629.7:004.6

К. К. Матвєєв, І. В. Віщун

ПЕРСПЕКТИВИ ВПРОВАДЖЕННЯ ЗАХИСТУ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ БЕЗПІЛОТНИХ АВІАЦІЙНИХ КОМПЛЕКСІВ НА ОСНОВІ БЛОКЧЕЙН

Аннотація: *розглянуто впровадження блокчейн-технологій для захисту програмного забезпечення безпілотних авіаційних комплексів.*

Ключові слова: *блокчейн, безпілотний авіаційний комплекс, захист програмного забезпечення, кібербезпека.*

Abstract*: the introduction of blockchain technologies to protect the software of unmanned aircraft systems is considered.*

Keywords: *blockchain, unmanned aircraft complex, software protection, cyber security.*

В сучасному світі стрімкий розвиток технологій вимагає створення ефективних рішень для забезпечення безпеки. Станом на 2021 рік, 45% респондентів зазначили, що їхні компанії працюють над безпечним обміном інформацією за допомогою блокчейну[2], що робить його найпопулярнішим варіантом використання цієї технології. Це свідчить про актуальність блокчейну як засобу підвищення безпеки та зниження ризиків кіберзагроз. Одним із перспективних рішень у цьому напрямку є впровадження блокчейн-технологій. Захист програмного забезпечення безпілотних авіаційних комплексів (далі - БпАК) стає критичним завданням, оскільки вони використовуються у військовій, комерційній та цивільній сферах.

Блокчейн, за визначенням IBM, є «спільним, незмінним реєстром, який сприяє процесу фіксації транзакцій та відстеження активів у бізнес-мережі»[3]. Це система, яка дозволяє безпечно, прозоро та економічно ефективно відстежувати будь-що, що має цінність. Назва «блокчейн» походить від того, що кожна транзакція записується у вигляді «блоку» даних. Такий блок може містити різні типи інформації, такі як кількість, ціна або місцезнаходження. Коли актив переходить від одного власника до іншого, блоки формують ланцюг, де зберігаються деталі кожної транзакції, включаючи час та послідовність. Однією з ключових переваг блокчейну є відсутність єдиної точки відмови. Кожен ланцюг незмінний, тому жоден учасник не може видалити або змінити блок. Це робить майже неможливим втручання у криптографічний ланцюг, оскільки для підтвердження точності кожної транзакції використовується узгоджений механізм консенсусу. Використання блокчейну у БпАК може забезпечити надійний захист програмного забезпечення та управління даними. Блокчейн дозволить фіксувати кожну операцію, пов'язану з польотами, передачу команд, оновлення програмного забезпечення та обмін інформацією між дронами й центрами управління. Таким чином, підробка даних або хакерські атаки стають практично неможливими, оскільки кожен етап перевіряється та зафіксований у незмінному ланцюгу транзакцій.

Алгоритм роботи після впровадження блокчейну буде працювати так, що перед початком польоту його план та початкові команди заносяться в блокчейн. Це забезпечує їхню незмінність і захищеність, а також гарантує, що всі наступні дії дрона будуть базуватися на підтверджених і перевірених даних. Безпосередньо перед стартом безпілотний лвтальний апарат (далі - БпЛА) отримує підтвердження, що команди пройшли перевірку та успішно занесені в останній блок ланцюга. Під час польоту, у разі отримання нових команд або зміни маршруту, БпЛА звертається до блокчейну для перевірки автентичності команд. Локальний клієнт, встановлений на дроні, перевіряє, чи збігається хеш нової команди з тим, що зберігається в блокчейні. Якщо автентичність підтверджується, дрон виконує отримані вказівки. Щодо оновлення програмного забезпечення, кожне оновлення підписується цифровим ключем розробника і проходить через блокчейн-мережу для перевірки. Оновлення буде встановлене на дрон лише після того, як усі вузли мережі підтвердять транзакцію, що забезпечує його безпеку і захист від підробки. У випадку відмови зв'язку, БпЛА використовує кешовані правила і останні перевірені команди, що дає йому змогу безпечно завершити місію або повернутися на базу. Це гарантує надійність роботи навіть у складних умовах або при втраті з'єднання з центром управління. Проте, незважаючи на ці переваги, блокчейн-

технології мають і свої недоліки, які можуть стати викликом при їх впровадженні в систему БпАК. Його ресурсомісткість є важливою проблемою. Хоча використання легких клієнтів може зменшити навантаження, блокчейн все одно потребує значних обчислювальних ресурсів та енергії. Це особливо актуально для дронів, у яких ресурси, як обчислювальні, так і енергетичні, є обмеженими. Ще одним недоліком є затримки, які можуть виникати під час верифікації транзакцій. Якщо мережа блокчейну велика або перевантажена, це може спричинити затримки в обробці даних. У критичних місіях, таких як рятувальні операції або військові завдання, ці затримки можуть негативно вплинути на ефективність виконання місії. Також важливо врахувати складність реалізації блокчейн-технологій. Інтеграція блокчейну з існуючими системами управління дронами потребує значних інженерних зусиль і ретельної розробки, що може ускладнити впровадження.

В умовах війни впровадження блокчейн-технологій для захисту програмного забезпечення БпАК стикається з кількома значними викликами. Насамперед, складність та ресурсомісткість цієї технології роблять її важкою для реалізації в умовах обмежених ресурсів, де кожен дрон повинен бути максимально енергоефективним та швидко реагувати на зміну обстановки. Також нестабільність мережевих з’єднань у бойових умовах, особливо у віддалених або ворожих регіонах, значно ускладнює використання блокчейну, який потребує постійного і надійного зв'язку для ефективної роботи. Однак, попри всі ці труднощі, блокчейн має значний потенціал для підвищення безпеки та надійності дронів у майбутньому. Його здатність забезпечувати незмінність та автентичність команд і даних, знижувати ризики кібератак може стати важливим інструментом для підвищення інформаційного захисту ефективності БпАК. В перспективі, коли інфраструктурні обмеження будуть зняті, а технології стануть більш адаптованими, блокчейн може стати ключовим рішенням для забезпечення захисту програмного забезпечення БпАК і ефективного застосування БпЛА у військових операціях.

Список використаних джерел:

1. Chin K. The Role of Cybersecurity in Blockchain Technology | UpGuard. *Third-Party Risk and Attack Surface Management Software | UpGuard*. URL: https://www.upguard.com/blog/the-role-of-cybersecurity-in-blockchain-technology (дата звернення: 17.10.2024).
2. Global use cases for blockchain technology | Statista. *Statista*. URL: https://www.statista.com/statistics/878732/worldwide-use-cases-blockchain-technology/ (дата звернення: 17.10.2024).
3. IBM. What Is Blockchain? | IBM. IBM - United States. URL: https://www.ibm.com/topics/blockchain (дата звернення: 17.10.2024).
4. Rethinking Cybersecurity Through Blockchain. *Infosys Germany - IT Business Services & Consulting - Overview*. URL: https://www.infosys.com/insights/cyber- security/cybersecurity-blockchain.html (дата звернення: 21.10.2024).
5. UAVLance. An Overview Of UAV Hardware Components and Software. *Medium*. URL: https://medium.com/@UAVLance/an-overview-of-uav-hardware-components-and-software-2df983222e31 (дата звернення: 17.10.2024).

Матвєєв Кирил Костянтинович – слухач Кафедри військової підготовки, Вінницький національний технічний університет, м. Вінниця, e-mail: kir28mat@gmail.com.

Віщун Ігор В’ячеславович – викладач Кафедри військової підготовки, Вінницький національний технічний університет, м. Вінниця, e-mail: vishchunihor@gmail.com

Matveev Kyryl Kostiantynovych – student of the Department of Military Training, Vinnytsia National Technical University, Vinnytsia, e-mail: kir28mat@gmail.com.

Ihor Vyacheslavovych Vishchun – lecturer at the Department of Military Training, Vinnytsia National Technical University, Vinnytsia, e-mail: vishchunihor@gmail.com