УДК 004.056

ІННОВАЦІЙНІ ПІДХОДИ ДО ЗАХИСТУ БЕЗПЕКИ ІНФОРМАЦІЙНИХ КАНАЛІВ КЕРУВАННЯ В КОНТЕКСТІ РОЗВИТКУ АВТОНОМНИХ СИСТЕМ

Вельма І.Ю.,
Науковий керівник – д. т. н., проф. Мартинчук О. О.
Харківський національний університет радіоелектроніки, каф. ІКІ
м. Харків, Україна
e-mail: ihor.velma@nure.ua

In the modern world, the importance of autonomous systems such as unmanned aerial vehicles (UAVs), autonomous vehicles, and robots is growing. These systems require reliable and secure management, but they also become targets for potential cyberattacks. As a result, there is a need for innovative approaches to protecting the information channels of these systems.

На сьогоднішній день інформаційні канали керування автономними системами стають дедалі більш вразливими перед кіберзагрозами через низку факторів. Перш за все, зростаюча кількість підключених пристроїв і збільшення обсягу передаваних даних створюють більше можливостей для зловмисників здійснювати атаки. Відкритість інтернету дещо ускладнює захист каналів передачі даних, оскільки це може створювати можливості для зловмисників перехоплювати інформацію, що передається через мережу. Зловмисники можуть використовувати різноманітні методи для атак на інформаційні канали керування. Наприклад, вони можуть перехоплювати передані дані, щоб отримати доступ до конфіденційної інформації або внести зміни до команд, що керують автономною системою. Можливість модифікувати або блокувати передачу даних може призвести до серйозних наслідків, таких як аварії або порушення безпеки, зокрема в областях, де автономні системи залежать від неперервного зв'язку з операторами або іншими системами для нормальної роботи. Загрози для інформаційних каналів керування автономними системами наголошують на необхідності постійного вдосконалення заходів безпеки та використання передових технологій для захисту цих каналів від кібератак.

Одним із перспективних напрямків є застосування штучного інтелекту та машинного навчання для виявлення та запобігання кібератак на інформаційні канали керування. Це означає застосування алгоритмів та моделей, які навчаються на основі великої кількості даних, щоб автоматично виявляти аномальну або підозрілу активність у мережі та реагувати на неї. Наприклад, системи машинного навчання можуть аналізувати трафік мережі для виявлення незвичайних патернів або атак, а потім надавати відповідні заходи безпеки, такі як блокування підозрілих джерел або виявлення зламаної аутентифікації. Ці методи дозволяють

покращити ефективність захисту інформаційних каналів керування та забезпечити вчасну реакцію на потенційні загрози кібербезпеки.

Додатковим інноваційним підходом є використання блокчейн-технологій для створення безпечних та недоступних до модифікації інформаційних каналів керування. Блокчейн може забезпечити захист від фальсифікації та змін даних, що передаються між автономними системами та їхніми контролерами.

Блокчейн - це розподілена база даних, яка зберігається на кожному пристрої в мережі, і що містить набір записів, які називаються блоками. Кожен блок містить інформацію, час та дату, а також посилання на попередній блок у ланцюжку, що робить його неможливим для зміни без зміни всіх попередніх блоків у ланцюжку. Це робить блокчейн особливо відповідним для створення безпечних інформаційних каналів. [1]

Коли мова йде про інформаційні канали керування в автономних системах, блокчейн може забезпечити безпеку від фальсифікації та несанкціонованого доступу. Наприклад, дані, що передаються між автономними пристроями та їхніми контролерами, можуть бути записані у блокчейні. Це робить їх неспроможними до модифікації або видалення без відома всіх учасників мережі. Крім того, блокчейн може забезпечити захист від зловмисників, оскільки будь-яка спроба змінити дані буде легко виявлена завдяки системі реєстрації та підтвердження транзакцій.

Використання блокчейн-технологій для створення безпечних та недоступних до модифікації інформаційних каналів керування є потужним інноваційним рішенням, яке може допомогти забезпечити безпеку та надійність в управлінні автономними системами.

Застосування інноваційних підходів до захисту інформаційних каналів керування вже має практичні застосування. Наприклад, деякі компанії вже використовують системи аналізу великих даних для виявлення загроз та аналізу поведінки систем.

У сучасному світі захист інформаційних каналів керування автономних систем стає все більш важливою проблемою. Інноваційні підходи, такі як застосування штучного інтелекту та машинного навчання, а також використання блокчейн-технологій, можуть допомогти підвищити ефективність захисту та забезпечити безпеку та надійність управління автономними системами.

Список використаних джерел:

1. Блокчейн (blockchain, ланцюжок блоків). URL: https://alpari.com/ru/beginner/glossary/blockchain/ (дата звернення: 01.03.2024)