечення, яке керує безпровідним зв'язком, налаштуваннями мережі, захистом даних тощо. Включає в себе драйвери бездротових карт, протоколи комунікації (наприклад, TCP/IP), програми для налаштування мережі тощо.

5. Хаби і комутатори: Вони використовуються для розподілу даних між

пристроями в мережі. Хаби передають дані всім пристроям у мережі, в той час як комутатори спрямовують дані лише до призначеного отримувача.

6. Інтернет-шлюзи: Вони забезпечують доступ до Інтернету для безпровідних пристроїв, підключених до мережі.

7. Мережеве управління і безпека: Включає в себе програмне забезпечення для управління мережею, моніторингу та діагностики проблем, а також засоби забезпечення безпеки мережі, такі як аутентифікація, шифрування даних, брандмауери тощо.

Щоб обґрунтувати актуальність роботи із дослідження і покращення використання саме бездротових систем, можемо відобразити їх вплив на різні аспекти життя людини і описати детальніше деякі пункти:

1) Пристрої – бездротові системи знайшли широке застосування у цілій низці пристроїв, які функціонують і обмінюються даними без використання кабелю, і в теперішній час триває тенденція до переобладнання навіть звичних проводових девайсів у бездротовий варіант, зокрема:

– комп'ютери та ноутбуки. Ці пристрої використовують бездротові технології, такі як Wi-Fi (Wireless Fidelity), для підключення до локальних мереж або безпосередньо до Інтернету. Вони дозволяють користувачам працювати з даними та використовувати ресурси мережі без необхідності фізичного підключення кабелів;

– смартфони та планшети. Ці пристрої не лише підключаються до Wi-Fi для доступу до Інтернету, але також можуть використовувати мобільні мережі (які використовують бездротові технології, такі як 4G та 5G) для забезпечення доступу до даних там, де немає Wi-Fi. Ще одною бездротовою технологією, без якої неможливо уявити сучасний гаджет є супутникова навігація з використанням системи GPS;

– зарядні пристрої. Останнім часом у бездротових технологіях також почали використовуються енергетичні властивості електромагнітних хвиль, завдяки чому багато сучасних пристроїв мають можливість бездротового заряджання своєї акумуляторної батареї;

– IoT-пристрої та давачі. Цей пункт включає в себе широкий спектр пристроїв, від домашніх термостатів та вимикачів освітлення до "розумних" камер відеоспостереження та датчиків вологості. Вони використовують бездротові технології, такі як Wi-Fi, Bluetooth або навіть низькоенергетичний протокол зв'язку для IoT (наприклад, Zigbee або Z-Wave), щоб обмінюватися даними з іншими пристроями або хмарними сервісами;

– бездротові динаміки та навушники. Ці пристрої зазвичай використовують Bluetooth для бездротового з'єднання зі смартфонами, планшетами чи навіть комп'ютерами для відтворення аудіоконтенту;

– читальні пристрої (eReaders). Ці пристрої, такі як Amazon Kindle або Barnes & Noble Nook, використовують бездротові технології для завантаження електронних книг з Інтернету або інших джерел;

– домашні мультимедійні центри. Ці пристрої, такі як сучасні телевізори або стрімінгові приставки, можуть підключатися до Wi-Fi для доступу до відео-, аудіо- та інших медіаконтентів через Інтернет, а також бути під’єднаними до звукових станцій чи проекторів через протокол Bluetooth;

– геолокаційні пристрої. Сюди можна віднести GPS-навігатори, мобільні пристрої із GPS та інші геолокаційні пристрої, що використовують технологію супутникового зв’язку для отримання інформації про місцезнаходження.

2) Точки доступу. Бездротові точки доступу (Wireless Access Points або WAPs) є ключовим елементом будь-якої бездротової мережі. Вони виконують роль моста між бездротовими пристроями (наприклад, комп'ютерами, смартфонами, планшетами) та кабельною фізичною мережею.

Головні функціональні можливості точки доступу полягають у тому, що вона відповідає за керування підключенням пристроїв до мережі. Вона встановлює бездротове з'єднання з пристроями, автентифікує їх та надає доступ до ресурсів мережі, таких як дані з Інтернету або файли на локальному сервері.

Підключення до мережі: Точка доступу може працювати як самостійний пристрій або бути частиною глобальної мережевої інфраструктури, яка включає маршрутизатори, комутатори та інші пристрої.

Безпека: Точки доступу забезпечують захист мережі шляхом використання різноманітних протоколів шифрування, таких як WEP, WPA (Wi-Fi Protected Access), WPA2 або WPA3, що запобігає несанкціонованому доступу до мережі.

Широкий діапазон: Сучасні точки доступу підтримують різні бездротові стандарти, такі як 802.11ac, 802.11ax (Wi-Fi 6), які забезпечують високу швидкість передачі даних та покращену стабільність зв'язку [26].

Управління мережею: Деякі точки доступу мають можливість централізованого управління через спеціальне програмне забезпечення або хмарні платформи, що дозволяє адміністраторам керувати роботою мережі, та відслідковувати параметри її функціонування, включаючи налаштування безпеки, контроль пропускної здатності тощо.

Місцезнаходження: Деякі точки доступу можуть підтримувати технології місцезнаходження (наприклад, через Wi-Fi-маяки або RFID), що дозволяє визначати фізичне положення бездротових пристроїв у мережі.

Масштабованість і відновлення роботи в разі відмови: Бездротові системи набагато краще піддаються масштабованості та реструктуризації мережі за такої потреби, оскільки позбавленні головного обмеження, порівняно із іншими типами систем: вони не потребують прокладання кабелів зв’язку для безпосереднього електричного з’єднання між собою. Для зміни конфігурації бездротової системи достатньо лише замінити/встановити необхідне додаткове обладнання і провести його конфігурацію. Також бездротові системи можуть забезпечити вищу відмовостійкість, адже можуть автоматично переключатися на резервні канали зв’язку у випадках відмови основного каналу, при чому інший канал зв’язку (у випадку бездротової системи) може означати навіть звичайну зміну частоти каналу [27].

Управління пропускною здатністю: Деякі точки доступу можуть надавати можливості управління пропускною здатністю, що дозволяє призначати пріоритети для різних типів трафіку та обмежувати швидкість передачі даних.

Бездротові мережеві мости: будь-яка точка доступу у бездротових

мережах також може бути використана в якості моста або ретранслятора (точки розширення), що знову ж таки покращує масштабованість таких систем і дозволяє збільшувати зону покриття і максимальну дальність зв'язку між різними абонентами таких мереж із мінімальними затратами ресурсів.

3) Мережеві карти – це пристрої, котрі пов'язують кінцевого користувача з мережею, також їх називають кінцевими вузлами або станціями (host). Прикладом даних пристроїв є персональний комп'ютер чи робоча станція (потужний комп'ютер, який виконує функції, що вимагають великої обчислювальної потужності, як наприклад, обробка відео, моделювання фізичних процесів тощо).

Мережева карта – це друкована плата, котра вставляється в слот материнської плати комп'ютера, або зовнішній пристрій. Кожний адаптер NIC має свою унікальну MAC-адресу. Дана адреса використовується для організації роботи таких пристроїв у мережі. Мережеві пристрої здебільшого забезпечують транспортування даних, котрі необхідно передавати між пристроями кінцевого користувача.

Сьогодні складно знайти мережеві пристрої які виконують тільки одну функцію, як бачимо навіть звичайна точка доступу має широкий набір функцій і параметрів, які можна змінювати і налаштовувати. Часто виробники інтегрують в один пристрій декілька функцій, котрі раніше виконувалися окремими пристроями в мережі.

Через це поділ на типи пристроїв в теперішній час може бути досить умовним. Одним із прикладів такої інтеграції, є маршрутизатори з вбудованими DCHP-серверами.

1.3. Класифікація бездротових мереж

Серед усіх телекомунікаційних систем, системи на основі бездротових технологій передачі інформації розвиваються найбільш інтенсивно. На ринку

представлений широкий асортимент обладнання який в собі містить реалізацію тих чи інших бездротових технологій, призначених як для побудови чи приєднання до бездротових мереж (Wi-Fi, GSM, WiMax), так і для під'єднання периферійних пристроїв чи гарнітури, здійснення автентифікації, банківських розрахунків, відстеження чи навігації (Bluetooth, GPS, NFC, Bluetooth, RFID, FM-радіо, тощо).

При розгляді бездротових мереж передачі інформації за їх розміром і охопленням можна виділити чотири основні види, які представлені на рисунку.

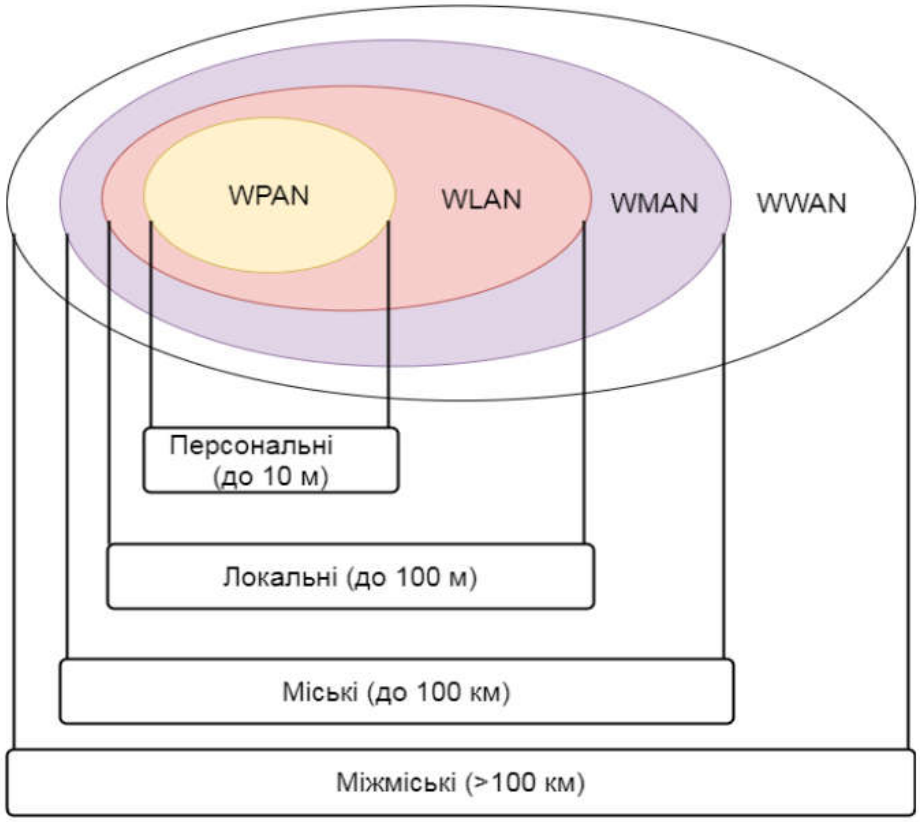


Рисунок 1.2. Основні види бездротових мереж за їх масштабом

– Бездротові персональні мережі (WPAN):

Радіус дії: від декількох сантиметрів до 10-15 метрів.

Призначення: з'єднання пристроїв в межах робочого місця, наприклад, телефону та ноутбука.

Швидкість передавання даних: від 10 Мбіт/с до 1 Гбіт/с.

Технології: Bluetooth, Zigbee, RFID, NFC (Near Field Communication).

– Бездротові локальні мережі (WLAN):

Радіус дії: до 100 метрів, може бути більше з використанням підсилювачів.

Призначення: створення бездротових мереж в будівлях і на відкритих майданчиках для доступу до Інтернету.

Швидкість передачі даних: від декількох Мбіт/с до десятків Гбіт/с в залежності від стандарту Wi-Fi.

Технології: Wi-Fi 802.11a/b/g/n/ac/ax.

– Бездротові міські мережі (WMAN):

Радіус дії базової станції: до 10 км.

Призначення: побудова розподілених бездротових мереж в містах або корпоративних середовищах.

Швидкість передачі даних: від декількох Мбіт/с до сотень Мбіт/с.

Технології: WiMAX (IEEE 802.16), LTE (Long-Term Evolution), 5G.

– Бездротові глобальні мережі (WWAN):

Радіус дії: покриття може охоплювати великі території або навіть всю планету за допомогою супутників.

Призначення: глобальний доступ до мережі з будь-якого місця на Землі.

Швидкість передачі даних: від кількох кілобіт/с до десятків Мбіт/с залежно від технології.

Технології: GPRS, EDGE, 3G, 4G LTE, 5G, StarLink, GPS та інші супутникові мережі.

Ці типи мереж використовуються в різних сферах, від особистих зв'язків до комерційних та військових застосувань.

Вони забезпечують широкі можливості для зв'язку та доступу до інформації у будь-якому місці і в будь-який час.

1.4. Технології безпровідних інформаційних систем

Бездротові технології – дуже широке поняття, яке включає в себе різноманітні технології та системи, що служать для передачі інформації на

відстань кількома точками, не вимагаючи при цьому їх з’єднання дротами. Для передачі інформації можна використати оптичне або лазерне випромінювання, інфрачервоне випромінювання чи радіохвилі. Існує декілька бездротових технологій, найчастіше відомих користувачам за їх маркетинговим назвами, наприклад такими як Wi-Fi, WiMAX, Bluetooth, тощо [28, 29].

Бездротові технології зазвичай призначені для організації магістральних каналів зв’язку та так званої ефективної "останньої милі" зв’язку незалежно від існування існуючих каналів зв’язку. Порівняно з традиційними дротовими мережами бездротова технологія має ряд переваг. Однією з таких головних переваг є можливість зручно і швидко встановлювати мережеві з’єднання в з будь-якої точки. Широке застосування бездротових мереж в громадських місцях дозволяє встановлювати зв’язок з мережами Інтернет, обмінюватися електронною поштою і файлами, завантажувати інформацію.

Бездротові технології достатньо прості та недорогі з точки зору їх монтажу. Вартість домашніх та комерційних бездротових пристроїв стабільно продовжує знижуватися. Проте, незважаючи на зниження вартості, при цьому швидкість передачі даних зростає, а функціональність цих пристроїв покращується, що забезпечує більшу швидкість і надійність зв’язку. Бездротові технології розширюють можливості застосування мереж, уникаючи обмежень, що властиві кабельним з’єднанням.

WiMAX. Worldwide Interoperability for Microwave Access – жаргонна назва технології, метою розробки якої є надання універсального бездротового зв'язку на великих відстанях і для різноманітних пристроїв (робочих станцій, портативних комп'ютерів, мобільних телефонів). Заснована на стандарті IEEE 802.16, назва якого Wireless MAN. Насправді, це два стандарти. Стандарт WiMAX IEEE 802.16d: безпровідний зв’язок між стаціонарними вузлами, до яких територіально прив’язані користувачі. Пропускна здатність до 70 Мбіт/с, радіус дії радіохвиль до 80 км. На базі таких ліній зв’язку створюють муніципальні мережі. Стандарт WiMAX IEEE 802.16e: для мобільних користувачів. Пропускна здатність до 40 Мбіт/с, радіус дії радіохвиль до 5 км.

Wi-Fi. Технологія бездротового зв’язку, відома як Wi-Fi або Radio Ethernet IEEE 802.11, представляє собою перший промисловий стандарт, що дозволяє створювати бездротові локальні мережі (WLAN) на невеликій території. Це означає, що декілька користувачів можуть мати однаковий доступ до спільного каналу передачі даних.

Цей стандарт було розроблено Інженерним інститутом електротехніки та радіоелектроніки (IEEE) і його можна розуміти як аналог до стандарту 802.3 для традиційних дротових Ethernet мереж. Центральним елементом бездротової мережі Wi-Fi є точка доступу (Access Point), яка може бути підключена до наземної мережевої інфраструктури, і здійснювати передачу радіосигналу [30].

Цей стандарт здобув широкого поширення і використання, що спонукало його подальший розвиток. Так, організація Wi-Fi Alliance вже представила новітній стандарт бездротового зв’язку Wi-Fi 802.11ah, відомий як "Ha Low". Діапазон частот цього стандарту становить 900 МГц. На цій частоті сертифіковані Wi-Fi пристрої зможуть працювати на порівняно більшій відстані і з мінімальними витратами енергії. На відміну від існуючих сьогодні стандартів із частотами 2,4 ГГц і 5 ГГц, Wi-Fi 802.11ah збільшує радіус дії сигналу щонайменше вдвічі, забезпечуючи надійніший зв’язок, навіть коли на шляху від абонента до точки доступу радіохвилі долають серйозні перешкоди, такі як стіни і перекриття. Особливу увагу слід звернути на те, що новий стандарт, завдяки використанню альтернативної частоти, не так піддається впливу завад від мікрохвильових печей та інших побутових приладів. [31]

Стандарти для бездротового зв’язку WiFi беруть початок ще з 1997 року із прийняттям стандарту для бездротових мереж IEEE 802.11. Станом на зараз, сімейство стандартів WiFi вже містить такі специфікації:

802.11 – перший стандарт. Забезпечує роботу на швидкості від 1 до 2 Мбіт/с.

802.11a – стандарт WLAN для пристроїв із частотою 5 ГГц. Дозволяє забезпечити швидкість до 54 Мбіт/с.

802.11b – покращений стандарт частоти 2,4 ГГц. Дозволяє збільшити

швидкість передавання до 11 Мбіт/с.

802.11e – стандарт, який регламентує єдині вимоги до якості запитів, що повинні підтримуватися інтерфейсами WLAN сімейства IEEE.

802.11f – регламентує взаємодію між точками доступу одного рівня.

802.11g – покращений стандарт WLAN 2.4 ГГц, у якому прописана нова підтримувана техніка модуляції. Дозволяє підняти швидкість передачі до 54 Мбіт/с для мереж на частоті 2.4ГГц.

v802.11h – окремий стандарт для частоти 5 ГГц, який описує використання WLAN в регіонах Європи і Азії.

802.11i – стандарт, який містить оновлення в протоколах безпеки і системи автентифікації, що виправляє проблеми із захищеністю, властиві для попередніх версій.

Bluetooth. Технологія Bluetooth (відповідає стандарту IEEE 802.15) представляє собою першу розробку в області організації бездротових персональних мереж (WPAN – Wireless Personal Network). Ця технологія дозволяє ефективно передавати голосові дані та цифрову інформацію через радіоканал на невеликих відстанях від 10 до 100 метрів в діапазоні частот 2,4 ГГц. Вона також дозволяє з'єднання мобільних телефонів, персональних комп'ютерів та інших пристроїв. У даний час стандарт Bluetooth налічує в собі понад 10 профілів, які представляють собою набори функцій для пристроїв, що використовують технологію Bluetooth.

Групою розробників SIG затверджені такі базові профілі:

– A2DP (Advanced Audio Distribution Profile) профіль, який описує передавання музики у бездротові навушники;

– AVRCP (Audio / Video Remote Control Profile) профіль керування телевізорами;

– FTP (File Transfer Profile) профіль, який дозволяє здійснювати обмін файлами і даними;

– HFP (Hands-Free Profile) профіль, який також описує роботу із бездротовими навушниками, але для завдань розмови по телефону;

– LAP (LAN Access Profile) профіль, який дозволяє за допомогою іншого Bluetooth-пристрою мати доступ до мереж LAN, WAN або Internet;

– SAP, або просто SIM (SIM Access Profile) профіль для надання доступу до SIM-картки пристрою через Bluetooth;

Узагальнюючи, можна стверджувати, що технологія Bluetooth володіє всіма перевагами бездротових систем, включаючи мобільність та компактність; простоту використання готових модулів; високу швидкість передачі; достатній рівень безпеки даних; доступність; необхідність авторизації пристрою; низький поріг чутливості до перешкод (залежно від товщини та матеріалу перешкоди); достатньо високий рівень стандартизації. Проте, ця технологія має і свої недоліки: наприклад, якщо двоє користувачів бажають здійснити обмін даними, то під час пошуку пристроями один одного будуть виявлені всі увімкнені пристрої, які знаходяться на відстані 10-15 метрів, що може викликати значну затримку при початковій ініціалізації сеансу зв’язку між пристроями.

ZigBee. Технологія бездротової передачі даних ZigBee виникла на ринку після впровадження Bluetooth та Wi-Fi. Розробка технології ZigBee була обумовлена, перш за все, необхідністю забезпечення невисокої вартості та низького енергоспоживання апаратної частини для застосунків, таких як дистанційне керування воротами, пристроями освітлення, отримання інформації з давачів. Мережі ZigBee відносяться до мереж, що само-організовуються та самовідновлюються. Завдяки своєму програмному забезпеченню такі пристрої самостійно знаходять одне одного, встановлюють зв’язок і утворюють мережу, а при виході з ладу певного вузла інші пристрої мають привілеї на реорганізацію мережі і зміну маршруту.

Порівняно із Wi-Fi, використання ZigBee має перевагу за відношенням "дальність/швидкість/енергоспоживання". Але поряд з цим має декотрі недоліки: рівень стандартизації протоколу є не вичерпний, відсутня єдина апаратна чи програмна база для проектування програм високої складності; не надто швидка передача інформації (якщо брати абсолютну оцінку, без відношення до інших параметрів); а також висока ймовірність обмежень

сумісності у роботі між пристроями різних виробників.

NFC. Технологія високочастотного електромагнітного зв'язку малого радіусу дії. Вона дозволяє обмінюватися даними між пристроями, що знаходяться на відстані менше 20 см. Технологія схвалена ISO / IEC як стандарт ECMA. Вона є розширенням технології безконтактних комунікацій стандарту ISO 14443.

У стандарті NFC реалізується електромагнітний зв'язок між двома рамковими антенами, що знаходяться в межах 20 см одна від одної, без застосування феромагнітного сердечника. Технологія працює в діапазоні частот близько 13,56 МГц, має ширину смуги пропускання майже 2 МГц. Швидкість передачі даних – 106, 212 або 424 кбіт / с. Дана технологія застосовується насамперед у мобільних пристроях.

NFC-пристрої можуть використовуватися:

– в якості безконтактної картки для оплати різних послуг, наприклад проїзду в громадському транспорті;

– для зчитування RFID-міток в магазині;

– для спільної роботи з пристроями, що працюють за технологією Bluetooth, зокрема для передачі по Bluetooth даних з одного мобільного телефону на інший. Для цього достатньо зблизити на відстань менше 20 см два мобільних телефони, що підтримують цю технологію, або просто стикнутися ними;

– в якості електронних ключів для доступу до пристрою або проходу в приміщення;

– як посвідчення особи, тощо.

Окрім стандартизованих і ліцензованих протоколів і засобів бездротового радіозв’язку, для користування є доступними спеціальні діапазони радіочастот, котрі можна займати своїми власними застосунками і пристроями, без необхідності оформлення додаткових документів (зокрема в Українському Державному Центрі Радіочастот). В Україні такі діапазони прописані в

регулюючих документах, зокрема у Національній таблиці розподілу смуг радіочастот [32] .

Найменш обмеженими для аматорського та побутового використання є частоти, що знаходяться в таких діапазонах як 868/915 МГц, 2.4 ГГц та 5.8 ГГц, ці діапазони в Україні узгоджені із аналогічними Європейськими стандартами використання ефіру [33,34] .

IR 2030 Short Range Devices

Interface / Notification number / Date	Application	Comments to application	Frequency band	Maximum transmit power / Power spectral density / Fieldstrength	Comments to Maximum transmit power / Power spectral density / Field strength	Channelling	Channel access and occupation rules	Informative Reference
IR2030/1/38	Non-specific short-range devices	Airborne use is notpermitted.	918.5 - 918.9 MHz 919.7 - 920.1 MHz	100 mW e.r.p.			Duty Cycle limit ≤ 0.01% and limited to a maximum transmit on-time of 5ms/1s	EN 300 220
IR2030/1/22	Non-specific short-range devices	Equipment may beused airborne.	2400 - 2483.5 MHz	10 mW e.i.r.p.				EN 300 440
IR2030/1/23	Non-specific short-range devices	Equipment may beused airborne.	5725 - 5875 MHz	25 mW e.i.r.p.				EN 300 440
IR2030/1/24	Non-specific short-range devices	Equipment may beused airborne.	24.150 - 24.250 GHz	100 mW e.i.r.p.				EN 300 440
IR2030/1/45	Non-specific short-range devices	Equipment may be used airborne.	57 - 64 GHz	100 mW e.i.r.p. 13 dBm/MHz e.i.r.p. 10 dBm transmitter power				EN 305 550

Рисунок 1.3. Регламент частот згідно стандарту IR2030 [33]

Як бачимо із рисунку, у зведеній таблиці документу IR2030 є прописаний регламент використання для кожних конкретних смуг частот із вказанням максимальної допустимої потужності передавачів для цих діапазонів. Додатково у декотрих полях можна спостерігати примітки "Airborne use is not permitted" або "Equipment may be used airborne", що вказує нам на заборону або дозвіл використання цієї частоти у передавачах, що будуть встановлені у пристроях які можуть здійснювати переміщення повітрям.

Використання цих частот дуже поширене радіолюбителями та конструкторами, що займаються робототехнікою та дистанційно керованими

пристроями, серед яких особливе місце останнім часом займають безпілотні апарати (БПА).

Сучасні безпілотні пристрої із дистанційним керуванням стрімко розвиваються і займають все нові ніші у повсякденній людській діяльності. Якщо колись вони переважно були предметом хобі окремих ентузіастів (машинки з радіокеруванням, кораблики, тощо.), то тепер такі пристрої перекривають широкий спектр задач, навіть на рівні організацій та держави – від моніторингу стану конструкцій і контролю території аграріїв, аж до пошуково-рятувальних та військових операцій [35-38].

Одним із видів таких дистанційно керованих пристроїв є безпілотні літальні апарати (БПЛА), або їх комплекси, що було розглянуто в опублікованій раніше статті за тематикою дисертації [39]. Безпілотна авіація в теперішній час активно розвивається та інтегрується до глобальної авіаційної системи загалом. Розроблення, випробування та використання безпілотних авіаційних систем проводиться в наш час майже в усіх країнах світу, зокрема і в Україні.

На актуальність даного питання вказують і інші автори і дослідники, зокрема Станіслав Слободяник, та співавтори у роботі [40] висвітлили поточне зростання і приватного і державного інтересу до БПЛА-систем, зокрема у військовій сфері, де держава виступає основним замовником, споживачем і інвестором. Висвітлюється також стрімкий історичний розвиток та оцінені перспективи майбутнього розвитку використання БПЛА, включаючи автономні системи та рої дронів.

Одними із найбільш актуальних напрямків сучасних досліджень з метою покращення характеристик стійкості роботи як самого апарату, так і його систем навігації є розробки систем навігації на основі штучного інтелекту, моделей нечіткої логіки, тощо [37-38,40-41].

Такі системи дозволяють як летіти і орієнтуватися на місцевості апарату в автономному режимі, так і виконувати якісь певні задачі в автономному режимі польоту. Такі засоби частково задовольняють виконання поставлених перед БПЛА задач, та підвищують можливості управління безпілотними апаратами, в

тому числі у випадку втрати зв’язку. Але ці рішення не задовольняють задачу захисту самого каналу зв’язку із апаратом і не забезпечують виконання завдань, які потребують постійного моніторингу отримуваних від БПЛА параметрів чи своєчасного коригування його роботи оператором, що в певних умовах може бути дуже суттєвим обмеженням для використання БПЛА.

1.4. Особливості застосування інформаційних бездротових систем у мережах та комунікаціях військового призначення

Інформаційні мережі застосовуються у багатьох сферах діяльності військових формувань і наближених до них цивільних організацій. У таких комунікаціях важлива швидка та безперебійна передача інформації з високим рівнем конфіденційності та захисту, а також висока мобільність засобів зв’язку. Завдяки цьому, при побудові сучасних інформаційно-телекомунікаційних систем зв’язку військового призначення провідне місце займають технології бездротового зв’язку на основі радіохвиль [42] .

Основні сфери застосування таких комунікацій у військовій справі:

Командне-керівництво: Військові інформаційні мережі використовуються для керування військовими операціями, обміну командними та тактичними даними між командуванням та підрозділами на полі бою, а також для координації дій різних військових формувань.

Розвідка та розвідувальні операції: Інформаційні мережі використовуються для збору, обробки та аналізу розвідувальної інформації, що дозволяє здійснювати ефективний розвідувальний процес та приймати обґрунтовані рішення.

Логістика та управління ресурсами: Інформаційні мережі допомагають військовим організаціям у керуванні постачанням, логістичною підтримкою та управлінні ресурсами під час ведення військових операцій.

Медицина та евакуація: У військових госпіталях та медичних стабілізаційних пунктах інформаційні мережі використовуються для електронного медичного обліку, моніторингу стану поранених, їх кількості, та

обміну оперативною медичною інформацією із медичними установами.

Кібербезпека та захист інформації: Військові інформаційні мережі обов’язково включають в себе системи кіберзахисту, які забезпечують захист від атак, та засобів придушення зв’язку, здійснюють шифрування конфіденційної інформації та контроль доступу до систем.

Навчання та тренування: Інформаційні мережі використовуються для проведення навчальних та тренувальних заходів, моделювання військових сценаріїв, симуляції бойових дій та обміну досвідом між військовими підрозділами.

Бездротові інформаційні системи та мережі грають ключову роль у військових системах зв'язку та системах, що можуть мати подвійне призначення, забезпечуючи передачу даних, команд, координацію дій, за одночасного забезпечення необхідного рівня безпеки такої комунікації. Зокрема, про це чітко свідчить досвід проведення бойових дій у сучасних військових конфліктах – високоякісна система управління військовими силами стає однією з ключових умов успішного виконання бойових завдань, адже оперативне управління військами необхідно здійснювати практично в режимі реального часу [43].

Система військового зв’язку, що буде використовуватися у процесі вирішення цих завдань, повинна відповідати жорстким вимогам бойової готовності, функціональної сумісності, стійкості, мобільності, пропускної спроможності та безпеки [44,45].

Основні критерії виконання таких вимог функціонування:

Захищеність даних: такі інформаційні мережі повинні мати найвищий рівень захищеності, оскільки вони обмінюються найбільш конфіденційною та важливою інформацією.

Резервування та відновлення: Системи повинні бути здатні до автоматичного переключення на резервні канали у разі відмови або атаки.

Конфіденційність та автентифікація: Важливо мати механізми для перевірки ідентичності та автентифікації користувачів, щоб уникнути

несанкціонованого доступу.

Мобільність та спілкування в режимі реального часу: Інформаційні мережі повинні забезпечувати миттєву передачу даних та команд для оперативного реагування на зміни в ситуації. Використовувані у них системи зв'язку повинні бути здатні до роботи в динамічних умовах, наприклад, на полі бою або під час виконання розвідувальних операцій, що вимагає від них швидкого розгортання, можливості передавання інформації на великі відстані, тощо [46].

В сучасних умовах ведення бойових дій, а також спираючись на досвід АТО та ООС, система зв'язку ЗС України зазнала кардинальних змін, зокрема таких як застосування самоорганізованих мереж та перехід на сучасні цифрові засоби зв'язку. Так, на початках проведення гібридної війни у Східних регіонах нашої країни ЗСУ мали у використанні застарілі, в основному аналогові, засоби зв'язку, які були дуже слабо захищені і не придатні до використання в умовах проведення бойових дій.

Оскільки виробничих потужностей і запасу часу на розробки нових засобів бракувало, Збройні Сили України комплектувалися цивільним обладнанням радіозв'язку, яке зарекомендувало себе значно краще, але все ж не задовольняло вимоги, що висуваються до зразків озброєння та військової техніки, таких як застосування у важких погодних умовах, протидія засобами радіоелектронної боротьби та радіоелектронної розвідки, надійна система шифрування, тощо.

Незважаючи на такі недоліки, тенденція застосування Збройними Силами засобів передачі даних, що походять із комерційних компаній, продовжується й надалі і такі пристрої знаходять широке застосування у військовій сфері.[47]

У теперішній час це зумовлено основним чином через дуже широку лінію бойового зіткнення і масштабність вторгнення, що вимагає великої кількості засобів зв'язку одночасно. Така потреба в даний час не може бути закрита лише засобами виключно військового зв'язку.

Головною особливістю застосування інформаційних систем і мереж у військових умовах є те, що в теперішніх конфліктах збройні сили здійснюють

часті оперативні маневри на місцевості і зв’язок та керування ними здійснюється майже повністю за допомогою бездротових систем, переважно із застосуванням радіозв’язку та радіоелектронних засобів.

Це тягне за собою значне поширення та розвиток засобів радіо-електронної боротьби, завдання яких вивід з ладу систем керування та зв’язку противника, зниження ефективності засобів технічної розвідки, зниження точності окремих видів озброєнь. Такий вплив може мати короткостроковий тимчасовий або досить тривалий характер, в окремих випадках застосування засобів РЕБ у комбінації із іншими засобами ураження може призводити навіть до знищення радіо-електронних засобів [48].

Можливі режими роботи засобів РЕБ, їх потужності, частотні діапазони і інші робочі характеристики визначаються у їхніх тактико-технічних характеристиках (ТТХ). Якщо проаналізувати ТТХ вже існуючих і використовуваних засобів РЕБ [49-53], а також перспективних розробок у складі ЗС РФ та інших держав, можна побачити особливості і тенденції їх розробок:

– масове виготовлення і постановка невеликих але дуже мобільних засобів РЕБ невисокої потужності для локального використання;

– початок використання БПЛА у якості носіїв засобів ретрансляції, радіоелектронної розвідки та придушення;

Як найоптимальніший при цьому розглядається варіант застосування загороджувальних завад широкого набору (гармонічні, шумові, псевдохаотичні, тощо). Вони подавлюють і виводять з ладу канали зв’язку не залежно від типу модуляції сигналу, кодування, тощо, що значно скорочує час реакції пристроїв РЕБ, оскільки не потрібно попередньо аналізувати структуру сигналу, для гарантованого придушення достатньо лише забезпечити необхідний рівень потужності встановлюваних завад [54].

Поширення БПЛА зачепило і військову сферу. На даний момент основна частина повітряних розвідувальних операцій, коригування вогню артилерії, планування і супровід наступальних чи оборонних операцій проводяться виключно із засобами безпілотної авіації. Що зумовлює критичну потребу у

надійному зв’язку, стійкому до засобів придушення та радіоперехоплення, адже при роботі БПЛА у тилу противника, чи над лінією зіткнення вивід з ладу каналу зв’язку із безпілотником, чи системи його керування призведе до безповоротної втрати апарату. Виконання бойових чи розвідувальних завдань потребує постійного моніторингу отримуваних від БПЛА параметрів чи своєчасного коригування його роботи оператором, тому більшість військових застосувань БПЛА не є автономними, а майже повністю керованими оператором [55].

За повідомленнями ГУР МО України, засоби РЕБ зараз дуже активно застосовуються саме для ведення розвідки за роботою БПЛА, блокування ліній радіозв’язку, виведення з ладу систем зв’язку на основі GSM-технології та систем навігації на основі GPS-технології, що може значно ускладнювати використання безпілотних авіаційних комплексів [56].

При втраті основного каналу зв’язку і керування безпілотником, порівняно із цивільним використанням, в бойових умовах у нас зазвичай не буде можливості дістатися місця втрати зв’язку із БПЛА, щоб знайти і забрати апарат.

Висновки до 1 розділу

В даному розділі було розглянуто та проаналізовано аспекти застосування інформаційних мереж для обміну і передавання даних, використовувані у них технології, зокрема бездротові системи обміну даними, проаналізовано їх поточне використання у сферах діяльності людини, як цивільного спрямування так і військового.

В результаті спостерігаємо таку тенденцію, що у сучасному світі інформаційні системи та мережі зайняли провідне місце у найбільш різноманітних сферах діяльності людини, від повсякденних цивільних і побутових потреб, до інформаційно-аналітичних систем військових формувань, та засобів військового зв’язку. Через це спостерігаємо постійний ріст потреб у швидкості передавання та обсягах передаваних даних.

Серед технологій функціонування інформаційних систем найбільш актуальним і передовим напрямком розвитку є бездротові телекомунікаційні технології. Використання і популярність бездротових систем пов'язані з їхніми значними перевагами перед іншими системами: вони забезпечують відносно легку побудову як великих і розгалужених мереж, так і простого з’єднання двох абонентів за принципом "точка-точка", такі системи легко масштабувати, один пристрій може поєднувати в собі багато функцій, окрім безпосередньо встановлення зв’язку (наприклад, автентифікація, регулювання швидкості трафіку, вибір каналу зв’язку, тощо).

Другий аспект висновку – високий розвиток технологій бездротового зв’язку є одним із факторів, який сприяв розвитку безпілотних пристроїв, які зараз є передовим напрямком розробок в області сучасних технологій.

Безпілотні апарати дозволяють проводити виміри, спостереження чи маніпуляції в тому чи іншому середовищі, на великій відстані, висоті чи глибині без присутності оператора. Така їх особливість корисна у важкодоступних місцях і абсолютно незамінна при необхідності роботи в обстановці, де присутність людини шкідлива для здоров’я або небезпечною для життя.

Результати аналізу вказують, що аналогічні тенденції спостерігаються і для систем зв’язку військового призначення. У теперішніх реаліях проведення бойових дій, та із врахуванням досвіду АТО та ООС, повномасштабного вторгнення росії в Україну, бездротові системи стали основою систем зв’язку військового призначення. Радіозв’язок надає вагому перевагу за рахунок підвищення мобільності військових формувань, оперативності командування, розвідки, планування операцій та інших задач. Особливу роль у теперішньому конфлікті відіграє розвиток та використання безпілотних авіаційних систем. Безпілотні комплекси застосовуються для розвідки, спостереження, коригування роботи інших формувань, для нанесення безпосереднього ураження самим безпілотником, та навіть для налагодження і покращення характеристик зв’язку (безпілотники-ретранслятори).

В ході аналізу виявлено таку проблему – через широкий масштаб фронту,

великі залучені сили і, відповідно, великі запити на зв’язок у Збройних Сил України, потужностей виробництва і матеріального забезпечення для перекриття таких запитів у даний час критично бракує. Це спричинило використання у військовій сфері засобів зв’язку цивільного походження та цивільного призначення для перекриття нагальних потреб у зв’язку. Аналогічна ситуація і з БПЛА: промислових військових апаратів із відповідними характеристиками не достатньо навіть для часткового покриття потреб армії, через що більша частина безпілотників збирається із запчастин і деталей цивільного походження.

З цього можна констатувати, що задачі щодо захисту бездротових систем наразі є дуже актуальними і потребують подальшої роботи та аналізу щодо їх вирішення. Тому особлива увага у роботі буде присвячена проблематиці захисту бездротових систем, зокрема таким, що можуть мати подвійне призначення, а також питанням захисту бездротових систем зв’язку і керування безпілотними пристроями. Основний акцент при цьому слід зробити саме на способи покращення захищеності і стійкості існуючих бездротових технологій, які відносно нещодавно перемістилися із цивільної сфери і знайшли своє військове використання. Захист таких систем, у теперішній час, Збройними Силами потребується найбільш гостро.

РОЗДІЛ 2. ПРОБЛЕМАТИКА ЗАХИСТУ ІНФОРМАЦІЇ ПРИ ПЕРЕДАВАННІ БЕЗДРОТОВИМИ СИСТЕМАМИ

Передавання інформації з обмеженим доступом у інформаційних мережах є невід'ємним аспектом використання сучасних комунікацій. Цей процес вимагає іншого порядку організації зв'язку із визначеними, строгими правилами та включає в себе певні ключові елементи забезпечення інформаційної безпеки, які варто розглянути [57].

Криптографія: Криптографія – основа безпеки інформації. Вона використовує математичні алгоритми для шифрування даних, що робить їх незрозумілими для тих, хто не має відповідного ключа для розшифрування.

Протоколи безпеки: Протоколи безпеки, такі як SSL/TLS та HTTPS, забезпечують безпечне з'єднання між двома сторонами в мережі. Вони використовують криптографію для захисту даних від перехоплення та модифікації.

Системи ідентифікації та аутентифікації: Системи ідентифікації та аутентифікації використовують для перевірки особи користувача, який намагається отримати доступ до інформації. Вони можуть включати в себе паролі, біометричні дані, двофакторну автентифікацію та інше.

Політики доступу: Політики доступу визначають, хто має право доступу до певної інформації та як цей доступ контролюється. Вони можуть бути особливо важливими для організацій, на яких обробляється конфіденційна інформація.

Фізична безпека: Фізична безпека є важливою частиною захисту інформації. Вона може включати в себе заходи, такі як блокування серверних приміщень та захист від несанкціонованого фізичного доступу.

Резервне копіювання та відновлення: Резервне копіювання даних та їх відновлення є основою для забезпечення їх цілісності та доступності у випадку втрати або пошкодження.

Ці елементи разом формують комплексний підхід до передавання інформації з обмеженим доступом в інформаційних мережах. Вони допомагають забезпечити, що конфіденційна інформація залишається недоступною для несанкціонованого доступу.

2.1. Структура рівнів захисту інформації в безпровідних мережах на основі моделі OSI

Безпека бездротових мереж (БМ) сьогодні є одним з актуальних завдань Національної стратегії Індустрії 4.0 щодо комунікаційних технологій функціонування інтелектуальних об'єктів у сферах: освіти, медицини, банківської сфери, транспортної інфраструктури, енергетики, екології [58].

На практиці ефективно застосовують безпровідні мережі: міські – IEEE 802.16 (Wi-MAX); глобальні – UMTS, GSM, LTE; локальні IEEE 802.11 (Wi-Fi); IEEE 802.15.4a (ZigBee); персональні – IEEE 802.15.1(Bluetooth). Мережева модель взаємодії таких відкритих систем OSI є прийнята і впроваджена на державному рівні відповідним стандартом ДСТУ. [59] Вона дозволяє аналізувати загрози основним профілям безпеки інформації БМ відповідно до рівнів: фізичного, мережевого, канального, транспортного, прикладного, сеансового, представлення.

В межах моделі OSI взаємодія обидвох систем відбувається у вигляді двох моделей – горизонтальної та вертикальної [60].

У горизонтальній моделі розглядається взаємодія між застосунками одного рівня у обидвох кінцевих точках; така взаємодія вимагає підтримки абонентами однакових протоколів для певного рівня. У вертикальній моделі розглядається взаємодія рівнів лише на стороні одного із абонентів, використовуючи відповідні інтерфейси. На одній стороні кожний рівень або надає послуги рівню вище, або отримує їх від рівня нижчого за свій (за винятком прикладного і фізичного рівнів: прикладний надає послуги користувачу, а фізичний не використовує послуг ніяких сервісів).

Розглянемо технології безпеки безпровідних мереж (БМ) згідно з загрозами рівням моделі OSI.

Фізичний рівень. Тут загрозами є такі: фізичні крадіжки даних та устаткування; втрата потужності; фізичне пошкодження або знищення даних і устаткування; зовнішні несанкціоновані зміни у функціональному середовищі (додавання/видалення ресурсів, передачі даних, змінних носіїв); приховане перехоплення даних з клавіатури чи інших засобів вводу інформації; вимкнення фізичних каналів передачі даних. Технології безпеки: електронний механізм блокування для реєстрації та авторизації; застосування PIN-кодів і паролів; біометричні системи аутентифікації; закриття периметру і корпусів мережі; відео та аудіо спостереження; електромагнітне екранування.

Канальний рівень. Тут загрозами є такі: підміна MAC-адреси; обхід технологій VLAN; spanning Tree для передавання пакетів у нескінченний цикл; використання помилок алгоритму; затоплення комутаторами всіх портів; несанкціоноване підключення до БМ. Технології безпеки: не використовувати вразливі засоби мереж VLAN для захисту інформації; БМ необхідно захищати з використанням вбудованого шифрування, автентифікації та фільтрації MAC-адрес; фізична ізоляція різних зон мережі за допомогою брандмауерів.

Мережевий рівень. Тут загрозами є такі: підміна IP-адреси – джерело помилкового рішення після дії шкідливих пакетів; підміна маршруту – поширення неправдивої топології мережі; проблеми одноразової ідентифікації. Технології безпеки: моніторинг програмного забезпечення для мінімізації можливих зловживань; використання міжмережевих екранів із потужною політикою фільтрації; застосування політики управління маршрутами – жорсткі фільтри маршрутів і антиспуфінг.

Транспортний рівень. Тут загрозами є такі: перевантаження транспортного рівня через велику кількість звернень до номерів портів обмежує можливості ефективної фільтрації трафіку; неправильне передавання пакетів; відмінності в реалізації транспортних протоколів дають можливість здійснити несанкціонований доступ; механізми передавання пакетів можуть слугувати

предметом підміни атак на базі сформованих пакетів і спричиняти руйнування чи захоплення контролю над мережами. Технології безпеки: строгі правила брандмауера, які обмежують доступ до певних протоколів (наприклад, номер портів TCP/UDP або тип ICMP); посилення механізмів ідентифікації з'єднань для уникнення атак та захоплення контролю над мережами; перевірка брандмауером усіх пакетів з аналізом вмісту і з'єднання дозволяє надійно закрити доступ до мереж шкідливим пакетам.

Сеансовий рівень. Тут загрозами є такі: передача під час сеансу інформації (ім'я користувача та пароль) у відкритому вигляді, що дозволяє її перехоплення і несанкціоноване використання; ідентифікація сеансу може бути предметом підміни і викрадення; здійснення атак на облікові дані з метою доступу на встановлення сеансу; слабкий чи відсутній механізм автентифікації; витік інформації через невдалі спроби автентифікації. Технології безпеки: зашифрований обмін та зберігання паролів; обмежений термін дії для паролів і повноважень користувачів; обмеження невдалої спроби встановлення сеансу за допомогою механізму синхронізації; захист інформації про ідентифікацію сеансу за допомогою криптографічних засобів.

Рівень представлення. Тут загрозами є такі: ; криптографічні недоліки може бути використано для обходу захисту конфіденційності; ненавмисне чи необачне використання зовнішніх даних, які вводяться в контексті управління може привести до віддаленої витоку інформації; погана обробка даних може привести до збою програм. Технології безпеки: ретельний і безперервний огляд рішень криптографії для забезпечення завдань безпеки відносно загрози; контроль дій користувачів та функцій управління; ретельна перевірка даних, які вводяться до програми.

Прикладний рівень. Тут загрозами є такі: збої програмного забезпечення при великих навантаженнях; недоліки програмного забезпечення, наявність можливостей обійти стандартні засоби управління безпекою; недостатній контроль засобів захисту, в результаті чого буде надмірний чи недостатній доступ до мережі; використання безкоштовних ресурсів та програм невідомого

походження. Технології безпеки: реалізація криптографічного та антивірусного захисту даних; прості та прозорі механізми забезпечення безпеки, з метою уникнення складностей у конфігуруванні; контроль на рівні програм визначає і забезпечує доступ до ресурсів.

Даний огляд класифікації бездротових мереж та спосіб використання моделі OSI, як рівневого підходу до забезпечення безпеки мереж можна проглянути в опублікованій за темою роботи праці [61], де також проаналізовано загрози на 7-ми рівнях моделі OSI, а також приведено відповідні технології безпеки мереж.

Тепер розглянемо більш детально аспекти захисту бездротових мереж згідно виділених нами рівнів моделі OSI. На основі такої класифікації було розроблено чималу кількість схожих за принципом підходів щодо забезпечення захисту, наприклад багаторівневий захист технологій функціонування інтелектуальних об’єктів [62].

Фізичний рівень (Physical Layer)

Фізичний захист пристроїв: Забезпечення безпеки фізичного доступу до пристроїв, наприклад, контроль доступу до обладнання.

Захист фізичного середовища поширення: забезпечення стабільності зв’язку через радіоканал, обмеження зони покриття контрольованим периметром, адже інформація у бездротових системах передається відкритим простором, що означає можливість її перехоплення або пошкодження.

Канальний рівень (Data Link Layer)

MAC-фільтрація (MAC Filtering): Встановлення правил, що дозволяють чи блокують доступ до безпровідної мережі на основі фізичних адрес пристроїв (MAC-адрес).

WPA/WPA2/WPA3 (Wi-Fi Protected Access): Використання протоколів безпеки Wi-Fi для шифрування даних і забезпечення безпеки мережі.

WPA (Wi-Fi Protected Access) – це протокол, яким об'єднання Wi-Fi Alliance замінило протокол WEP. У ньому вдосконалено обробку ключів безпеки та авторизації користувачів. WEP надає всім авторизованим системам один ключ, а

WPA використовує протокол цілісності тимчасового ключа (TKK), що динамічно змінює ключ, використовуваний системами. Це не дозволяє зловмисникам створити власний ключ шифрування, який відповідає захищеній мережі. Стандарт шифрування TKIP згодом був замінений розширеним стандартом шифрування (Advanced Encryption Standard, AES).

WPA2 – розвиток протоколу WPA, заснований на механізмі мережі високої безпеки (RSN) і працює у двох режимах: персональний режим (WPA2-PSK) – застосовується в домашніх мережах; корпоративний режим (WPA2-EAP) – для мереж організацій та комерційного використання.

В обох режимах використовується протокол CCMP, заснований на алгоритмі розширеного стандарту шифрування (AES), що забезпечує автентифікацію та цілісність повідомлення. Протокол CCMP є більш надійним, ніж вихідний протокол TKIP, що використовується у WPA.

WPA3 – розвиток протоколів WPA-WPA2, у ньому реалізовані такі нові функції для особистого та корпоративного використання: у WPA3 використовується протокол DPP (Device Provisioning Protocol) для мереж Wi-Fi, що дозволяє користувачам використовувати мітки NFC або QR-коди для підключення пристроїв до мережі; для забезпечення безпеки WPA3 використовує шифрування GCMP-256 замість 128-бітного шифру; протокол SAE (одночасна автентифікація рівних) – цей протокол використовується для створення безпечного "рукостискання", при якому мережевий пристрій підключається до бездротової точки доступу, і обидва пристрої обмінюються даними для перевірки аутентифікації та підключення.

Мережевий рівень (Network Layer)

VPN (Virtual Private Network): Створення захищеного тунелю для передачі даних через незахищені мережі, що дозволяє шифрувати та захищати інформацію.

Firewall: Використання мережевого брандмауера для фільтрації трафіку, блокування небажаних підключень та захисту мережі від зовнішніх атак.

Транспортний рівень (Transport Layer)

Шифрування на рівні транспортного протоколу: Використання протоколів шифрування, таких як SSL/TLS, для захисту передачі даних між пристроями та серверами.

Сертифікат SSL/TLS – це цифровий об'єкт, який дозволяє системам перевіряти особистість та згодом встановлювати зашифроване мережеве з'єднання з іншою системою за допомогою протоколу Secure Sockets Layer/Transport Layer Security (SSL/TLS). Сертифікати використовуються у рамках криптографічної системи, відомої як інфраструктура відкритого ключа (PKI). PKI дає одній стороні можливість встановлювати справжність іншої сторони за допомогою сертифікатів (за умови, що обидві сторони довіряють третій стороні, відомій як центр сертифікації). Таким чином, сертифікати SSL/TLS діють як цифрові посвідчення особи для захисту мережевих підключень та встановлення автентичності веб-сайтів в Інтернеті, а також ресурсів у приватних мережах.

Сеансовий рівень (Session Layer)

На сеансовому рівні (Session Layer) моделі OSI захист інформації зазвичай здійснюється за допомогою механізмів, які забезпечують безпечне управління та збереження інформації під час встановлення, управління та завершення сесійного з'єднання між пристроями.

Шифрування сеансів: Для забезпечення конфіденційності даних, що передаються під час сеансів, використовують механізми шифрування. Один із популярних методів – використання протоколів шифрування на сеансовому рівні, таких як SSL/TLS, які забезпечують захищену передачу даних між пристроями.

Управління сеансами: Важливим аспектом захисту є ефективне управління сеансами. Це включає в себе створення, управління та завершення безпечних сесійних з'єднань між клієнтами та серверами, що дозволяє забезпечити безпеку даних під час їх передачі.

Автентифікація сеансів: Ще одним важливим аспектом захисту є аутентифікація сеансів, тобто перевірка та підтвердження ідентичності сторін,

що здійснюють сеансові з'єднання. Це може включати використання сертифікатів, логінів та паролів або інших механізмів аутентифікації.

Прикладний рівень (Application Layer)

Шифрування на рівні додатків: Використання протоколів шифрування, таких як HTTPS, для захисту передачі даних між додатками і серверами.

На прикладному рівні (Application Layer) моделі OSI захист інформації зазвичай включає в себе використання різних протоколів та методів шифрування для забезпечення конфіденційності, цілісності та доступності даних, що передаються між додатками і серверами [97]. Ось деякі основні аспекти захисту на прикладному рівні:

Шифрування даних: Одним з основних заходів захисту на прикладному рівні є використання протоколів шифрування, таких як SSL/TLS (Secure Sockets Layer/Transport Layer Security). Ці протоколи забезпечують захищене з'єднання між клієнтом і сервером та шифрують дані, що передаються між ними, що робить їх недоступними для несанкціонованого доступу.

Автентифікація і авторизація: Для захисту інформації на прикладному рівні також використовують механізми автентифікації користувачів і авторизації доступу до ресурсів. Наприклад, перед виконанням критичних операцій користувачі можуть пройти аутентифікацію з використанням ідентифікаторів, паролів або біометричних даних.

Контроль доступу: Контроль доступу до ресурсів на прикладному рівні дозволяє обмежити права доступу користувачів до конфіденційної інформації. Це може включати створення різних рівнів доступу для різних користувачів і груп користувачів.

Механізми аудиту: Деякі системи також використовують механізми аудиту і журналювання для відстеження дій користувачів і виявлення можливих атак або порушень безпеки.

Використання безпечних протоколів комунікації: Застосування безпечних протоколів комунікації, таких як HTTPS для веб-додатків, дозволяє захищати дані під час їх передачі через мережу.

2.2. Сучасні підходи до забезпечення захисту передачі інформації бездротовими мережами

Бездротові мережі відіграють ключову роль у забезпеченні зв'язку та обміну інформацією в різних сферах життя, включаючи комерційні, громадські, медичні, та військові сектори.

Сучасні підходи до забезпечення безпеки передачі інформації бездротовими мережами, особливо коли мова йде про зв'язок з безпілотними літальними апаратами (БПЛА), набувають надзвичайної важливості у зв'язку зі зростаючим зацікавленням у використанні цієї технології у військових операціях та інших сферах.

Одним із найважливіших аспектів безпеки є шифрування переданих даних. Це процес застосування криптографічних методів для забезпечення конфіденційності та безпеки інформації під час передачі або зберігання. Два основних елементи шифрування – це використання потужних алгоритмів шифрування та безпеки комунікаційних каналів.

Один із найбільш надійних алгоритмів шифрування – Advanced Encryption Standard (AES). Він був прийнятий Національним інститутом стандартів і технологій США (NIST) як стандарт шифрування замість старішого DES (Data Encryption Standard) у 2001 році. AES використовується для шифрування конфіденційної інформації, такої як фінансові дані, паролі, особисті повідомлення тощо. Особливість AES полягає у тому, що він пропонує різні рівні захисту, включаючи ключі різної довжини, включаючи 128, 192 та 256 біт. Використання довгих ключів у AES підвищує рівень безпеки, оскільки ускладнює завдання для криптоаналітиків [63].

Переваги AES:

– Високий рівень стійкості до злому;

– Широке поширення та підтримка;

– Ефективність та швидкість роботи;

– Підтримка різних довжин ключів.

У 2003 році в ході операції "Іракська свобода" американські військові

використовували шифрування з використанням AES для захисту комунікаційних каналів між військовими частинами. Це дозволило уникнути прослуховування та несанкціонованого доступу до важливих військових командних структур.

Тому, важливо зазначити, що AES з використанням довгих ключів, надають високий рівень захисту від несанкціонованого доступу до інформації, що передається між контрольним центром і БПЛА.

Крім використання міцних алгоритмів шифрування, важливо також застосовувати криптографічні протоколи для захисту конфіденційності переданих даних. Такими протоколами є TLS (Transport Layer Security) або SSL (Secure Sockets Layer) вони забезпечують безпеку при обміні даними через Інтернет, забезпечуючи шифрування даних, що передаються між клієнтом і сервером.

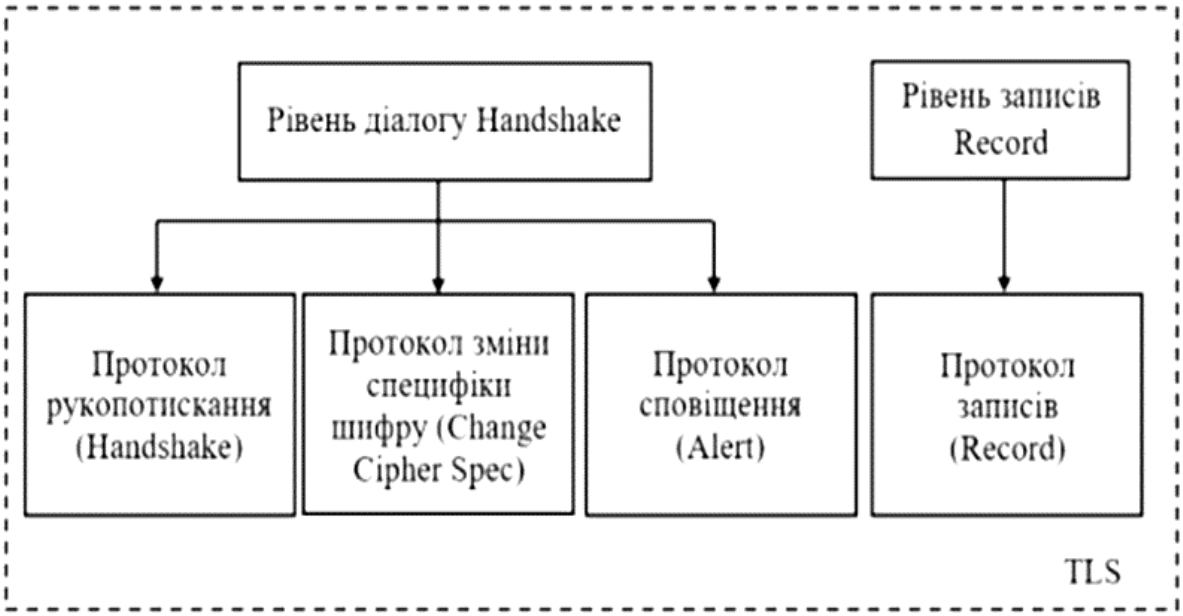


Рисунок 2.1. Архітектура протоколу TLS

TLS використовує асиметричне шифрування для автентифікації, симетричне – для конфіденційності та коди автентичності повідомлень для збереження цілісності повідомлення. Основним ядром протоколу є технологія комплексного використання як асиметричних так і симетричних криптосистем.

До даного протоколу ввійшли два протоколи: протокол запису і протокол

діалогу, котрий складається з 3-х підпротоколів (протокол рукопотискання, протокол сповіщення та протокол зміни специфікації шифру) [64].

Перелічені протоколи дозволяють створювати безпечні з'єднання надійно захищаючи інформацію від прослуховування та злому. Хоча TLS зазвичай вважається більш безпечним і сучасним, SSL залишається важливим для сумісності з старішими системами та пристроями .

Переваги TLS/SSL:

– Захист даних від прослуховування та перехоплення;

– Автентифікація серверів;

– Захист від атак типу "людина посередині".

Для забезпечення цілісності та конфіденційності даних, також використовують методи аутентифікації, такі як цифрові підписи та алгоритми перевірки цілісності даних. Це дозволяє впевнитись, що інформація не була змінена або підроблена під час передачі. Цифровий підпис – це електронний еквівалент звичайного підпису. Вони створюються за допомогою криптографічних алгоритмів та ключів, а їхня головна мета – підтвердження автентичності даних та відправника.

Алгоритми перевірки цілісності даних використовують хеш-функції, або коди перевірки цілісності (CRC). Хеш-функції генерують унікальний хеш (фіксованого розміру) на основі вмісту даних. Якщо дані змінюються, хеш також змінюється. При отриманні даних отримувач може перевірити хеш для того, щоб переконатися, чи вони не були піддані незаконним змінам.

Однією з потрібних вимог у застосуваннях бездротових сенсорних мереж (WSN) є перевірка автентичності сенсорних вузлів. Ці сенсорні вузли здатні сприймати навколишнє середовище, значно швидше обробляти дані, зберігати та агрегувати дані та, нарешті, передавати їх між іншими сенсорними вузлами і базовою станцією в мережі [65].

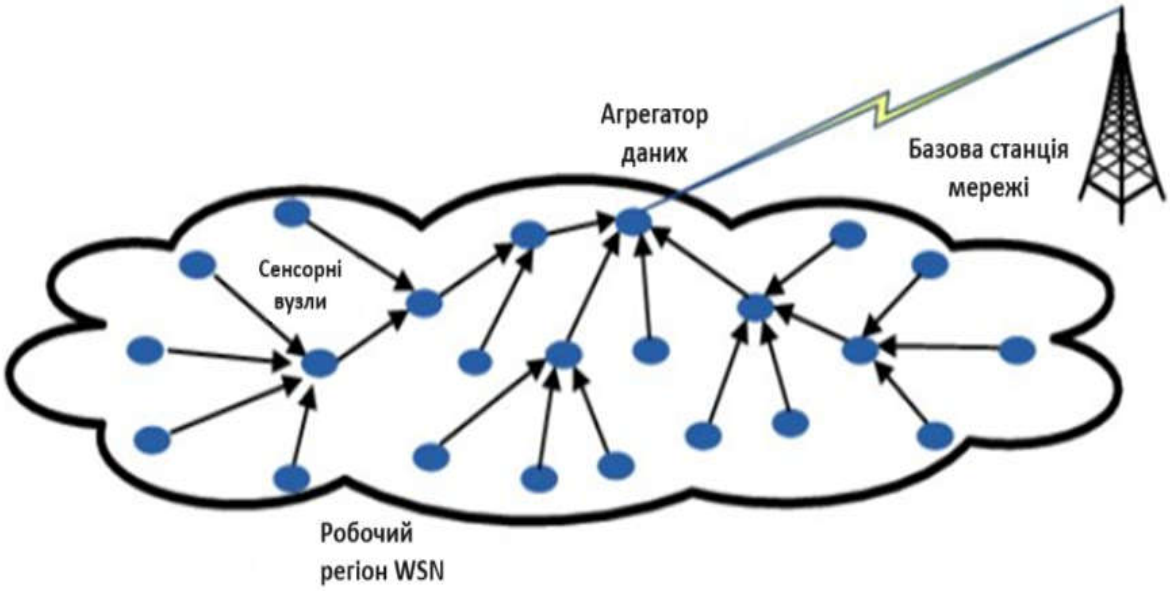


Рисунок 2.2. Агрегація даних у бездротовій сенсорній мережі

Це дозволяє підвищити рівень захисту від різних видів атак, таких як атаки відтворення та атаки уособлення. Крім цього, згідно вимог військового застосування бездротових сенсорних мереж [66], такі заходи дозволяють зменшити накладні витрати на обчислення та зв’язок, а також споживання заряду батареї автономних пристроїв.

Тому Muzzammil Hussain та Usha Jain у своєму дослідженні пропонують ефективний і безпечний протокол автентифікації для WSN з контекстом для військових програм. Цей протокол передбачає використання індивідуальних цифрових сертифікатів для підтвердження легітимності вузлів датчиків. Вузли попередньо завантажуються відкритим ключем базової станції та отримують свій сертифікат під час розгортання.

Цей сертифікат потім використовується для взаємної автентифікації між сенсорними вузлами, що забезпечується відповідно до вимог безпеки військових застосувань. Цей протокол відповідає різним вимогам безпеки з низькими обчислювальними та комунікаційними витратами [67].

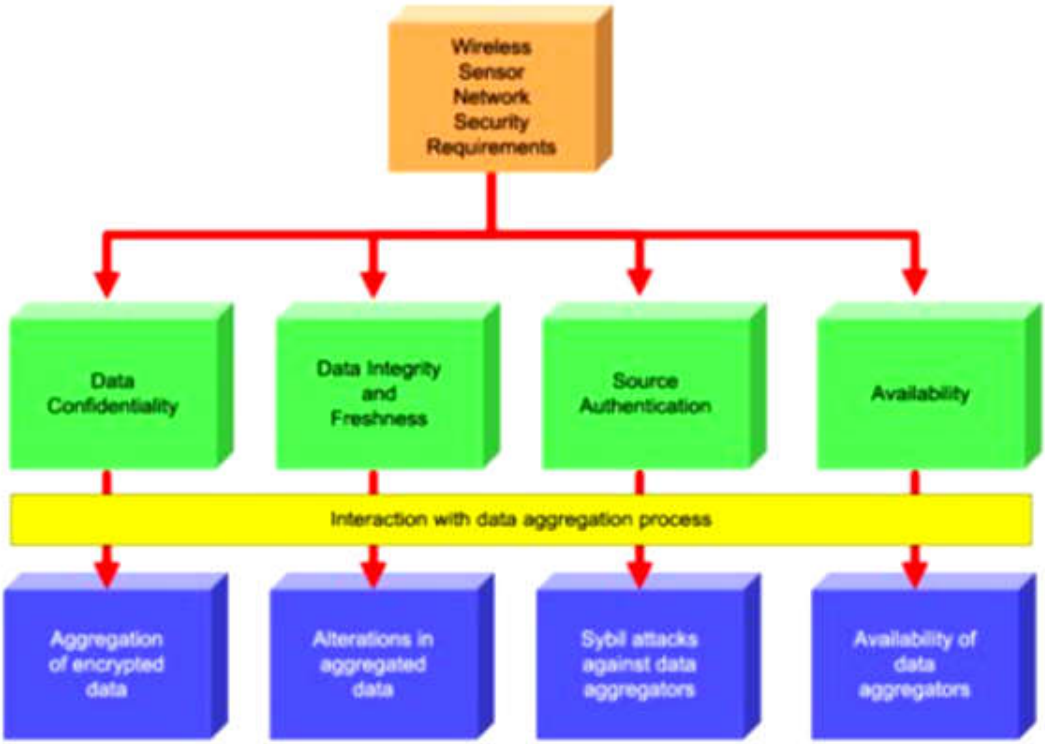


Рисунок 2.3. Взаємодія між безпекою бездротової сенсорної мережі та процесом агрегації даних

Оскільки БПЛА є дуже схильні до кібератак, таких як перехоплення даних, придушення каналу зв’язку, маніпулювання програмним забезпеченням та GPS-спуфінг, використання у них таких механізмів як шифрування, аутентифікації та авторизації є надважливим [68].

Окрім технічних засобів захисту важливо враховувати фізичну безпеку обладнання. Це пов'язано з тим, що БПЛА, будучи відносно не великим і не стаціонарним пристроєм можуть бути викрадені або пошкоджені фізично, що може привести до витіккання конфіденційної інформації, або до використання БПЛА в злочинних цілях.

Перший крок у забезпеченні фізичної безпеки – обмеження доступу до самого пристрою. В контексті зберігання пристроїв це може бути досягнуто за допомогою механічних замків та систем автентифікації, таких як сканери відбитків пальців, магнітні зчитувачі, тощо. Доступ до основних компонентів БПЛА має бути обмежений та контрольований, щоб уникнути

несанкціонованого доступу та змін у конфігурації або програмному забезпеченні пристрою. Додаткові заходи можуть включати в себе встановлення фізичних бар'єрів, таких як огорожі або контейнери, які захищають пристрій від доступу осіб без відповідного дозволу.

Також на вищих рівнях захисту можна запровадити системи виявлення вторгнень, які спостерігають за навколишньою областю пристрою і сповіщають про будь-які спроби несанкціонованого доступу або виявлення небажаної активності. Це можуть бути такі системи, як Snort, Suricata, McAfee Network Security Platform та Zeek. Кожна з них має свої переваги і недоліки.

У дослідженні [69] лідером за значною частиною показників було обрано Snort, який може визначати атаки під прикриттям, а також здатний як виявляти, так і одразу блокувати широкий спектр атак. Має лише один недолік – однопотоковість, яка не дозволяє забезпечити швидку роботу [69].

Окрім цього, важливо проводити постійний моніторинг та аналіз стану роботи і функціонування пристрою, що дозволить вчасно виявляти потенційні атаки та реагувати на них, забезпечуючи безпеку зв'язку з БПЛА на всіх етапах його використання.

Сучасні стратегії захисту бездротових систем передавання інформації, включаючи ті, що застосовуються до безпілотних літальних апаратів (БПЛА), є над важливими для забезпечення їхньої безпеки та ефективності. Щоб забезпечити надійний та безпечний зв'язок з цими пристроями, необхідно досліджувати можливості використання у них новітніх методів шифрування, методів аутентифікації, фізичного захисту та постійного моніторингу загроз.

Комбінування цих підходів здатне дозволити створити ефективну систему захисту, яка мінімізує ризики кібератак, несанкціонованого доступу або недозволеної маніпуляції пристроєм. Такий підхід дозволяє забезпечити оптимальний рівень безпеки в умовах високої технологічної складності та росту загроз кібербезпеки.

2.3. Огляд та аналіз методів приховування безпровідних каналів зв’язку

Як і будь-яка технологія, безпровідні мережі зв'язку мають свої слабкі сторони. Однією з них є вразливість до перехоплення та підслуховування даних. Тому в цьому підрозділі ми детально розглянемо методи приховування безпровідних каналів зв’язку.

Почнемо зі стеганографії. Стеганографія – наука про зберігання й передавання таємних повідомлень прихованими каналами, котрі створюються всередині відкритих каналів передавання так, щоб факт передавання таємних даних залишався невідомим для неавторизованого користувача [70].

Стеганографія, як метод приховування інформації, може використовувати різні підходи, зокрема, на основі обробки зображень у просторових і трансформованих доменах, таких як дискретне косинусне перетворення (DCT) і дискретне вейвлетне перетворення (DWT) [71]. У своєму дослідженні автор Хусейн та інші представив огляд методів стеганографії просторової області, що реалізують підходи найменшого значущого біта (LSB) [72].

Але можна констатувати один критичний недолік цих методів: підходи до застосування стеганографії досліджувалися в літературі без урахування сегменту бездротового зв'язку із його специфічними шумовими властивостями. Тому класичне використання стеганографії при передаванні сигналу ефіром є не доцільним, оскільки найменш значущі біти з великою ймовірністю можуть бути спотворені. З огляду на розвиток засобів зв'язку та важливість захисту інформації, особливо при передачі через бездротовий зв'язок, дослідники почали досліджувати надійність стеганографії для ситуацій погіршенні якості зв'язку.

OFDM (Orthogonal Frequency Division Multiplexing) є однією з найбільш поширених технологій бездротового зв'язку. Його особливість полягає у використанні багатьох ортогонально модульованих вузькосмугових сигналів, що дозволяє уникнути складних фільтрів вирівнювання та ефективно використовувати частотний спектр [73].

Ця особливість робить OFDM достатньо стійким до шумів та спотворень у каналі зв'язку. У контексті використання методів захисту і приховування інформації, це означає, що при такому виді модуляції інформація, яка вбудовується у сигнал, може залишатися достатньо стійкою та надійною для впровадження методів стеганографії, зокрема у випадку зовнішніх впливів на канал зв'язку, таких як шуми, спотворення сигналу.

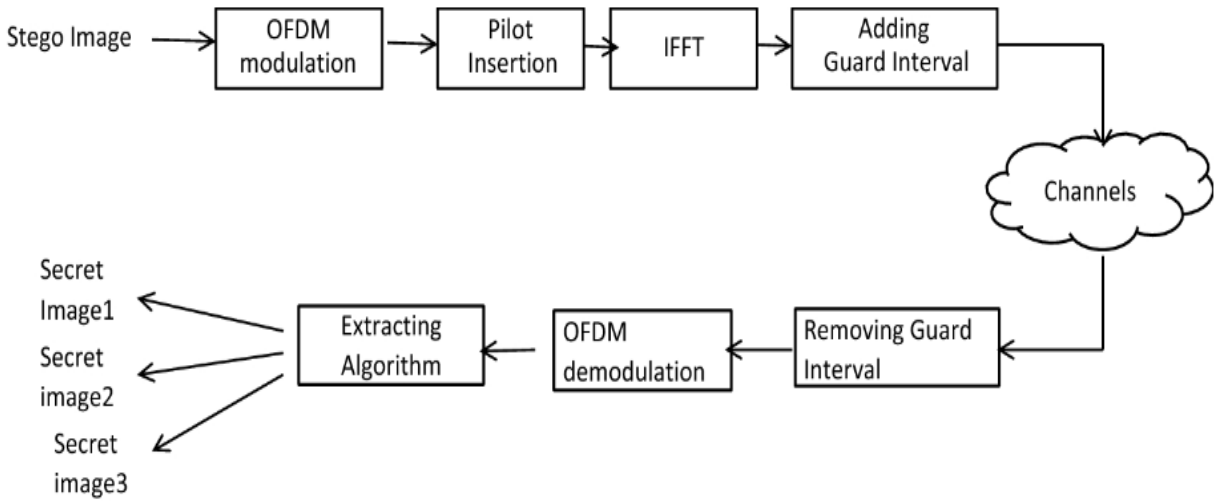


Рисунок 2.4. Модель OFDM для стеганографії зображення

У дослідженні [74] проаналізовано вплив AWGN (Additive White Gaussian Noise) та каналів багатопроменевого завмирання на стеганографічні зображення, які передаються через систему OFDM. AWGN відіграє роль шуму у бездротовому зв'язку, тоді як канали багатопроменевого завмирання відображають проблеми, пов'язані зі змінною якістю каналу в залежності від умов поширення сигналу.

Для зменшення спотворень, що можуть виникати у бездротових каналах, була запропонована модифікація системи OFDM. Ця модифікація включає застосування оцінки каналу та фільтрації для компенсації помилок у бездротових каналах, а також використання адаптивного вирівнювання та кодування, що сприяє зменшенню впливу шумів і змін у каналі зв'язку. Зокрема, використання оцінки каналу LS (Least Squares) дозволяє отримати кращу якість реконструйованих зображень, це видно на рис. 2.5.

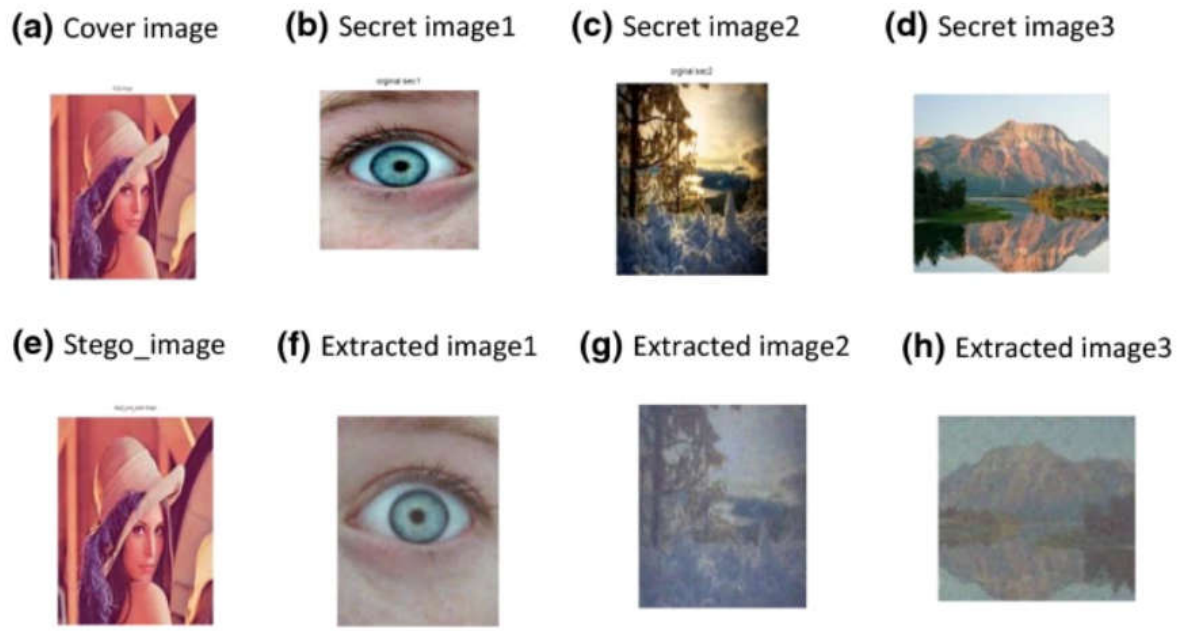


Рисунок 2.5. Реконструйовані зображення

Крім того, у даній статті був врахований ефект Доплера на реконструйованих зображеннях, переданих через OFDM із модифікацією. Врахування цього ефекту сприяє більш точному відтворенню зображень у складних умовах бездротового зв'язку, дозволяючи зберегти високу якість переданих стеганографічних даних. Результати моделювання показали перспективи в розробці більш ефективної схеми кольорової стеганографії, яка враховує специфіку бездротового зв'язку [74].

У контексті ж застосування БПЛА, стеганографію теоретично можна використовувати для передачі конфіденційних даних через зв'язок із безпілотником, при цьому зовнішній спостерігач не помітить такої передачі. Наприклад, прихована інформація може бути вбудована в медіадані, які передаються через канали зв'язку БПЛА, такі як відеопотік (зображення з камери на літальному апараті) або звук (за наявності мікрофона на борту).

Однак, потрібно врахувати кілька важливих факторів: по-перше, при використанні БПЛА для військових завдань сам відео- або звуковий потік може стати інформацією з обмеженим доступом і потребуватиме захисту; по-друге, важливо враховувати, що використання стеганографії може вимагати додаткових ресурсів для вбудовування та вилучення інформації, що може

призвести до збільшення обчислювального навантаження та споживання ресурсів, що може впливати на швидкість обробки даних апаратом.

З цього можна зробити висновок, що стеганографія для використання у БПЛА більшою мірою підходить тільки при впровадженні її у безпілотники великої потужності, більшість популярних сьогодні БПЛА "коптерного" типу, не мають достатніх ресурсів для забезпечення надійного функціонування таких методів захисту. Тому стеганографія має серйозні обмеження для застосування на борту невеликих пристроїв безпілотної авіації, що може використовуватися в умовах збройного конфлікту.

2.4. Огляд застосування криптографії для забезпечення конфіденційності безпровідної мережі

Використання криптографії для забезпечення конфіденційності безпровідної мережі є ключовим елементом захисту. Конфіденційність даних має на увазі, що пакети даних, які передаються в мережі, не можуть бути прочитані пасивними зловмисниками, але можуть бути прочитані тільки тими користувачами чи вузлами мережі, яким вони призначалися [75].

У дослідженнях із бездротових сенсорних мереж (WSN), криптографічні методи можна систематизувати так:

– Криптографія з відкритим ключем;

– Криптографія з симетричним ключем;

– Протоколи керування криптографічними ключами;

– Протоколи безпечної маршрутизації;

– Методи визначення вторгнень.

Як приклад криптографічних протоколів з відкритим ключем можна привести протоколи Diffie-Hellman і RSA. Вони використовуються для забезпечення безпеки комунікацій шляхом обміну публічними ключами.

Однак ці методи вимагають великої обчислювальної потужності, що може становити проблему, особливо в умовах експлуатації вузлів WSN під впливом DOS-атак або обмежених ресурсів [75].

У порівнянні з методами з парою ключів, криптографічні методи з використанням симетричного ключа вимагають менше ресурсів. Це було продемонстровано у дослідженні [76]. З його результатів бачимо, що для шифрування даних методом RSA на процесорі MC68328 dragonball може бути витрачено близько 42 мдж на блок даних розміром 1024 біти, тоді як для шифрування 128-бітного блоку методом AES ця витрата становить лише 0,106 мдж.

В іншій статті дослідники продемонстрували, що за достатнього вдосконалення та оптимізації криптографічних методів на основі відкритих ключів, вони можуть успішно застосовуватись у бездротових сенсорних мережах, маючи при цьому нижче споживання енергії [77].

Серед таких методів варто відзначити схему Робіна, RSA та методи на основі еліптичних кривих (ECC). Останній відзначається тим, що при меншому розмірі ключа він забезпечує такий же рівень безпеки, що дозволяє зменшити навантаження на вузли за рахунок зниження витрат на обробку та передачу інформації. Але незважаючи на наведені аргументи на користь використання криптографічних методів з відкритим ключем в WSN, вони все одно залишаються досить енерговитратними.

Тому наступний розглянутий метод це криптографія з симетричним ключем. Найпоширенішими алгоритмами шифрування з симетричними ключами є RC4, RC5, MD5, SHA-1 та IDEA. В роботі [78] приведено аналіз та порівняння методів з використанням симетричних ключів RC5 і TEA. Також розглянуті такі блокові шифри на системах IAR, як RC5 і RC6, Rijndael, MISTY1, KASUMI і Camellia. Параметрами для порівняння були обсяг коду, обсяг пам'яті даних і кількість циклів CPU.

В результаті описаних у статті експериментів було виявлено, що Rijndael найбільш підходить для забезпечення високого рівня безпеки та енергоефективності в WSN, тоді як MISTY1 може бути використаний для зберігання даних і забезпечення енергоефективності.

Враховуючи обмеження ресурсів пристроїв WSN, криптографічні методи з

використанням симетричного ключа є більш пріоритетними для використання в таких мережах [75].

Далі розглянемо використання протоколів управління криптографічними ключами. Основна мета цих протоколів – встановлення потрібних ключів між вузлами мережі для безпечного обміну даними, тобто забезпечення конфеденційності. Важливо, щоб ці протоколи підтримували можливість додавання та видалення вузлів з сенсорної мережі, враховуючи обмежені ресурси пристроїв WSN. На відміну від аналогічних рішень для ad-hoc мереж, протоколи управління ключами в WSN використовують в основному криптографічні методи з симетричними ключами.

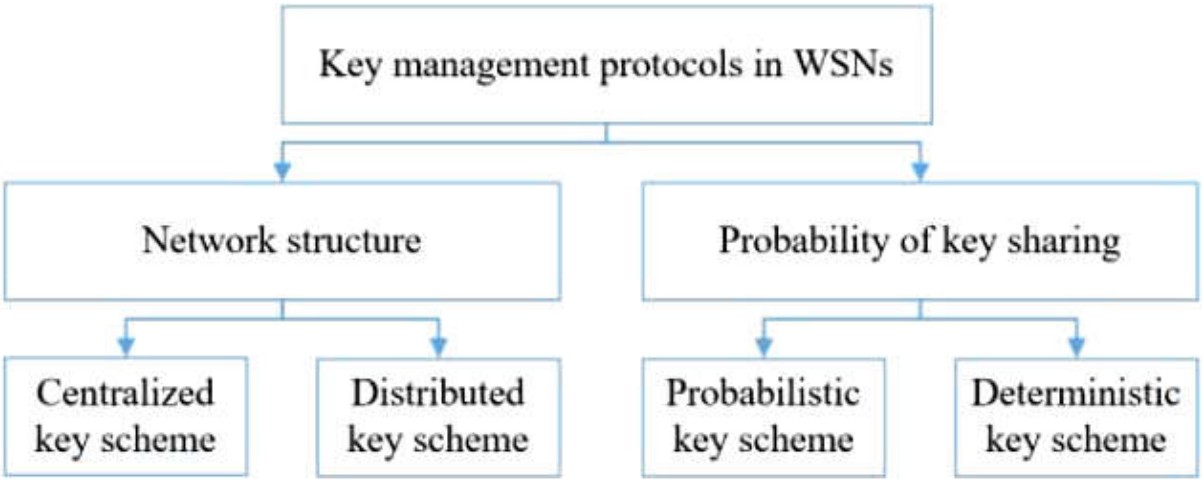


Рисунок 2.6. Класифікація протоколів керування ключами у WSN

Наступний розглянутий криптографічний метод – використання протоколів безпечної маршутизації. Протоколи маршрутизації в бездротових сенсорних мережах (WSN) можуть бути різними за структурою мережі: flat-based (однорівнева), ієрархічна або на основі розташування.

Багато з них недостатньо забезпечують безпеку мережі, оскільки часто не містять вбудованих заходів безпеки. Наприклад, енергозалежна маршрутизація (GEAR) може бути вразливою через нестійкий обмін інформацією про місцезнаходження. Хоча протоколи безпечної маршрутизації добре вивчені для ad-hoc мереж, вони не завжди підходять для сенсорних мереж через відмінності технологій [75].

Найкращий захист інформації в мережі – це поступова відмова у функціонуванні замість миттєвого виходу з ладу. Щоб реалізувати такий підхід, треба, щоби робота протоколів маршрутизації сповільнювалася повільніше, аніж зростала кількість скомпрометованих вузлів в сенсорній мережі [79].

Варто зазначити, що протоколи безпечної маршрутизації в WSN значною мірою залежать від використання протоколів управління криптографічним ключем, оскільки перед початком роботи протоколів маршрутизації вузлів мережі вже мають бути видані ключі безпеки.

Останній метод, який був розглянутий – використання методів виявлення вторгнень. Механізми безпеки в мережах моніторингу не можуть гарантувати повну безпеку, оскільки вузли можуть бути захоплені зловмисниками. Автентифікація та шифрування даних недостатні, тому важливе виявлення та реагування на вторгнення. Такі системи виявлення вторгнень (IDS) допомагають виявляти підозрілі дії та класифікуються на rule-based і anomaly-based.

Проте, налаштування IDS у сенсорних мережах вимагає часу та енергії. Але коректна комунікація між вузлами важлива для ефективного реагування на загрози в мережі [75].

Переваги використання криптографії:

Забезпечення конфіденційності: Криптографія шифрує дані, роблячи їх незрозумілими для тих, хто не має ключа дешифрування. Це гарантує, що лише авторизовані користувачі можуть отримувати доступ до інформації, що передається.

Захист від втручання: Криптографічні протоколи гарантують цілісність даних, що робить неможливим для зловмисників зміну або фальсифікацію інформації, що передається.

Захист від радіоелектронної розвідки: Шифровані дані не можуть бути прочитані ворожими розвідслужбами, що ускладнює для них отримання інформації про військові дії.

Важливо зазначити, що модель FPV (First Person View), яку

використовують наші військові, особливо вразлива до атак через свою залежність від безпровідного зв'язку. Захист цього каналу зв'язку за допомогою заходів забезпечення конфіденційності є критично важливим для забезпечення безпеки та успішності операцій.

Тож використання криптографії та інших засобів забезпечення конфіденційності безпровідної мережі є невід'ємною частиною захисту БПЛА, особливо моделей FPV, які використовуються у військових операціях. Застосування криптографічних протоколів гарантує конфіденційність даних, захищає від втручання та маніпулювання, а також ускладнює ворогу ведення радіоелектронної розвідки.

2.5. Застосування завадостійкого кодування для забезпечення відмовостійкості бездротової мережі

У сучасних умовах, коли безпека зв'язку стає все більшою проблемою через розвиток кіберзагроз та можливість перехоплення інформації, застосування завадостійкого кодування стає вирішальним аспектом. Це означає, що дані, які передаються через бездротові мережі, кодуються таким чином, що навіть при наявності завад чи спроби перешкоджання, інформація залишається непошкодженою та доступною лише для авторизованих користувачів.

Завадостійкі коди є одинми із найефективніших засобів забезпечення досить високої достовірності передачі інформації. Розглянемо принцип роботи завадостійкого кодування в бездротових мережах. Під час передачі даних через бездротові канали, інформація може бути спотворена або пошкоджена через різноманітні завади. Це може призвести до помилок у прийнятому повідомленні. Для виявлення та виправлення цих помилок використовуються завадостійкі коди.

Завадостійкі коди забезпечують можливість виявлення і (або) виправлення помилок у переданому повідомленні. Вони досягають цього шляхом введення додаткових символів у кодоване повідомлення, які називаються перевірочними або контрольними символами. Ці додаткові символи генеруються згідно з

певними правилами, які дозволяють виявити та виправити помилки.

Збільшення кількості таких контрольних символів у коді підвищує його здатність виявляти та виправляти помилки, але водночас знижує швидкість передачі інформації через канал зв'язку. Таким чином, вибір оптимальної кількості контрольних символів є компромісом між надійністю передачі даних і швидкістю комунікації [80].

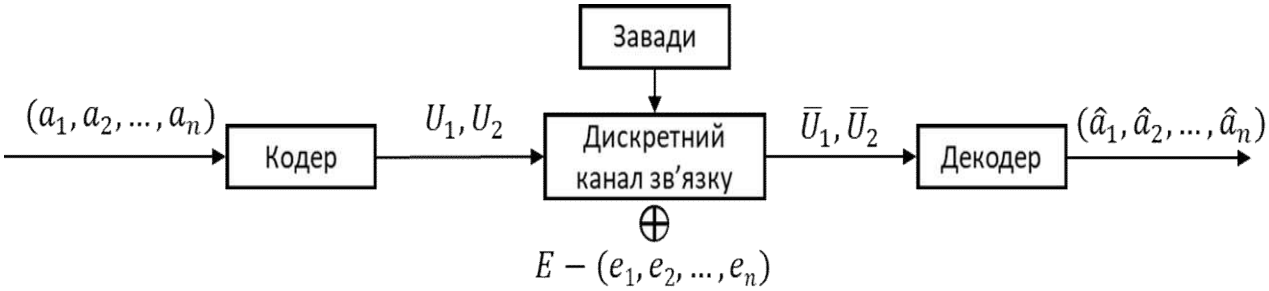


Рисунок 2.7. Спрощена схема системи передавання інформації при завадостійкому кодуванні

Реалізація завадостійких кодів основана на використанні алгебраїчних структур (полів, груп, кілець), які визначають правила формування кодових комбінацій, виявлення та виправлення в них помилок. Для передавання кодових комбінацій між кодером і декодером використовують дискретні канали зв'язку – це сукупність технічних засобів, які включають середовище розповсюдження, сигнали на вході і виході котрого приймають кінцеве число значень (Рис. 2.7.). Найпростішою моделлю дискретного каналу є двійковий канал зв'язку з завадою, яка адитивно взаємодіє з сигналом [80].

Завадостійкі коди мають доволі обширну класифікацію (Рис. 2.8.).

Класифікація завадостійких кодів включає рівномірні і нерівномірні типи. Рівномірні коди мають постійну кількість розрядів у всіх кодових комбінаціях, тоді як нерівномірні мають різну кількість розрядів. Вони поділяються на надмірні, що включають безперервні і блокові коди.

Надмірні коди можуть бути роздільними або нероздільними, де роздільні поділяють кодові комбінації на інформаційні та перевірочні символи. Роздільні блокові коди поділяються на несистематичні та систематичні, при цьому

останні базуються на лінійній алгебрі та інших математичних підходах. Вони можуть застосовуватися в системах зберігання даних, таких як RAID.

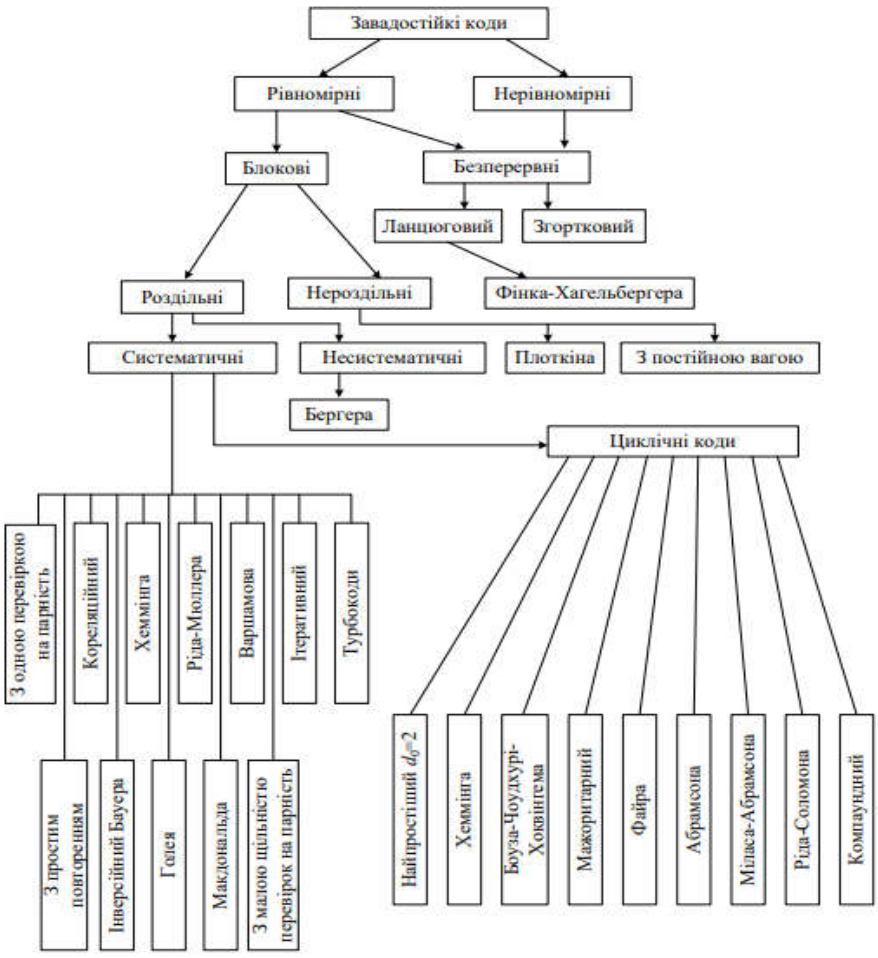


Рисунок 2.8. Класифікація завадостійких кодів

До систематичних кодів відносяться коди з перевіркою на парність (чи непарність), інверсний код Бауера, коди з повторенням, кореляційний, коди Варшамова, Хеммінга, Голея, Макдональда, Ріда-Мюллера, ітеративний код, коди з малою щільністю перевірок на парність. Їх використовують в мережах передачі даних, сховищах даних, а також у пристроях для запису і читання даних, наприклад, в оптичних дисках. Різновидом систематичних кодів є циклічні коди.

До найбільш відомих ціклічних кодів належать мажоритарні коди, компаундні коди, коди Хеммінга, Боуза-Чоудхурі-Хоквінгема, Міласа-Абрамсона, коди Файра, Абрамсона, Ріда-Соломона. Вони широко

використовуються у зберіганні та передачі даних, таких як флеш-пам'ять, тверді диски, CD, DVD, баркоди, QR-коди, а також в бездротових комунікаціях, наприклад, в Wi-Fi, LTE і Bluetooth. Ці коди мають специфічну властивість циклічної перестановки символів, що зберігає принципи кодування. Крім цього, важливим напрямком є застосування згорткових кодів для ефективного виявлення та виправлення помилок у каналах передачі даних. Ці коди застосовуються в бездротових мережах, наприклад, в стандарті Wi-Fi [80].

Завадостійке кодування, що вже використовується в класичних комп'ютерах, також є важливим для квантових комп'ютерів. Це продемонстровно в статті [81], що циклічні коди на основі теорії лінійних послідовних схем, представляють собою дієвий інструмент для забезпечення надійності обчислень у квантових системах. Циклічні коди, які використовують функції переходів та виходів для ефективного кодування та декодування даних, виявляються ключовим кроком у розв'язанні проблеми достовірності результатів квантових обчислень. Ці коди показують свою перспективність, зокрема в квантових каналах зв'язку, де надійність є особливо критичною.

Загалом застосування завадостійких кодів включає телефонію, цифрове телебачення, безпровідні комунікації, мережеві протоколи передачі даних, зберігання даних на носіях, а також інші сфери, де важлива надійність інформації та мінімізація помилок у передачі даних. Крім того, у військовому застосуванні, де безпека і конфіденційність інформації мають вирішальне значення, використання цього кодування стає обов'язковим. Це дозволяє забезпечити захищений канал зв'язку між військовими БПЛА та їхніми операторами, уникнути перехоплення ворожими силами або кіберзлочинцями, а також зберегти недоступність для несанкціонованого доступу.

До переваг застосування завадостійкого кодування відносяться збільшення стійкості мережі до різного роду завад і атак, забезпечення конфіденційності інформації, а також підвищення надійності передачі даних навіть в умовах низької якості сигналу або активних спроб перешкоджання.

Проте застосування завадостійких кодів у системах передачі інформації

має свої недоліки. Один з них полягає в тому, що методи кодування не завжди адаптовані до змінюючихся умов у каналі передачі даних. Таким чином, в процесі розробки кодів доводиться враховувати лише найсприятливіші умови, що може призвести до введення надмірності (додаткових перевірочних символів). Це, у свою чергу, може знизити швидкість передачі даних у тих випадках, коли рівень завад низький.

Крім того, одним з основних обмежень практичного застосування завадостійких кодів є складність процесу декодування. Це може виражатися в великій кількості логічних елементів у декодері або у великій кількості обчислювальних операцій, необхідних для декодування сигналу. Тому при розробці кодів необхідно враховувати баланс між складністю декодування та ефективністю корекції помилок [80].

В цілому, завадостійке кодування відіграє важливу роль у забезпеченні відмовостійкості бездротових мереж, зокрема в контексті військових застосувань, де вона стає невід'ємною частиною стратегічного комунікаційного забезпечення.

Висновки до 2 розділу

В цьому розділі було докладно проаналізовано проблематику захисту передавання інформації бездротовими системами, зокрема в контексті використання безпілотних авіаційних систем цивільного походження, що відносно нещодавно почали використовуватися у військових цілях. Цивільні пристрої не розраховані на роботу у зоні бойових дій і потенційно такі засоби можуть не мати здатності до надійного функціонування за межами приміщення за будь-яких погодних умов, не мати достатньо надійних систем шифрування та кодування каналів і також – бездротові цивільні системи і пристрої не розраховані на роботу в умовах використання противником засобів РЕБ, РЕР, радіопеленгаційних станцій, пристроїв електромагнітного придушення, тощо.

На основі аналізу структури моделі системи функціонування відкритих систем OSI, а також додатків і застосунків, використовуваних на різних рівнях

моделі взаємодії відкритих систем, вдалося зробити ранжирування методів та засобів захисту інформації при передачі бездротовими системами відповідно до рівня функціонування того чи іншого методу.

Сучасні підходи до забезпечення захисту інформації при передачі бездротовими системами дозволили розробити достатньо ефективні і надійні системи захисту. Проте, огляд і аналіз сучасних досліджень і публікацій вказує на необхідність модифікації існуючих та розроблення додаткових заходів для запобігання перехопленню інформації, придушення каналів зв'язку та іншим заходам із захисту інформації на найнижчих рівнях моделі осі зокрема на фізичному та канальних рівнях.

Для забезпечення відмовостійкості бездротових систем зв'язку та керування, особливо в контексті масового використання цивільних безпілотних літальних апаратів, необхідно врахувати можливість виникнення радіочастотних перешкод та шумових завад, які штучно створюються противником для придушення і виведення з ладу систем керування нашими БПЛА, "обману" їхніх навігаційних систем шляхом прямих активних атак, а також атакам засобами розвідки на протоколи передачі даних, для перехоплення інформації з них. А також, для спроб реалізації розглянутих методів захисту, необхідно врахувати обмеження у продуктивності цивільних безпілотників зокрема, та автономних вбудовуваних систем в цілому.

РОЗДІЛ 3. ПОКРАЩЕННЯ ЗАХИЩЕНОСТІ БЕЗДРОТОВИХ СИСТЕМ КЕРУВАННЯ ТА ЗВ'ЯЗКУ В КОНТЕКСТІ БПЛА

Враховуючи сучасні умови стрімкого розвитку технологій, завдяки чому тепер світ стикається із новими викликами у військовій сфері, а також особливо у контексті російського вторгнення до нашої держави, у даному дослідженні особлива увага приділена питанню захисту таких систем зв'язку та керування різноманітними пристроями, які перемістили свою сферу використання із цивільних задач, задач пошуку/порятунку рятувальними службами, до задач військової галузі, таких як розвідка, евакуація, нанесення безпосереднього вогневого ураження чи коректування роботи інших формувань, завдання координації проведення операцій за участі кількох формувань, доставка провізії на позиції із використанням керованих безпілотних пристроїв у випадках, коли класична логістика ускладнена, або не можлива, тощо. Це обумовлено декількома ключовими факторами:

Стратегічна важливість: Системи зв'язку та керування є життєво важливими для ефективного ведення військових операцій. Вони забезпечують координацію дій, передачу інформації та управління ресурсами. Їхнє пошкодження або втрата може призвести до серйозних наслідків.

Сучасні загрози: З розвитком технологій з'являються нові загрози для систем зв'язку та керування. Це включає кібератаки, електронну війну, а також фізичні атаки. Російське вторгнення підкреслює актуальність цих загроз.

Потреба в модернізації: Багато систем зв'язку та керування, які використовуються сьогодні, були розроблені декілька десятиліть тому і можуть не відповідати сучасним вимогам. А також, багато сучасних систем, які стрімко почали використовуватися у військових завданнях мають в першу чергу цивільне призначення, через що вони за своїми параметрами і технічними характеристиками часто не відповідають сучасним потребам щодо їхнього максимально ефективного використання у військовій сфері. Проведення подальшої роботи дозволить модернізувати ці системи, розширити їхні

можливості і функціонал, та забезпечити їхню сумісність із сучасними технологіями та завданнями, які будуть перед ними поставлені.

Забезпечення переваги: Ефективний захист систем зв'язку та керування без сумніву надає значну перевагу на полі бою. Це дозволяє забезпечити надійність комунікацій, швидкість реагування та гнучкість управління об'єднаннями, забезпечує можливість планування складніших операцій або належного та своєчасного реагування на зміну обстановки чи якісь дії вчинені стороною противника.

3.1. Постановка задачі захисту інформації при передачі бездротовими мережами зв'язку та керування

Серед різноманіття засобів і пристроїв, у керуванні якими застосовуються бездротові мережі, як вже було сказано, найбільш актуальними на даний час є безпілотні пристрої, серед яких найбільшого поширення отримали безпілотні авіаційні комплекси. Про що, зокрема, свідчить їх постійний і стрімкий розвиток.

В даний час існує низка потужних ударних і розвідувальних безпілотних комплексів, найвідоміші з яких вітчизняні БПЛА "Лелека", "Фурія", "Валькірія", легендарний турецький "TB-2 Bayraktar". Проте активна робота по виготовленню, розробці і вдосконаленню безпілотних систем проводиться постійно, про що свідчить ряд нових розроблених українських БПЛА, включаючи такі моделі як "Берегиня", "Грім", RAM UAV, "Демон-Е", "Демон-Т", "Велика Химера", F-2M, "Горлиця", "Мисливець", "Сокіл-300" – описані розробки включають в себе як розвідувальні дрони, так і навіть ударні їх варіанти.

Українські БПЛА мають чималий інноваційний потенціал, який багато чим зумовлений здатністю адаптуватися до складних метеоумов та змін електромагнітної обстановки, а також можливістю виконувати різноманітні функції, від розвідки до ударних операцій. Але, не зважаючи на таке різноманіття засобів, кількість а інколи й можливість використання таких

потужних БПЛА промислового рівня, порівняно із запитами на них у українського війська, нажаль, є дуже недостатньою.

Також є потреба у компактних безпілотних комплексах, які оператор може переносити на собі, і запускати без додаткових пристроїв чи певної необхідної інфраструктури (злітні смуги, майданчики, платформи, тощо), або у великій кількості максимально недорогих засобах, призначення яких: доставка корисного навантаження "в один кінець". Тому переважна більшість безпілотних засобів розвідки і ураження на теперішній час являє собою малогабаритні і малопотужні комплекси, складені ентузіастами із запчастин, призначених в першу чергу для цивільного використання, таких як SpeedyBee, Arduino, тощо, або цивільні моделі БПЛА мультикоптерного типу, найбільш популярні з яких Autel, DJI Mavic. Приклад такого засобу можна побачити на рисунку.

Рис. 3.1 Типова конструкція ударного/розвідувального БПЛА

Використаним для прикладу БПЛА є так званий FPV-дрон. Такі пристрої зараз масово виготовляються за програмою "Народний дрон" від Міністерства цифрової трансформації України. Схематика і програмні рішення, на яких будуються такі апарати мають цивільне походження і в цих реаліях перед нами постає проблема недостатньої захищеності таких засобів, а також певне обмеження їхніх характеристик у визначених цивільним законодавством межах. Ця проблема гостро потребує вирішення, оскільки це призводить до значних втрат безпілотної техніки і засобів у випадку використання противником навіть компактних і простих засобів РЕБ.

Виходячи з цього, задачі щодо захисту бездротової системи керування та зв’язку, яка ставиться для дослідів та подальшої роботи полягають у вирішенні питань захисту саме компактних, не великих за своїми габаритами та тактично-технічними характеристиками безпілотних комплексів в умовах їхнього використання збройними формуваннями. Такі комплекси зараз найбільш масово використовуються і мають при цьому дуже посередній, або й зовсім низький, за військовими критеріями, рівень захисту, орієнтований у першу чергу на запобігання можливим викликам їхнього цивільного використання.

Серед них: невелика кількість вільних каналів радіозв’язку у діапазоні робочих частот передавача, необхідність роботи на значній дистанції при діючому обмеженні максимальної потужності радіопередавача, можлива інтерференція сигналу із іншими джерелами радіосигналів, випадкові електромагнітні завади у каналі зв’язку від об’єктів і підприємств промисловості, тощо.

Для вирішення цих задач у дослідах і експериментах буде використовуватися і аналізуватися така ж схемотехнічна база, яка застосовується для виготовлення даних дронів або аналогічні, сумісні із ними пристрої. Це забезпечить наближення експерименту до умов існуючих задач захисту системи зв’язку та керування безпілотними пристроями. Зокрема, контролерів управління, таких як Arduino, SpeedyBee, тощо, а також відповідних їм модулів передавачів, найбільш поширені із яких це передавачі

сімейства CrossFire виробника TBS.

Також серед умов та обмежень у даній роботі розглядається критерій ресурсоємності впровадження тих чи інших рішень, зокрема вартість такого впровадження і витрати енергії на його функціонування. Адже безпілотні пристрої є автономні і мають вбудований акумулятор для своєї роботи.

3.2. Обґрунтування основних положень та принципів пропонованої концепції захисту передаваних даних

Слідкуючи за зведеннями із зони бойових дій, дописами у популярних сервісах обміну повідомлень інформаційного характеру, написаних діючими військовослужбовцями служби аеророзвідки (мається на увазі аеророзвідка із використанням саме безпілотних комплексів), з'єднань служб ударних БПЛА, новин та звітів офіційних каналів таких служб як Служба Безпеки України, Головне управління Розвідки України, Сили Спеціальних Операцій Збройних Сил України, а також офіційних сторінок конкретних бригад, можна проаналізувати принципи роботи таких бригад і способи застосування безпілотних засобів у бойових операціях. Разом з тим, часто у них можна зустріти і опис наявних проблем із використанням таких безпілотних засобів, серед яких основну нішу займають проблеми, які відносяться до таких властивостей безпеки інформації, як конфіденційність та доступність.

Основна проблема з точки зору конфіденційності у найбільш поширених не дорогих БПЛА (в тому числі ударних FPV-дронах) відеосигнал із літального апарату передається відкритим каналом і за відкритим цивільним протоколом на тому чи іншому визначеному каналі у діапазонах частот цивільного використання, таких як 2.4 ГГц або 5.8 ГГц.

Це призводить до кількох негативних наслідків: найперше – такий невеликий діапазон легко тримати під контролем і у разі виявлення початку передачі відеосигналу противник буде розуміти, що на стороні наших угруповань запущений у повітря безпілотний пристрій; другий аспект – маючи

необхідне обладнання, або звичайний приймач такої ж моделі і такого ж діапазону частот, що підтримує використовуваний протокол передавання відео, противник має можливість прийняти відеосигнал із нашого БПЛА і відтворювати його на своєму дисплеї.

При перехопленні сигналу відео на певній відстані від місця запуску, або вже безпосередньо над своїми позиціями, противник матиме можливість проаналізувати потенційний напрямок подальшого польоту БПЛА, виявити місця, що викликали у нас зацікавленість, знати які пристрої, позиції, засоби, тощо, наш БПЛА зміг виявити під час польоту. Внаслідок чого противник зможе відповідним чином відреагувати на це, здійснивши передислокацію, чи вживши інших заходів, що зведе нанівець проведену розвідку.

У випадку перехоплення відео із ударного БПЛА, противник матиме можливість слідкувати за напрямком руху дрону і потенційно передбачити місце майбутнього нанесення вогневого ураження і, використовуючи засоби свого зв'язку, передати цю інформацію потрібним особам, таким чином попередивши їх, що також може негативно вплинути на ефективність використання нашого апарату.

Але можливий і інший, на порядок гірший сценарій, пов'язаний із конфіденційністю інформації, переданої із засобів БПЛА. Якщо у противника наявний приймальний пристрій із достатнім рівнем підсилення, або потужності сигналу від відеопередавача нашого пристрою в точці розташування противника достатньо для задовільного прийому сигналу відео із працюючого БПЛА ще у момент його злету із позиції чи посадки на позицію – це надасть противнику можливість проаналізувати орієнтири, що потенційно можуть потрапити на відео.

Це призведе до розкриття точного місцерозташування позиції операторів чи їх помічників, розташування і конфігурацію засобів зв'язку, в тому числі і польового, який не відноситься до керування самим апаратом, місцерозташування інших об'єднань та підрозділів, загальну організацію оборонних рубежів, конфігурації траншей та інших візуальних відомостей, які

можуть потрапити в кадр, поки пристрій пролітатиме ще над нашими позиціями. Перехоплена таким чином інформація є надзвичайно цінною і надає велику перевагу противнику. Враховуючи наявні у противника засоби ураження, це з високою ймовірністю призведе до дуже серйозних і трагічних наслідків, оскільки сама інфраструктура зв'язку та систем керування БПЛА на даному етапі протистояння – ціль номер 1 для засобів ураження противника.

Так, у інформаційному зведенні від бійця Сил Оборони України Бровді Роберта Йосиповича із позивним "Мадяр" можна зустріти детальний приклад трагічного для нас використання противником такої вразливості. На відео видно, що сили РЕР противника виявили відеосигнал із українського БПЛА і спостерігали за шляхом його повернення на позиції, попутно фіксуючи орієнтири. Через деякий час в мережу потрапило відео із розвідувального БПЛА ЗС РФ, на якому було видно момент ураження позиції операторів, ймовірно, за допомогою ОТРК "Іскандер" [82].

Якщо розглянути наші безпілотні пристрої і дані, що вони нам надають, як сервіс, то стає можливо визначити проблему доступності, яка при застосуванні таких засобів у військових цілях полягає у наступному: БПЛА під час роботи керується інструкціями, які отримує каналом радіозв'язку від пульта керування оператора і по мірі того як пристрій віддаляється на більшу відстань, природньо зменшується потужність сигналу на приймальній антені апарату. В таких умовах наш безпілотник, порівняно із дистанцією до нашого пристрою керування, ще й знаходиться значно ближче до супротивника, що надає змогу останньому використовуючи засоби радіоелектронної боротьби опромінювати приймальну антену нашого апарату шумовим сигналом схожого або дещо ширшого спектру і більшої потужності, порівняно із сигналами керування пульта. Це значно погіршить якість зв'язку і при достатній потужності засобу РЕБ може призвести до неможливості розпізнавання радіоприймачем апарату сигналів від власної станції керування і відповідно до втрати зв'язку.

В умовах бойових дій це означає гарантовану втрату літального апарату. Так, опираючись на слова бійця сил аеророзвідки Тараса Білки у інтерв'ю

каналу ISLND TV, що розміщене на їх YouTube-каналі [83], можна констатувати, що втрати безпілотної техніки середнього і нижнього сегменту на ділянках їхнього застосування коливається в межах 80-85 відсотків. Звичною є ситуація, коли із 11 запущених ударних FPV-дронів цілі досягає лише два безпілотника.

Опираючись на це, сформулюємо основні положення, що покладені в пропонований концепт покращення захисту бездротової системи безпілотних пристроїв:

– необхідно забезпечити неможливість виявлення і перехоплення противником сигналу передавання відео;
– у випадку перехоплення сигналу відео, необхідно унеможливити для противника його відтворення;
– або ускладнити його відтворення таким чином, щоб проміжок часу для його відтворення був більший за той, протягом якого противник матиме користь від отриманої із відео інформації;
– необхідно забезпечити покращення стійкості нашої бездротової системи керування до засобів радіопридушення та/або забезпечити для такої системи можливість відновлення зв’язку, якщо вже застосованих методів виявилося не достатньо і зв’язок було втрачено, або критично знизилась його якість.

Ці положення орієнтовані на вирішення двох основних описаних проблем у захищеності БПА: конфіденційності їхніх даних та доступності їх керування, в умовах їхнього подвійного та безпосередньо військового використання.

Безпілотний авіаційний пристрій навіть не високого класу (FPV наприклад), не дивлячись на його невеликі розміри та відносно не високі обчислювальні потужності, насправді являє собою достатньо складну інформаційну систему. Вона складається із цілого набору окремих компонентів.

У кожному з таких компонентів є інкапсульований набір специфічних виконуваних ним функцій, набір налаштувань, параметрів а також зовнішніх інтерфейсів. Інтерфейси кожного компонента БПЛА підтримують стандартні для такого роду пристроїв протоколи обміну даними та командами, завдяки

чому усі компоненти взаємозв’язані між собою в єдину мережу (Рис 3.2).

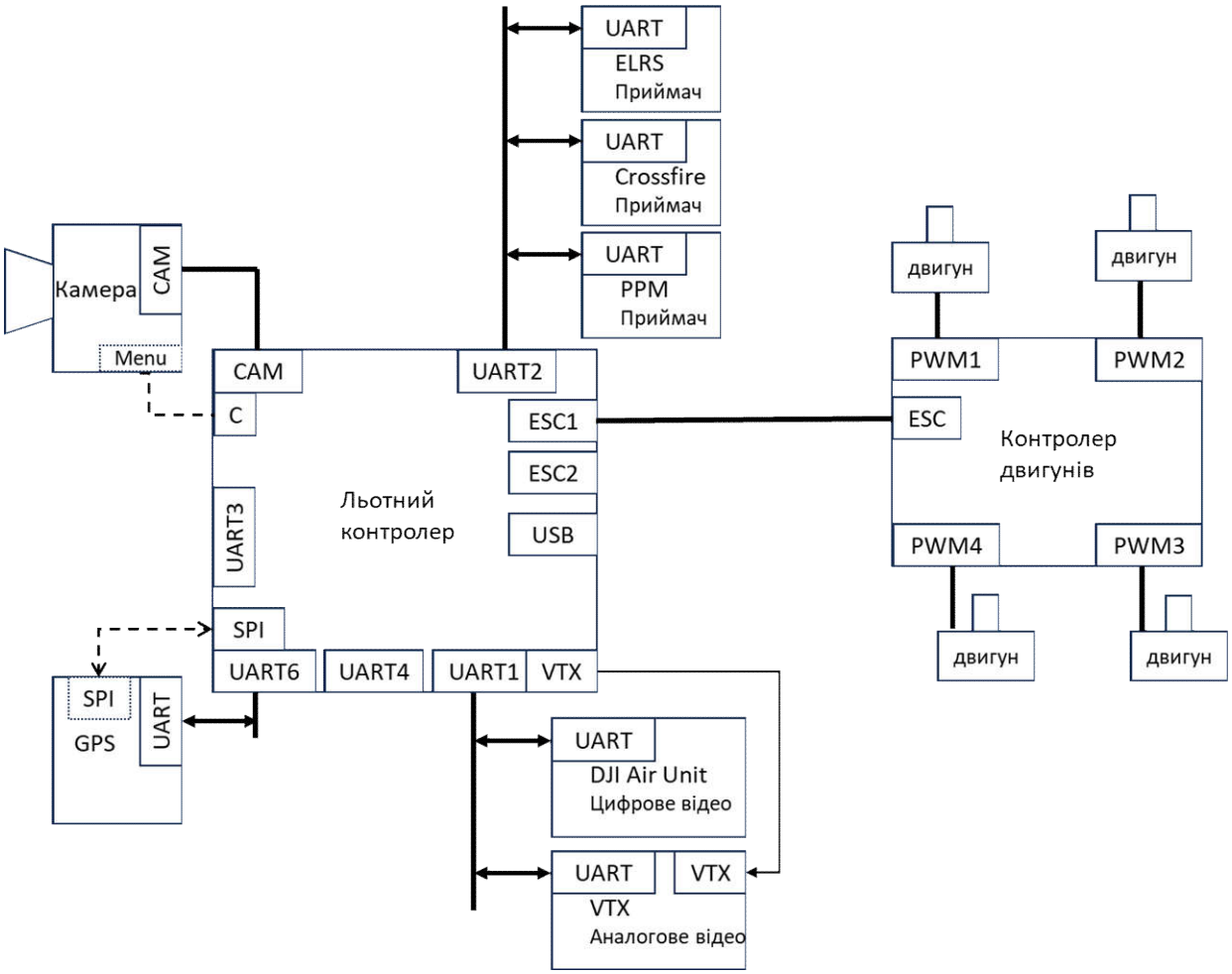


Рисунок 3.2. Класична структура взаємодії компонентів безпілотного FPV апарату

Як вже було сказано, функції і параметри складових компонентів у таких пристроях є інкапсульовані. Це означає, що ми не можемо змінити алгоритми роботи чи виконувані функції такого компонента безпосередньо у ньому самому. Наприклад, для контролера двигунів ESC, чи відеопередавача VTX, виконувані функції запрограмовані заводом-виробником. Але використовувані для обміну даними порти зв’язку (UART, SPI), також підтримують протоколи і команди для керування цими компонентами і налаштування їхньої роботи. Завдяки цьому є можливою зміна налаштувань компонентів, в тому числі під час роботи і польоту БПЛА.

Для реалізації системи захисту конфіденційності і забезпечення

доступності пропонується така ідея – у схему апарату впроваджується вбудований пристрій як зовнішній модуль на базі мікроконтролера. У звичайних умовах функціонування він не бере безпосередньої участі у роботі чи керуванні безпілотним апаратом, а лише веде спостереження за його роботою, тобто записує необхідні дані у пам’ять і проводить моніторинг параметрів функціонування пристрою.

У випадку, коли контролер виявить відповідну команду оператора або наявність умов спрацювання "тригерів", що позначають позаштатну ситуацію він вмикається в роботу вже у активну фазу і використовує порти керування компонентами апарату для реалізації заходів безпеки. Умовно такий алгоритм можна відобразити блок-схемою:

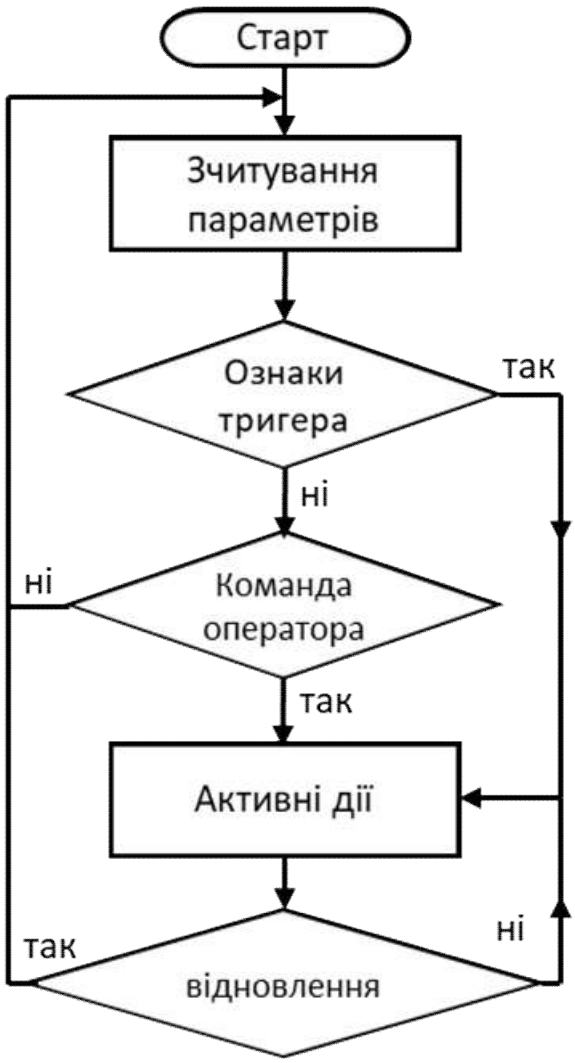


Рис. 3.3. Блок-схема алгоритму роботи вбудованої системи

Використання запропонованої концепції дозволить нам уникнути зниження продуктивності бортових систем безпілотних апаратів, не вимагає втручання у їхню роботу за умови коли все працює належним чином, але при цьому дозволить забезпечити покращення надійності і захищеності роботи такого пристрою при спробах розкрити вміст даних при передаванні ним інформації, при спробах придушення зв’язку із пристроєм чи іншому впливу на канал зв’язку, націленим на зниження його надійності.

Також такий підхід забезпечує нам потенційну можливість для модернізації вже існуючих апаратів шляхом впровадження в них такого вбудованого мікроконтролерного пристрою та виконання деяких переналаштувань базових його елементів, без необхідності заміни компонентів чи капітальної перепрошивки ПЗ "бортового" обладнання.

Для забезпечення збереження конфіденційності даних у системі передавання відеосигналу із БПЛА було обрано так зване легковагове шифрування, оскільки воно надає змогу забезпечити базовий криптографічний захист, який у більшості випадків буде достатнім для закриття відеосигналу від несанкціонованого перегляду за оптимального рівня потужностей, які необхідні для його реалізації, що дасть змогу впровадити його у компактного розміру вбудований пристрій.

Для забезпечення доступності самої системи керування безпілотним пристроєм було реалізовано багатогранний підхід, який включає у себе кілька певних етапів для підвищення стійкості і відповідно різних методів, що застосовуються на кожному із таких етапів, відповідно до зовнішньої обстановки і даних, що отримуються контролером апарату із модуля радіозв’язку.

При розробці концепції було використано і розроблено комплекс заходів для забезпечення за даних умов і обчислювальних обмежень максимально можливого рівня доступності нашого пристрою при використанні закладених у схемотехніку безпілотних пристроїв базових функцій.

3.3. Заходи забезпечення конфіденційності та приховування відеосигналу у БПЛА

Як було описано у концепції – в першу чергу захисту підлягає відеосигнал передавача безпілотного апарату, як найцінніша для противника інформація. В результаті проведеного раніше аналізу ми змогли виділити основні чинники, які забезпечують противнику розкриття даних із камери:

– передавання відео у відкритому форматі;

– достатня потужність сигналу відеопередавача;

– несуча частота сигналу у межах стандартних каналів 5.8 МГц діапазону.

Жоден із існуючих методів захисту каналів зв’язку на сьогодні не здатен одночасно захистити систему відеозв’язку БПЛА за всіма виділеними чинниками. А для деяких із них, як наприклад для критерію потужності передавача, на даний час не пропонувалося конкретних особливих заходів мінімізації їхнього впливу.

Тому вирішення даної проблеми вимагає комплексного підходу. На основі цього пропонується комбінування кількох заходів безпеки одночасно, серед яких є як і класичні, так і ідейно новий підходи.

3.3.1. Легковагове шифрування відеопотоку

У більшості використовуваних безпілотних літальних апаратів відеосигнал та керування апаратом, здійснюється на різних частотах, залежно від моделей передавачів, які зв’язані із основними модулями апарата тим чи іншим портом. Для того, щоб запровадити механізм шифрування у таку систему найбільш оптимальний варіант – використати впроваджений у апарат мікроконтролер у конфігурації проміжної ланки у зв’язку між відео модулем та передавачем.

Цей контролер буде виконувати роль проміжного "шифратора" даних, що передаються із відеомодуля. Існує два основних варіанти роботи системи передавання відео, перша з них передбачає залучення до процесу передавання відео основного контролера апарату.

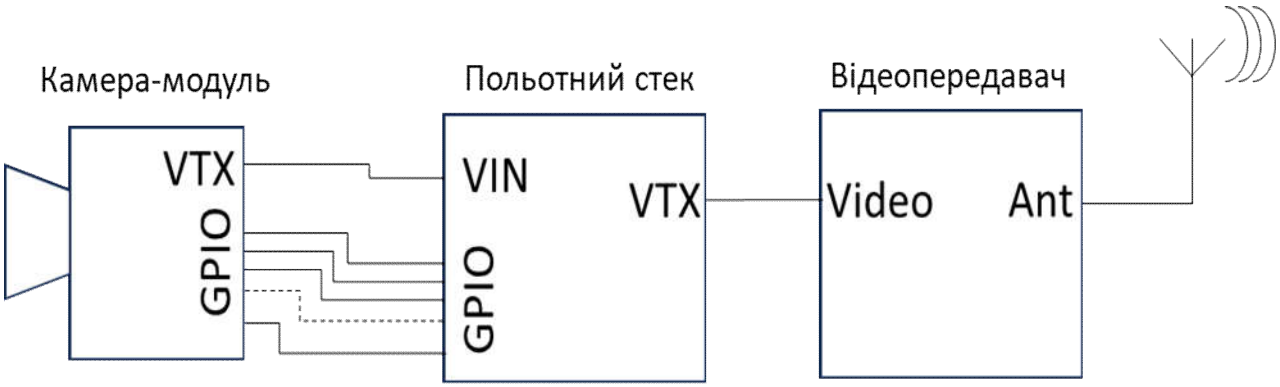


Рисунок 3.4 Передавання відеосигналу через контролер апарату

Другий варіант функціонування відео системи передбачає, що основний контролер здійснює лише опосередковане керування камерою, та не бере участі у процесі передавання відео.

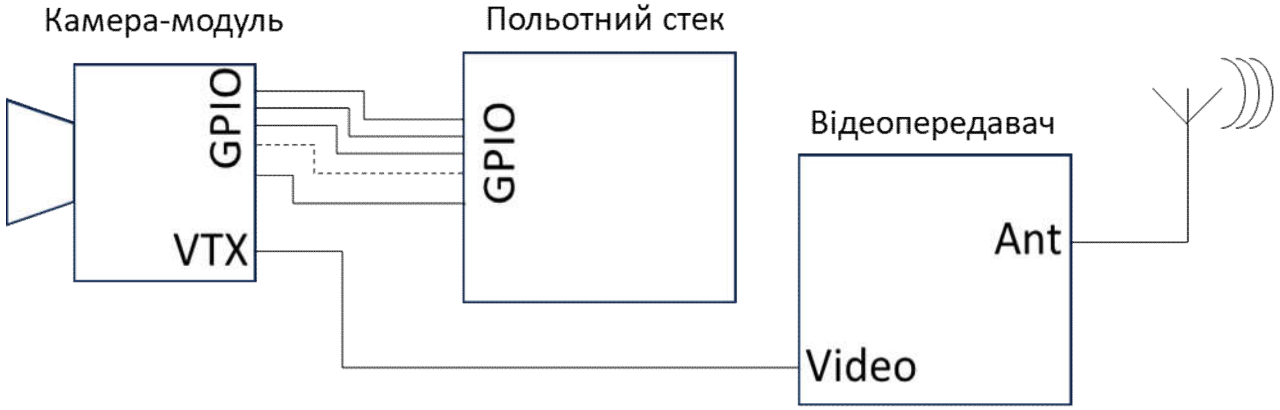


Рисунок 3.5 Передавання відеосигналу напряму передавачем апарату

Обидва варіанти роботи підтримують будь-який формат відео, як аналоговий, так і цифровий. Основна відмінність полягає у тому, що при передаванні відео через польотний контролер (чи інший керуючий пристрій у випадку іншого типу безпілотного апарату) на нього може накладатися додаткова інформація, така як швидкість, висота, положення і кут нахилу пристрою відносно лінії горизонту та інші дані для кращої візуалізації умов роботи апарату оператором.

Приклад такого виводу можна побачити на рисунку 3.6 – в даному випадку ми бачимо на дисплеї інформацію про рівень заряду батареї у вольтах, час від моменту увімкнення передавача у секундах, режим управління БПЛА а також

інформаційне повідомлення "LOW VOL" яке додатково сигналізує нам про низький рівень заряду батареї.

А також, при роботі системи відео за принципом, відображеним на рисунку 3.4, можливе використання протоколів вищого рівня, для оптимізації обміну даними між головним контролером і передавачем, узгодження їхньої роботи, налаштувань швидкості, тощо.

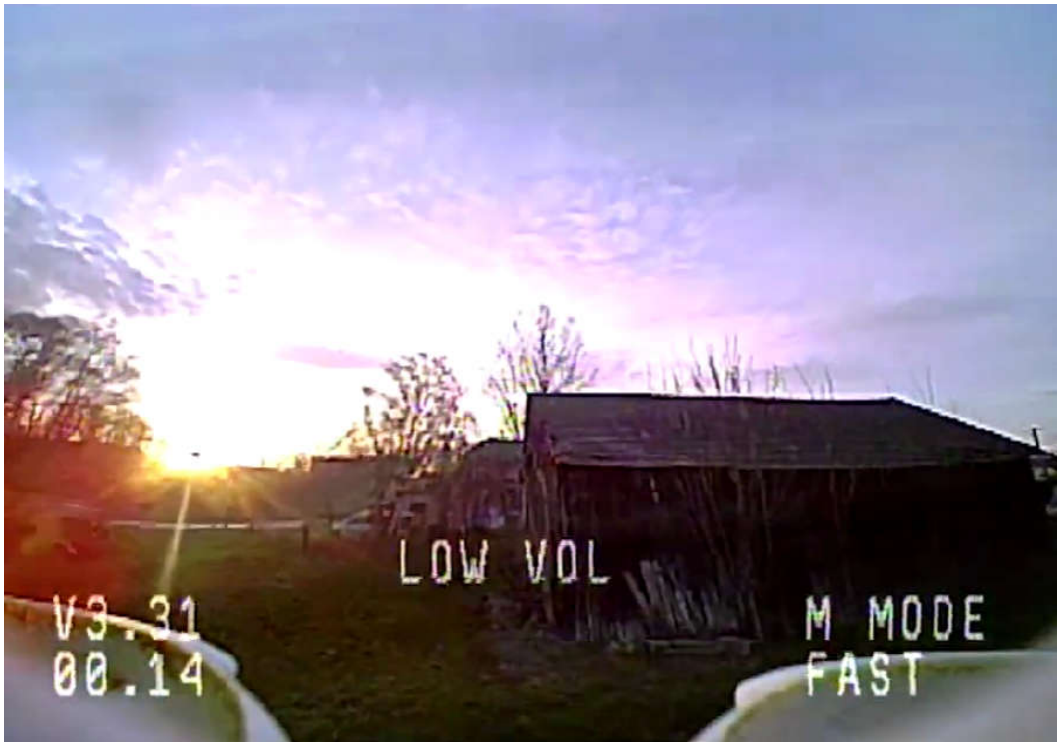


Рисунок 3.6. Вивід на відео додаткової інформації від контролера польоту

Оскільки у лінії зв’язку між пристроєм керування і передавачем VTX може використовуватися різний протокол передачі, відповідно до виробника цих пристроїв, більшу практичну значимість для оптимальної і відносно не трудомісткої реалізації криптографії має канал видачі відеосигналу безпосередньо із блоку запису і управління відеокамери.

У модулі камери, у разі застосування обладнання орієнтованого на використання аналогової камери, передаються не перетворені аналогові сигнали таких протоколів як PAL/NTSC, тощо. У разі використання техніки, розрахованої на передачу цифрового сигналу, на порти виводу від модуля камери в більшості популярних моделей іде передавання вже кодованого

цифрового сигналу із застосуванням стандартизованих для застосування у FPV чи інших безпілотних системах кодеків (наприклад DJI Digital FPV), але алгоритм більшості таких кодеків є патентованою технологією, використання якої для виробника таких пристроїв вимагає оплати і ліцензії [84].

Тому на ринку таких рішень можна зустріти також багато пристроїв які мають можливість виводу цифрового сигналу у вигляді синхронізованої послідовності безпосередніх значень кольорів пікселів за відповідною даному модулю колірною схемою.

Для передавання такого об’єму інформації пристроями відео застосовується або швидкісний послідовний, або паралельний порт передачі даних, при цьому паралельний порт дозволяє передати більший об’єм даних за однаковий час, порівняно із послідовними портами передачі.

Щоб розрахувати мінімальну задовільну частоту передачі даних для стабільного передавання зображення без втрати кадрів за необхідної нам роздільної здатності відеомодуля, (наприклад у FPV-апарату) використаємо таку формулу (3.1):

$$f_{t_{min}} = N_{pix} * f_{frm} * d_c \tag{3.1}$$

де:

N_{pix} – це кількість пікселів у зображенні;

f_{frm} – це необхідна нам частота оновлення зображення, кадрів/сек;

$f_{t_{min}}$ – мінімально необхідна для заданих умов частота передавання одиниць інформації, біт/сек;

d_c – кількість біт, що необхідно передати для відображення кольору кожного пікселя (залежить від параметра глибини кольору), за умови використання конкретного виду порту: послідовних (SPI, I2C, UART, тощо); або паралельних портів (4-8-16 виводів, тощо).

Для "класичної" конфігурації БПЛА бажана роздільна здатність коливається в межах 1-2 мегапікселі, а частота кадрів 8-24 кадрів/сек. За

приведеною вище формулою можна у форматі таблиць підсумувати мінімально необхідні параметри передачі зображення для послідовного і паралельного порту відповідно.

Таблиця 3.1

Параметри для передавання послідовним портом

Мінімально необхідна швидкість передачі, МГц	Роздільна здатність, пікс.	Частота кадрів, $с^{-1}$	Значень на піксель, од
128	1000000	8	16
160	1000000	10	16
256	1000000	16	16
320	1000000	20	16
384	1000000	24	16
256	2000000	8	16
320	2000000	10	16
512	2000000	16	16
640	2000000	20	16
768	2000000	24	16

Таблиця 3.2

Параметри для передавання паралельним портом

Мінімально необхідна швидкість передачі, МГц	Роздільна здатність, пікс.	Частота кадрів, $с^{-1}$	Значень на піксель, од
16	1000000	8	2
20	1000000	10	2
32	1000000	16	2
40	1000000	20	2
48	1000000	24	2
32	2000000	8	2
40	2000000	10	2
64	2000000	16	2
80	2000000	20	2
96	2000000	24	2

Варто зазначити, що для більшості наявних на ринку мікроконтролерів із сегментів "Low-Cost" та "Low-Power" типові значення робочої тактової частоти процесора коливаються у межах від 16 до 128 МГц. Контролери із тактовою частою понад 128 МГц, відносяться до вищого сегменту ринку, мають значно вищу вартість, а найголовніше – вони споживають порівняно більше енергії ніж їхні "слабші" моделі, що обмежує їхню придатність до використання у автономних пристроях, що живляться від батареї.

Однією із умов нашої роботи і досліджень є саме врахування ціни рішення і його енергозатратність, тому для реалізації криптоалгоритму розглядаємо лише контролери нижнього і середнього сегменту. Це в свою чергу накладає суттєве обмеження на можливості використання криптографії для захисту каналу передавання відео.

Із обчислених у таблиці результатів видно, що для криптографічного захисту на базі мікроконтролера оптимальним є використання роздільної здатності 1 Мп., за такого значення можна використовувати частоту кадрів до 10 кадрів/с. У разі гострої потреби у збільшенні роздільної здатності до 2 Мп, частота кадрів повинна бути обмежена – не більш як 8 кадрів/сек.

Разом з цим запас продуктивності мікроконтролера всеодно залишається невеликим: при зйомці з частотою 8 к/с в режимі 1 Мп із 128 000 000 операцій мікроконтролера в секунду 16 000 000 операцій затрачається лише на зчитування інформації, тобто кожна восьма операція МК – зчитування чергового значення. В таких умовах використання "важких" і потужних алгоритмів шифрування (як от алгоритму "Калина", використаного у роботі [85]) призведе до втрати кадрів зображення, оскільки поки МК буде зайнятий шифруванням він "пропустить" чергові значення.

Для реалізації криптографічних заходів у таких обмежених умовах дуже добре зарекомендували себе так алгоритми так званого "легковагового" шифрування. Наприклад, у роботі [86] була реалізована криптографія в межах корпусу RFID-мітки. Тому, для захисту відео-даних при їх передачі, було вирішено використати алгоритм, який базується на властивості математичної

операції додавання за модулем "2" :

$$(x_p \oplus k) \oplus k = x_p \tag{3.2}$$

Відповідно шифрування й розшифрування відбувається за наступною схемою (Рис. 3.7):

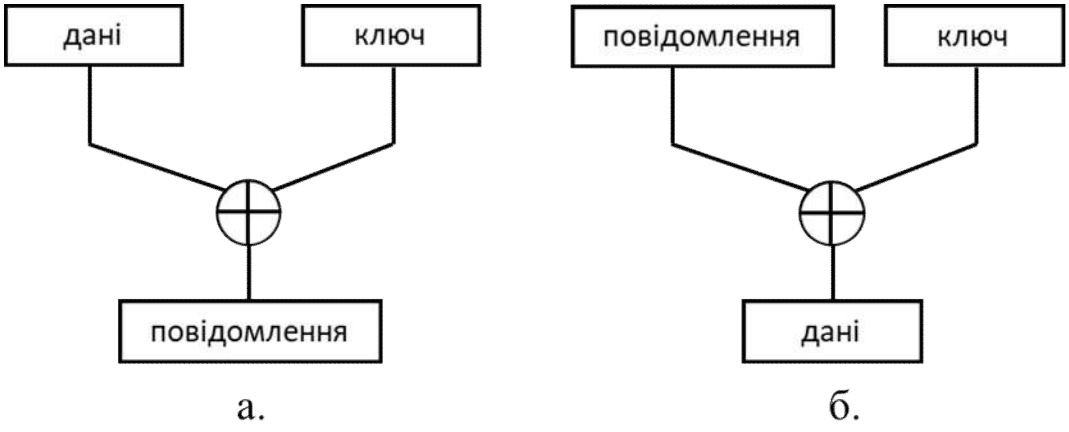


Рисунок 3.7. Схема шифрування даних від камери:
а. – шифрування; б. – розшифрування.

Цей спосіб шифрування має відносно слабку криптостійкість, але він здатен задовольнити завдання ускладнення відтворення сигналу відео при його перехопленні і прибрати один із чинників перехоплення: відкритість каналу. Оскільки в умовах бойових дій БПЛА постійно переміщується, дані з його камери можна вважати інформацією із коротким "часом життя". Тому навіть кількахвилинна затримка із розкриттям інформації із кадру може позбавити цінності її вміст.

Можна підсумувати, що запропоноване використання на борту безпілотника мікроконтролера, дозволяє з його допомогою реалізувати криптографічний механізм, який ускладнить для противника розкриття переданого сигналу.

Проте цей підхід має цілий ряд обмежень: ми змушені обмежувати частоту кадрів або роздільну здатність відео, щоб МК встигав виконати процес "прийняти/обробити/передати"; криптографічний алгоритм, який можна

реалізувати таким чином має невисокий показник стійкості; застосувати такий спосіб захисту можна лише для відеомодулів, що передають дані у форматі цифрових значень.

3.3.2. Керування частотою передачі за допомогою мікроконтролера

Для мінімізації впливу наступного чиннику перехоплення: стандартної і відомої противнику частоти передачі використаємо можливості МК, щодо налаштування і зміни деяких параметрів самого відеопередавача.

Якщо під’єднати порт вводу-виводу мікроконтролера до керуючого входу відеопередавача, ми зможемо за допомогою МК змінювати його параметри згідно потрібного нам алгоритму.

В такому режимі ми можемо використати менеджмент параметрів VTX як засіб захисту відеоканалу від перехоплення даних, а в окремих випадках і від його виявлення. Для налаштувань нам доступні дві функції: функція зміни несучої частоти та функція регулювання потужності передачі сигналу. Для обидвох із них було запропоновано варіант їх нестандартного використання з метою підвищення рівня захисту.

Розглянемо можливість зміни частоти першою з них.

Зміна несучої частоти сигналу, як засіб захисту каналу зв’язку здатна забезпечити як конфіденційність передаваних даних у каналі, так і в певних обставинах приховування самого каналу зв’язку.

Врахувавши параметри технологічних рішень, що використовуються у сучасних системах безпілотної авіації (такі продукти як "SpeedyBee", "TBS", "Happymodel", "TBS CrossFire", "Arduino Arduflight", тощо) та результати проведеного аналітичного огляду джерел, мною пропонується метод регулярного перелаштування частоти як найбільш вдалий і оптимальний для застосування його у БПЛА. Поряд з цим, в контексті впровадження його у БПЛА він ще й дуже зручний у реалізації, що також було висвітлено у роботі, опублікованій за результатами дослідження.[87]

Це зумовлено тим, що для більшості популярних моделей приймачів

(наприклад сімейства "TBS CrossFire") є можливість задання значень частоти передачі сигналу на рівні програмного коду та команд на порт керування налаштуваннями, що не вимагає натискання кнопок, чи зміни фізичних параметрів якихось елементів мікросхеми і може відбуватися дистанційно. При цьому, для приймача типової цивільної робочої частоти 868 МГц, цю зміну можна провести в досить широкому діапазоні: від 860 МГц аж до 928 МГц і для приймача 5.8 ГГц: від 5705 МГц до 5945 МГц (Табл. 3.3,3.4).

Таблиця 3.3

Параметри частотних діапазонів передавача 868/915 МГц [88]

Frequency Setting	Frequency	Max. power level	Settings locked	Operating frequency
868	868 MHz	No limitations	No	860-885 MHz
915	915 MHz	No limitations	No	902-928 MHz
868CE	868 MHz, LBT technique	No limitations	No	860-885 MHz
915C-Tic	915 MHz	No limitations	No	915-928 MHz
915FCC	915 MHz	No limitations	No	902-927 MHz
868 Race	868 MHz	No limitations	No	860-885 MHz
915 Race	915 MHz	No limitations	No	902-928 MHz

Таблиця 3.4

Параметри частотних діапазонів передавача 5.8 ГГц [88]

Channel	1	2	3	4	5	6	7	8	
Band A	5865	5845	5825	5805	5785	5765	5745	5725	MHz
Band B	5733	5752	5771	5790	5809	5828	5847	5866	MHz
Band E	5705	5685	5665	5645	5885	5905	5925	5945	MHz
Airwave	5740	5760	5780	5800	5820	5840	5860	5880	MHz
Race Band	5658	5695	5732	5769	5806	5843	5880	5917	MHz

Передавач можна переналаштовувати на роботу на той чи інший канал відповідно до цих таблиць.

Для реалізації такого методу до звичайної схеми безпілотника (Рис. 3.2.)

необхідно підключити мікроконтролер таким чином, щоб з'єднати порт вводу/виводу МК із керуючим входом передавача:

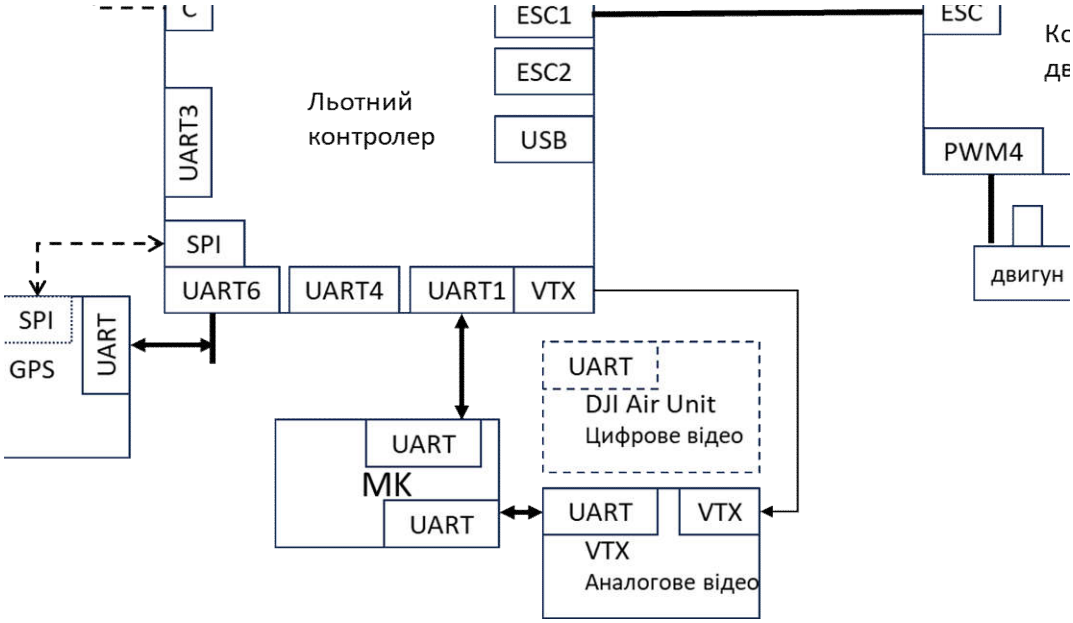


Рисунок 3.8. Схема під'єднання МК до відеопередавача

Після цього, застосовуючи керуючі команди ми регулярно змінюємо частоту передавання згідно алгоритму, або перебираючи визначений набір каналів. Наочно такий процес передавання буде виглядати таким чином:

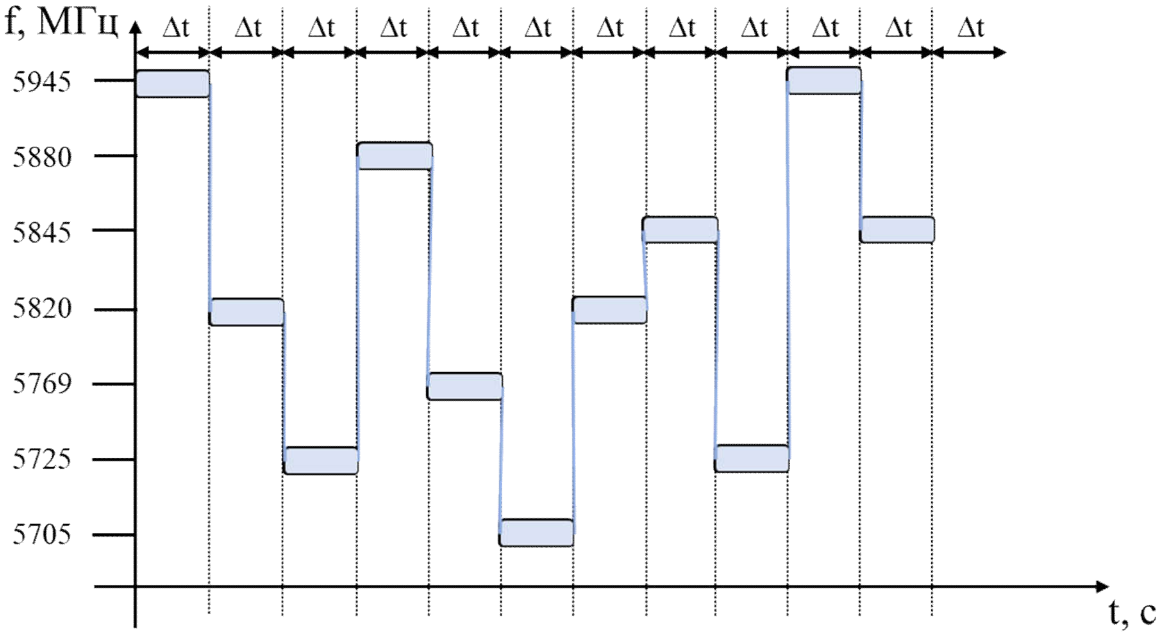


Рисунок 3.9. Частотно-часова схема захищеного передавання відео

Для даного методу рівень захищеності каналу S буде залежати від двох основних параметрів: розмір вибірки каналів N, та розмір часового проміжку Δt.

При цьому між ними діє наступна залежність:

$$\lim_{N \to max\, \Delta t \to min} S(N, \Delta t) = S_{max} \tag{3.3}$$

$$\lim_{N \to min\, \Delta t \to max} S(N, \Delta t) = S_{min} \tag{3.4}$$

Як бачимо, для забезпечення максимального рівня захищеності нам треба забезпечити якомога більшу вибірку каналів і якомога менший часовий інтервал передачі на кожній частоті. В таких умовах противнику буде дуже складно не тільки приймати і зчитувати сигнал, але й виявити його.

За достатньо високої частоти переналаштування, навіть у позитивному для противника випадку виявлення сигналу час часового контакту приймача із сигналом буде обмежений інтервалом передачі даного сигналу на цій частоті, після чого він знову буде змушений сканувати ефір засобом розвідки.

Для організації вибірки несучих частот доцільно використати масив, у якому зберігатимуться значення частот каналів і при виклику функції зміни частоти передавання зчитувати чергове значення.

Такий метод дозволить суттєво збільшити швидкодію і зменшити затрати ресурсів, у порівнянні із обчисленням наступного випадкового значення, адже обсяг пам’яті сучасних контролерів дозволяє зберігати достатньо велику кількість даних і вибірка значень частот не займатиме великого проміжку частку пам’яті.

А обчислення певного чергового псевдовипадкового значення вимагатиме регулярного використання обчислювальних ресурсів від контролера, що в свою чергу призведе і до додаткового споживання енергії.

Пропонується наступний алгоритм роботи мікроконтролера в режимі реалізації системи захисту.

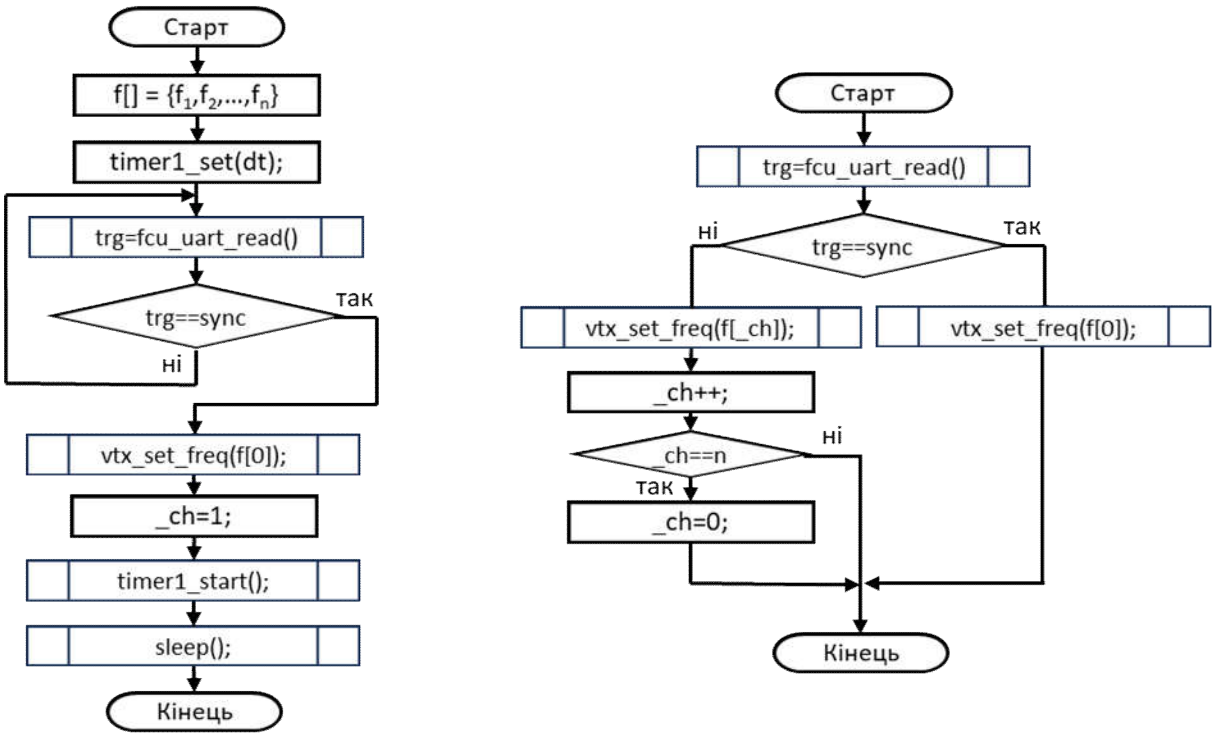


Рис. 3.10. Типовий алгоритм роботи МК при реалізації частотного стрибання:
а.) – ініціалізація; б.) – ітерації переналаштування

Для рівномірного часового інтервалу переналаштування пропонується, як видно із блок-схеми, використання вбудованих у мікроконтролер незалежних таймерів, це зумовлено їхньою високою точністю. При ініціалізації задається значення Δt для лічильника таймера, встановлюється початкове значення частоти $f[0]$ після чого таймер запускається і контролер можна перевести у режим пониженого енергоспоживання. У момент спрацювання таймера ми встановлюємо частоту $f[ch]$ і збільшуємо ch на одиницю для наступної ітерації. Тут ch – це значення номеру каналу, яке зберігається у пам'яті контролера, а $f[n]$ це масив значень частотних каналів вигляду:

$$f[n] = \begin{bmatrix} 5880 \\ 5769 \\ 5725 \\ \cdots\cdots \\ 5950 \end{bmatrix} \tag{3.5}$$

Також у запропонованому алгоритмі можна побачити звертання через порт UART до контролера польоту із наступною перевіркою значення тригера. Це зроблено з метою забезпечення можливості ручної синхронізації переналаштування частот між передавачем та приймачем.

Маючи канал керування дроном, ми можемо присвоїти одній із опціональних кнопок функцію ручної синхронізації захисту відео. Мною таке використання є переконливо рекомендованим, оскільки забезпечить нам можливість дистанційно з пульта "аварійно" скинути частоту передачі на першу із набору і здійснити запуск процесу перелаштування з початку для випадку розсинхронізації відео чи інших перебоїв у роботі.

Дуже важливим аспектом цього методу є синхронізація, адже якщо приймач і передавач будуть перелаштовувати частоту не одночасно це призведе до погіршення якості або втрати зв’язку. У реалізації методу частотного стрибання для БПЛА можливі два варіанти порушення синхронізації – відставання моменту зміни частоти приймача від дрону, або його випередження.

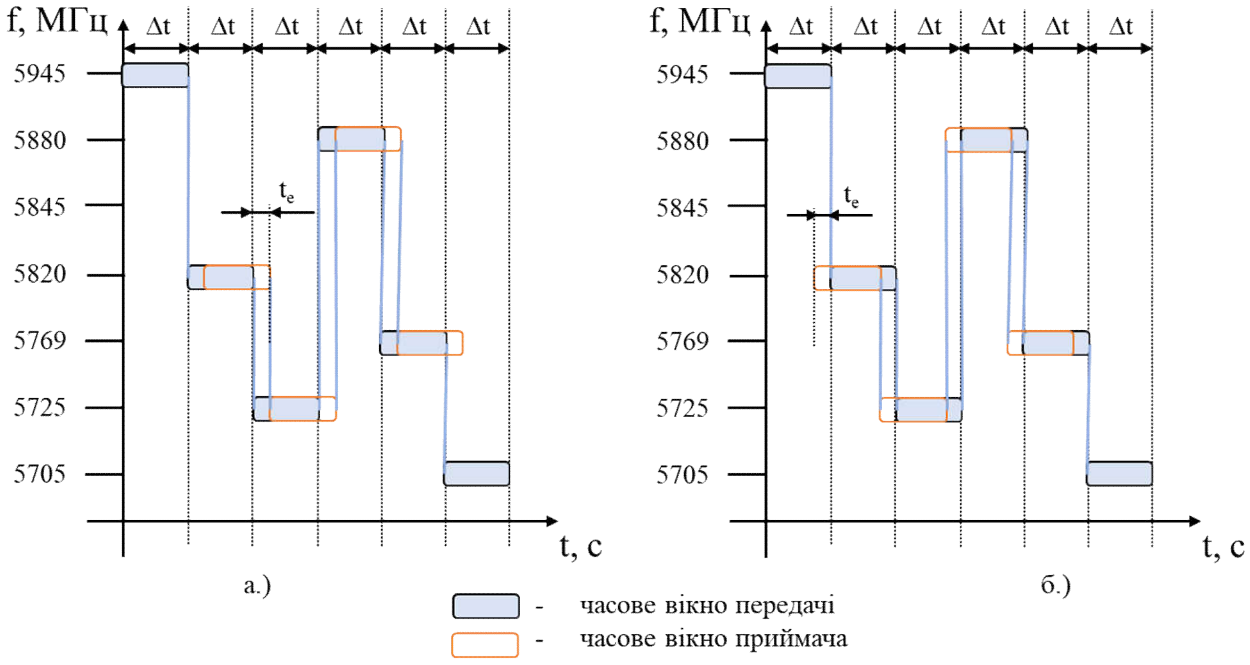


Рисунок 3.11. Можливі варіанти розсинхронізації приймача:
а.) відставання; б.) випередження

Синхронізацію ми розглядаємо саме із точки зору приймального пульта, оскільки система передачі відео із БПЛА на землю є симплексною і не передбачає можливості безпосереднього зворотного зв'язку. Таким чином дрон умовно має роль "ведучого", а наземна система здійснює коректування прийому.

В таких умовах пропонується програмно виконувати адаптивне підлаштування часового вікна. Для цього, разом із самим процесом переналаштування частоти приймача, прийому і відтворення самого сигналу, на стороні оператора будемо здійснювати також програмний моніторинг рівня сигналу $S(t)$ в межах часового вікна передачі Δt і записувати його значення як часову функцію $F(t)$. Тоді ми зможемо прослідкувати енергетичну зайнятість даного проміжку часу. Який теоретично може мати три стани:

$$F(t) = s(t), t \in [0, \Delta t] \tag{3.6}$$

$$F(t) = \begin{cases} s(t), t \in [0, t_в] \\ \approx 0, t \in [t_в, \Delta t] \end{cases} \tag{3.7}$$

$$F(t) = \begin{cases} \approx 0, t \in [0, t_в] \\ s(t), t \in [t_в, \Delta t] \end{cases} \tag{3.8}$$

У випадку, коли функція має вигляд (3.6) – це ознака найкращого стану прийому сигналу – увесь проміжок зайнятий сигналом. Здійснюємо прийом у такому ж режимі. Коли функція матиме вигляд (3.7) – це ознака, що приймач перелаштовує частоту із затримкою, відносно дрону. Необхідно здійснити для наступної ітерації коректування: прискорити на час $t_{cor} = \Delta t - t_в$.

Коли функція матиме вигляд (3.8) – це ознака, що приймач перелаштовує частоту швидше за дрон. Необхідно здійснити для наступної ітерації коректування: зробити затримку на час $t_{cor} = t_в$.

Отже пропонована система забезпечує два види синхронізації – постійна програмна адаптація прийому сигналу, та аварійне скидання і старт передачі із нульової відмітки.

3.3.3. Адаптивна регуляція потужності передавача

Розглянемо останній фактор розкриття інформації відео – це достатня потужність сигналу від відеопередавача у точці знаходження засобів приймання противника.

Для протидії цьому, пропонується адаптивна зміна потужності передавача відео, відповідно до рівня потужності вхідного сигналу від пульта керування.

Якщо повторно розглянути схему з'єднання МК і відеомодуля приведену на рисунку 3.8. Видно, що було передбачено також з'єднання через послідовний порт UART із польотним контролером. Це дає нам змогу робити запити і отримувати дані від головного контролера безпілотника. Це вже можна було спостерігати у пропонованому алгоритмі відновлення синхронізації, де через послідовний порт ми отримували інформацію щодо вхідних команд з пульта і перевіряли активацію програмованої кнопки на пульті керування.

Для реалізації захисту каналу передавання відео через адаптивну зміну потужності пропонується така ідея – з певною частотою запитувати у польотного контролера миттєве значення параметрів його роботи і виділяти із його відповіді значення якості сигналу від пульта керування. Після чого, базуючись на даних про якість сигналу керування, корегувати потужність передачі сигналу відео.

Хоч канал передачі сигналів від пульта керування не має безпосереднього відношення до зв'язку із каналом передавання відео – це зазвичай дві розділені між собою системи. Проте обидві системи для передавання інформації використовують радіохвилі, з чого випливає їхня спільна особливість – потужність сигналу на приймачі обернено пропорційна відстані від безпілотного пристрою до пульта оператора. Тобто зі зближенням безпілотника до пульта керування рівень сигналу зростає. Це можна виразити через границі:

$$\lim_{l \to 0} P(s_{man}(t)) = P_{M_{max}} \tag{3.9}$$

$$\lim_{l \to 0} P(s_{vid}(t)) = P_{V_{max}} \tag{3.10}$$

де для (3.9) та (3.10) l – відстань між пультом і безпілотним апаратом, $P(s(t))$ – функція потужності сигналу для каналів керування та передачі відео відповідно.

Порівнявши (3.9) і (3.10) можна зробити висновок, що має місце така залежність:

$$\lim_{P(s_{man}(t)) - P_{M_{max}}} P(s_{vid}(t)) = P_{V_{max}} \tag{3.11}$$

Користуючись властивістю (3.16), пропонується використання інформації про якість вхідного сигналу керування для приблизної оцінки відстані від безпілотного пристрою до оператора, а також здійснення регулювання потужності передавача відео на основі даних якості сигналу керування.

Польотні контролери, як правило, передають значення якості сигналу пульта у вигляді числового значення різного діапазону, наприклад [0-100]% або [0-1024]од., що в конкретному випадку означає або відсоток значення потужності відносно максимального рівня, або умовне числове позначення без конкретних одиниць виміру. Така варіативність методу представлення може завдавати проблем і незручностей при впровадженні пропонованої системи у безпілотні апарати різних виробників, тому щоб абстрагуватися від конкретного способу числового представлення рівня потужності сигналу, скористаємося відносним його представленням за таким принципом: зберігаємо максимальне значення якості сигналу $P_{M_{max}}$ і при отриманні від польотного контролера поточного значення якості сигналу $P_{M_{curr}}$, значення функції потужності сигналу обчислюватимемо за формулою:

$$P(s_{man}(t)) = \frac{P_{M_{max}}}{P_{M_{curr}}} * 100. \tag{3.12}$$

Після виконання такої процедури, незалежно від виробника і моделі

контролера маємо фіксовані межі значень:

$$P(s_{man}(t)) \in [0;100] \tag{3.13}$$

Тепер, коли маємо однозначне представлення рівня сигналу і приблизної оцінки дистанції до передавача, на основі цього вже можемо регулювати потужність відеосигналу за єдиним принципом. Математичну функцію регулювання потужності відеопередавача можна представити у такому вигляді:

$$P(s_{vid}(t)) = \begin{cases} 20\%, P(s_{man}(t)) \in [90;100] \\ 40\%, P(s_{man}(t)) \in [70;90] \\ 80\%, P(s_{man}(t)) \in [45;70] \\ 100\%, P(s_{man}(t)) \in [0;45] \end{cases} \tag{3.14}$$

Це є пропонований варіант розподілу потужності на основі теоретичного припущення щодо співвідношення рівнів сигналу між каналом керування і каналом відео. Можна побачити, що потужність сигналу відео є дещо зміщена відносно рівня потужності сигналу передавача, тобто вони не йдуть рівномірно між собою. Таке припущення зумовлено тим, що передавання відео і сигналів керування відбувається на різних частотах.

Зазвичай відео передається на частоті 5.8 ГГц, в той час коли керування пристроєм може здійснюватися, в залежності від виробника, на частоті або 2.4 ГГц або на ще менших частотах, таких як 868 МГц або 915 МГц. Виходячи з цього, керуємося гіпотезою, що дальність передачі (максимальна) і рівень втрат на затухання сигналу на певній відстані в каналі керування є дещо нижчою, ніж в каналі передачі відео. Оскільки відомо, що довші хвилі є більш стійкими і за схожих рівнів потужності забезпечують більшу дальність передачі ніж короткі хвилі.

Для кожного конкретного апарату доцільно здійснювати корегування такого співвідношення. Для цього в ході збірки пристрою і налагодження його роботи можна здійснювати тестові випробування з різними варіантами співвідношення і обрати найбільш оптимальне.

Використання запропонованого методу дозволить нам мінімізувати одразу дві загрози.

Перша з них – це загроза того що при поверненні БПЛА ми прилетимо на свою позицію на максимальній потужності передачі відео, в результаті чого противник зможе, прийнявши потужний сигнал, змалювати розміщення нашої позиції.

Друга загроза, яку дозволить мінімізувати цей метод, полягає в тому що ми зможемо запобігти можливому зворотному варіанту розвитку ситуації: ми навпаки відлетіли занадто далеко на невисокому рівні потужності сигналу відео, в результаті чого ми втратимо відео.

Впровадження пропонованої автоматичної системи дозволить нам автоматизувати процес регуляції відео, унеможливити противнику перехоплення сигналу із апарату, який повертається на свою позицію, та виключити вплив на цю загрозу людського фактору (тобто убезпечить систему від помилкового налаштування потужності оператором).

3.4. Концептуальні основи заходу протидії засобам придушення бездротових систем зв’язку із безпілотними пристроями

Як вже було сказано раніше, розглянуті нами БПА являють собою досить складні інформаційні системи. Якщо брати до уваги їхні властивості, структуру системи їх керування, функціонування а також функції, які вони виконують, за цими критеріями ми можемо віднести такі безпілотні пристрої до розряду засобів які представляють собою кіберфізичну систему. Так, структура КФС повинна включати у собі три головні складові: кіберсистему, мережу зв’язку та контрольований фізичний процес [92].

У безпілотних системах кожна складова є присутньою (Рис. 3.12). В нас є мережа зв'язку: канал передачі даних. В нас є фізичні процеси які можна спостерігати (це може бути як і вимірювання якихось значень давачами безпілотника, так і наприклад, в контексті військового застосування,

спостереження, запис і передавання відео з місцевості під час завдань розвідки). І, відповідно, є присутньою кіберсистема обчислення і обробки даних, яка може представляти собою пульт керування оператора чи масштабну розгалужену бездротову сенсорну мережу.

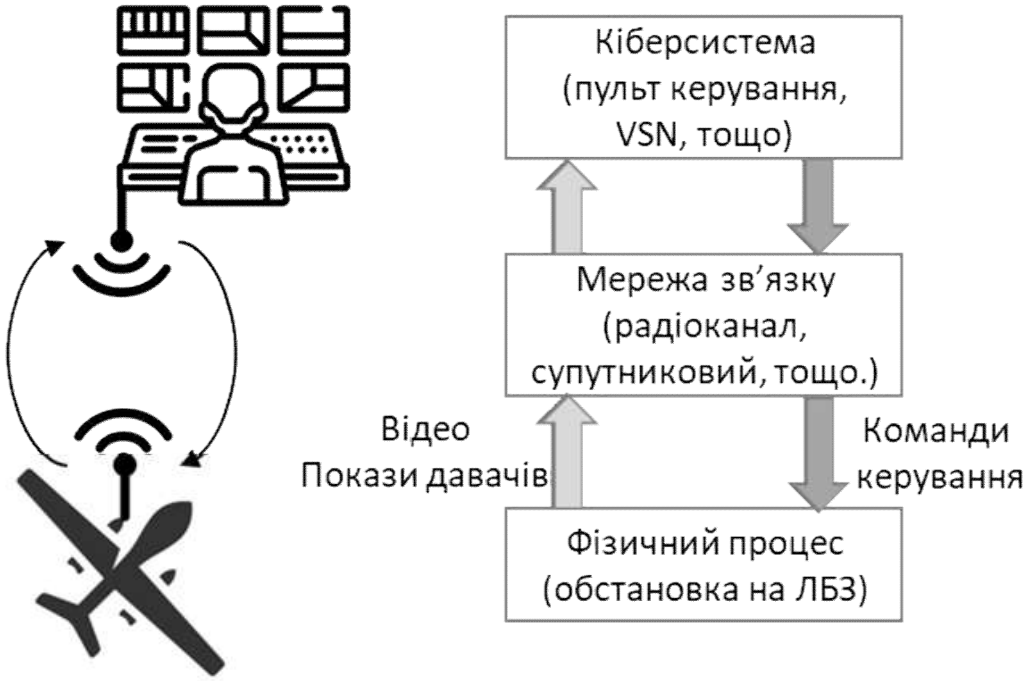


Рисунок 3.12. Складові безпілотної системи як елементи КФС

Здійснений в роботі аналіз поточних досягнень і актуальних наукових розробок в сфері методів захисту інформації та методів оцінки захищеності інформації проводився в контексті використання безпілотних пристроїв. Тому нами розглядалися наукові теорії та розробки щодо захисту і оцінки захищеності інформації для всіх таких систем та елементів які: або мають безпосереднє відношення до систем БПА; або описані в них моделі можуть бути абстрактно чи безпосередньо застосовані до моделей систем керування, функціонування та використання БПА. До них ми віднесли роботи щодо методик діагностування і оцінки захищеності інформаційних систем; підходи з оцінки ефективності систем зв'язку; методики оцінки кібернетичної захищеності систем зв'язку спецпризначення тощо. А відповідно до викладеного вище обґрунтування, розглянули також теорії щодо оцінки захищеності та стійкості кіберфізичних систем.

Під час аналізу методів захисту інформації, методів оцінки захищеності в інформаційних системах, кіберфізичних системах, було виявлено те, що має місце деяка неповнота і недостатність існуючих теорій з оцінки захищеності при їх застосуванні по відношенню до БПА і, відповідно, застосовуваних на її основі методів захисту інформаційних та кіберфізичних систем. Тому існує реальна потреба у їхньому вдосконаленні і впровадженні у них нових наукових положень, для їхнього повноцінного застосування в контексті захисту безпілотних апаратів, зокрема безпілотних авіаційних пристроїв.

Для подальшого обґрунтування результатів проведеного аналізу теорій і пояснення запропонованого шляху і концепцій їхнього розвитку та покращення, ми зробимо прив'язку в першу чергу до методик оцінювання захищеності таких систем. Тому що процес оцінювання є невід'ємною складовою процесу захисту через їх причинно-наслідковий взаємозв'язок: щоб знати "що захистити" і "чи треба захистити" необхідно попередньо провести оцінку; після того як ми впровадили заходи захисту, щоб знати наскільки вони ефективні, знову ж таки, для цього застосовуються методи оцінювання. Тому відправною точкою аналізу і розвитку теорії було саме оцінювання захищеності.

У різних існуючих теоріях розглядається схожий між собою за набором ресурсів і характеристик спектр загроз та процедур захисту і пропонуються різноманітні методи, для надання інтегральної оцінки рівня захищеності. Зокрема, у роботі [90] розрахунок параметрів захищеності ІС проводиться з отриманням кінцевого середньозваженого значення $\sum KZ$:

$$\sum KZ = \frac{(K_1 * KZ_1) + (K_2 * KZ_{2.1}) + (K_3 * KZ_{2.3}) + ... + (K_{10} * KZ_4)}{KZ_1 + KZ_{2.1} + KZ_{2.2} + KZ_{2.3} + KZ_{2.4} + KZ_{3.1} + ... + KZ_4} \quad (3.15)$$

де K_i – вагові коефіцієнти критерію, а KZ_i – значення рівня захищеності по критерію. Серед критеріїв, що враховані у компонентах KZ, є такі:

– виконання вимог з організації кіберзахисту системи зв’язку; оцінка захищеності від загроз витоку візуальної інформації;

– оцінка кіберзахищеності системи зв’язку від загроз викрадення, знищення

апаратних засобів чи матеріальних носіїв інформації через несанкціонований доступ;

– оцінка кіберзахищеності системи зв'язку від заходів розвідки кібернетичної інфраструктури; оцінка кіберзахищеності системи зв'язку від заходів навмисного кібернетичного впливу на функціонування кібернетичної інфраструктури;
– оцінка кіберзахищеності системи зв'язку по виконанню вимог програмного захисту.

Останні роботи по удосконаленню методики оцінки кібернетичної захищеності інформаційних систем під впливом на них деструктивних впливів, зокрема розглянуті у статті [91], присвячені визначенню числових значень кібернетичної захищеності кожного компонента $P_{КЗ(K_jZ_i)}$, кожного засобу $P_{КЗ(Z_i)}$, та системи в цілому $P_{КЗ(S)}$. Для цього беруться до розгляду числові параметри сукупностей компонентів системи $\{K_j\}$ та засобів системи $\{Z_i\}$. Результативна нормована оцінка стану кіберзахищеності системи, запропонована у цій роботі виражається формулою:

$$P_{КЗ(S)} = \sum_{i=1}^{l} (P_{КЗ(Zi)} \times W_{FZi} \times W_{Zi}) \qquad (3.17)$$

де l – кількість засобів у складі системи, W – коефіцієнти функціональності засобів, та вагові коефіцієнти важливості кожного із засобів.

Для оцінки функціональності, стану кіберзахищеності одиничних елементів у цьому підході розглядаються такі критерії як перевірка правильності налаштувань кожного компонента, захищеність від впливу шкідливого ПЗ, можливість безперервної оцінки вразливостей, безпека конфігурацій для апаратного та програмного забезпечення, наявність системи облікових записів, наявність контролю бездротового доступу, захист прикладного ПЗ, наявність тестів на проникнення, тощо.

Праця [92], у котрій розглянуто питання оцінки захищеності власне

кіберфізичних систем, містить широкий огляд існуючих підходів до практики оцінки стану КФС. Із її змісту, та проведеного автором аналізу, можна виділити наступні типові вразливості, що беруться до розгляду при оцінці стану захищеності КФС:

- апаратні вразливості – включають в себе недоліки власне апаратного забезпечення. Як правило, приймається гіпотеза, що виправити їх дуже складно і оптимальним та достатнім заходом протидії вважається обмеження фізичного доступу;
- вразливості програмного забезпечення – розглядаються на рівнях операційної системи, прикладного ПЗ, забезпеченні протоколів зв'язку, а також на рівні системи обробки помилок у роботі КФС. До них відносять переповнення буфера, недостатність чи відсутність систем шифрування/кодування, помилки у коді, тощо;
- технічні вразливості – розглядаються в контексті ненавмисних помилок користувача чи оператора;
- вразливості управління – вразливості високого рівня, які полягають у використовуваних політиках безпеки, тощо;
- вразливості мережі – вразливості конфігурації та технологій передачі даних. До їх критеріїв відносять захищеність до прослуховування даних, підміни або знищення, відмови в доступі, розвідувальні атаки, тощо.

Роботи щодо захисту систем зв'язку спеціального призначення, зокрема [90], проводять оцінку ефективності і захищеності системи зв'язку за принципом врахування не повного набору показників системи, а лише найбільш вагомих. У даній роботі таким показником вважається доступність системи зв'язку, а для оцінки ефективності зв'язку використовується параметр ймовірності доступу легітимного користувача з першої спроби:

$$P^{Д} = a(D, P_i^{Д}) \tag{3.16}$$

де $D = \{d_1, d_2, d_3, ..., d_L\}$ – вектор, який описує умовну доступність до

каналу зв'язку у оперативному просторі в точці d_L, яка містить певний набір елементів системи зв'язку; $P_i^{Д}$ – об'єктова стійкість таких елементів зв'язку.

У цій роботі частково береться до уваги питання просторового розділення засобів зв'язку і прогнозована оцінка покриття оперативного простору доступом до ресурсу системи зв'язку.

Як бачимо із приведених прикладів, в класичних теоріях захисту інформаційних систем розглядаються схожі набори загроз, можливих атак і методи захисту інформаційних та кіберфізичних систем. Які покривають певні, загально прийняті критерії і дозволяють комплексно оцінювати і підвищувати захищеність тих чи інших систем.

Але, як було сказано раніше, нами було виявлено певну неповноту в контексті їхнього застосування до сучасних безпілотних пристроїв. Вона полягає у тому, що більшість розглянутих критеріїв та способів захисту стосуються таких характеристик стану самої системи, які ми можемо розглядати як статичні.

Динамічні процеси, які враховуються у таких оцінках і заходах захисту, враховують факт застосування активних чи пасивних заходів зі сторони зловмисника. При цьому ми відштовхуємося від принципу, що система під час роботи знаходиться у своєму звичному робочому стані, а зловмисник може здійснити атаку з метою реалізації певної загрози системі.

У таких підходах не міститься вичерпного обґрунтування впливу на рівень захищеності системи того факту, що система (у нашому випадку безпілотний апарат) може мати можливість самостійно змінювати свою зовнішню обстановку шляхом переміщення у просторі. Причому такі зміни можуть бути дуже динамічними.

Особливо це важливо для випадку коли ми беремо до розгляду аспект захисту доступності безпілотних літаючих апаратів, оскільки в силу своєї особливості (переміщення в повітрі) вони можуть розвивати відносно високу швидкість, здійснювати швидкі маневри і переміщатися на великі відстані за відносно невеликий проміжок часу, що призводить до швидкої і в загальному

випадку непередбачуваної зміни обстановки.

Беззаперечно, застосування класичних підходів та теорій дає нам у результаті покращення характеристик безпілотних пристроїв, підвищення рівня їхньої стійкості, це дає нам можливість рухатися на більші відстані, наближатися до зон просторового зашумлення ближче, але для таких результатів застосування цих заходів завжди є певна верхня межа, через що завжди існує зона гарантованого ураження системи зв'язку безпілотного пристрою. Для наочного обґрунтування цих аспектів розглянемо схематичний рисунок залежності електромагнітної обстановки від координати місця розташування безпілотника, за умови використання БПЛА для завдань розвідки в межах ЛБЗ (Рис. 3.13)

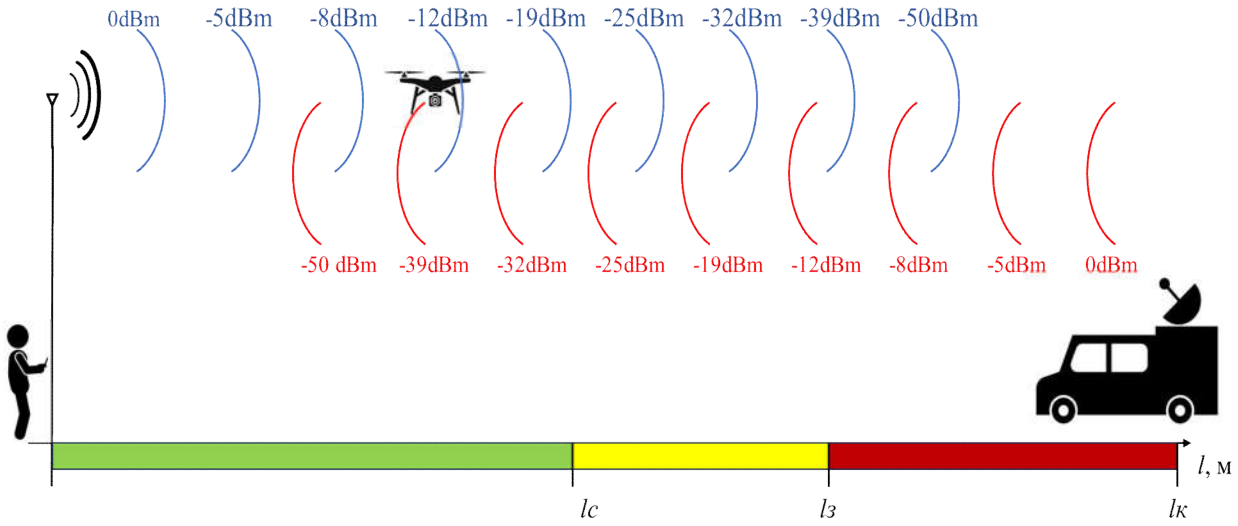


Рисунок 3.13. Схема залежності співвідношення сигналу і завад від місця роботи при використанні БПЛА

У лівій частині рисунку знаходиться умовний оператор БПЛА, у правій частині рисунка – умовний противник, який являє собою транспортний засіб, обладнаний мобільною системою РЕБ. По осі x узагальнено позначена дистанція роботи пристрою вздовж траєкторії польоту і, відповідно, збільшення відстані позначає переміщення БПЛА до позицій супротивника.

Синіми і червоними хвилями відзначено напрямок поширення радіохвиль керування і засобу РЕБ відповідно, та прогнозовані рівні сигналу в певних

точках простору. Умовні значення $l_C, l_З, l_K$ – означають межу зони стабільної роботи, межу зони впливу завад за збереження можливості керування апаратом та межу зони критичного впливу завад із втратою керування апаратом відповідно.

При польоті у зоні розвідки для відношення сигнал/шум приймача нашого безпілотного апарату, як видно із рис.3.13, діє така закономірність:

$$\lim_{l \to l_k} \frac{s_{man}(t)}{s_{noise}(t)} = 0 \tag{3.17}$$

З цього випливає, що відстані l_C, на якій закінчується стабільний прийом сигналу і розпочинається помірний вплив завад, та відстань $l_З$ на якій вплив завад переходить критичну межу і призводить до втрати зв'язку напряму пов'язані із можливостями приймача сигналу по детектуванню сигналу (порогове значення SNR для розпізнавання сигналу) та конфігурації енергетичного розподілу сигналу передавача. Тобто використання класичних засобів покращення зв'язку та підвищення його завадозахищеності (такі як завадостійке кодування, використання ретрансляторів, антен з високим коефіцієнтом підсилення, тощо) впливає на захищеність безпілотного пристрою, але при цьому змінюються лише статичні параметри конфігурації зон можливостей пристрою. Якщо заходи захисту представити у вигляді певної множини $S = \{S_1, ..., S_n, ..., S_N\}$, то:

$$\lim_{N_S \to N_{max}} l_C = l_{C_{max}}, \tag{3.18}$$

$$\lim_{N_S \to N_{max}} l_З = l_K \tag{3.19}$$

Тобто при збільшенні кількості і якості застосованих заходів захисту дистанція впевненого прийому збільшується до певного максимального значення, а дистанція зони впливу завад за збереження задовільного прийому прямує до значення l_K, що відповідає повній відстані від оператора до місця

розташування засобу РЕБ, при цьому розмір зони повного подавлення прямує в теорії до 0. На практиці ж, звичайно, не вдасться реалізувати систему яка забезпечить розподіл зон із абсолютним виключенням зони повного ураження, такі зони залишатимуться.

Відповідно необхідно додатково впровадити у існуючі теорії оцінки захищеності інформаційних систем та систем зв'язку, які можуть бути застосовані для оцінки стійкості безпілотних пристроїв, можливість врахування впливу переміщення цих пристроїв у просторі та врахування поточного місця розташування.

Для врахування впливу такого факту переміщення безпілотного пристрою, внаслідок його власної поїздки, польоту, чи плавання пропонується ввести деяку функцію $R(x,y,z)$ (з англ. *Resilience* – стійкість), залежності рівня стійкості систем БПА від його просторових координат (абсолютних, чи відносних). Ця функція відображатиме залежність рівня стійкості пристрою в тій чи іншій точці до обставин навколишнього середовища в межах значень від "0" до "1", тобто:

$$\exists R(x,y,z) \mid \forall (x,y,z) R(x,y,z) \in [0;1] \tag{3.20}$$

Таку функцію можна як враховувати самостійно, так і застосовувати її для адаптації тих чи інших теоретичних методів оцінки захищеності для оцінювання систем, які можуть здійснювати самостійні переміщення, шляхом мультиплікації.

Тобто, якщо розглядати будь-яку із приведених раніше для прикладу теоретичних методик, при результуючій статичній оцінці стійкості системи Z_i визначення фінального рівня стійкості переміщуваної системи (позначимо його R_{fin}) підлягає загальному принципу:

$$\forall \{Z\} R_{fin} = Z_i \times R(x,y,z) \tag{3.21}$$

Для відображення сутності цієї теорії і обґрунтування мультиплікативного

механізму її впливу розглянемо топографічну ситуативну схему використання безпілотного пристрою (Рис.3.14).

У даній схемі, позначки мають таке значення:

 - особовий склад противника

 - певні засоби противника (наприклад, міномет)

 - засоби РЕБ противника

 - наш керований безпілотний літальний апарат

 - ближня зона дії РЕБ (повний вивід з ладу каналу зв'язку БПЛА)

 - дальня зона дії РЕБ (перебої і завади у каналі зв'язку БПЛА)

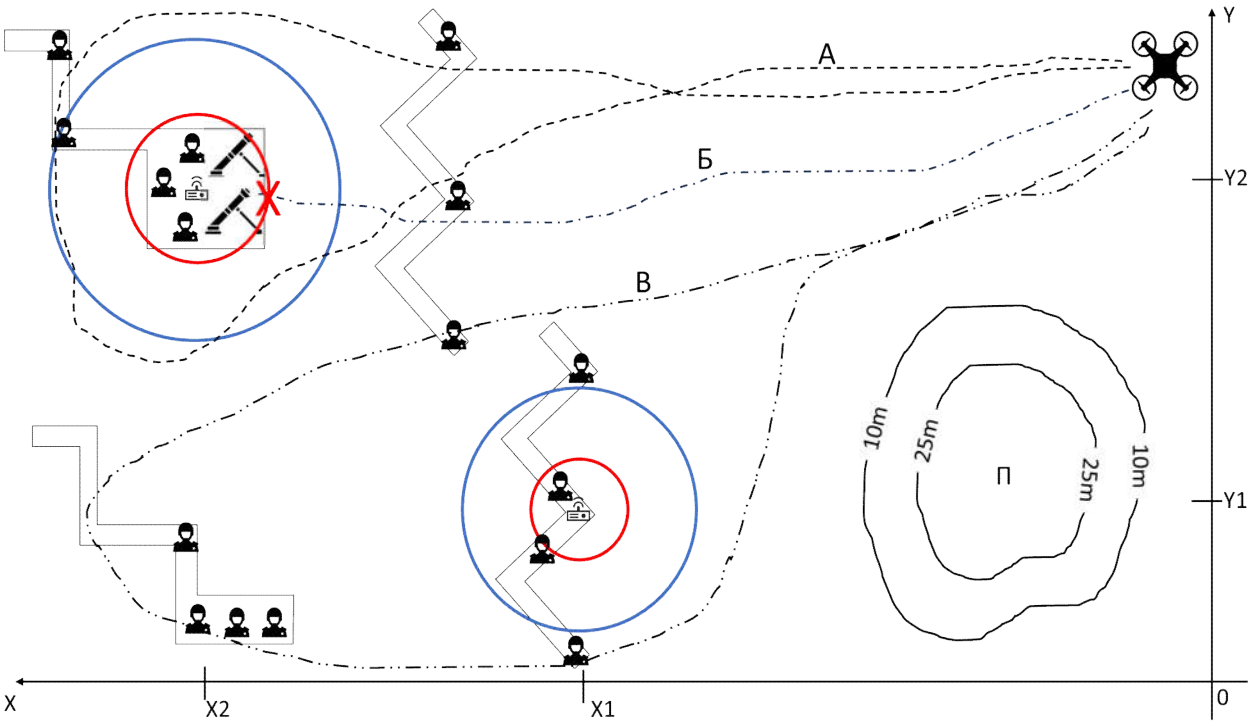


Рисунок 3.14. Топографічна схема зображення можливих варіантів поведінки БПЛА у певній оперативній обстановці

На цій схемі ми бачимо модель згідно якої може працювати безпілотний апарат в умовах його використання як засобу розвідки у зоні бойових дій. Схематично зображені розташування траншей противника, його засоби

вогневого ураження (у схемі для прикладу зображені два міномети), розташування особового складу, а також зображені умовні місцерозташування засобів радіоелектронної боротьби, які відповідають точкам із координатами *(X1,Y1),(X2,Y2)*, призначення яких якраз боротьба із нашим безпілотником, також колами зображено орієнтовну конфігурацію зон впливу ворожого РЕБ: зона у якій погіршується якість зв'язку але бортових систем забезпечення стабільності і захисту цілісності каналу зв'язку все ще достатньо для задовільної роботи відповідає синьому колу (відповідає зоні в межах дистанцій $l_C - l_3$ рис.3.13), а червоному колу відповідає зона у якій потужність випромінювання сигналу РЕБ значно перевищує можливості протидії нашого апарату і зв'язок із ним повністю втрачається (відповідає зоні в межах дистанцій $l_3 - l_K$ рис.3.13).

Розглянемо три окремі випадки, можливі під час роботи даного апарату, і для кожного випадку приймаємо, що використовується один і той же БПЛА із однаковими параметрами:

– при польоті оператором дрону по траєкторії, позначеній буквою "А", оператор матиме можливість безперешкодно розвідати передню лінію траншей і їхнє обладнання, а на підльоті до позицій мінометного підрозділу він вже потрапляє у зону дії РЕБ і може спостерігати погіршення роботи пристрою, але все ще керувати ним і мати можливість завершити роботу поверненням на базу;
– при польоті оператором дрону по траєкторії, позначеній буквою "В", оператор розвідає передню і другу лінію оборонних траншей, при цьому він оминає всі засоби РЕБ і не відчує жодних перешкод чи збоїв у роботі апарату, в результаті чого успішно виконає завдання і повернеться на базу;
– при польоті оператором дрону по траєкторії, позначеній буквою "Б", оператор на прямій ділянці маршруту, при підльоті до переднього краю розташування мінометного розрахунку потрапляє у зону дію РЕБ-у і, якщо він вчасно не відчує проблем із управлінням, чи не встигне вжити необхідних заходів, він залітає у ближню зону ураження засобу

радіоелектронної боротьби і повністю втрачає зв'язок із апаратом і можливість керувати ним.

Із приведеного для прикладу теоретичного експерименту бачимо, що хоч і властивості нашої системи не змінювалися, заходи захисту у всіх трьох випадках згідно початкової умови також були ідентичні, але результат роботи вздовж трьох розглянутих траєкторій отримуємо різний – від стабільної роботи апарату на всьому проміжку роботи, аж до повної втрати апарату. При цьому розуміємо, що оцінки захищеності згідно існуючих критеріїв залишаються без змін.

Для запропонованого підходу ж, із рис.3.14 матимемо, що в околі точок $(x_1, y_1); (x_2, y_2)$ значення функції $R_{fin} = Z_i \times R(x_1, y_1, z_1) \approx 0$, тоді відповідно виразу (3.21) матимемо, що

$$R_{fin} = Z_i \times R(x_1, y_1, z_1) = Z \times 0 = 0 \qquad (3.22)$$

при $Z_i = const$, що відповідає фактичній поведінці системи. Таким чином бачимо доцільність застосування запропонованої теорії і врахування її впливу саме за мультиплікативним принципом.

Прогнозування поведінки цієї функції є дуже складною задачею, особливо в умовах застосування таких систем для виконання військових завдань. Це зумовлено кількома чинниками:

– при роботі на своїй оперативній ділянці оператор пристрою не має карти, чи схеми, аналогічної рис.3.14., тобто йому наперед не відомі можливі зони радіоелектронного впливу на системи БПА;
– в деяких умовах (наприклад аеророзвідка в умовах бойових дій) також маємо тенденцію того, що засоби придушення наших пристроїв зазвичай є надійно замаскованими і навіть при прямому курсі на них, оператор може до останнього не знати/не бачити небезпеки;
– також часто буває таке, що увімкнення засобу РЕБ, чи зниження рівня сигналу від природних перешкод відбувається стрімко та миттєво і оператор, навіть по факту втрати обладнання, не завжди може конкретно

позначити на карті небезпечну зону.

Наближені припущення, щодо поведінки $R(x,y,z)$ можна здійснити у випадку візуального виявлення засобів протидії апарату, наявності попередньо зібраної інформації, а також враховуючи деякі особливості навколишнього середовища. Так, у рис.3.14. бачимо топографічне зображення пагорба "П", отже розуміємо, що якщо ми будемо рухатися на висоті меншій, ніж висота пагорба, то зона за пагорбом (відносно позиції пульта керування) потенційно буде зоною локального мінімуму значення функції $R(x,y,z)$.

Аналітичний опис за допомогою рівняння чи математичного виразу цієї функції залишається відкритою науково прикладною задачею і закладає основу для подальших досліджень.

У цій науковій роботі для опису поведінки цієї функції будемо використовувати загальний теоретичний принцип опису не передбачуваних систем – принцип "чорної скриньки" [93].

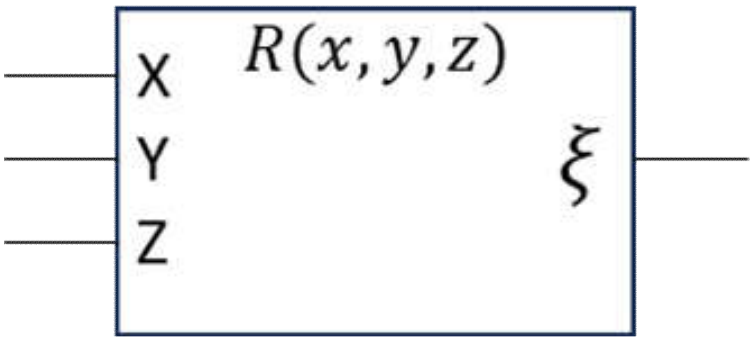


Рисунок 3.15. Функція просторової стійкості системи, як "чорна скринька"

Відповідно приймаємо твердження, що у даний час дізнатися конкретне числове значення цієї функції можна лише емпіричним шляхом, маючи можливість впливу на вхідні параметри системи, змінювати їх і слідкувати за вихідним значенням, яке являє собою деяку випадкову величину ξ.

3.5. Пропонований алгоритм автономної роботи апарату при втраті зв'язку задля його відновлення

Оскільки, як вже було обґрунтовано, робота сучасних безпілотних засобів є

майже повністю контрольована оператором, а при втраті зв’язку з апаратом, в умовах військового застосування повернення апарату неможливе, розуміємо, що стан каналу зв’язку пульта із апаратом має критичне значення. Вихід з ладу каналу керування означатиме безумовну втрату апарату, тому якість передавання сигналу можемо фактично прийняти тим самим показником загальної стійкості системи із виразу (3.21).

Тому, базуючись на основі обґрунтованої нами теорії, пропонується впровадити у безпілотну систему новий засіб захисту, назвемо його "аварійне відновлення". Умовно його можна розділити на дві частини: пасивні заходи, та активні заходи (які перемикаються за певними показниками, відповідно до концептуального алгоритму, описаного нами у рис.3.3.).

Пасивні заходи цього методу захисту стійкості каналу зв’язку бездротової системи керування полягають у використанні моніторингу та запису значення якості зв’язку у залежності від переміщення безпілотного пристрою у просторі, та збереження даних шляху такого переміщення у пам’яті із прив’язкою до значень часу, а також, збереження власне самих значень якості зв’язку, що було представлено у опублікованій праці [94].

Маючи достатню в часі просторову вибірку такої інформації можна реалізовувати активну складову даного методу захисту, яка полягає у поверненні апарату при зникненні зв’язку із пультом за зворотнім маршрутом, який, завдяки збереженій нами інформації, аналогічний тому, за яким наш апарат залетів у зону зникнення зв’язку. Це дає змогу повторювати траєкторію польоту (або поїздки чи плавання) і, відповідно, повертатися до області покриття найкоротшим маршрутом.

Пропонований метод не призначений для постійного підвищення стійкості зв’язку чи покращення його якості, його завдання забезпечити підвищення загального рівня доступності безпілотної системи шляхом надання можливості виходу із критичної ситуації, коли втрачено зв’язок із апаратом, що вже відлетів на значну відстань, або знаходиться на підконтрольній ворогу території.

Для реалізації такого методу, для кожної із можливих осей переміщення,

необхідно записати координати в певний момент часу як функцію від часу $x(t), y(t), z(t)$. Другий параметр моніторингу – якість зв'язку. Необхідно також фіксувати якість зв'язку у тій чи іншій координаті. Це дасть змогу фіксувати, коли матиме місце факт зниження якості зв'язку для того, щоб приймати рішення: "ми потрапили під вплив засобу придушення і треба переключатися із моніторингу на алгоритм повернення назад". Для вирішення завдання запису даних моніторингу під час польоту бортова система БПЛА повинна з певною визначеною частотою відслідковувати переміщення апарату і записувати маршрут у пам'ять як дискретну вибірку.

Для реалізації усіх цих завдань і самого методу "аварійного відновлення" загалом, будемо використовувати той же принцип, що і у випадку із забезпеченням конфіденційності зв'язку – використання вбудованої системи на основі МК. При чому за достатньої кількості його портів і достатнього рівня продуктивності немає потреби використовувати кілька контролерів для різних завдань, цілком може бути достатнього одного потужнішого.

Для запису параметру якості зв'язку є два можливих варіанти: можна записувати якість зв'язку як функцію від координат $L(x, y, z)$, або записувати якість зв'язку як функцію від часу $L(t)$ із наступною синхронізацією в часі значень функцій запису пройдених координат і функції запису якості зв'язку.

Враховуючи особливості функціонування запам'ятовуючих пристроїв у цифрових системах, а також принцип роботи арифметично-логічного пристрою на яких базуються мікропроцесори (чи наприклад мікроконтролер із вбудованою пам'яттю) більш доцільним і оптимальним у реалізації являється другий варіант запису даних положення і якості зв'язку – як двох функцій часу із синхронізацією по часу. Програмно і апаратно таку синхронізацію дуже легко організувати – достатньо запустити алгоритм моніторингу і запису одночасно і зберігати їх у одному масиві даних. Для прикладу, можна організувати сховище польотних даних в умовний масив значень "flight_data[]", який матиме такі параметри:

flight_data[time] flight_data[x] flight_data[y] flight_data[z] flight_data[link_q];

Дані, збережені у такому масиві можуть мати наступний вигляд:

Таблиця 3.5

Приклад організації запису даних для методу повернення

flight_data[time]	flight_data[x]	flight_data[y]	flight_data[z]	flight_data[link_q]
1	1	2	1	95%
2	5	5	3	95%
3	8	10	9	85%
4	17	26	19	90%
…	…	…	…	…
T_n	X_n	Y_n	Z_n	Q_n

Отже ми отримаємо масив даних за певний останній час польоту і зможемо аналізувати його або в режимі реального часу, або із невеликою затримкою задля виявлення таких позаштатних ситуацій як, наприклад, значне зниження якості зв'язку чи раптове повне зникнення зв'язку. Якщо така ситуація виникне, маючи такий масив даних, ми зможемо передавати дані польоту і координат у зворотному порядку на контролер управління безпілотним апаратом і ініціювати його повернення у зворотному порядку (Рис 3.16.).

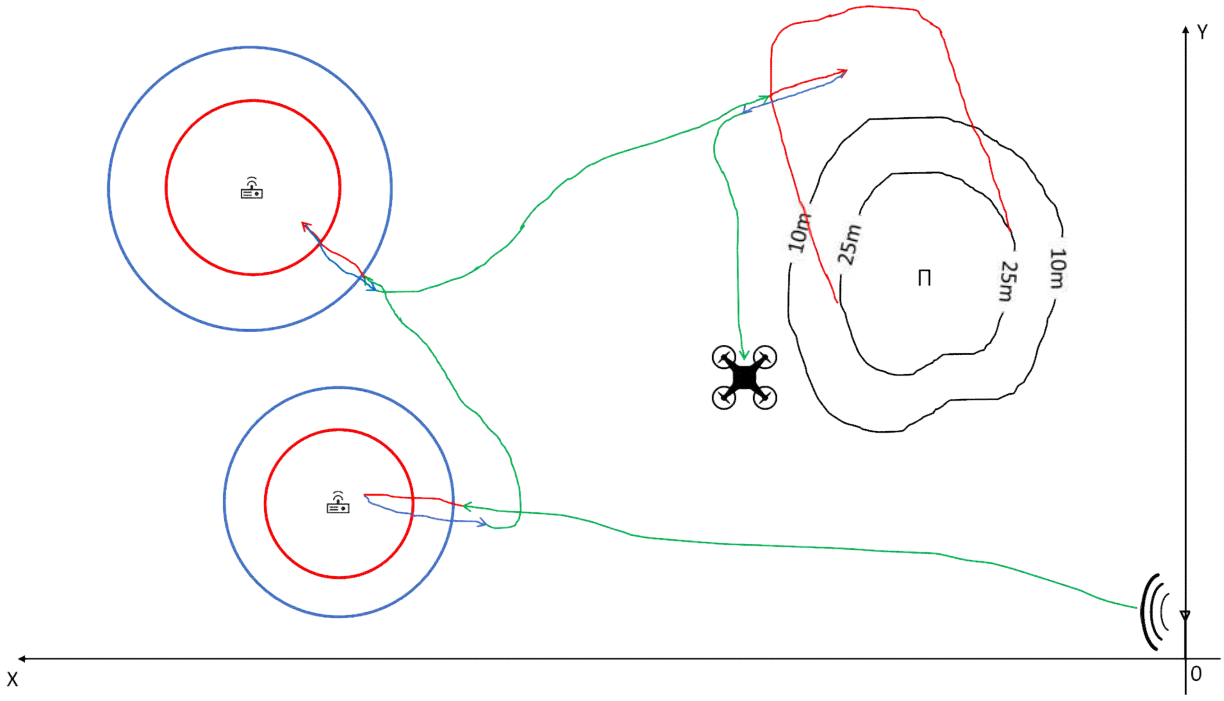


Рисунок 3.16. Схема переміщення БПЛА при наявності запропонованого методу захисту

- траєкторія стабільного керованого польоту;

- траєкторія польоту під впливом сильних завад і виходу з ладу системи керування

- траєкторія автономного повернення за збереженими даними.

Такий підхід має ряд переваг – у звичайному режимі алгоритм не втручається у роботу безпілотного апарату, а тільки здійснює моніторинг його параметрів і записує необхідні із них у пам’ять, що дозволяє зберегти продуктивність системи керування БПЛА і не викликати затримок і збоїв у його роботі.

Друга перевага – якщо ми записуватимемо параметри польоту апарату за його інерційними показниками, без прив’язки до зовнішніх параметрів та сигналів, які можуть бути скомпрометовані, наш метод буде стійким до будь-яких засобів радіо-електронної боротьби, в тому числі GPS-спуфінгу, оскільки опиратиметься лише на фізичні показники польоту.

Третя перевага – повернення по зворотній траєкторії, аналогічній траєкторії підльоту дає можливість дістатися точки задовільного зв’язку у найкоротший шлях, порівняно із стандартною процедурою "повернення додому" яка інколи присутня у базовому програмному забезпеченні польотних контролерів і полягає у поверненні за допомогою GPS по прямій траєкторії до точки запуску, ігноруючи всі маневри і рухи до цього.

Такі переваги і можливості пропонованого методу доводять його високу перспективність впровадження і доцільність подальшої роботи і практичних розробок щодо розвитку і реалізації цієї ідеї у фізичний пристрій для покращення його характеристик.

Висновки до 3 розділу

В даному розділі були запропоновані методи покращення існуючих засобів

захисту а також запропоновано та науково обґрунтовано нову ідею для покращення стійкості та захищеності каналу зв'язку перед засобами РЕБ.

Запропоновані методики мають вагоме значення у питаннях захисту інформації в бездротових системах зв'язку та керування безпілотних апаратів. Перш за все, це зумовлено тим, що для реалізації кожного із запропонованих методів було проведено попередній аналіз використовуваних в тому чи іншому безпілотному апараті схемотехнічних рішень. Після чого, усі розроблені методи захисту опиралися на результати цього аналізу і механізм їх роботи вибудовувався таким чином, щоб максимально забезпечити практичну реалізацію кожного методу захисту інформації за рахунок власних можливостей відповідних компонентів безпілотного апарату. Це дозволило впровадити максимально ефективні засоби захисту як для конфіденційності інформації при її передачі (відеосигнал від БПЛА), так і для доступності апарату (працездатність каналів зв'язку системи керування апаратом).

Запропонований підхід до реалізації заходів захисту, зокрема: використання зовнішнього мікроконтролера, робота даного мікроконтролера в режимі "менторства" і втручання його лише у випадку позаштатної ситуації, а також робота усіх запропонованих методів захисту через керування налаштуваннями існуючих елементів БПЛА – дозволили повною мірою забезпечити реалізацію обраного для роботи принципу: "оптимальний рівень захисту за оптимального рівня затрат".

Описана у розділі практична реалізація методів захисту не вимагає перепрограмування компонентів БПЛА, чи їхньої заміни. Також, таким способом можна реалізувати дані методи захисту навіть у вже зібраних і функціонуючих БПЛА шляхом невеликої модернізації.

У запропонованих варіантах практичної реалізації розроблених методів також є враховані обмеження продуктивності та обсягу пам’яті як самих безпілотних систем так і класичних мікроконтролерних засобів, що використовуються для побудови вбудованих систем.

Запропонований метод аварійного відновлення зв'язку забезпечить

можливість покращення захищеності системи керування в тому числі й інших безпілотних пристроїв, які не є обладнані запропонованою системою захисту. Цього можна досягнути завдяки можливості зондування оперативного простору захищеним БПЛА. При спрацюваннях механізму повернення, оператор зможе скласти собі топографічну схему розташування небезпечних зон, після чого дрони, які не обладнані такою системою захисту, вже відправлятимуться по заздалегідь випробуваному безпечному маршруті.

РОЗДІЛ 4. ЕКСПЕРИМЕНТАЛЬНІ ДОСЛІДЖЕНЯ ЗАПРОПОНОВАНИХ МЕТОДІВ ПОКРАЩЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ У БЕЗДРОТОВИХ СИСТЕМАХ

Розділ 4 дисертації присвячений практичному втіленню теоретичних положень, що були сформульовані та обґрунтовані в попередніх розділах. Цей розділ представляє собою важливий етап дослідження, на якому теоретичні моделі та концепції перетворені в конкретні практичні реалізації. Детально розглядаються всі етапи реалізації, включаючи вибір та конфігурацію обладнання, розроблене програмне забезпечення, а також процеси тестування та відлагодження. Особлива увага приділяється аналізу характеристик роботи реалізованих систем та їх ефективності. Цей розділ дозволяє перевірити та підтвердити висновки, отримані на основі теоретичних досліджень, та оцінити їх практичну аплікацію.

4.1. Комплексний метод забезпечення конфіденційності системи бездротового відеозв’язку безпілотного апарату

Згідно пропонованого у розділі 3 підходу до реалізації захисту конфіденційності відео у БПЛА, було реалізовано обидва методи забезпечення конфіденційності за допомогою МК: менеджмент потужності, та частотне переналаштування. Для випробування і оцінки роботи цих систем мною було зібрано стаціонарний лабораторний макет на базі мікроконтролера виробника "Cypress Semiconductor". Далі по пунктах буде розглянуто і описано основні аспекти проведеного дослідження, включно із отриманими результатами та їх оцінкою.

4.1.1. Загальна реалізація системи керування відео передавачем

Як було сказано раніше, відеопередавачі, що використовуються у FPV дронах, зазвичай у своєму функціоналі не мають прямої можливості реалізації будь-яких методів захисту із тих, які ми розглянули. Проте, завдяки

запропонованому впровадженню мікроконтролера у схему БПЛА, реалізація методів захисту стає можливою через відповідне програмування МК і керування з його допомогою передавачем VTX.

Така можливість з’явилася відносно нещодавно – останніми роками у нових моделях відео передавачів з'явилися нові виводи у контролерах ("IRC", "SA" або "S-Audio") і для деяких із цих передавачів в інструкції згадувалося що VTX підтримує IRC Tramp або Smart Audio. Але належного опису цього функціоналу не було, тільки вказувалося, що ці протоколи дозволяють керувати відео передавачем на рівні коду, користуючись цим самим виводом SA чи IRC. За останній рік ця ситуація покращилася – компанія TeamBlackSheep опублікувала інструкцію по протоколу SmartAudio і певні дані по ньому з'явилися [95]. А от про протокол IRC досі немає жодної інформації крім того, що він просто є.

У використовуваній нами для лабораторного зразка мікросхемі передачі відео використовується протокол SmartAudio, тому надалі користуватися ми будемо протоколом SA і зосередимо увагу на ньому.

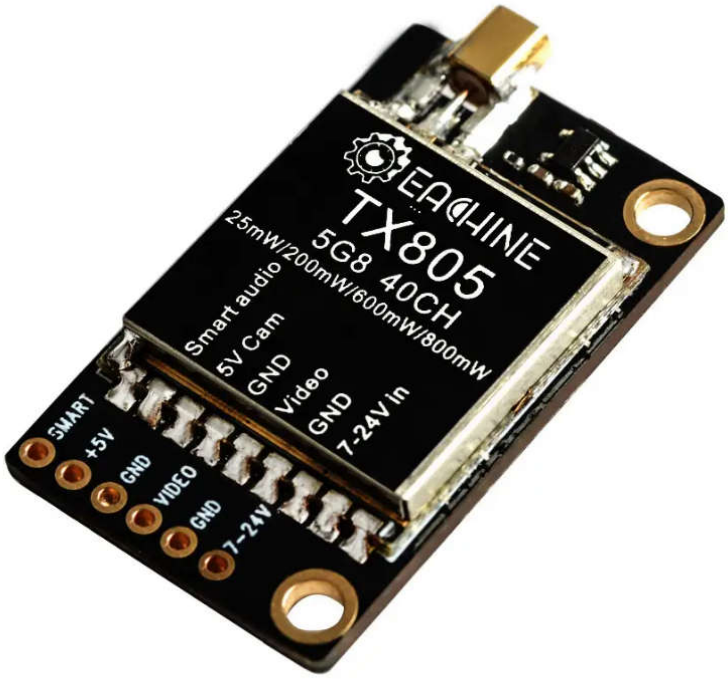


Рисунок 4.1. Передавач Eachine TX805 (бачимо зліва вивід "SMART")

Працює даний протокол через послідовний порт UART, але не в класичному його варіанті (два виводи RX, TX) а в однопроводовому, який працює у напівдуплексному режимі (один вивід, який змінює режим RX/TX у часі). Реалізовано це таким чином: VTX завжди знаходиться у режимі "Slave" і "слухає" вхід SA, на наявність команди ззовні. Коли на вхідний порт приходить команда із визначеного протоколом SA переліку, контролер її опрацьовує, переходить у режим "Master" і дає відповідь із результатом виконання команди, після чого знову переходить у режим "Slave". Із цього виходить дві особливості, які треба врахувати у алгоритмі роботи МК:

– після відправки команди, необхідно із режиму передавання переключити вивід порта на режим прийому і "слухати" відповідь;

– маючи відповідь, вже немає необхідності перевіряти виконання команди – нове значення параметру, зміна якого була прописана у запиті, міститиметься у отриманій відповіді (якщо воно відповідає новому – зміна відбулася, відповідно якщо воно відповідає старому значенню – під час виконання запиту мала місце якась помилка).

Другим аспектом функціонування є те, що параметри апаратного інтерфейсу зв’язку відео передавача є строго визначені протоколом SA:

– Швидкість передачі (UART baud rate): 4800 бод;

– Конфігурація кадру: 1 стартовий біт, 2 стоп-біти;

– Рівень логічної "1": 0.9-3.3 В;

– Рівень логічного "0": 0-0.5 В;

– Початок передачі: здійснюється із рівня логічного "0".

Щодо швидкості передачі необхідно зазначити, що і самі виробники конкретних пристроїв передавання і опис протоколу SA вказує на те, що контролер зв’язку через UART використовує внутрішній осцилятор мікросхеми, який має деякий температурний дрейф частоти, тому під час роботи при нагріванні і вистиганні відеопередавача можлива зміна швидкості роботи UART у межах -/+5%. Це необхідно обов’язково врахувати у програмній реалізації протоколу UART на стороні МК.

Команди від мікроконтролера до VTX мають наступну структуру:

<Start_code><Command><Frame_Len><Payload><CRC>, де:

Start_code – байт синхронізації і байт заголовку (сталі: 0xAA 0x55)

Command – один байт команди (див. перелік нижче)

Frame_Len – один байт, вказує кількість байт у Payload

Payload – байти параметрів команди (для кожної індивідуально)

CRC – контрольна сума команди (визначається циклічним кодом із твірним поліномом $x^7+ x^6+ x^4+ x^2+ x^0$ – 0xD5).

У застосованій нами мікросхемі передавача використовується протокол SmartAudio V2. Цей протокол містить такий набір команд:

- Get Settings 0x01
- Set Power 0x02
- Set Channel 0x03
- Set Frequency 0x04
- Set operation mode 0x05

При відправці запиту від МК до VTX також є одна особливість: у запиті код команди (у списку вище) повинен бути логічно зсунутий на 1 біт вліво із встановленням "1" у наймолодший біт. Наприклад, для Set Power (0x02), запит матиме вигляд: 0xAA 0x55 0x05 0x01 0x02 0x8A

При відповіді VTX зсуває код команди вправо на 1 біт, а також для всіх команд, крім Get Settings, додає зарезервоване значення 0x01, таким чином, відповідь матиме вигляд:

0xAA 0x55 0x02 0x03 0x02 0x01 0xA0

Ці основні особливості визначають порядок роботи МК при звертанні і отриманні даних від VTX, решта функціоналу МК відповідатиме лише алгоритмам впроваджуваних методів захисту і особливостям їх реалізації на конкретній платформі.

Для створення макету, на якому проводилися експерименти, було використано мікроконтролер CY8CKIT-049-42XX, який підключався до відеомодуля через порти вводу-виводу і до ноутбука через порт USB.

Вигляд лабораторного макету для експериментів із VTX приведено на рис. 4.2. Схема електричних з’єднань зображена на рис. 4.3.

Тут варто зазначити, що з’єднання здійснене напряму проводом між виводом порту МК "P1.4" і виводом "SMART", хоча і протокол SA регламентує рівень "1" у 3.3В, але для даної мікросхеми виробник зазначив "5V tolerance", що означає, що вивід підтримує 5-вольтову логіку.

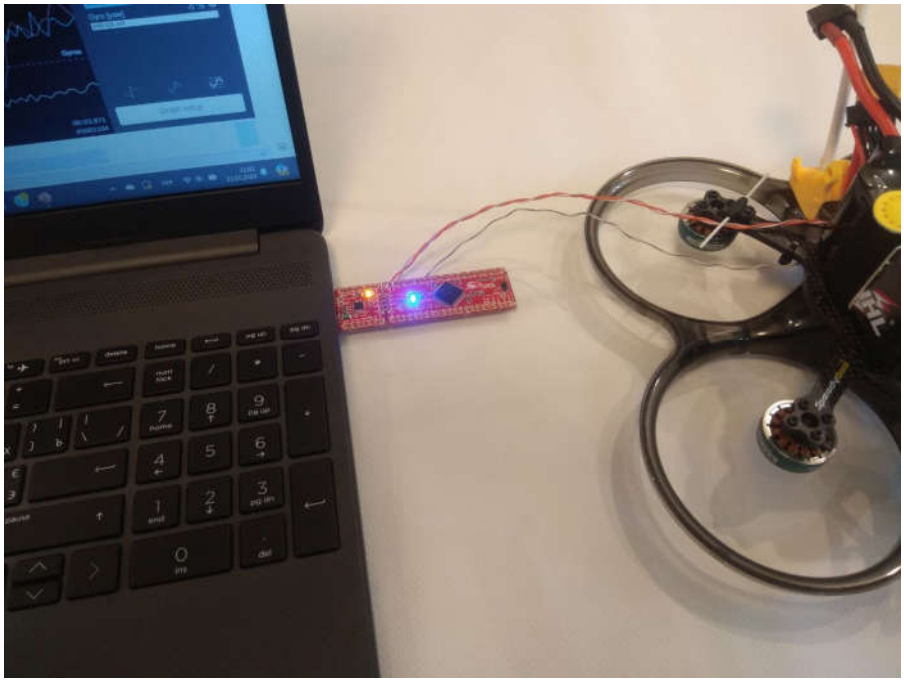


Рисунок 4.2. Лабораторний макет для проведення експерименту із VTX

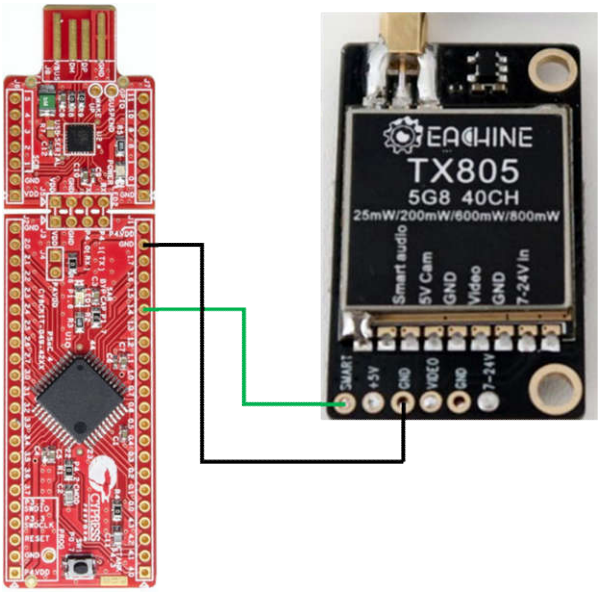


Рисунок 4.3. Схема з’єднання між МК та VTX

Між рисунками є деяке не співпадіння – на фото дротів є три, а з'єднань на схемі є два. Причина – при цьому експерименті червоний дріт "VDD +5V" МК був не під'єднаний до "5V" VTX, тому що схема МК отримувала живлення від ПК через порт USB, а схема відеопередавача живилася від батареї і з'єднання їхнього живлення між собою призвело б до прямого підключення виводу порту USB ПК із потужною батареєю. З'єднані були лише порти UART та контакти GND, для електричного узгодження рівнів.

Для експериментального дослідження властивостей використовуваного протоколу в контексті реалізації запропонованих методів та заходів захисту, були написані відповідні коди програмної реалізації цих методів. Після чого, при роботі цих алгоритмів із різними параметрами було проведено "захоплення" процесу комунікації між МК та VTX, за допомогою програми RealTerm. Що дозволило оцінити роботу методу в кожних конкретних умовах.

Для роботи із VTX, в контексті реалізації засобів захисту, було розроблено коди програми мовою C++, для забезпечення виконання базових положень роботи протоколу, описаних у цьому пункті. Під розробкою, в даному випадку, мається на увазі як і безпосереднє написання нового коду програми, так і адаптація існуючих програмних шаблонів, якщо схожі по функціоналу функції вже були описані раніше для інших платформ. Наприклад, для напівдуплексного режиму UART існує ціла низка програмних реалізацій для різних платформ, в тому числі Cypress. Тому, зокрема низько рівневі функції передавача UART, будуть просто підтягнуті із існуючої бібліотеки і дещо адаптовані під поставлені задачі.

Однією із найважливіших функцій роботи протоколу є обчислення контрольної суми, без якої запити МК ігноруватимуться. Лістинг її коду можна побачити нижче:

```
    #define POLYGEN 0xd5
    static    uint8_t    sa_CRC8(const    void*    data,    uint32_t
length)//crc8_dvb_s2_update
    {
      uint8_t crc = 0;
      const uint8_t* p = (const uint8_t*)data;
      const uint8_t* pend = p + length;
```

```
  for (; p != pend; p++)
  {
    //crc = crc8_dvb(crc, *p, 0xD5);
    crc ^= *p;
    for (uint8_t i = 0; i < 8; ++i)
    {
      if (crc & 0x80)
      {
        crc = (crc << 1) ^ POLYGEN;
      }
      else
      {
        crc = crc << 1;
      }
    }
  }
  return crc;
}
```

Інші аспекти реалізації, такі як версії протоколу, структура кадру, визначення параметрів роботи, тощо, прописані у файлах-заголовках `VTX_SmartAudio.h`, `VTXControl.h`, лістинг яких можна побачити у Додатках.

4.1.2. Система частотного переналаштування

Для реалізації механізму частотного стрибання було написано код програми який реалізовує, на основі переривань таймера, стабільне із періодом в 200 мілісекунд виконання функції зі зміни частоти передавання відео за принципом, розробленим у Розділі 3.

Як і було запропоновано, перемішування частот каналів було здійснене попередньо на етапі запису їх набору у пам’ять МК. У такому режимі, цей набір каналів зберігається у вигляді масиву відповідних значень:

```
int ch_mix[] = {1, 23, 11, 40, 20, 9, 6, 28,
                25, 26, 36, 15, 32, 3, 18, 39,
                5, 22, 35, 24, 13, 4, 27, 33,
                37, 8, 29, 34, 30, 17, 7, 19,
                38, 31, 2, 14, 10, 21, 16, 12};
```

Що дозволяє зменшити обчислювальне навантаження на систему.

Лістинг основних структурних компонентів, що відповідають за реалізацію методу частотного стрибання можна побачити нижче:

```
    #include "mbed.h"
    #include "VTXControl.h"
    #define time_to_check 0.2 //200мс
    #define AUX_2 15
    //#define VTX_Freq_Test  //тестовий режим для SetFrequency

    int ch_mix[] = {1, 23, 11, 40, 20, 9, 6, 28, 25, 26, 36, 15,
32, 3, 18, 39, 5, 22, 35, 24, 13, 4, 27, 33, 37, 8, 29, 34, 30,
17, 7, 19, 38, 31, 2, 14, 10, 21, 16, 12};
    int ch_freq[] = {5782, 5940, 5995, 5115, 4859, 5002, 6010,
5345};
    int flight_data[300][20]; //дані від контролера польоту

    // Старт індекси
    int current_ch = 0;
    int current_freq = 0;
    // Індекс останнього запису у масиві
    int last_index;

    // Об'єкт функцій керування VTX
    VTXControl vtx;

    Ticker VTX_Freq_Timer;

    void VTX_Freq_Timer_ISR() {
        // Перевірка даних від польотного контролера
        if (flight_data[last_index][AUX_2] > 1800) {
            vtx.setChannel(ch_mix[0]);
        } else {
    #ifdef VTX_Freq_Test
            vtx.setFrequency(ch_freq[current_freq]);
            current_freq = (current_freq + 1) % (sizeof(ch_freq) /
sizeof(ch_freq[0]));
    #else
            vtx.setChannel(ch_mix[current_ch]);
            current_ch = (current_ch + 1) % (sizeof(ch_mix) /
sizeof(ch_mix[0]));
    #endif
        }
    }

    int main() {
        VTX_Freq_Timer.attach(&VTX_Freq_Timer_ISR, time_to_check);

        while (1) {
            // Код отримання і обробки даних із польотного стеку
пропустимо, для даного методу він не суттєвий
            // Більшість часу контролер переводимо в режим сну,
вся його робота "зібрана" на перериваннях
            sleep();
```

```
        }
    }
```

Експеримент проводився таким чином: відеопередавач вмикається на передачу сигналу, після чого мікроконтролером здійснюється постійне керування відеопередавачем за допомогою протоколу SmartAudio. Під час обміну командами і запитами, дані обміну між МК та VTX захоплювалися програмою RealTerm для подальшої оцінки (Рис.4.4). Рядок `#define VTX_Freq_Test` представляє собою активацію режиму відлагодження, який забезпечує задання параметрів несучої робочої частоти сигналу за допомогою команди SetFrequency. Ця команда встановлює частоту не за номером каналу зі стандартної таблиці, а за переданим числовим значенням, що теоретично може дозволити встановлювати частоти із нестандартним кроком, що не співпадатимуть зі значеннями таблиці.

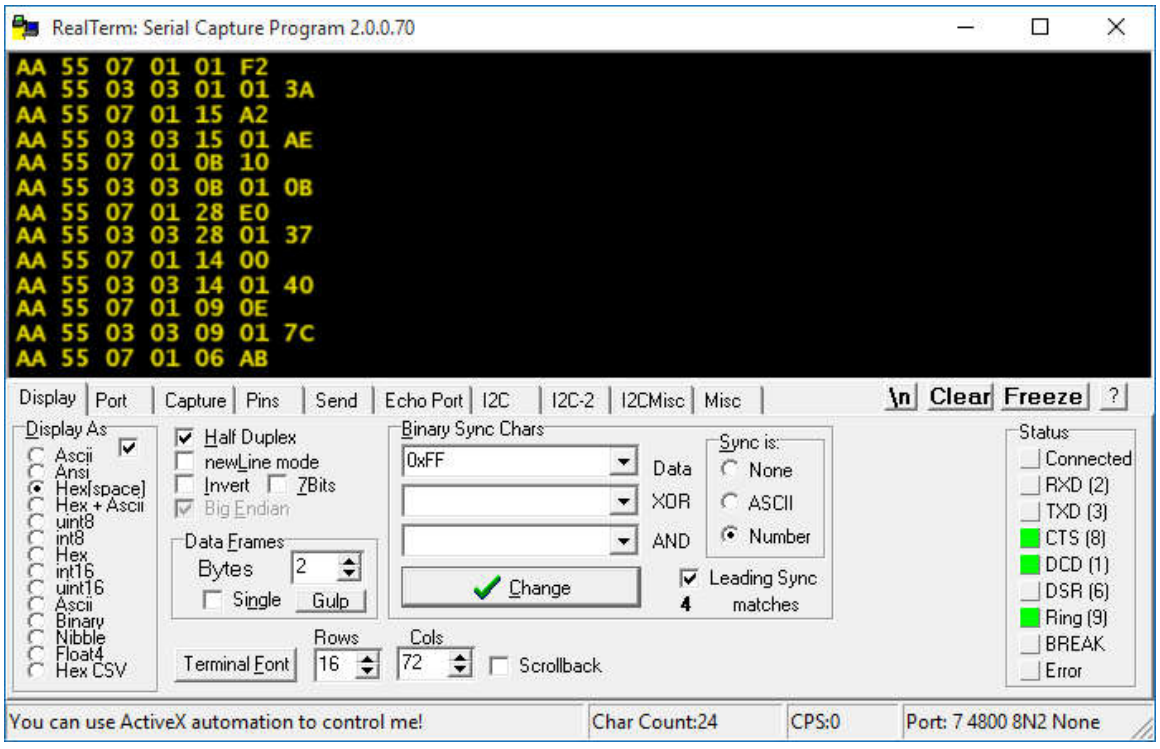


Рисунок 4.4. Захоплення даних програмою RealTerm

Як бачимо із рисунку, дані у RealTerm відображаються і записуються у шістнадцятковому форматі. Для кращого їхнього розуміння і можливості подальшого аналізу і оцінки, проінтерпретуємо значення одного набору передаваних байтів інформації:

Таблиця 4.1

Значення байтів запиту до VTX

0xAA	0x55	0x07	0x01	0x01	0xF2
Байт синхронізаці	Байт синхронізації	Байт команди SetChannel	Байт к-сті аргументів	Аргумент (номер каналу 1)	Байт контрольна сума

Таблиця 4.2

Значення байтів відповіді від VTX

0xAA	0x55	0x03	0x03	0x01	0x01	0x3A
Байт синхр.	Байт синхр.	Байт відп. SetChannel	Байт к-сті аргум.	Аргумент (номер каналу 1)	Резерв. байт	Байт контрольна сума

А також маємо такий загальний лістинг обміну у RealTerm:

```
0xAA 0x55 0x07 0x01 0x01 0xF2
0xAA 0x55 0x03 0x03 0x01 0x01 0x3A
0xAA 0x55 0x07 0x01 0x15 0xA2
0xAA 0x55 0x03 0x03 0x15 0x01 0xAE
0xAA 0x55 0x07 0x01 0x0B 0x10
0xAA 0x55 0x03 0x03 0x0B 0x01 0x0B
0xAA 0x55 0x07 0x01 0x28 0xE0
0xAA 0x55 0x03 0x03 0x28 0x01 0x37
0xAA 0x55 0x07 0x01 0x14 0x00
0xAA 0x55 0x03 0x03 0x14 0x01 0x40
0xAA 0x55 0x07 0x01 0x09 0x0E
0xAA 0x55 0x03 0x03 0x09 0x01 0x7C
...  ...  ...  ...  ...  ...  ...
```

Із цих результатів бачимо, що відбувається поступове змінення робочої несучої частоти відповідно до випадкового порядку каналів, записаного у масив.

Отже маємо результат, що запропонований метод працює належним чином, і також – дана реалізація є робочим і придатним до використання способом частотного переналаштування на базі безпілотника недорогого сегменту.

Як було сказано у розділі 3, одним із параметрів захищеності системи при використанні цього способу є період зміни несучої частоти. Тому наступним кроком, необхідно було проекспериментувати із часовим проміжком зміни частоти. Для цього проведено кілька ітерацій запуску написаного коду із різними часовими проміжками, та зафіксовано обмін даними між МК та VTX. Це дало змогу оцінити відсоток пропущених команд на тій чи іншій швидкості:

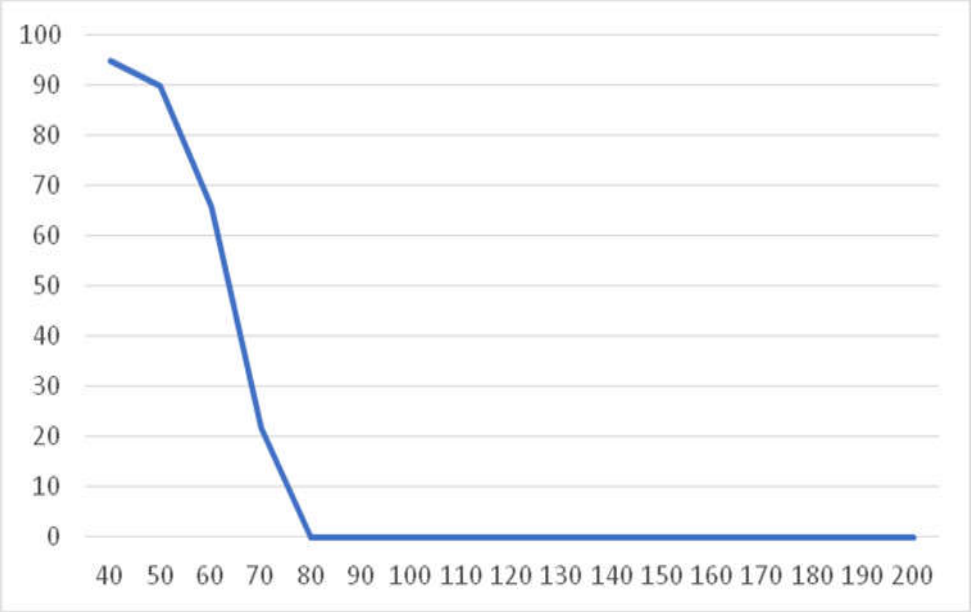


Рисунок 4.5. Результат перевірки роботи із різним періодом (крок 10мс)

Із графіку ми бачимо, що починаючи зі значення періоду у 80 мілісекунд і більше спостерігається стабільна робота системи переналаштування без пропусків команд чи затримок. Якщо ж зменшувати період нижче від значення 80 мс, то вже зі значення у 70 мс починаються одиничні пропуски команд, тобто VTX не встигає обробити кожну команду і виконати її. І цей відсоток зі зменшенням періоду до 40 мс тільки збільшується і прямує до 100%.

Оскільки передавання відео є симплексним і синхронізація передбачена лише на стороні прийому, пропуск великого відсотка частотних перелаштувань дроном може призвести до розсинхронізації приймача та передавача. Тому режимів роботи із можливістю пропуску переналаштувань допускати ми не можемо і приймаємо мінімальний робочий період для даної апаратної реалізації на рівні 80 мілісекунд.

Такий результат корелюється із очікуваним і частково навіть дещо перевершив мої прогнози, оскільки сеанс зв'язку із VTX, тобто передавання йому команди, займає до 40 мс. Опис протоколу Smart Audio, в свою чергу, регламентує час виконання команди і відповіді VTX до 100 мс. Відповідно, отриманий результат – стабільна робота при 80 мілісекунд означає, що виконання команди і відповідь у цьому відео передавачі займають до 40 мс, що є дуже хорошим показником.

Завдяки режиму відлагодження ми змінювали алгоритм роботи таким чином що замість функції Set_Channel використовувалась функція Set_Frequency. Відмінність її полягає в тому, що вона в якості аргументу приймає конкретне значення несучої частоти і налаштовує передавач на роботу на цій конкретній частоті. Здійснивши кілька ітерацій роботи із переналаштуванням за допомогою цієї функції ми отримали дещо неочікувані і дуже позитивні результати роботи цієї функції. Проглянемо лістинг отриманого захоплення даних через RealTerm:

```
0xAA 0x55 0x09 0x02 0x16 0x96 0x3A           (5782)
0xAA 0x55 0x04 0x04 0x16 0x96 0x01 0xF3 (5782)
0xAA 0x55 0x09 0x02 0x17 0x34 0x41           (5940)
0xAA 0x55 0x04 0x04 0x17 0x34 0x01 0x2B (5940)
0xAA 0x55 0x09 0x02 0x17 0x6B 0xCA           (5995)
0xAA 0x55 0x04 0x04 0x17 0x6B 0x01 0x12 (5995)
0xAA 0x55 0x09 0x02 0x13 0xFB 0x3C           (5115)
0xAA 0x55 0x04 0x04 0x13 0xFB 0x01 0xCF (5115)
0xAA 0x55 0x09 0x02 0x12 0xFB 0x07           (4859)
0xAA 0x55 0x04 0x04 0x13 0xFB 0x01 0xCF (5115)
```

Як бачимо, у запиті: `0x09` – команда зміни частоти за значенням, `0x02` – значення кількості аргументів, яких для цієї команди є два, і наступні 2 байти задають числове значення частоти. Для зручності сприйняття інформації, справа у дужках я вказав відповідне десяткове значення аргументу при кожному обміні. Порядок рядків тут такий: запит МК -> відповідь VTX і так далі. Якщо проаналізувати ці дані, то бачимо, що передавач без проблем переключився на

частоту 5782 МГц, що не входить до стандартного переліку у таблиці 3.4., після чого переключився на частоти 5940 МГц та 5995 МГц, які взагалі виходять за межі діапазону значень таблиці!

Після такого результату була здійснена спроба перемикання частоти у напрямку її зниження. Бачимо, що передавач переключився на частоту 5115 МГц, після чого, при спробі змінити частоту на ще нижчу – 4859 МГц, відеопередавач уже відповів не зміненим значенням, тобто перемикання на таку частоту не можливе. Шляхом подальших експериментів, було уточнено емпіричний діапазон роботи приймача, який склав від 5000 МГц до 6000 МГц.

Отримані результати експерименту підтверджують ефективність і можливість оптимального застосування частотного стрибання для захисту навіть відносно недорогих БПЛА, які зараз складають основну частку використовуваних СОУ апаратів. А також, дозволяють зробити висновок, що використання функції зміни частоти за її безпосереднім числовим значенням є ефективнішим та доцільнішим ніж використання функції зміни частоти за номером її каналу із таблиці за кількома критеріями: – можливість вибору значення частоти із стандартного діапазону із не стандартним кроком; – можливість вибору частоти яка виходить за межі стандартних частот.

Використання нестандартних частот для відео дає нам велику перевагу у захисті конфіденційності каналу передавання відео, оскільки велике число компактних пристроїв перехоплення відео із безпілотника є розраховані на роботу БПЛА у межах стандарту (а деякі взагалі лише на набір стандартних значень каналів). Завдяки цьому унеможливити для противника перехоплення нашого відео можна буде навіть без стрибання частоти, простою зміною робочого каналу на той, що відносно далеко виходить за межі стандарту.

Проте варто зазначити, що при проведенні цього експерименту були явно помітні артефакти на відео, отриманому із БПЛА, та помітно погіршувалася якість зв’язку (погіршення кольорів, короткі "завмирання" картинки). Це проявлялося при значному виході частоти за межі стандартних. Теоретично припускаю, що це пов’язано із частотними характеристиками використовуваної

антени. АЧХ антени для 5.8 МГц відеозв’язку має резонансну частоту близько 5790 МГц і далі спостерігається різке затухання коефіцієнта підсилення поза смугою у 150 МГц. Це означає, що для стабільної роботи при виході за межі діапазону, необхідно застосовувати додаткові рішення для забезпечення задовільної якості зв’язку на цих частотах. Серед таких рішень – заходи антенного проектування. Найбільш доцільно буде використати антену, яка одразу є розрахована на роботу на цих, нижчих частотах. Це питання вимагає досліджень і експериментів із різними конфігураціями антенних засобів і наразі залишається відкритим. Воно буде покладене в основи подальшої наукової діяльності із покращення захищеності систем БПЛА.

4.1.3. Система керування потужністю передавача

Для забезпечення менеджменту потужності було написано код програми, який реалізовує перевірку середнього значення потужності сигналу керування кожних 20 секунд (можна програмно змінювати) і відповідно до отриманого значення здійснює коректування потужності передавання відео згідно співвідношення, запропонованого у Розділі 3. Лістинг основних структурних компонентів, що відповідають за реалізацію даного методу приведено нижче:

```
    #include "mbed.h"
    #include "VTXControl.h"
    #define timestamp 0
    #define link_rate 4
    #define time_to_check 20.0
    #define VTX_Man_Debug //визначаю режим відладки, для виведення
в UART додаткових параметрів

    // Масив потужностей відео
    const uint16_t powers_v21[4] = {14,20,26,30};
    // Існуючий масив даних, який постійно оновлюється через дані
від BlackBox
    int flight_data[300][20];
    // Індекс останнього запису у масиві
    int last_index;

    // Таймер
    Ticker VTXPower_Timer;

    Serial VTX_UART(PA1_4);
```

```
    // Об'єкт VTXControl
    VTXControl vtx;

    void calculate_and_set_power() {
        int sum = 0;
        int count = min(100, last_index+1);

        for (int i = last_index; i > last_index - count; i--) {
            sum += flight_data[i][link_rate];
        }
        int avg = sum / count;

        // Вибираємо потужність
        int pwrLevel;
        if (avg >= 91) {
            pwrLevel = powers_v21[0];
        } else if (avg >= 71) {
            pwrLevel = powers_v21[1];
        } else if (avg >= 46) {
            pwrLevel = powers_v21[2];
        } else {
            pwrLevel = powers_v21[3];
        }
        // Встановлюємо потужність
        vtx.setPower(pwrLevel);

        #ifdef VTX_Man_Debug

VTX_UART.printf(flight_data[last_index][timestamp],avg);
        #endif
    }

    int main() {
        VTXPower_Timer.attach(&calculate_and_set_power,
time_to_check);

        while (true) {
            // Код отримання і обробки даних із польотного стеку
пропустимо, для даного методу він не суттєвий
            // Більшість часу контролер переводимо в режим сну,
вся його робота "зібрана" на перериваннях
            sleep();
        }
    }
```

Експеримент проводився шляхом переміщення лише пульта керування, оскільки макет (Рис.4.2) був представлений стаціонарною збіркою. Під час цих переміщень, дані обміну між МК та VTX захоплювалися програмою RealTerm для подальшої оцінки (Рис.4.6). Рядок `#define VTX_Man_Debug`

представляє собою активацію режиму відлагодження, який забезпечує виведення додаткових параметрів (часу чергового переривання таймеру, та середнього значення потужності сигналу керування), завдяки яким ми можемо оцінити правильність реалізації і механізм роботи запропонованого методу.

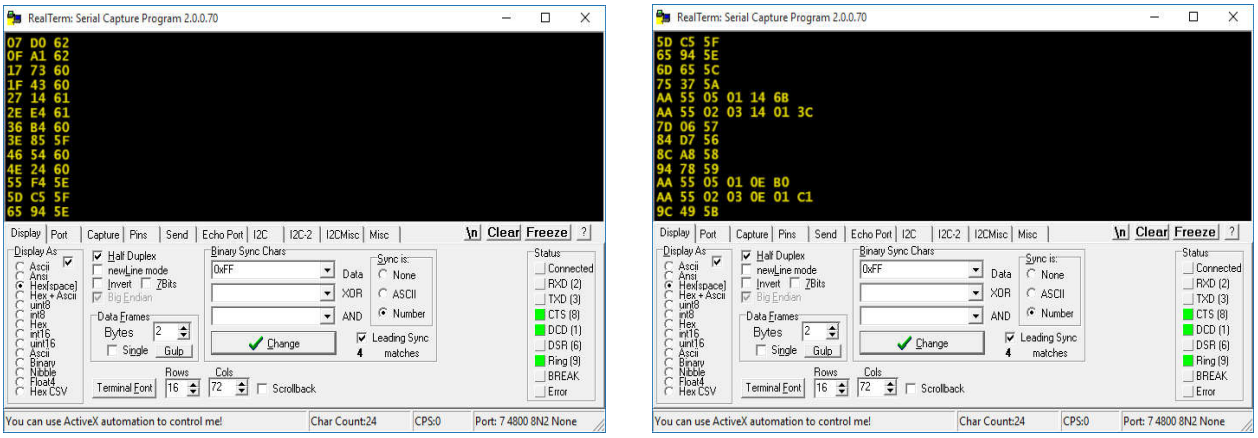


Рисунок 4.6. Захоплення даних програмою RealTerm

Як бачимо із рис.4.6, дані у RealTerm відображаються і записуються у шістнадцятковому форматі. Для зручнішого їх подальшого аналізу і оцінки необхідно перевести їх у десяткову форму (окрім команд обміну між МК та VTX), маємо такий лістинг виводу у RealTerm:

```
Час          сер. потужність
20,00        98
40,01        98
60,03        96
……           …
300,07             90
0xAA 0x55 0x05 0x01 0x14 0x6B
0xAA 0x55 0x02 0x03 0x14 0x01 0x3C
320,06             87
340,07             86
360,08             88
380,08             89
0xAA 0x55 0x05 0x01 0x0E 0xB0
0xAA 0x55 0x02 0x03 0x0E 0x01 0xC1
400,09             91
```

Завдяки режиму відлагодження на кожній ітерації пробудження МК від таймера ми отримуємо вивід часу пробудження у секундах та обчислене значення середнього арифметичного якості сигналу. Із отриманих даних бачимо, що до часової відмітки у 300 сек, при стабільно високій якості сигналу відбувалося лише виведення даних режиму відладки, обміну між МК та VTX не було. При переході сигналу на рівень нижчого проміжку ми побачили захоплений обмін:

```
0xAA 0x55 0x05 0x01 0x14 0x6B
0xAA 0x55 0x02 0x03 0x14 0x01 0x3C
```

Який означає: `0x05` – команда зміни потужності, `0x14` – значення аргументу, що відповідає десятковому значенню 20 (тобто 40% потужності передавача). На даний запит прийшла відповідь, параметри якої означають: `0x02` – підтвердження отримання команди зміни потужності, `0x14` – нове значення потужності (як бачимо, воно відповідає запиту, тобто команда виконана успішно).

Після цього, при значенні потужності у межах визначеного проміжку знову спостерігалося лише виведення даних для відладки.

Варто зазначити, що при проведенні цього експерименту якихось артефактів на відео, отриманому із БПЛА, або помітного погіршення якості зв’язку чи його переривання не спостерігалося. Це означає, що наші співвідношення між потужностями сигналу керування і сигналу відео можна відкоригувати навіть у напрямку збільшення дистанції роботи відео передавача без збільшення потужності.

Окремими пунктами чи експериментом висвітлювати це і приділяти цьому увагу у даній роботі не будемо, оскільки даний факт – це нюанси практичної реалізації методу, які залежать від тої чи іншої апаратної платформи. Але в загальному – це підтверджує наше припущення, зроблене у Розділі 3, щодо того, що для кожної апаратної конфігурації того чи іншого БПЛА необхідно здійснювати настройку такої таблиці відношень у залежності від робочих частот та моделей використовуваних передавачів.

4.2. Система аварійного відновлення зв’язку бездротової системи керування БПЛА

Даний підрозділ дисертаційного дослідження присвячений випробуванню та дослідженню використання запропонованої нової ідеї врахування переміщення інформаційної системи в просторі для моніторингу рівня захищеності, та його підвищення за допомогою зміни свого просторового місця розташування.

У першу чергу реалізації і дослідженню параметрів роботи підлягає пасивний етап функціонування даної пропонованої системи. Він є першим кроком і найбільш основним етапом роботи методу, оскільки від його точності і релевантності записаних ним даних залежить вся подальша робота системи відновлення.

4.2.1. Вибір способу отримання даних польоту

Для запису і збереження обґрунтованої нами емпіричної функції $R(x, y, z)$ необхідно забезпечити для себе можливість отримання даних про політ БПЛА, якість зв'язку із ним та інших параметрів які можуть бути корисними.

Для запису координат, враховуючи застосований метод впровадження засобів захисту – зовнішній мікроконтролер, є кілька можливих шляхів, які можна спробувати для реалізації:

– підключення до схеми БПЛА навігаційного модуля GPS;

– підключення до схеми МК навігаційного модуля GPS;

– підключення до схеми МК зовнішніх давачів просторового положення (швидкості, повороту, тощо);

– отримання можливих даних із давачів які є присутні у конкретного польотного контролера.

Варіант із використанням навігаційних засобів на базі технології GPS (незалежно від місця впровадження: чи у політний контролер, чи у мікроконтролер) ми відхиляємо. Причиною цьому є описана раніше атака "GPS-спуфінг", яка означає підміну даних сигналу GPS таким чином, що давач не

коректно зчитує своє розташування.

Оскільки використовувані противником засоби РЕБ мають потужні можливості для здійснення атаки "GPS-спуфінг", а вбудовані мікросхеми GPS навігації не мають належного функціоналу для протидії такій атаці, використання GPS модулів несе в собі загрозу, що при втраті зв'язку відбудеться ситуація яка в англомовній літературі називається терміном "fly-away", тобто коли алгоритми польоту і навігації ведуть дрон у невідомому напрямку.

Для уникнення такої вразливості доцільно орієнтуватися на власні інерційні показники руху апарату.

Це можна забезпечити за допомогою останніх двох методів: застосування додаткових зовнішніх давачів, або застосування давачів, наявних у схемі самого контролера польоту (Рис. 4.7.).

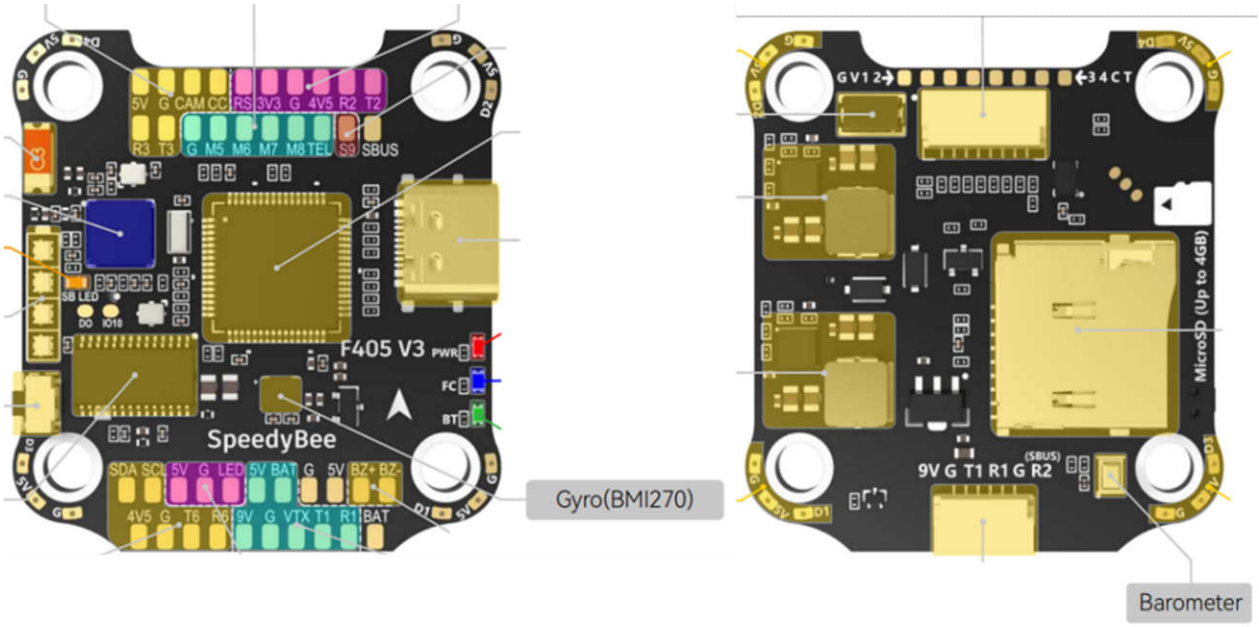


Рисунок 4.7. Давачі контролера SpeedyBee F405 V3
(а – гіроскоп, б – барометричний давач висоти) [96]

Застосування зовнішніх давачів, порівняно із використанням вбудованих, є більш ресурсо-затратним, оскільки в першу чергу необхідно закупити самі давачі, та окрім цього, при їх підключенні додатково необхідно провести настройку і калібрування цих давачів. А давачі, що є на борту контролера

польоту, вже налаштовані і відкалібровані, тому із польотного стеку можна отримувати вже нормовані їхні показники.

Наприклад, як бачимо із рис.4.7 – один із найбільш популярних контролерів "SpeedyBee" на борту містить комбінований давач гіроскоп+акселерометр на фронтальній стороні і на тильній стороні також додатково має барометричний давач висоти польоту.

Значень, які ми можемо отримувати із цих давачів, є цілком достатньо для відслідковування відносних координат переміщення безпілотного апарату у просторі, тому було вирішено використовувати дані, отримувані із контролера польоту.

4.2.2. Відбір та опрацювання отриманих від польотного стеку значень

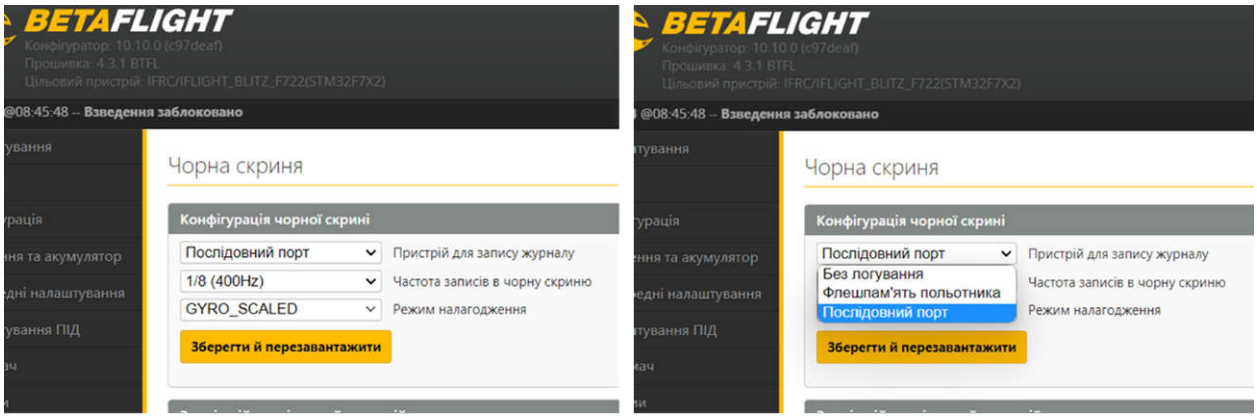
Прямого способу отримувати дані із польотного контролера які він отримує і обробляє в даний момент часу у більшості популярних польотних стеків не існує.

Проте, майже у кожному із них існують інструменти відлагодження побудованої безпілотної системи, які працюють за принципом "чорного ящика" (BlackBox).

Зазвичай його використовують для так званого "post-flight" аналізу параметрів польоту, що дає змогу коректно налаштувати параметри обробки команд пульта, отриманих значень давачів, розміщення центру мас апарату, тощо. Для цього, під час "прошивки" контролера керування налаштовують функцію BlackBox.

Налаштування полягає у виборі частоти збереження окремих кадрів, місця чи пристрою збереження цілого лог-файлу, параметрів порту передачі даних, тощо. Власне вибір місця збереження лог-файлу і дає нам можливість опосередкованим чином отримувати дані польоту практично в режимі реального часу.

Серед можливих варіантів місця збереження є варіант "послідовний порт" (Рис.4.8.,"б").



а.) б.)

Рисунок 4.8. Настроювання параметрів "BlackBox" у середовищі програматора BetaFlight (а – частоти запису кадру, б – місце виводу даних)

Очевидно, що для отримання і збереження даних у мікроконтролер, необхідно обрати місце збереження "Послідовний порт" (Рис. 4.8. "б"). А от для вибору частоти запису (Рис. 4.8. "а") необхідно враховувати необхідний баланс "точність визначення/обсяг обчислень".

Якщо припустити, що максимальна швидкість котру може розвинути наш безпілотник сягає 150 км/год (~41,67 м/с), можна обчислити максимальну відстань, яку може подолати наш безпілотник між двома окремими кадрами запису у BlackBox із допомогою елементарного виразу: $l = \frac{V_{uav}}{f_{blbox}}$.

Таблиця 4.3

Максимальне переміщення БПЛА між кадрами за різних частот запису BlackBox

Частота кадрів, Гц	Пройдена відстань, м
400	0,104
800	0,052
1600	0,026
2400	0,017
3200	0,013

Як бачимо, при швидкості безпілотника у 150 км/год його переміщення фіксуватимуться кожні ~10 см за частоти логування 400 Гц. Якщо також врахувати два факти: ця швидкість обрана із великим запасом (звичні швидкості для FPV не сягають і 100 км/год); пам'ять мікроконтролера є обмежена (близько 1МБ), то стає очевидно, що для задачі забезпечення доступності системи керування БПЛА, частота у 400 Гц є цілком прийнятною із точки зору точності запису і максимально оптимальною із точки зору використання ресурсу пам'яті.

Налаштування BlackBox-UART за замовчуванням є наступними: швидкість передачі (baud rate) – 115200 бод, логіка – 8N1. Для обраних параметрів збереження лог-файлів необхідності змінювати їх немає.

Структура та порядок передавання даних польоту через послідовний порт UART у пристрій запису BlackBox, на жаль, не є задокументованою: і в інтернеті, і в документах відсутній опис яким чином і в якому порядку ці дані передаються. Тому список доступних для отримання і запису метрик був визначений емпіричним шляхом при тестових реєстраціях потоку даних blackbox, а також за допомогою аналізу програмного коду застосунків для аналізу вмісту лог-файлів (зокрема Cleanflight BlackBox Explorer). Згідно проведеного аналізу застосунків, а також тестових записів BlackBox, мною було визначено список полів, які ми можемо отримувати, а також їхній фізичний чи логічний зміст (за який параметр та чи інша метрика відповідає).

Таблиця. 4.4

Метрики, отримувані за допомогою логування BlackBox

Назва метрики	Значення
rc_Command[A]	Значення крену від пульта керування
rc_Command[E]	Значення тангажу від пульта керування
rc_Command[R]	Значення рискання від пульта керування
rc_Command[T]	Значення тяги від пульта керування
AUX_1	Значення положення програмованої кнопки aux1
……	……

AUX_12	Значення положення програмованої кнопки aux12
PID_P[3]	Масив значень налаштуваня "Proportional" для кожної осі
PID_I[3]	Масив значень налаштуваня "Integral" для кожної осі
PID_D[3]	Масив значень налаштуваня "Derivative" для кожної осі
Battery_vol	Рівень заряду батареї
Compass[3]	Масив значень показу магнетометра для кожної осі
Baro_Alt	Значення висоти за показом барометра
Gyro[3]	Масив значень показів гіроскопа для кожної осі
Acc[3]	Масив значень акселерометра для кожної осі
Motor[4]	Масив значень обертів кожного двигуна
PID_Sum[3]	Результати сумування значень PID для кожної осі
PID_Error[3]	Результат обчисленої похибки PID для кожної осі
Loop	Номер ітерації обчислення у режимі "ARMED"
Loop_time	Час роботи системи дрона у режимі "ARMED"
Gyro.Scale	Опорне значення шкали гіроскопа, для приведення числового значення з АЦП до значення град/с^2
ACC.1G	Опорне значення шкали акселерометра, для приведення значення з АЦП до значення м/с^2
RC Rate	Частота пакетів керування
RC Expo	Числове значення відносної якості сигналу керування

У даній таблиці представлено список основних отриманих і визначених дослідним шляхом метрик, які передає контролер польоту через механізм BlackBox. При виводі значень на послідовний порт UART присутні також деякі додаткові значення, визначити значення яких наразі не вдалося.

Але зважаючи на той факт, що під час польоту та маневрування ці "не відомі" показники змінюються несуттєво і не залежать від виконуваних маневрів апарату, можна зробити висновок, що дані метрики не мають прямої залежності чи зв’язку із маневрами та траєкторією польоту БПЛА. Тому, для даного методу захисту ними можна знехтувати.

Для реалізації і забезпечення правильної роботи запропонованих методів захисту серед всієї множини отримуваних метрик було обрано ті, які найбільше відповідають поставленим завданням. До таких метрик належать:

– команди пульта керування;

– опорні значення гіроскопа та барометра;

– показники часу та кількості ітерацій від моменту взведення системи;

– показники акселерометра по кожній з осей;

– показники гіроскопа по кожній з осей;

– значення барометричної висоти;

– значення напрямку згідно показу магнітного компасу;

– значення якості зв'язку сигналу керування;

– значення програмованих кнопок AUX на пульті керування оператора.

Кожна з метрик була обрана відповідно до інформації яку вона надає для забезпечення функціонування наших методів. Зокрема, команди пульта керування, показники акселерометра по кожній із осей, показники гіроскопа по кожній із осей, значення барометричної висоти, значення напрямку згідно показу магнітного компасу, а також опорні значення гіроскопа та барометра необхідні для отримання інформації про пройдений шлях та траєкторію переміщення нашого пристрою. Показники часу та кількості ітерацій потрібні для процесу обробки даних після польоту та оцінювання результатів проведеного експерименту.

Значення якості зв'язку сигналу керування необхідне нам для отримання вибірки значень, необхідних для належної роботи системи менеджменту потужності відео передавача, описаної у попередньому пункті розділу.

Значення положення програмованих кнопок "AUX" на пульті керування оператора необхідне нам для забезпечення можливості керування системою захисту відео оператором, а також можливості скидання записаного маршруту у поточному методі захисту.

Після отримання даних значень необхідно також забезпечити конвертацію декотрих із отримуваних значень. Так, якщо покази барометричної висоти,

напрямку за магнітометром, опорних значень давачів є статичними і вираженими в потрібних нам одиницях виміру, то покази акселерометра та гіроскопа записують інерційні моменти переміщення пристрою: лінійне $a(t)$ [м/с^2], та кутове $\varepsilon(t)$ [град/с^2] прискорення.

Для перетворення цих значень у значення переміщення і положення – метри та градуси відповідно, необхідно скористатися інтегруванням, оскільки між цими значеннями у фізиці мають місце такі співвідношення:

$$s(t) = \int v(t)dt, \tag{4.1}$$

$$v(t) = \int a(t)dt, \tag{4.2}$$

$$a(t) = \int \omega(t)dt, \tag{4.3}$$

$$\omega(t) = \int \varepsilon(t)dt, \tag{4.4}$$

де: $s(t)$ – переміщення, $v(t)$ – швидкість,

$a(t)$ – лінійне прискорення, $\omega(t)$ – кутова швидкість,

$\varepsilon(t)$ – кутове прискорення.

Для практичної реалізації цього методу було написано код програми, який реалізовує отримання, відбір, обробку та збереження у флеш-пам’ять отримуваної інформації.

Лістинг основних компонентів програми приведено нижче.

```
#include "mbed.h"
#include "FlashIAP.h"

// UART object
Serial uart(PA_9, PA_10); // TX, RX

// Flash object
FlashIAP flash;

// Data structures
struct GyroData {
    float roll;
```

```
        float pitch;
        float yaw;
    };

    struct AccelData {
        float x;
        float y;
        float z;
    };

    // Function to read data from UART
    void readData(GyroData* gyro, AccelData* accel) {
        // TODO: Implement UART reading here
    }

    // Function to compute integral
    float computeIntegral(GyroData* data) {
        // TODO: Implement integral computation here
        return 0.0;
    }

    // Function to compute double integral
    float computeDoubleIntegral(AccelData* data) {
        // TODO: Implement double integral computation here
        return 0.0;
    }

    // Function to write data to flash
    void writeToFlash(float gyroIntegral, float
accelDoubleIntegral) {
        // TODO: Implement flash writing here
    }

    int main() {
        while (true) {
            GyroData gyro;
            AccelData accel;

            // Read data from UART
            readData(&gyro, &accel);

            // Compute integrals
            float gyroIntegral = computeIntegral(&gyro);
            float                accelDoubleIntegral                =
computeDoubleIntegral(&accel);

            // Write results to flash
            writeToFlash(gyroIntegral, accelDoubleIntegral);
        }
    }
```

4.2.3. Методика та результати проведення експерименту.

Для оцінки можливостей використання запропонованого методу, а також оцінювання його точності за використання тих чи інших наборів метрик було розроблено лабораторний макет з використанням того ж МК, але у мобільному, автономному виконанні (Рис.4.9).

Така реалізація лабораторної моделі забезпечує можливість пілотувати апарат у звичному режимі і не впливає на роботу БПЛА. Це дозволило проводити експерименти на основі польотних випробувань, які є максимально наближеними до реальних умов роботи запропонованого методу відновлення зв’язку.

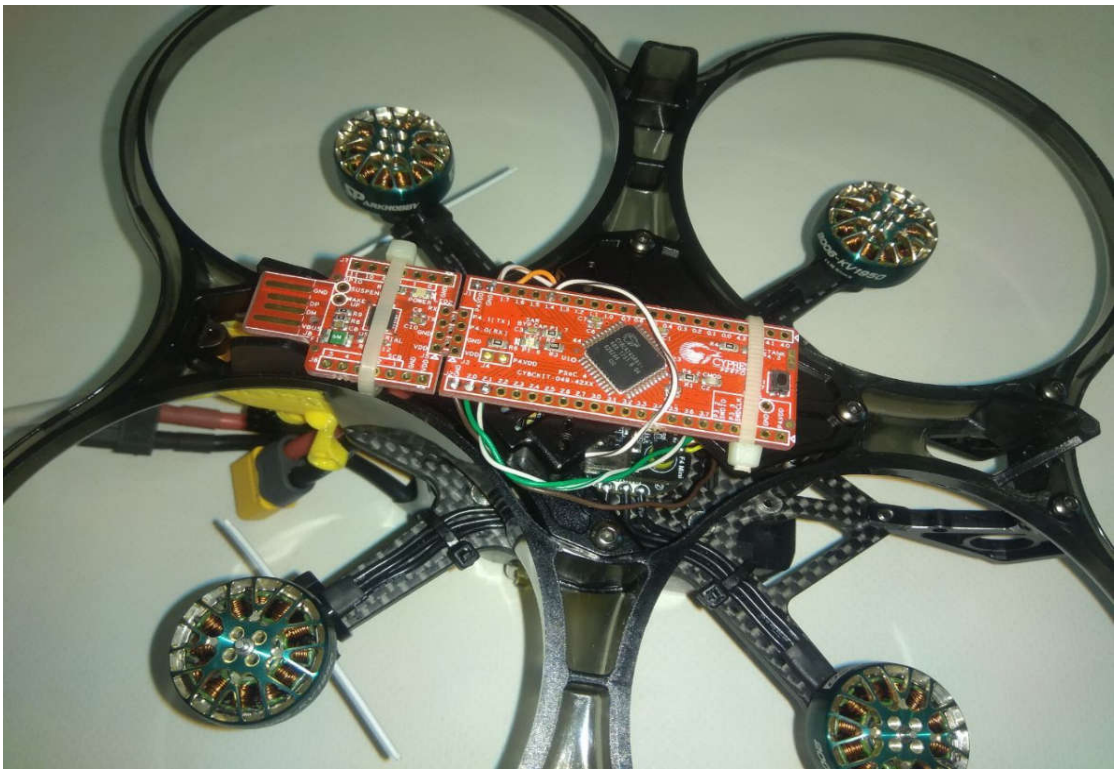
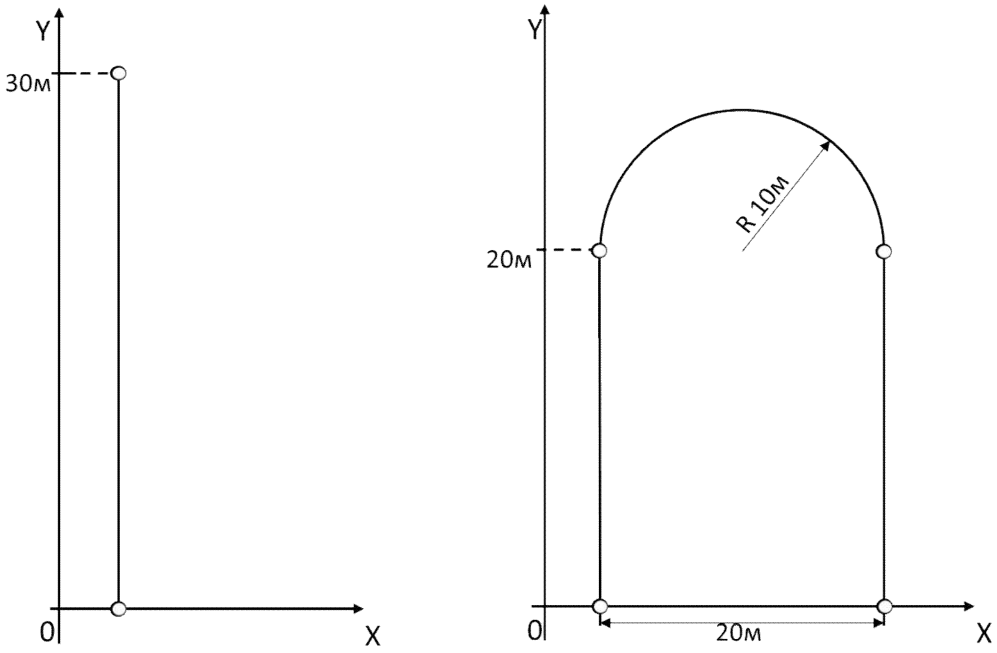


Рисунок 4.9. Лабораторний макет для експериментів
із запису даних у BlackBox

Методика проведення експерименту полягала у наступному: на рівному майданчику розміром 40х40 метрів було виміряно та зроблено розмітку двох варіантів чітко визначеної траєкторії для польоту безпілотника: пряма лінія, та

маршрут із кривою (Рис.4.10 "а, б"). Після чого, за допомогою пульта дистанційного керування, безпілотник розміщувався у початковій позиції маршруту, вмикався на запис маршруту запрограмований у мікроконтролер алгоритм, та здійснювався політ по розміченій траєкторії.

Після польоту записаний маршрут за допомогою USB завантажувався на комп'ютер для подальшої обробки. Польоти здійснювалися багатократно для кожного вибраного набору метрик відстеження переміщення БПЛА задля отримання множини варіантів записаного переміщення. Відповідно, оцінка відхилення записаного за конкретним набором метрик маршруту від реального проводилася за обчисленим середнім значенням похибки декількох спроб.



а. б.

Рисунок 4.11. Конфігурація контрольного польоту:
а) пряма траєкторія; б) маршрут із кривою

Така геометрична конфігурація маршрутів на місцевості дозволила спростити обчислення відхилення записаного маршруту від реального, оскільки координати кожного еталонного маршруту можна описати аналітичним математичним виразом на неперервній ділянці. Тому, обробка результату для оцінки похибки відбувалася так:

– після польоту із отриманої вибірки значень траєкторії обиралася опорна змінна ("x" або "y", залежно від траєкторії і її ділянки);
– для кожного дискретного значення опорної змінної математично обчислювалося значення залежних змінних згідно виразу, яким описується еталонний маршрут;
– для кожного дискретного значення координат записаного маршруту обчислювалося абсолютне відхилення від еталонного маршруту $\Delta s(x,y,z)$;
– із множини обчислених значень абсолютного відхилення для усього маршруту обчислювалося середнє значення відхилення за маршрут $\Delta s_{avg} = \frac{\sum \Delta s(x,y,z)}{N_s}$, де N_s – загальна кількість дискретних значень;
– і для кращої наочності і інформативності результату переводили середнє значення відхилення Δs у відносну величину $\delta s = \frac{\Delta s}{l} * 100\%$, де l – загальна довжина пройденого шляху.

Тут варто зазначити, що такий підхід має один недолік: є висока ймовірність отримати значну похибку експерименту. Так, при помилці оператора літального апарату реальна траєкторія руху може відхилитися від еталонного розміченого маршруту і, навіть якщо алгоритм МК точно збереже пройдений маршрут, через таке відхилення реальної траєкторії від математично описаного еталону будуть отримані спотворені результати.

Для мінімізації впливу цього фактору було вирішено жорстко зафіксувати допустимий маршрут у просторі за допомогою так званих "воріт" (Рис.4.12), які використовуються зазвичай для проведення змагань.

Для використовуваного в роботі дрона типорозміром 3,5” (3,5 дюйма) придбані кільця обмежили простір в межах 10-ти сантиметрів справа/зліва і 7-ми сантиметрів зверху/знизу. Усі спроби експерименту, при яких відхилення оператором від маршруту було більшим за ці значення, закінчувалися зіткненням безпілотника із воротами та його падінням. Такі спроби було легко виявити і відкинути їхні результати.

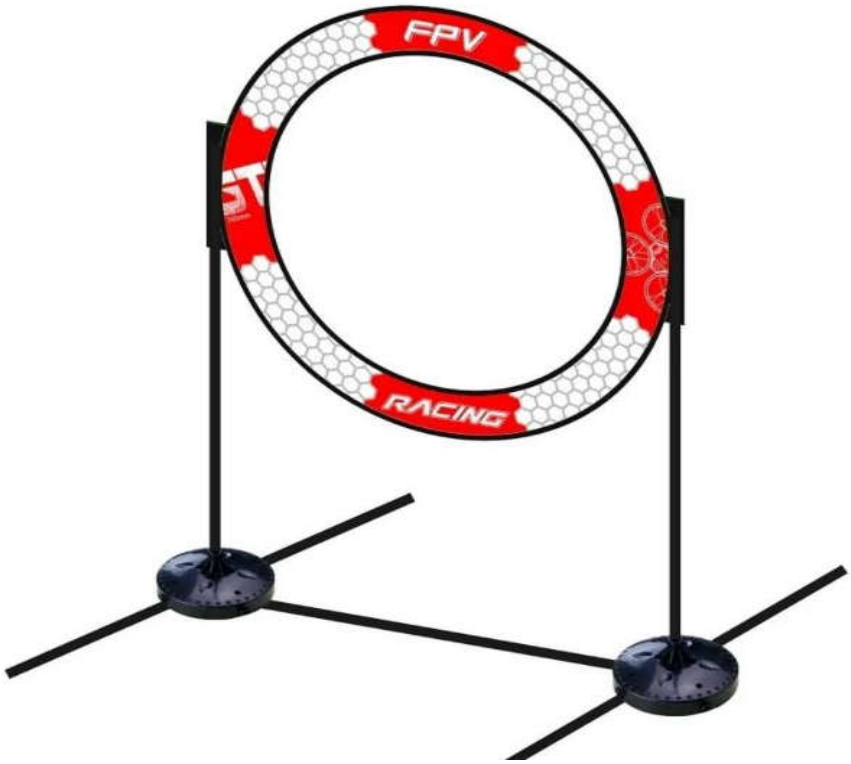


Рисунок 4.12. Ворота, використані для обмеження можливого відхилення маршруту

Таким чином, максимальну відносну похибку проведення експерименту було обмежено до таких значень:

– для прямолінійної траєкторії

$$\delta E = \frac{0.1}{30} * 100\% = 0.33\% \tag{4.5}$$

– для маршруту із кривою

$$\delta E = \frac{0.1}{71.42} * 100\% = 0.14\% \tag{4.6}$$

Після цього стало можливим проведення експериментальних польотів зі сталою точністю визначення відхилення записаного маршруту. Щоб збільшити репрезентативність вимірювання, для кожного набору метрик було здійснено не менше 20-ти польотів (маються на увазі лише вдалі спроби – всі дані польотів, що закінчувалися падінням від удару об ворота, відкидалися).

У якості першого набору метрик, було обрано покази акселерометра, згідно припущення, що вони дозволяють відслідковувати переміщення безпілотника за трьома осями OX, OY, OZ і цього буде достатньо. Проте, тестові польоти показали, що таке припущення було хибним.

Для акселерометра польотного контролера осі відліку прискорення фіксовані відносно його корпусу, відповідно, коли дрон повертає довкола своєї осі на певний кут, траєкторія його руху у просторі змінюється, а покази акселерометра далі показують рух прямо, оскільки вісь відліку "повернула" разом із корпусом. Із цього робимо висновок, що такий набір метрик допускає відслідковування лише прямолінійного польоту і ігнорує будь-який поворот корпусу. Тому результат відхилення для польоту за маршрутом умовно приймаємо за 100% і для наступних експериментів за різних умов використовувати даний набір метрик немає сенсу.

Базуючись на цьому, наступні експерименти проводилися із фіксуванням метрик, які дозволяють відслідковувати і просторове переміщення БПЛА і його повороти довкола осей корпусу. Серед обраних основних метрик було сформовано такі набори:

- Акселерометр+гіроскоп: Acc[x] + Acc[y] + Acc[z] + Gyro[r] + Gyro[p] + Gyro[y];
- Акселерометр+гіроскоп: Acc[x] + Acc[y] + Acc[z] + Gyro[y];
- Акселерометр+магн.компас: Acc[x] + Acc[y] + Acc[z] + Compass[x] + Compass[y];
- Акселерометр+гіроскоп+барометр: Acc[x] + Acc[y] + Gyro[y] + Baro_Alt;
- Акселерометр+барометр+магн.компас: Acc[x] + Acc[y] + Compass[x] + Compass[y] + Baro_Alt;
- Команди пульта керування: rc_Command[A] + rc_Command[E] + rc_Command[R] + rc_Command[T];

Після проведення польотів, обробки отриманих даних на ПК та обчислення середніх відхилень, результати експерименту, для кращого сприйняття і порівняння, було записано у зведену таблицю експерименту (Табл.4.5).

Таблиця 4.5

Зведений результат польотних експериментів

Умови / Метрики	прямо	маршрут	Прямо, вітер	Маршрут, вітер	Прямо, ел.магн поле	Прямо, масивн. ферром.
acc_x, acc_y, acc_z	0,667%	100%[1]	---[1]	---[1]	---[1]	---[1]
acc_x, acc_y, acc_z, gyro_r, gyro_p, gyro_y	0,6%	0,56%	0,833%	0,686%	---[2]	---[2]
acc_x, acc_y, acc_z, gyro_y	0,633%	0,61%	1,267%	0,91%	---[2]	---[2]
acc_x, acc_y, acc_z, mag	1,3%	1,82%	1,6%	2,212%	54,5%	16,17%
acc_x, acc_y, baroAlt, gyro_y	14,83%	17,43%	27,97%	26,16%	---[2]	---[2]
acc_x, acc_y, baroAlt, mag	15,03%	18,27%	30,13%	29,84%	94,81%	38,17%
rc_Com_A, rc_Com_E, rc_Com_R, rc_Com_T	98%[3]	93%[3]	54%[3]	38%[3]	---[2]	---[2]

[1] – експеримент показав наднизьку точність, подальші спроби не мали сенсу;

[2] – експерименти із такими метриками за заданих умов до розгляду не включені – жодного взаємозв'язку між умовами і результатом;

[3] – результат обчислювався як функція кореляції.

Із результатів проведених досліджень можна зробити висновок, що використання запропонованого методу відслідковування траєкторії із набором

показів акселерометра та гіроскопа, за всіма трьома осями їхньої роботи, дає найкращі результати відслідковування траєкторії.

Також цей набір показників має найвищу стабільність до умов навколишнього середовища, оскільки результати проведених експериментів залежали від погодних умов (поривів вітру, бокового вітру, тощо) мінімально (похибка запису зросла з 0,6% до 0,833% та з 0,56% до 0,686% для прямолінійної та кривої траєкторій відповідно) і зовсім не спостерігалося залежності від зовнішніх фізичних впливів, таких як електромагнітне поле чи проходження безпілотника повз масивні металеві об'єкти або лінії електропередачі. Але цей набір метрик поряд із високою точністю має свої недоліки та обмеження.

Як було описано вище – всі значення отримувані від акселерометра та гіроскопа мають потребу у подвійному інтегруванні для переведення їх показів у значення переміщення, а також вимагають достатньо великого об'єму пам'яті, оскільки одна точка в просторі представляється шістьма значеннями, кожне з яких займає два байти пам'яті.

Друга особливість використання даного набору значень походить якраз із його високої точності – такий набір метрик дуже чутливий до якості збірки безпілотника. Якщо у конструкції присутні послаблені елементи чи кріплення, чутливості акселерометра і гіроскопа достатньо для того, щоб фіксувати паразитні вібрації від таких місць. Ці вібрації мають негативний вплив на точність вимірювань і не завжди їх можна відфільтрувати.

Також, результати показали, що для зменшення затрат пам’яті, можливе використання показів акселерометра та показу гіроскопа тільки за однією його віссю – рискання. Такий набір має дещо меншу точність ніж попередній набір, разом з тим, точність все ще залишиться порівняно високою.

Використання значення показу барометричного висотоміра дозволяє значно зменшити об'єм використаної пам'яті, але результати експериментів показали що барометричний висотомір, на жаль, має високу похибку вимірювання висоти і дуже нестійкий до поривів вітру під час польоту. Навіть

за прямолінійного польоту поривчастий боковий чи лобовий вітри спричиняли значне відхилення показу висоти польоту, виміряної мікроконтролером (хоча сам безпілотник під час руху летів на фіксованій висоті).

Також збільшення погрішності показу барометра викликали різкі маневри безпілотника: якщо різко розганятися або зупинятися, чи здійснювати різкий маневр повороту – спостерігалася зміна показів висоти. Це є дуже серйозною перешкодою для використання цього показника, особливо за польоту на низькій висоті, оскільки така похибка може призвести до зіткнення БПЛА із землею.

І остання з фіксованих метрик – це покази магнітного компаса. Їх використання не дає значного виграшу в об'ємі використовуваної пам'яті, але його перевагою, порівняно з будь-якими іншими метриками, є те, що він записує абсолютне положення безпілотника відносно сторін світу (тобто кут азимута). Працює компас у будь-якому положенні БПЛА і вказує напрямок на північ тривимірним вектором.

Проте, під час випробувань було виявлено, що його використання призводить до великої похибки запису маршруту, особливо при здійсненні швидких маневрів безпілотником та польотах у зоні дії магнітного чи електромагнітного поля. Механізм появи першої похибки полягає в тому, що магнітометр має деяку інерційність і записує кут повороту з невеликим відставанням. Це особливо відчутно при різких маневрах.

Друга похибка вже є більш серйозною проблемою: магнітометр, через свою високу чутливість для фіксування напрямку магнітного поля землі, є дуже нестійким до впливу на нього електромагнітного випромінювання, магнітних полів. Це особливо наочно відобразив експеримент прямого польоту під впливом електромагнітного поля – при польоті безпілотника під ЛЕП похибка виміру максимально наблизилася до 100% і дорівнювала 94,81%.

Висновки до 4 розділу

Цей розділ був присвячений практичній реалізації та випробуванню ефективності запропонованих методів захисту. Зокрема, досліджувалися

концепція захисту "оптимальний захист за оптимального рівня затрат"; спосіб реалізації методів захисту: зовнішній керуючий мікроконтролер; а також спосіб функціонування засобів захисту: шляхом керування налаштуваннями відео передавача та періодичного отримання метрик польоту від контролера польоту.

Запропоновані нами засоби показали свою високу ефективність для реалізації у безпілотних авіаційних системах. Зокрема, система менеджменту потужності, згідно проведеного дослідження, працює належним чином згідно заданого алгоритму, споживання енергії мікроконтролером відбувається лише у моменти пробудження, а решту часу мікроконтролер перебуває в режимі пониженого енергоспоживання. Отримані результати підтвердили, що запропоновані нами співвідношення рівнів потужності передавачів можна значно змістити у напрямку збільшення відстані за одного і того ж рівня потужності передавача відео, оскільки якість відео залишалася високою навіть до самого моменту переключення потужності на вищу.

Запропонований варіант частотного переналаштування дав позитивні результати, а саме: мінімально допустимий період перемикання частоти склав 80мс (при очікуваному не менше 150мс, оскільки час передачі команди близько 40мс, а сам протокол SA регламентує перемикання в межах ~100мс).

Другий позитивний аспект нашої реалізації – експерименти показали, що використаний для експериментів відеопередавач, запропонованим нами методом, можна перемикати на частоти, які не входять у стандартну таблицю каналів. Таким чином можна розширити діапазон його роботи в межах: від 5 ГГц до 6 ГГц, що дає значну перевагу для захисту дрона.

Експерименти із третім запропонованим методом із загальної комплексної системи захисту – це є тести методу відслідковування траєкторії польоту, задля повернення БПЛА із зони втрати зв’язку. У цьому методі ми розглядали множину варіантів отримуваних метрик для відслідковування пройденої траєкторії. Результати показали, що найбільш ефективним набором метрик є комбінація із акселерометра та гіроскопа зі зчитуванням їхніх значень по всіх трьох осях. При цьому, за необхідності зменшення обсягу даних та обсягу

обчислень, можна записувати покази гіроскопа лише за віссю рискання, адже експерименти показали, що точність знижується не сильно (похибка прямолінійного польоту зросла із 0.833% лише до 1.267%).

Використання інших метрик, таких як покази магнітометра або барометричного висотоміра, не рекомендується. Результати експериментів виявили, що покази висотоміра є неточними і нестійкими до поривів вітру, не стабільно працюють у різних погодних умовах. Магнітометр має досить високу точність, але в його роботі спостерігалася інерційність (тобто "відставання" показу від зміни положення дрону). Також було виявлено сильний вплив на покази магнітометра електромагнітних наведень та масивних об'єктів здатних до намагнічування (великі металеві конструкції, тощо).

Результати проведених експериментів приводять нас до позитивного загального висновку щодо використання запропонованих методів захисту. Проте залишилися окремі питання, що потребують подальшого дослідження.

Зокрема, потребують подальших досліджень та випробувань такі аспекти:

– Застосування методів антенного проектування для використання їх у методі частотного переналаштування: експерименти показали погіршення якості зв’язку відео при перемиканні на частоти нижче 5600МГц із використанням стандартної 5.8ГГц "lollipop" антени, тому максимально рівномірне покриття усього частотного діапазону 5-6ГГц потребує додаткового вирішення;
– Розроблення методики щодо швидкої і найменш ресурсомісткої оцінки співвідношення потужностей між сигналами відео та керування. Проведені експерименти показали, що запропонована у Розділі 3 таблиця співвідношення потребує коригування. На це вказує той факт, що кожен VTX може мати різні набори потужностей, відповідно необхідне налаштування на кожен із таких наборів.

ВИСНОВКИ

В роботі вирішено важливу науково-прикладну задачу щодо підвищення захищеності та відмовостійкості процесів передачі інформації у бездротових системах, в контексті сучасного застосування цивільних засобів у завданнях військового та подвійного призначення, що зокрема дозволяє забезпечити можливість роботи засобів зв’язку та дистанційного керування безпілотними пристроями в умовах активного електромагнітного протиборства (в тому числі і за допомогою засобів радіо-електронної боротьби).

Зроблений у роботі аналіз сучасного стану розвитку і впровадження бездротових систем у різні застосунки забезпечив можливість здійснення оцінки та відбору найбільш критично чутливих до стану зв’язку застосування таких систем. З’ясовано, що захист бездротових систем комунікації та керування безпілотних пристроїв на даний час є найбільш актуальним і гострим питанням, яке диктується їх стрімким поширенням, та збільшенням функцій і завдань, які вони можуть виконувати.

Особливу увагу у роботі приділено військовій сфері, оскільки під час захисту нашої держави від нападу агресора, ширина фронту і розміри зони бойових дій призвели до того, що з’явилася сучасна тенденція масового використання у військових операціях та військових діях цивільних засобів зв'язку та керування, в тому числі і масового використання засобів безпілотної авіації цивільного походження. Таке застосування безпілотних пристроїв зумовлює необхідність у значно жорсткіших вимогах до їхнього захисту аніж ті, які у них забезпечені виробником чи розробником.

Запропоноване нами у роботі вдосконалення методики оцінки захищеності інформаційних та кіберфізичних систем дозволило обґрунтовано застосовувати критерій просторового переміщення для оцінки захищеності безпілотних систем та систем, здатних до самостійного переміщення, і надало теоретичну основу для застосування принципово відмінних засобів захисту (зокрема,

засобів щодо забезпечення високої доступності та відновлюваності зв’язку).

У роботі розроблено моделі і алгоритми для захисту бездротових систем безпілотних пристроїв, які дозволили підвищити "живучість" системи керування та системи відео-зв’язку в умовах активного протиборства, що дозволяє суттєво зменшити втрати обладнання через функціонування ворожих засобів придушення.

Завдяки результатам проведеного аналізу та дослідження можливостей базових елементів, використовуваних у сучасних рішеннях БПЛА, реалізована комплексна система заходів захисту повною мірою реалізовує обрану для роботи концепцію: "оптимальний захист за оптимального рівня затрат". Це забезпечується, насамперед, використанням для побудови алгоритмів роботи МК механізмів переривань від таймерів та зміни стану вхідних портів. Завдяки цьому мікроконтролер понад 50% часу знаходиться у режимі зниженого енергоспоживання і виконує свої функції під час "прокидання" від переривань.

Другий чинник, що зумовлює високу ефективність пропонованих засобів захисту та їхньої реалізації – "менторський" режим роботи мікроконтролера. Пропоновані методи не потребують необхідності зміни деталей чи заміни компонентів БПЛА. Методи захисту реалізовуються шляхом керування необхідними характеристиками самих використовуваних у схемі пристрою передавачів та контролерів шляхом використання їхніх програмних інтерфейсів.

Реалізовані у вищеописаних пунктах підходи до впровадження запропонованих заходів захисту надають ще одну перевагу: зосередження управління функціоналом системи захисту у вбудованій системі (мікроконтролер) і побудова його на властивостях власних компонентів БПЛА дозволили забезпечити можливість впровадження даних заходів захисту не лише на етапі проектування та виготовлення, але й на етапі функціонування. Тому навіть існуючий пристрій, який вже виконує свої функції, можна забезпечити запропонованими засобами захисту шляхом досить не складної модернізації (зміна деяких налаштувань і встановлення у апарат запрограмованого мікроконтролера). Така модернізація може проводитися

навіть у "польових" умовах.

Проведені нами експериментальні дослідження розроблених методів захисту та способів їх практичної реалізації дали позитивні і дещо неочікувані результати, адже значення певних отриманих параметрів перевершили значення, які були прогнозовані. Тобто, окрім покращення захисту інформації у бездротових системах БПЛА за рахунок самого факту забезпечення можливості впровадження пропонованих методів захисту, було також виявлено, що деякі пристрої мають можливість "виходити" за рамки своїх задокументованих характеристик та надавати додаткові можливості щодо покращення захищеності за рахунок їх програмного зовнішнього керування.

Зокрема, використання протоколу SmartAudio для керування VTX мало забезпечити можливість перемикання частоти із періодом 150 мс та більше. Але експерименти показали, що використана у лабораторному макеті мікросхема працює більш як вдвічі швидше і дозволяє здійснювати стабільну зміну частоти кожних 80мс.

Позитивний результат було отримано при дослідженні характеристик перемикання частотних каналів: очікувалося перемикання у межах базових 40-ка каналів. Але в експерименті було виявлено, що функція Set_Frequency протоколу SA дозволяє відходити як і від табличних значень частот каналу, так і взагалі за рамки передбаченого документацією діапазону. Для дослідженої мікросхеми відеопередавача отриманий результат діапазону допустимих частотних переналаштувань становив 5000-6000 МГц (замість очікуваного 5650-5950 МГц).

Щодо запропонованого у роботі методу забезпечення захисту системи зв’язку і керування БПА шляхом його повернення із зони придушення засобів противника, можна також підсумувати, що практичні експерименти із реалізованим алгоритмом відслідковування і запису пройденого шляху продемонстрували його високу ефективність та точність.

Згідно методики проведеного експерименту було здійснено "обліт" запропонованої та розробленої системи захисту на базі БПЛА типорозміром 3.5

дюйми на майданчику 40х40 метрів за двома маршрутами: прямолінійний (протяжністю 30 м) та маршрут із кривою (протяжністю 71.42 м).

За результатами експерименту із випробування системи відстеження та відновлення робимо висновок, що з точки зору точності найоптимальнішим є використання набору метрик акселерометр (3 осі) + гіроскоп (3 осі). Даний набір показав високу точність (похибка відстеження прямолінійного польоту і маршруту з кривою складає 0.6% і 0.56% відповідно) і високу стійкість до впливу на апарат поривів вітру та інших перешкод (похибка зросла лише до 0.833% та 0.686% відповідно). Разом з тим, такий набір вимагає більшого обчислювального ресурсу – кожне із отриманих значень давача потребує обчислення подвійного інтегралу для перетворення значення у розмірність відстані в метрах. Якщо для гіроскопа обмежити набір осей до одної (вісь рискання) можна значно зменшити кількість обчислень. При цьому ми отримуємо зменшення точності, але вона все ще залишається прийнятною, оскільки похибка зростає із 0.833% до 1.267% для прямолінійного польоту.

Використання таких метрик, як покази магнітометра та барометричного висотоміра нами не рекомендується. Барометричний висотомір має низьку точність (похибка прямолінійного польоту складає 14.83%) і невисоку стійкість до вітру (за наявності вітру похибка зростає аж до 27.97%). Магнітометр має досить високу точність (похибка для прямого і маршрутного польотів складає 1.3% і 1.82% відповідно). Але він має низьку стійкість до електромагнітних завад та впливу масивних об’єктів-феромагнетиків (у електромагнітному полі похибка зростає аж до 54.5%).

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Vasylkivskyi , M., Nikitovych , D., Boldyreva , O., & Yakubivska , N. (2023). Intelligent technologies for adjusting the physical layer of mobile networks. COMPUTER-INTEGRATED TECHNOLOGIES: EDUCATION, SCIENCE, PRODUCTION, (51), 148-160. DOI: 10.36910/6775-2524-0560-2023-51-19.
2. Вишневский В. М. Энциклопедия Wi MAX: Путь к 4G /В.М. Вишневский, С.Л. Портной, И.В. Шахнович / – М.: Техносфера. – 2009. 472с.
3. І.В. Бурляй. Системи радіозв'язку та їх застосування оперативно-рятувальною службою / І.В. Бурляй, Б.Б. Орел, О.М. Джулай: Посібник. Чернігів: РВК "Деснянська правда", – 2007. – 288 с.
4. О.М. Ляшук. MHED – Високоефективний метод захисту даних на основі багатошарового гібридного шифрування. Вісник Національного технічного університету України "КПІ". 2014. Вип. 56. – С. 144-151.
5. Д.А. Гриб. Принципи, методи і технології ведення збройної боротьби, управління силами і засобами в умовах активного інформаційного протиборства конфліктуючих сторін / Д.А. Гриб, Б.О. Демідов, Ю.Ф. Кучеренко, А.М. Ткачов, Т.В. Кулєшова // Наука і техніка Повітряних Сил Збройних Сил України. – 2019. – Том 1, № 43. – С. 12-22.
6. Мао В. Современная криптография: теория и практика / В. Мао. – М. : Видавничий дім "Вільямс". – 2005. – 763
7. Худавердова А.О. Інформаційна війна сьогодення та можливі методи боротьби. Інформаційна агресія Російської Федерації проти України : матеріали наук. семінару ХНУ ПС ім. І.Кожедуба, 21.10.2020. Харків : ХНУ ПС ім. І.Кожедуба, – 2020. – С. 1-5.
8. Шишацький, А.В. Системи радіозв’язку з псевдовипадковим переналаштуванням робочої частоти / А.В. Шишацький, О.В. Кувшинов // Наука і техніка Повітряних Сил Збройних Сил України. – 2016. – № 4 (25). – С. 117-121.

9. М.Д. Ільїнов, Т.Г. Гурський, І.В. Борисов, К.М. Гриценок. Лінії радіозв'язку та антенні пристрої : навч. посіб. Київ : Військовий інститут телекомунікацій та інформатизації, – 2018. – 249 с.
10. С.А. Іваненко. Визначення незайнятих частотних каналів у когнітивних радіомережах методами виявлення та розпізнавання сигналів в умовах апріорної невизначеності : дис. канд. Техн. наук. : 05.12.17 / Харківський національний університет радіоелектроніки. Харків, – 2019. – 156 с.
11. Л.М. Карпуков, О.В. Щекотихін, Д.К. Савченко. Удосконалений спосіб та пристрій маскування конфіденційної інформації. Радіотехнічні поля, сигнали, апарати та системи : матеріали Міжнар. наук.-практ. Конф. Запоріжжя : ЗНТУ, – 2019. – С. 213-215.
12. Телекомунікаційні та інформаційні мережі : Підручник [для вищих навчальних закладів] / П.П. Воробієнко, Л.А. Нікітюк, П.І. Резніченко. – К.: САММІТ-Книга, – 2010. – 708 с.
13. Згуровський М.З., Сергієнко І.В. Інформаційні технології у сучасному суспільстві // Вісник НАН України. – 2000. – №12. – С. 9-16.
14. Довгий С.О., Савченко О.Я., Воробієнко П.П. та ін. Сучасні телекомунікації: мережі, технології, економіка, управління, регулювання / За ред. С.О. Довгого. – К.: Український Видавн. Центр, – 2002. – 520 с.
15. Dudykevych V., Mykytyn G., Kuten R., Halunets M. The security features of wireless networks of intellectual transport system // Захист інформації і безпека інформаційних систем : матеріали VIII Міжнародної науково-технічної конференції, 11-12 листопада, – 2021, Львів. – 2021.
16. Дудикевич В. Б., Микитин Г. В., Кутень Р. Б., Сидорик Д. О. Комплексна модель безпеки інтелектуальної кіберфізичної транспортної системи // Інформаційна безпека та інформаційні технології : збірник тез доповідей VI Всеукраїнської науково практичної конференції молодих учених, студентів і курсантів, м. Львів, 30 листопада 2023 року. Львів. – 2023.
17. М.З. Згуровський, Ю.І. Якименко, В.І. Тимофєєв. Інформаційні мережеві технології в науці і освіті. System Research & Information Technologies. №3. –

2002. – С 43-56.

18. Наміот, Д. Є. Розумні міста 2016 /Д.Е. Наміот // International Journal of Open Information Technologies. – 2016. – Т.4. – №.1. – С. 1-3.
19. Дудикевич В. Б., Микитин Г. В., Галунець М. О., Кутень Р. Б. Безпека комунікаційного середовища кіберфізичної системи інтелектуального моніторингу повітря // Сучасні методи, інформаційне, програмне та технічне забезпечення систем керування організаційно-технічними та технологічними комплексами : матеріали IX Міжнародної науково-технічної Internet-конференції (Київ, 25 листопада 2022 р.). – 2022.
20. Згуровський М.З., Сергієнко І.В. Стан та перспективи розвитку інформаційних технологій в Україні // Матеріали Міжнародного конгресу "Інформаційне суспільство в Україні – стан, проблеми, перспектива" (Київ, 25–27 вересня 2000 року). – К.: НТУУ "КПІ", – 2000. – С. 29-37.
21. Дудикевич В. Б., Микитин Г. В., Галунець М. О., Кутень Р. Б. Кіберфізична система "розумний дім": структура – загрози – безпека // Інформаційна безпека та інформаційні технології : збірник тез доповідей IV Міжнародної науково-практичної конференції, ІБІТ 2022, м. Львів, 30 листопада 2022 року. – 2022.
22. International Telecommunication Union. Trends in Telecommunication Reform 2016: Regulatory Incentives to Achieve Digital Opportunities. [Електронний ресурс]. – Режим доступу: https://digitalregulation.org/wp-content/uploads/Compil_Trends16-E-web.pdf.
23. Challoo, R. An overview and assessment of wireless technologies and co existence of ZigBee, Bluetooth and Wi-Fi devices / R. Challoo, A. Oladeinde, N. Yilmazer, S. Ozcelik, L. Challoo // Procedia Computer Science. – 2012. – Т. 12. – С.386-391.
24. Lee, JS "A comparative study of wireless protocols: Bluetooth, UWB, ZigBee, and Wi-Fi "/ JS Lee, YW Su, CCA Shen // Industrial Electronics Society, 2007. IECON 2007. 33rd Annual Conference of the IEEE. – IEEE, – 2007. – С.46-51.
25. Чистяков, В. А. Аналіз технологій бездротової передачі даних / Б. Є.

Миктибаев, А. Б. Жанбеков // Журнал наукових і прикладних досліджень. – 2016. – №1. – С. 166-169.

26. Вишневський, В.М. Широкосмугові бездротові мережі передачі інформації / В.М. Вишневський, А.І. Ляхов, С.Л. Кравець, І.В. Шахновіч // М .: Техносфера, – 2005. – 591с.
27. Свердлова, А. А. Огляд сучасних технологій бездротового зв'язку / А. Ю. Шмирін, С. В. Яковлєв С. В. // Студентська наука для розвитку інформаційного суспільства. Збірник матеріалів III Науково-технічної конференції. – 2015. – С. 92-94.
28. Джим, Г. Бездротові мережі. Перший крок (Cisco) / Джим Гейер // М .: Вільямс, – 2005. – 192 с.
29. Беделл, П. "Мережі. Бездротові технології "/ П. Беделл // М .: НТ Пресс, – 2008. – 448с.
30. Стрельников, А. Ю. Технологія бездротової передачі даних Wi-Fi / С. А. Страмоусова // Молодий вчений. – 2016.- №9-4 (113). – С. 67-69.
31. S. Aust, R. V. Prasad and I. G. M. M. Niemegeers, "IEEE 802.11ah: Advantages in standards and further challenges for sub 1 GHz Wi-Fi," 2012 IEEE International Conference on Communications (ICC), Ottawa, ON, Canada, 2012, pp. 6885-6889. DOI: 10.1109/ICC.2012.6364903.
32. Кабінет Міністрів України. "НАЦІОНАЛЬНА ТАБЛИЦЯ розподілу смуг радіочастот України". Затверджено постановою №1208 від 15.12.2005. [Електронний ресурс]. – Режим доступу: https://www.kmu.gov.ua/npas/25976178.
33. OFCOM. IR2030 – UK Interface Requirements. Licence Exempt Short Range Devices (SRDs). 2023. [Електронний ресурс]. – Режим доступу: https://www.ofcom.org.uk/__data/assets/pdf_file/0028/84970/ir-2030.pdf.
34. European Union. Comission Implementing Decision. "Amending Decision 2006/771/EC on harmonisation of the radio spectrum for use by short-range devices and repealing Decision 2005/928/EC". 2013. [Електронний ресурс]. – Режим доступу: http://data.europa.eu/eli/dec_impl/2013/752/oj.

35. Юн Х. М., Мединський Д. В. Використання безпілотних літальних апаратів в сільському господарстві. Високотехнологічні технології. 2017. № 4(36). С. 335-341. DOI: 10.18372/2310-5461.36.12232.
36. Лещенко Г. А., Мандрик Я. С., Стратонов В. М., Давидов С. А. Методи використання безпілотних літальних апаратів під час авіаційного пошуку та рятування. Високотехнологічні технології. 2021. № 3(51). С. 271-280. DOI: 10.18372/2310-5461.51.15998.
37. Глотов В., Гуніна А. Аналіз можливостей використання безпілотних літальних апаратів для аерофотозйомки. Сучасні досягнення геодезичної науки та виробництва. – 2014. № 2. – С. 65-70.
38. Є.А. Дружинін, М.І. Ковалевський, О.К. Погудіна, В.О. Черановський. Методи та інформаційні технології впровадження безпілотних літальних апаратів в повітряний простір України. Збройні системи та військова техніка. – 2021. № 4(68). – С. 84-90. DOI: 10.30748/soivt.2021.68.12.
39. Кутень Р., Ахмедова А. Підвищення рівня захищеності та життєздатності безпілотних авіаційних пристроїв // Безпека інформації. – 2024. – Т. 30, № 1. – С. 88–94. DOI: 10.18372/2225-5036.30.18609.
40. Слободяник С., Петренко С., Цибізов А., Бондаренко Ю. Можливі шляхи розвитку перспективних українських систем БПЛА, з урахуванням сучасних світових тенденцій. Журнал наукових статей "Соціальний розвиток та безпека", Том. 13, № 3, – 2023. С. 135-145. DOI: 10.33445/sds.2023.13.3.9.
41. Д. В. Стасенко, В. С. Яковина. Аналіз існуючих методів та засобів поліпшення навігації БПЛА за допомогою штучного інтелекту. Науковий вісник НЛТУ України. – 2023. Том. 33, № 4. – С. 78-83. DOI: 10.36930/40330411.
42. Бовда Е. М. Сучасні підходи в побудові системи управління інформаційно-телекомунікаційними мережами військового призначення / Бовда Е. М., Романюк В. А., Бовда В. Е. // ВІТІ. – 2021. – №6. –С. 20-29. [Електронний ресурс]. – Режим доступу: https://journal.viti.edu.ua/public/romanuk/2021/6_2021.pdf.

43. Бовда Е. М. Концептуальні основи синтезу автоматизованої системи управління зв'язком військового призначення / Е. М. Бовда, Ю. А. Плуговий, В. А. Романюк. // ВІТІ. – 2016. – №1. – С. 3–17. [Електронний ресурс]. – Режим доступу: https://www.viti.edu.ua/files/rom/2016/1_2016.pdf.
44. Скрынникова Н.С. Зарубежный опыт борьбы с терроризмом: механизмы противодействия / Н.С. Скрынникова //Науковий вісник Ужгородського національного університету. – 2014. – No 28(3). – С. 37-40.
45. Пермяков О.Ю. Інформаційно – телекомунікаційні технології і сучасна збройна боротьба / О.Ю. Пермяков,Н.О. Королюк // Збірник матеріалів науково-технічної конференції молодих учених "Актуальні проблеми інформацій-них технологій". – Київ, 20-21 листопада 2018 р. – С. 5-6.
46. Романюк В.А. Цільові функції оперативного управління тактичними радіомережами /В.А. Романюк// Збірник наукових праць ВІТІ НТУУ "КПІ". – 2012. – № 1. – С. 109 – 117. [Електронний ресурс]. – Режим доступу: https://www.viti.edu.ua/files/rom/2012/3_2012.pdf.
47. Міщенко Анатолій, Шишацький Андрій, Бондаренко Тетяна, Бігун Наталія, Ляшенко Ганна. Аналіз використання сучасних технологій радіозв'язку у збройних силах провідних країн світу. Системи обробки інформації. 2019. № 4(159). С. 50-57. DOI: 10.30748/soi.2019.159.06.
48. Попов А.О. Загальні тенденції розвитку засобів радіоелектронної боротьби / А.О. Попов, В.В. Твердохлібов //Озброєння та військова техніка. – 2014. – No 4(4). – С. 4-17
49. Методика оцінки стійкості системи військового зв'язку / М.О. Масесов, І.О. Бондаренко, О.І. Садиков,В.І. Макарчук // Збірник наукових праць Військового інституту телекомунікацій та інформатизації. – 2016. – No 1. – С. 94-102.
50. Якобінчук О.В. Методика оцінки розвідзахищеності системи зв'язку / О.В. Якобінчук // Труди академії. – 2009. –No 1(88). – С. 284-293.
51. Якобінчук О.В. Методика оцінки завадозахищеності системи зв'язку, радіотехнічного забезпечення та автоматизації управління / О.В. Якобінчук

// Системи озброєння і військова техніка. – 2009. – No 1(17). – С. 144-146.

52. Юхновський С.А. Часткова методика оцінки відповідності системи зв'язку потребам визначеної системи управління протиповітряною обороною / С.А. Юхновський, О.П. Кулик, І.Л. Костенко // Наука і техніка Повітряних Сил Збройних Сил України. – 2017. – No 2(27). – С. 124-126. DOI: 10.30748/nitps.2017.27.24.
53. Боговик А.В. Эффективность системы военной связи и методы ее оценки / А.В. Боговик, В.В. Игнатов. – СПб:Военная академия связи, 2006. – 183 с.
54. Заславець В.П., Долина М.П., Чечуй О.В. Особливості розрахунку завадозахищеності ліній радіозв'язку в умовах радіоподавлення (радіоелектронного конфлікту). Системи озброєння і військова техніка. 2020. № 1(61). С. 7-12. DOI: 10.30748/soivt.2020.61.01.
55. Кізло Л., Троценко О., Жук. О. Тенденції розвитку безпілотних літальних апаратів в Україні. Українські військові сторінки. – 2021. Доступно за адресою: https://www.ukrmilitary.com/2021/05/uav.html (Дата звернення: 17 лютого 2024).
56. Окупаційні війська на сході України активно використовують новітні російські засоби РЕБ та РЕР. Повідомлення Головного управління розвідки Міністерства Оборони України. [Електронний ресурс]. Режим доступу: https://gur.gov.ua/content/okupatsiini-viiska-na-skhodi-ukrainy-aktyvno-vykorystovuiut-novitni-rosiiski-zasoby-reb-ta-rer.html.
57. Організація захисту інформації з обмеженим доступом : підручник / А.М.Гуз, О.Д.Довгань, А.І.Марущак та ін.. ; за ред. Є.Д.Скулиша. – К. : Наук.- вид. відділ НА СБ України , 2011. – 376 с.
58. Юрчак Олександр. Українська стратегія Індустрії 4.0 – 7 напрямів розвитку. – [Електронний ресурс]. – Режим доступу: https://industry4-0-ukraine.com.ua/2019/01/02/ukrainska-strategiya-industrii-4-0-7-napriankiv-rozvutku/.
59. Інформаційні технології. Взаємозв'язок відкритих систем. Базова еталонна модель. Частина 1. Базова модель. (ISO/IEC 7498-1:1994, IDT) : ДСТУ

ISO/IEC 7498-1:2004. – [Чинний від 2015-08-21]. – К. : Держспоживстандарт України, 2015. 67 с. – (Національний стандарт України).

60. Б. Я. Корнієнко. Дослідження моделі взаємодії відкритих систем з погляду інформаційної безпеки. Наукоємні технології, 2012. № 3 (15). – С. – 83-89.
61. Дудикевич В. Б., Микитин Г. В., Кутень Р. Б., Галунець М. О. До питання безпеки безпровідних мереж на основі моделі OSI // Сучасні методи, інформаційне, програмне та технічне забезпечення систем керування організаційно-технічними та технологічними комплексами: матеріали VIII Міжнародної науково-технічної Internet-конференції (Київ, 26 листопада 2021 року). – 2021. – С. 201.
62. Дудикевич В. Б., Микитин Г. В., Галунець М. О., Кутень Р. Б., Васильєв Д. В., Бабенцов Г. А. Багаторівневий захист технологій функціонування інтелектуальних обєктів // Стан, досягнення та перспективи інформаційних систем і технологій : матеріали XXI Всеукраїнської науково-технічної конференції молодих вчених, аспірантів та студентів (Одеса, 21-22 квітня 2022 р.). – 2022.
63. FIPS. Advanced Encryption Standard (AES). National Institute of Standards and Technology. Gaithersburg. 2023. 46 p. DOI: 10.6028/NIST.FIPS.197-upd1.
64. Технології захисту інформації в інформаційно-телекомунікаційних системах : навч. посіб. / А. В. Жилін, О. М. Шаповал, О. А. Успенський ; ІСЗЗІ КПІ ім. Ігоря Сікорського. – Київ : КПІ ім. Ігоря Сікорського, Вид-во "Політехніка", 2021. – 213 с.
65. Akyildiz, Ian F., Weilian Su, Yogesh Sankarasubramaniam, Erdal Cayirci. Wireless sensor networks: a survey. Computer networks, 2002. №4(38). – P. 393-422.
66. Машталір В. В., Жук О. В., Міненко Л. М., Артюх С. Г. Концептуальні підходи застосування бездротових сенсорних мереж арміями передових країн світу. Сучасні інформаційні технології у сфері безпеки та оборони. 2023. №2(47). – С. 96-112. DOI: 10.33099/2311-7249/2023-47-2-96-112.
67. Jain, Usha & Hussain, Muzzammil. Securing Wireless Sensors in Military

Applications through Resilient Authentication Mechanism. Procedia Computer Science. 2020. – P. 719-728. DOI: 10.1016/j.procs.2020.04.078.

68. Боротьба з безпілотними літальними апаратами (за досвідом проведення ООС (раніше АТО)): Методичні рекомендації – м. Житомир, вул. Велика Бердичівська, 17а, 2019. – С.48.
69. Коробейнікова Т., Цар О. Аналіз сучасних відкритих систем виявлення та запобігання вторгнень. Grail of Science. 2023. – С. 317-325. DOI: 10.36074/grail-of-science.12.05.2023.050.
70. Romanova A., Toliupa S. Perspective steganographic solutions and their application //Proceedings of the VII Inter University Conference Engineer of XXI Century. – 2017. – T. 2. – C. 269-278.
71. Malathi, P., & Gireeshkumar, T. Relating the embedding efficiency of LSB steganography techniques in spatial and transform domains. Procedia Computer Science. 2016. №93. – С. 878–885.
72. Hussain, M., Wahab, A. W. A., Idris, Y. I. B., Ho, A. T. S., & Jung, K.-H. Image steganography in spatial domain: A survey. Signal Processing: Image Communication. 2018. №65. – С. 46-66.
73. Wang, Zhongpeng, Chen, Fangni, Qiu, Weiwei, Chen, Shoufa, Ren, Dongxiao. A two layer chaotic encryption scheme of secure image transmission for DCT precoded OFDM-VLC transmission. Optics Communications. 2018. №410. – С. 94-101.
74. Eyssa A.A., Abdelsamie F.E., Abdelnaiem A.E. Ефективний підхід до стеганографії зображень у системі бездротового зв’язку. Wireless Pers Commun. 2020. №110. – С. 321–337 DOI: 10.1007/s11277-019-06730-2.
75. Karpenko A., Bondarenko T., Ovsiannikov V., Martyniuk V. Забезпечення інформаційної безпеки в бездротових сенсорних мережах. Електронне фахове наукове видання "Кібербезпека: освіта, наука, техніка". 2020. №2(10). – С. 54-66. DOI: 10.28925/2663-4023.2020.10.5466.
76. NAI Labs. Constraints and approaches for distributed sensor network security". 2000. Tech. Report №00-010.

77. M. O. Rabin. Digitalized Signatures and Public-Key Functions as Intractable as Factorization. 1979. Tech. Rep.: Cambridge. MA.
78. Y. W. Law, J. M. Doumen, and P. H. Hartel. Benchmarking Block Ciphers for Wireless Sensor Networks (Extended Abstract). 2004. Proceedings 1st IEEE Int'l. Conf. Mobile Ad-hoc and Sensor Systems. IEEE Computer Society Press.
79. Karlof C., Wagner D. Secure routing in wireless sensor networks: attacks and countermeasures. Ad Hoc Networks. 2003. Vol. 1, no. 2-3. P. 293-315. DOI: 10.1016/s1570-8705(03)00008-8.
80. Батаєв О.П., Ковтун І.В., Корольова Н.А. Теорія електричного зв’язку: Навч. посібник. – Харків: УкрДАЗТ, 2010. – 630 с.
81. Семеренко В.П., Ткачук В.В. завадостійке кодування у квантових комп'ютерах. Збірник мат-лів XLIX наукової технічної конференції Вінницького Національного Технічного Університету (ВНТУ). 27-28 Квітня. 2020. – Вінниця. [Електронний ресурс]. Режим доступу: https://ir.lib.vntu.edu.ua//handle/123456789/29541.
82. YouTube©. Що повинен знати пілот дрону про прошивки, аероскопи, небезпеки та наслідки на фронті. Інформаційне відеозведення від бійця із позивним "Мадяр". [Електронний ресурс]. Режим доступу: https://www.youtube.com/watch?v=z2UsrGprdCw.
83. YouTube©. 10 тупих запитань АЕРОРОЗВІДНИКУ | Інтерв'ю з Тарасом Білкою. Інтерв'ю бійця каналу ISLND TV. [Електронний ресурс]. Режим доступу: https://www.youtube.com/watch?v=BgooPpioa4A.
84. DJI™ Digital FPV System Manual. [Електронний ресурс]. Режим доступу: https://dl.djicdn.com/downloads/DJI_Digital_FPV_System/20221208/DJI_Digital_FPV_System_User_Manual_EN.pdf.
85. Дудикевич В. Б., Микитин Г. В., Кутень Р. Б., Галунець М. О. Шифрування повідомлень в безпровідних мережах на основі алгоритму "Калина" // Інформаційна безпека та інформаційні технології : збірник тез доповідей V Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів (Львів, 26 листопада 2021 р.). – 2021.

86. Дудикевич В., Собчук І., Ракобовчук Л., Кутень Р. Легковаговагове шифрування для захисту даних RFID-міток // Захист інформації і безпека інформаційних систем: матеріали V Міжнар. наук.-техн. конф. – 2016.
87. Кутень Р. Застосування частотного переналаштування для захисту безпілотних літальних апаратів // Social Development and Security. – 2024. – Vol. 14, No. 2. – P. 64–73. DOI: 10.33445/sds.2024.14.2.7.
88. TBS CROSSFIRE R/C System: Adaptive Long-Range Remote-Control System User Manual. 2022. 88 С. [Електронний ресурс]. Режим доступу: https://www.team-blacksheep.com/media/files/tbs-crossfire-manual.pdf.
89. І.М.Козубцов, Л.М.Козубцова, В.В.Куцаєв, Т.П.Терещенко. Методика оцінки кібернетичної захищеності системи зв'язку організації. Modern Information Technologies in the Sphere of Security and Defence. № 1(31). 2018. – С. 43-46.
90. А. О. Зінченко, Р. В. Пікуль, К. А. Зінченко,…, Ю. І. Риндін. Методичний підхід з оцінки ефективності системи зв'язку спеціального призначення. Системи управління навігації та зв'язку. №1(59). – 2020. – С. 132-136. DOI: 10.26906/SUNZ.2020.1.132.
91. Козубцова Л.М. Удосконалена методика діагностування кібернетичної захищеності інформаційної системи з урахуванням деструктивних кібернетичних впливів. Комп'ютерно-інтегровані технології: освіта, наука, виробництво. №39. – 2020. – С. 127-135. DOI: 10.36910/6775-2524-0560-2020-39-22.
92. Ярощук І.В. Оцінка ризиків кіберфізичних систем на базі мікроконтролерів типу Arduino : кв. роб. магістр : 6.125 Тернопіль, 2020. 69с.
93. Димова, Г. О., & Ларченко, О. В. (2023). Обернені задачі аналізу нерегульованого об'єкта. Таврійський науковий вісник. Серія: Технічні науки, (6), 37-41. DOI: 10.32851/tnv-tech.2022.6.5.
94. Кутень Р.Б., Синявський О.Ю. Методи і засоби забезпечення стабільності та захисту радіозв'язку в умовах складної електромагнітної обстановки. Комп'ютерні системи та мережі. – 2024. №1(6). – С. 99-107. DOI: 10.23939/csn2024.01.099.

95. TBS Unify Pro / SmartAudio: User Manual. – 2018. 10 С. [Електронний ресурс]. Режим доступу: https://www.team-blacksheep.com/media/files/tbs_smartaudio_rev09.pdf.
96. SpeedyBee®. F405 V3 BLS 50A 30x30 Stack. User Manual. V1.0. 16 С. [Електронний ресурс]. Режим доступу: https://store-fhxxhuiq8q.mybigcommerce.com/product_images/img_SpeedyBee_F405_V3_Stack/SpeedyBee_f405_v3_stack_manual_en.pdf.
97. Дудикевич В. Б., Микитин Г. В., Галунець М. О., Кутень Р. Б., Ракочий В. І. Елементи безпеки провідних мереж на основі витої пари // Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення : збірник тез доповідей Міжнародної наукової інтернет-конференції (Тернопіль, 6-7 квітня 2022 р.). – 2022.

ДОДАТОК А.

Список публікацій здобувача та відомості про апробацію

Наукові праці, в яких опубліковано наукові результати дисертації:

1. Кутень Р. Застосування частотного переналаштування для захисту безпілотних літальних апаратів // Social Development and Security. – 2024. – Vol. 14, No. 2. – P. 64-73. DOI: 10.33445/sds.2024.14.2.7.
2. Кутень Р., Ахмедова А. Підвищення рівня захищеності та життєздатності безпілотних авіаційних пристроїв // Безпека інформації. – 2024. – Т. 30, № 1. – С. 88-94. DOI: 10.18372/2225-5036.30.18609.
3. Кутень Р.Б., Синявський О.Ю. Методи і засоби забезпечення стабільності та захисту радіозв'язку в умовах складної електромагнітної обстановки. Комп'ютерні системи та мережі. – 2024. №1(6). – С. 99-107. DOI: 10.23939/csn2024.01.099.

Наукові праці, які засвідчують апробацію матеріалів дисертації:

4. Дудикевич В. Б., Микитин Г. В., Кутень Р. Б., Галунець М. О. До питання безпеки безпровідних мереж на основі моделі OSI // Сучасні методи, інформаційне, програмне та технічне забезпечення систем керування організаційно-технічними та технологічними комплексами : мат-ли VIII Міжн. н.-т. Internet-конф. (Київ, 26 листопада). – 2021.
5. Дудикевич В. Б., Микитин Г. В., Кутень Р. Б., Галунець М. О. Шифрування повідомлень в безпровідних мережах на основі алгоритму "Калина" // Інформаційна безпека та інформаційні технології : збірник тез доповідей V Всеукраїнської н.-практ. конф. молодих учених, студентів і курсантів (Львів, 26 листопада). – 2021.
6. Dudykevych V., Mykytyn G., Kuten R., Halunets M. The security features of wireless networks of intellectual transport system // Захист інформації і безпека інформаційних систем : матеріали VIII Міжнародної науково-технічної конференції, 11-12 листопада, 2021, Львів. – 2021.
7. Дудикевич В. Б., Микитин Г. В., Галунець М. О., Кутень Р. Б. Кіберфізична система "розумний дім": структура – загрози – безпека // Інформаційна

безпека та інформаційні технології : збірник тез доповідей IV Міжнародної науково-практичної конференції, ІБІТ 2022, м. Львів, 30 листопада 2022 року. – 2022.

8. Дудикевич В., Собчук І., Ракобовчук Л., Кутень Р. Легковаговагове шифрування для захисту даних RFID-міток // Захист інформації і безпека інформаційних систем: матеріали V Міжнар. наук.-техн. конф. – 2016.

Інші публікації, що додатково відображають результати дисертації:

9. Дудикевич В. Б., Микитин Г. В., Галунець М. О., Кутень Р. Б., Ракочий В. І. Елементи безпеки провідних мереж на основі витої пари // Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення : збірник тез доповідей Міжнародної наукової інтернет-конференції (Тернопіль, 6-7 квітня 2022 р.). – 2022.
10. Дудикевич В.Б., Микитин Г.В., Галунець М.О., Кутень Р.Б., Васильєв Д.В., Бабенцов Г.А. Багаторівневий захист технологій функціонування інтелектуальних обєктів. Досягнення та перспективи інформаційних систем і технологій : мат-ли XXI Всеукр. н.-т. конф. молодих вчених, аспірантів та студентів (Одеса, 21-22 квітня). – 2022.
11. Дудикевич В.Б., Микитин Г.В., Кутень Р.Б., Сидорик Д.О. Комплексна модель безпеки інтелектуальної кіберфізичної транспортної системи // Інформаційна безпека та інформаційні технології : збірник тез доповідей VI Всеукр. н.-практ. конф. молодих учених, студентів і курсантів, (м. Львів, 30 листопада). – 2023.
12. Дудикевич В.Б., Микитин Г.В., Галунець М.О., Кутень Р.Б. Безпека комунікаційного середовища кіберфізичної системи інтелектуального моніторингу повітря // Сучасні методи, інформаційне, програмне та технічне забезпечення систем керування організаційно-технічними та технологічними комплексами : матеріали IX Міжнародної науково-технічної Internet-конференції (Київ, 25 листопада 2022 р.). – 2022.

ДОДАТОК Б. Акти впровадження

ЗАТВЕРДЖУЮ
Проректор з наукової роботи
Національного університету
«Львівська політехніка»
проф. _____ Іван ДЕМИДОВ
"06" _____ 2024 р.

АКТ
про використання результатів дисертаційної роботи
Кутеня Романа Богдановича
«Покращення захисту інформації при передачі бездротовими системами»
представленої на здобуття наукового ступеня доктора філософії за спеціальністю 125 – *Кібербезпека*

Комісія у складі – голови начальника науково-дослідної частини, д.т.н., ст. досл. Небесного Р.В. та членів: завідувача кафедри захисту інформації, д.т.н, професора Опірського І.Р., завідувача відділу науково-організаційного супроводу наукових досліджень, к.т.н. Лазько Г.В. і в.о. заступника начальника планово-фінансового відділу Фаст І.І., цим актом підтверджують, що результати дисертаційної роботи Кутеня Р. Б., використовувалися у відповідності до наукового напряму кафедри захисту інформації Національного університету "Львівська політехніка" - "Дослідження систем технічного захисту інформації, каналів зв'язку та комп'ютерних мереж, фізичного захисту інформації та криптографії.", в межах кафедральної науково-дослідної роботи: "Розроблення та удосконалення методів і засобів захисту інформації для протидії несанкціонованому доступу в інформаційно-комунікаційних мережах" (шифр ЗІ-7) (№ держреєстрації 0119U101690) (2019р.-2022р.);).

Кутень Р.Б. розробив метод забезпечення високої доступності бездротових систем зв'язку і керування здатних до переміщення, з використанням системи інерційного запису координат, на основі даних BlackBox. Цей метод включає в себе математичний апарат для розрахунку координат на основі миттєвих значень давачів, що дозволило забезпечити високу стійкість до засобів раліо-електронної боротьби. Також, розроблено системи частотного стрибання та менеджменту потужності сигналу для БПЛА, які використовують властивості їх базових елементів. Завдяки цьому підвищено рівень конфіденційності сигналу відео, за збереження високого рівня швидкодії та стабільності роботи самого пристрою.

Голова комісії,
начальник науково-дослідної
частини, д.т.н. ст. досл. _____ Роман НЕБЕСНИЙ

Члени комісії:
зав. каф. захисту інформації, д.т.н. проф. _____ Іван ОПІРСЬКИЙ

зав. відділу науково-організаційного
супроводу наукових досліджень, к.т.н. _____ Галина ЛАЗЬКО

в.о. заст. нач. планово-фінансового відділу _____ Ірина ФАСТ

ЗАТВЕРДЖУЮ

Проректор з науково-педагогічної роботи

Національного університету

«Львівська політехніка»

доц. _____ Олег ДАВИДЧАК

“___” _____ 202_ р.

АКТ

про впровадження результатів дисертаційної роботи в навчальний процес

Кутеня Романа Богдановича

«Покращення захисту інформації при передачі бездротовими системами»

представленої на здобуття наукового ступеня доктора філософії за спеціальністю

125 – *Кібербезпека*

Комісія НУ «Львівська політехніка» у складі:

Голова комісії – голова науково-методичної ради інституту комп’ютерних технологій та метрології, д.т.н., проф. Байцар Р.І.

Члени комісії:

Завідувач кафедри "Захист інформації", д.т.н., проф. Опірський.І.Р, доцент кафедри "Захист інформації", к.ф-м.н., Михайлова О.О. і старший викладач кафедри "Захист інформації", к.т.н., Луковський Т.І. даним актом підтверджує, що проведені дисертантом наукові дослідження виконувалися ним на кафедрі «Захист інформації» Національного університету «Львівська політехніка». Основні положення та результати дисертаційної роботи впроваджені у навчальний процес кафедри «Захист інформації» Національного університету «Львівська політехніка» при вивченні дисциплін:

- «Безпека технологій зв’язку» для студентів напрямку підготовки 125 “Кібербезпека”, спеціалізації «Системи технічного захисту інформації, автоматизація її обробки», тема №5 «Методи та засоби забезпечення завадостійкості каналів зв’язку» – засоби протидії системам радіо-електронної боротьби.

Голова комісії,
голова науково-методичної ради ІКТА
д.т.н., проф. Роман БАЙЦАР

Члени комісії:
зав. каф. ЗІ, д.т.н., проф. Іван ОПІРСЬКИЙ
доц. каф. ЗІ, к.ф-м.н. Ольга МИХАЙЛОВА
ст.викладач каф. ЗІ, к.т.н. Тарас ЛУКОВСЬКИЙ