DOI: 10.58254/viti.6.2024.03.59

УДК 623

канд. техн. наук Борисов І. В. ORCID: 0000-0003-2276-9913 (НДІ ВР)
канд. техн. наук Волков О. В. ORCID: 0000-0003-3777-6195 (ВА ім. Євгенія Березняка)

КІБЕРБЕЗПЕКА БЕЗПІЛОТНИХ АВІАЦІЙНИХ КОМПЛЕКСІВ ТА ОСОБЛИВОСТІ ЗАХИСТУ ВІД ПЕРЕХОПЛЕННЯ

У статті розглядаються ключові аспекти кібербезпеки безпілотних авіаційних комплексів (БпАК) в умовах сучасних військових конфліктів і технологічного прогресу, безпілотні системи стали важливими інструментами для збору інформації, ведення розвідки та виконання бойових завдань. Однак їх широке використання супроводжується новими кіберзагрозами, що потребують спеціалізованих заходів для забезпечення безпеки. Стаття аналізує основні види кіберзагроз, які можуть вплинути на БпАК, включаючи перехоплення комунікацій, несанкціонований доступ до управлінських систем і злом криптографічних захистів.

У статті також розглядаються сучасні методи і технології захисту, такі як криптографічні алгоритми, механізми аутентифікації та шифрування даних. Окрім того, аналізуються існуючі стандарти і практичні рішення для забезпечення захисту комунікаційних каналів. Остання частина статті присвячена новітнім трендам у сфері кібербезпеки БпАК та прогнозуванню майбутніх загроз. Розглядаються можливі рішення і підходи для покращення захисту безпілотних систем в умовах швидкої зміни кіберсередовища, а також, надаються рекомендації для вдосконалення систем безпеки БпАК, що включають інтеграцію нових технологій і адаптацію до нових загроз.

Ключові слова: *кібербезпека, безпілотні авіаційні комплекси, перехоплення, дистанційне управління, криптографічний захист, шифрування, аутентифікація.*

I. Borysov, O. Volkov Cyber security of unmanned aviation complexes and features of protection against interception.

The article considers the key aspects of cyber security of unmanned aerial systems (UAS) in the conditions of modern military conflicts and technological progress, unmanned systems have become important tools for gathering information, conducting intelligence and performing combat missions. However, their widespread use is accompanied by new cyber threats that require specialized measures to ensure security. The article analyzes the main types of cyberthreats that can affect UAS, including the interception of communications, unauthorized access to management systems and the breaking of cryptographic protections.

The article also discusses modern protection methods and technologies, such as cryptographic algorithms, authentication mechanisms and data encryption. In addition, existing standards and practical solutions to ensure the protection of communication channels are analyzed. The last part of the article is devoted to the latest trends in the field of cyber security of UAS and forecasting future threats. Possible solutions and approaches for improving the protection of unmanned systems in the rapidly changing cyber environment are considered, as well as recommendations are provided for improving the security systems of UAS, which include the integration of new technologies and adaptation to new threats.

Keywords: *cybersecurity, unmanned aerial systems, interception, remote control, cryptographic protection, encryption, authentication.*

Постановка проблеми. При відбитті широкомасштабної агресії рф проти України безпілотні авіаційні комплекси (БпАК) мають ключове значення в розвідці, спостереженні та веденні бойових операцій. Однак з розвитком технологій зростає і кількість кіберзагроз, які можуть значно вплинути на ефективність і безпеку застосування цих комплексів. Перехоплення сигналів управління і несанкціоноване дистанційне керування БпАК представляють серйозну загрозу, що може призвести до втрати контролю над апаратом, компрометації місії та небезпеки для виконання завдань військовими підрозділами.

Проблематика забезпечення кібербезпеки БпАК охоплює ряд критичних аспектів [1–3]:

уразливість до кіберзагроз. Атакуючі можуть перехоплювати сигнали управління БпАК, що дозволяє їм контролювати або змінювати поведінку дронів, а також, можуть намагатися інфікувати БпАК шкідливим програмним забезпеченням, яке може порушити роботу або викрасти дані;

недостатній рівень шифрування і аутентифікації. Якщо канали зв’язку не захищені належним чином, це створює можливість для прослуховування і перехоплення даних. Відсутність ефективних механізмів аутентифікації може дозволити неавторизованим особам отримати доступ до системи управління БпАК;

вразливе до атак програмне забезпечення може бути використане для здійснення атак або витоку даних. Якщо процес оновлення програмного забезпечення не є безпечним, зловмисники можуть запровадити шкідливий код;

у міру збільшення кількості БпАК зростає ймовірність проведення атак на великі групи дронів, що в подальшому ускладнює їх відновлення та подальшу експлуатацію;

взаємодія БпАК з іншими програмними сервісами (системами) може створювати додаткові канали впровадження вразливостей.

Отже, ці проблеми підкреслюють необхідність розробки і впровадження комплексних заходів для забезпечення кібербезпеки БпАК, включаючи новітні технології захисту, постійний моніторинг та удосконалення протоколів безпеки.

Аналіз досліджень. Результати аналізу бойового застосування БпАК та останні дослідження в області кібербезпеки БпАК [1–4] показують необхідність їх захисту від різноманітних загроз. Зокрема, слід звернути увагу на зростання кількості атак, спрямованих на перехоплення і маніпулювання сигналами управління БпАК, що може мати критичні наслідки для ефективності їх бойового застосування.

Метою статті є аналіз актуальних кіберзагроз для безпілотних військових апаратів, а також розробка та оцінка методів захисту від них.

Виклад основного матеріалу. У сучасних військових конфліктах БпАК відіграють критично важливу роль, забезпечуючи розвідку, спостереження та виконання різноманітних бойових завдань. Однак їх широке використання робить їх вразливими для кіберзагроз. Основними видами загроз та атак є [4–6]:

перехоплення сигналів управління. Зловмисники можуть перехоплювати і декодувати сигнали управління між оператором і БпАК та можуть генерувати фальшиві сигнали управління, щоб взяти контроль над БпАК;

атаки на програмне забезпечення (ПЗ). Зловмисники можуть впроваджувати віруси, трояни або інше шкідливе ПЗ для порушення функціональності або викрадення даних, а також, можуть використовувати відомі уразливості в програмному забезпеченні для отримання несанкціонованого доступу;

атаки на апаратне забезпечення. Атакуючі можуть намагатися фізично пошкодити апаратне забезпечення БпАК для його нейтралізації;

атаки на комунікаційні системи. Атакуючі можуть прослуховувати та аналізувати дані, що передаються між БпАК і його базовою станцією, а також, можуть створювати фальшиві точки доступу або мережі для спроби отримання даних або впливу на систему управління;

атаки на систему навігації. Зловмисники можуть підробляти сигнали GPS, щоб ввести БпАК в оману щодо його місцезнаходження або взагалі глушити сигнали GPS для перешкоджання навігації БпАК;

атаки на інфраструктуру управління. Атакуючі можуть намагатися зламати сервери або бази даних, які використовуються для управління БпАК, щоб викрасти або змінити інформацію, проводити збої у командуванні або порушення обробки даних;

використання методів соціальної інженерії для отримання доступу до облікових записів або систем управління БпАК.

Ці види загроз вимагають комплексного підходу до забезпечення кібербезпеки БпАК, включаючи використання сучасних технологій захисту, постійний моніторинг систем та регулярні оновлення програмного забезпечення.

Механізми перехоплення і впливу на управлінські системи БпАК можуть включати різноманітні техніки та методи [2, 4–6]. Ось деякі з них.

1. Перехоплення сигналів управління:

зловмисники можуть використовувати радіоапаратуру для перехоплення радіочастотних сигналів управління між оператором і БпАК. Це може включати як управлінські команди, так і дані з сенсорів;

після перехоплення сигналів, зловмисники можуть декодувати їх для розуміння протоколів комунікації і подальшого впливу на систему.

2. Атаки на канали зв’язку:

атакуючі можуть генерувати фальшиві сигнали (Spoofing) для управління БпАК або підробляти інформацію, яку БАК отримує від базової станції;

зловмисники можуть створювати електромагнітні перешкоди (Jamming) для блокування або спотворення комунікацій між БпАК і його контролером.

3. Атаки на протоколи зв’язку:

зловмисники можуть спробувати зламати або обійти механізми аутентифікації, що використовуються для підключення до БпАК;

якщо передача даних зашифрована, атакуючі можуть спробувати знайти вразливості в криптографічних алгоритмах для дешифрування інформації.

4. Внесення шкідливого коду:

атакуючі можуть використовувати вразливості в програмному забезпеченні БпАК для внесення шкідливого ПЗ або вірусів, які можуть змінити його поведінку або знищити дані;

атакуючі можуть підмінити оновлення програмного забезпечення БпАК на шкідливі версії для контролю над системою.

5. Злом системи навігації:

атакуючі можуть підробляти сигнали GPS (GPS-спуфінг), щоб ввести БпАК в оману щодо його реального місцезнаходження;

включення пристроїв для глушіння сигналів GPS (GPS-джаммінг), що призводить до втрати навігаційних даних і можливих аварійних ситуацій.

6. Компрометація комунікаційної інфраструктури:

зловмисники можуть зламати або впливати на базові станції, які управляють БпАК, щоб отримати контроль або порушити їхню роботу;

атакуючі можуть намагатися зламати сервери або системи управління для отримання доступу до інформації або контролю над БпАК.

7. Маніпуляція даними та командами:

атакуючі можуть маніпулювати або змінювати команди, які надходять до БпАК, щоб вплинути на його поведінку;

надання неправдивих або шкідливих даних БпАК, які можуть призвести до некоректних рішень або дій.

Ці механізми демонструють широкий спектр можливих атак на управлінські системи БпАК і підкреслюють важливість впровадження комплексних заходів для захисту від таких загроз.

Ось кілька реальних випадків атак на БпАК, які демонструють різноманітні способи, якими зловмисники можуть вплинути на ці системи:

1. Атака на дрони у конфліктних зонах. У 2018 році в Венесуелі відбулася спроба замаху на президента Мадуро за допомогою безпілотних літальних апаратів. Дрони, які були оснащені вибуховими пристроями, вибухнули під час виступу президента. Зловмисники використовували дрони для доставки вибухових пристроїв, це свідчить про можливість використання БпАК для атак на високопрофільні цілі.

2. GPS-спуфінг у Дубаї. У 2016 році в Дубаї дрони, які проводили геодезичні дослідження, були піддані GPS-спуфінгу. Це призвело до помилкових даних про їхнє

місцезнаходження. Зловмисники підробили сигнали GPS, щоб ввести дрони в оману і змусити їх працювати не в тому місці, де їх було заплановано.

3. Атака на комерційний дрон в США. У 2020 році дрон компанії Amazon був зламаний з метою отримання несанкціонованого доступу до комерційних даних. Зловмисники змогли використовувати уразливості в програмному забезпеченні дрона та перехоплювати його комунікаційні канали для отримання конфіденційної інформації.

4. Використання дронів для нагляду. У 2017 році в Китаї дрони, що використовувалися для нагляду, були захоплені і перепрограмовані для збору інформації та шпигунства. Атакуючі отримали доступ до системи управління дронами і перепрограмували їх для збору конфіденційної інформації.

Широкомасштабне вторгнення рф в Україну показало, що БпАК відіграють важливу роль у збройному протистоянні і стали мішенню для різних кіберзагроз і атак. Ось кілька прикладів.

1. Атаки на системи управління БпАК. Під час конфлікту на Донбасі неодноразово відзначено випадки перехоплення сигналів управління БпАК. Атакуючі використовували спеціальне обладнання для перехоплення і декодування радіочастотних сигналів. Зловмисники змогли змінити або вплинути на команди, що надходять до дронів, це дозволило їм контролювати або порушити роботу безпілотників.

2. Атаки на GPS-системи. Неодноразово повідомлялися випадки GPS-спуфінгу, коли російські сили намагалися підробляти сигнали GPS, що призводило до неправильної навігації дронів і спотворення даних розвідки.

3. Кібернетичні атаки на інфраструктуру БпАК. Це включало в себе спроби зламу систем управління дронами або проникнення у сервери для отримання доступу до даних. Атакуючі використовували різні методи, включаючи шкідливе ПЗ, фішинг або експлойти для отримання доступу до управлінських систем і даних.

4. Неодноразово зафіксовані випадки, коли обидві сторони використовують засоби радіоелектронної боротьби для перехоплення, глушіння сигналів або знищення дронів.

Ці випадки підкреслюють важливість забезпечення кібербезпеки та захисту дронів від різноманітних загроз. Вони також вказують на різні способи, якими БпАК можуть бути використані як інструменти для атак.

Таким чином, захист БпАК від перехоплення сигналів і комунікацій є критично важливим для забезпечення їхньої безпеки та ефективності. Основними ключовими особливостями і методами захисту від перехоплення є:

використання сучасних криптографічних алгоритмів для шифрування сигналів управління та даних, що передаються між БпАК і контролером;

аутентифікація і авторизація (впровадження багаторівневої аутентифікації, наприклад, паролі, біометричні дані та токени, для доступу до системи управління БпАК, включаючи перевірку прав користувачів);

зміна частот радіозв’язку за певним алгоритмом для ускладнення перехоплення і декодування сигналів (Frequency Hopping) та використання адаптивних алгоритмів для вибору частот і швидкої зміни частот для підвищення стійкості до перехоплення;

впровадження технологій для протидії глушінню сигналів, таких як автоматичне виявлення і переключення на вільні частоти та використання технологій для виявлення і протидії спуфінговим атакам, таких як перевірка автентичності сигналів;

встановлення систем для постійного моніторингу сигналів і виявлення аномалій або спроб перехоплення;

використання аналізу трафіку для виявлення підозрілих або ненормальних комунікаційних патернів;

впровадження захищених мікросхем і плат, які мають вбудовані механізми захисту від несанкціонованого доступу;

постійне оновлення програмного забезпечення БпАК для усунення вразливостей і захисту від нових загроз;

застосування безпечних протоколів для обміну даними, таких як SSL/TLS;

регулярне тестування систем на стійкість до різних типів атак, включаючи перехоплення, проведення незалежних аудитів і перевірок для виявлення можливих вразливостей.

Ці методи та технології забезпечують всебічний підхід до захисту БпАК від перехоплення сигналів і контролюють рівень їхньої безпеки в умовах сучасних кіберзагроз.

Крім того, технічні засоби захисту є критично важливими для забезпечення безпеки БпАК [3–6]. Ось основні компоненти та принципи використання криптографії, аутентифікації та шифрування даних.

1. Криптографія:

симетричне шифрування. Використовується один ключ для шифрування і дешифрування даних. Наприклад, AES (Advanced Encryption Standard). Переваги: швидкість і ефективність при великих обсягах даних. Недоліки: проблема безпечної передачі ключа;

асиметричне шифрування. Використовуються пари ключів: публічний і приватний. Публічний ключ для шифрування, приватний для дешифрування. Наприклад, RSA (Rivest-Shamir-Adleman). Переваги: безпека при передачі ключів, можливість підпису даних. Недоліки: повільніше порівняно із симетричним шифруванням;

гібридне шифрування. Поєднує симетричне і асиметричне шифрування для забезпечення високого рівня безпеки і швидкості. Наприклад, використання RSA для передачі симетричного ключа AES;

хеш-функції. Використовуються для забезпечення цілісності даних, перетворюючи інформацію в унікальний хеш-код. Наприклад, SHA-256, MD5. Переваги: легкість перевірки цілісності даних. Недоліки: не забезпечує конфіденційність даних.

2. Аутентифікація:

паролі. Стандартний метод аутентифікації, який включає в себе використання паролів або PIN-кодів. Переваги: простота впровадження. Недоліки: слабка захищеність, якщо паролі не є складними і змінюються не регулярно;

багатофакторна аутентифікація (MFA). Включає в себе два або більше факторів для підтвердження особи. Може бути комбінацією пароля, біометричних даних або одноразових кодів. Переваги: підвищена безпека. Недоліки: може бути більш складним у впровадженні і використанні;

біометричні дані. Використовують унікальні фізичні характеристики для аутентифікації, такі як відбитки пальців або сітківка ока. Переваги: високий рівень безпеки та зручність. Недоліки: може бути схильним до зловживань або помилок;

сертифікати цифрового підпису. Використовують пари ключів і сертифікати для підтвердження особи. Сертифікати видаються на основі довірених центрів сертифікації. Переваги: безпека і можливість перевірки автентичності даних. Недоліки: необхідність управління сертифікатами.

3. Шифрування даних:

шифрування даних при передачі. Забезпечує захист даних під час їх передачі каналами зв’язку. Використовуються такі протоколи, як TLS/SSL (Transport Layer Security/Secure Sockets Layer). Переваги: захист даних від перехоплення під час передачі. Недоліки: необхідність належного управління сертифікатами та ключами;

шифрування даних на диску. Забезпечує захист даних, що зберігаються на пристроях. Наприклад, AES може бути використано для шифрування файлів і баз даних. Переваги: захист

даних у випадку втрати або крадіжки пристроїв. Недоліки: необхідність управління ключами і можливість впливу на продуктивність;

шифрування метаданих. Захищає не тільки самі дані, але і метадані, такі як інформація про файли та їх структуру. Переваги: додатковий рівень захисту. Недоліки: може бути складним у реалізації та управлінні.

Критично важливим для забезпечення безпеки передачі даних є захист каналів зв’язку, особливо у випадку БпАК та інших критичних систем. Ось основні методи і технології захисту каналу зв’язку.

1. Шифрування каналу зв’язку:

SSL/TLS (Secure Sockets Layer/Transport Layer Security). Забезпечує шифрування даних, що передаються мережею і аутентифікацію сторін зв’язку. Широко використовуються в Інтернеті для захисту вебтрафіку. Переваги: високий рівень захисту даних від перехоплення і маніпуляцій. Недоліки: може впливати на продуктивність через додаткове навантаження на обробку даних;

IPsec (Internet Protocol Security). Протокол для захисту даних на рівні мережі, який забезпечує шифрування і аутентифікацію пакетів IP-трафіку. Переваги: широка підтримка і можливість захисту всього IP-трафіку. Недоліки: може бути складним в налаштуванні та управлінні;

VPN (Virtual Private Network). Створює зашифроване з’єднання через публічні мережі для забезпечення приватності і захисту даних. Переваги: захист даних від перехоплення в публічних мережах. Недоліки: може знижувати швидкість зв’язку.

2. Аутентифікація і авторизація:

багатофакторна аутентифікація (MFA). Включає кілька рівнів перевірки (наприклад, пароль плюс одноразовий код), щоб підтвердити особу користувача. Переваги: підвищує безпеку доступу до каналу зв’язку. Недоліки: може бути складним у впровадженні та використанні;

цифрові сертифікати. Використовуються для підтвердження ідентичності та встановлення зашифрованих з’єднань між двома сторонами. Переваги: забезпечує верифікацію і безпеку підключення. Недоліки: необхідність управління сертифікатами і довіреними центрами сертифікації.

3. Технології захисту від глушіння та перешкод:

частотна стрибкоподібність (Frequency Hopping). Зміна частот радіозв’язку за певним алгоритмом для ускладнення перехоплення і глушіння сигналів. Переваги: підвищує стійкість до перехоплення і глушіння. Недоліки: може ускладнити налаштування і синхронізацію;

антиджаммінг (Anti-jamming). Технології для виявлення і протидії глушінню сигналів, такі як автоматичне перемикання на чисті частоти. Переваги: підвищує надійність зв’язку в умовах електромагнітних перешкод. Недоліки: вимагає спеціалізованого обладнання та налаштування.

4. Контроль доступу і моніторинг:

системи контролю доступу. Впровадження засобів для обмеження доступу до каналу зв’язку на основі прав користувачів або груп. Переваги: захист від несанкціонованого доступу. Недоліки: потребує постійного моніторингу і управління правами доступу;

моніторинг трафіку. Використання інструментів для постійного моніторингу мережевого трафіку і виявлення аномалій або спроб перехоплення. Переваги: швидке виявлення і реагування на загрози. Недоліки: може бути ресурсоємним і вимагати спеціалізованого обладнання.

5. Інші методи:

захист від атак типу “Man-in-the-Middle” (MITM). Використання криптографії для забезпечення цілісності і конфіденційності даних, що передаються, щоб унеможливити

підробку або прослуховування з боку третьої сторони. Переваги: захищає від перехоплення і підробки даних. Недоліки: може вимагати складних алгоритмів і налаштувань;

сегментація мережі. Розділення мережі на сегменти для обмеження можливості доступу до критичних систем і даних. Переваги: знижує ризики при компрометації одного сегмента. Недоліки: може ускладнити управління і налаштування мережі.

Використання цих методів і технологій забезпечує багаторівневий підхід до захисту каналу зв’язку, знижуючи ризики перехоплення, глушіння і несанкціонованого доступу.

Аналіз сучасних рішень і стандартів захисту для БпАК включає в себе огляд існуючих технологій та підходів до забезпечення безпеки. Основні аспекти таких рішень і стандартів охоплюють захист комунікацій, захист даних, управління доступом, а також адаптацію до нових загроз.

Стандарти захисту від кіберзагроз:

NIST Cybersecurity Framework. Рамка для управління кіберзахистом, включаючи ідентифікацію, захист, виявлення, реагування і відновлення. Дозволяє організаціям розробити комплексний план кіберзахисту. Широко використовується в США і міжнародній практиці;

ISO/IEC 27001. Стандарт для системи управління інформаційною безпекою. Визначає вимоги для впровадження та підтримки системи управління безпекою інформації. Забезпечує структурований підхід до захисту інформації;

Zero Trust Security Model. Модель безпеки, яка припускає, що жоден користувач або пристрій не є довіреним, поки не буде перевірено. Підходить для сучасних розподілених і хмарних середовищ. Фокусується на постійній перевірці і контролі доступу;

Blockchain для безпеки даних. Використання технології блокчейн для забезпечення цілісності та автентичності даних. Може використовуватися для захисту транзакцій і даних у реальному часі. Забезпечує додатковий рівень захисту завдяки незмінності записів;

AI і Machine Learning для кіберзахисту. Використання штучного інтелекту та машинного навчання для виявлення аномалій і загроз у реальному часі. Збільшує ефективність моніторингу та реагування на кіберзагрози. Допомагає автоматизувати процеси виявлення та реагування на загрози.

Аналіз цих рішень і стандартів допомагає забезпечити комплексний підхід до захисту БпАК і інших критичних систем від різних типів загроз. Ось кілька прикладів реалізації таких рішень.

1. Шифрування та захист даних:

військові дрони США, такі як MQ-9 Reaper, використовують шифрування AES для захисту комунікацій між дронами і командними центрами. Це забезпечує захист передачі відео та інших даних від перехоплення і прослуховування. Як результат підвищення рівня безпеки даних і команд, що передаються через різні канали зв’язку;

інфраструктура критичних об’єктів. Для захисту комунікацій і даних в інфраструктурі критичних об’єктів, таких як енергетичні станції, використовуються протоколи TLS для шифрування інформації, що передається між контролерами і серверами. Як результат, зменшення ризику несанкціонованого доступу до критичних даних і контролю.

2. Аутентифікація та управління доступом:

компанія DJI використовує багатофакторну аутентифікацію для доступу до своїх систем управління дронами DJI. Користувачі повинні підтвердити свою особу через мобільний додаток і ввести пароль для доступу до функцій дрона. Як результат, збільшення рівня безпеки доступу до дронів і запобігання несанкціонованому управлінню;

системи управління доступом у хмарних середовищах. Хмарні платформи для управління БпАК часто використовують OAuth 2.0 і OpenID Connect для забезпечення безпечного доступу до даних і ресурсів. Це дозволяє інтегрувати сторонні сервіси і

забезпечити контроль доступу на основі токенів. Як результат, гнучке управління доступом і інтеграція з іншими сервісами при забезпеченні високого рівня безпеки.

3. Захист комунікацій:

військові дрони використовують технології частотної стрибкоподібності (FHSS) для захисту від глушіння і перехоплення сигналів. Це дозволяє змінювати частоти радіозв’язку у часі, ускладнюючи виявлення і перешкоджання;

впровадження адаптивних систем частотного стрибка (AFH) в безпроводових комунікаціях для безпілотних транспортних систем, що автоматично змінюють частоти залежно від наявних перешкод.

Критично важливим для забезпечення безпеки БпАК в умовах швидкого розвитку технологій є прогнозування нових типів загроз. Ось кілька потенційних загроз і можливих рішень для зниження їх рівня [5–7]:

1. Загрози на основі штучного інтелекту для атак на БАК, включаючи автоматизовані атаки, адаптивні алгоритми для обходу захисту і дезінформаційні кампанії. Можливими рішеннями є розробка систем AI, які здатні виявляти аномалії і небезпечні поведінки, базуючись на машинному навчанні та комбінація традиційних і AI-орієнтованих методів для посилення кіберзахисту.

2. Квантові комп’ютери можуть потенційно розшифровувати дані, які захищені сучасними криптографічними алгоритмами. Можливими рішеннями є розробка і впровадження нових криптографічних алгоритмів, стійких до атак квантових комп’ютерів та використання квантових ключів для забезпечення високого рівня безпеки.

3. Використання автономних дронів або роботизованих систем для атак на інші БпАК або критичні об’єкти. Можливими рішеннями є розробка і впровадження рішень для захисту від автономних атак, таких як виявлення і нейтралізація загроз.

4. Злом і маніпуляція компонентами Інтернету речей (IoT), які інтегруються з БпАК. розробка і впровадження спеціалізованих рішень для захисту компонентів IoT, таких як шифрування даних і аутентифікація пристроїв та впровадження строгих політик контролю доступу до IoT-компонентів і регулярне оновлення програмного забезпечення.

5. Злом або маніпуляції в динамічних мережах ad-hoc, де БпАК спілкуються між собою без фіксованої інфраструктури. Можливими рішеннями є розробка і впровадження протоколів комунікації, які забезпечують безпеку в ad-hoc мережах, використання криптографії для забезпечення захищеного зв’язку між пристроями в ad-hoc мережах.

Таким чином, ці рекомендації допоможуть у створенні більш стійкої та ефективної системи безпеки для безпілотних авіаційних комплексів, що забезпечить їхню захищеність від нових і існуючих загроз.

Висновки та перспективи подальшого дослідження

Дослідження виявило, БпАК стикаються з серйозними кіберзагрозами, такими як перехоплення сигналів управління, дистанційне захоплення контролю, вразливості ПЗ та ін. Найефективнішими методами захисту є криптографічний захист, багаторівнева аутентифікація, інтеграція механізмів безпеки в ПЗ та фізичний захист комунікацій [3–6]. Аналіз показує, що ці рішення значно підвищують захист БпАК від кіберзагроз, їх ефективність підтверджена реальними кейсами.

Попри досягнуті результати, є питання для подальших досліджень, зокрема розробка нових методів шифрування, стійких до майбутніх загроз, таких як квантові обчислення, а також дослідження захисту під час масованих атак. Подальші вдосконалення можуть включати адаптацію аутентифікаційних систем до бойових умов, впровадження машинного навчання для активного виявлення загроз і розробку нових комунікаційних протоколів, а також, розробка інтегрованих систем, що поєднують криптографію, контроль доступу та фізичний захист.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. P.-Y. Kong, A Survey of Cyberattack Countermeasures for Unmanned Aerial Vehicles," in IEEE Access, vol. 9, pp. 148244–148263, 2021, DOI: 10.1109/ACCESS.2021.3124996.

2. Z. Yu, Z. Wang, J. Yu, D. Liu, H. Herbert Song and Z. Li, "Cybersecurity of Unmanned Aerial Vehicles: A Survey," in *IEEE Aerospace and Electronic Systems Magazine*, vol. 39, no. 9, pp. 182–215, Sept. 2024, DOI: 10.1109/MAES.2023.3318226.

3. R. Alkadi, N. Alnuaimi, C. Y. Yeun and A. Shoufan, "Blockchain Interoperability in Unmanned Aerial Vehicles Networks: State-of-the-Art and Open Issues," in *IEEE Access*, vol. 10, pp. 14463–14479, 2022, DOI: 10.1109/ACCESS.2022.3145199. k

4. R. Guo, M. Huang, J. Li and J. Wang, "Cybersecurity of Unmanned Aerial Vehicles: A Survey," *2021 14th International Conference on Advanced Computer Theory and Engineering (ICACTE)*, Hangzhou, China, 2021, pp. 57–64, DOI: 10.1109/ICACTE53799.2021.00017.

5. L. Li, K. Qu and K.-Y. Lin, "A Survey on Attack Resilient of UAV Motion Planning," *2020 IEEE 16th International Conference on Control & Automation (ICCA)*, Singapore, 2020, pp. 558–563, DOI: 10.1109/ICCA51439.2020.9264513.

6. R. Hamadi, H. Ghazzai and Y. Massoud, "Reinforcement Learning Based Intrusion Detection Systems for Drones: A Brief Survey," *2023 IEEE International Conference on Smart Mobility (SM)*, Thuwal, Saudi Arabia, 2023, pp. 104–109, DOI: 10.1109/SM57895.2023.10112557.

7. M. Adil, M. A. Jan, Y. Liu, H. Abulkasim, A. Farouk and H. Song, "A Systematic Survey: Security Threats to UAV-Aided IoT Applications, Taxonomy, Current Challenges and Requirements With Future Research Directions," in *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 2, pp. 1437–1455, Feb. 2023, DOI: 10.1109/TITS.2022.3220043.