знаходження оптимального варіанта, адаптивний підхід до користувачів залежно від їх рівня, а у разі його розширення чи комбінації з іншими методами можна створити повноцінний шаховий двигун, який зможе давати точну оцінку навіть на достатній глибині розрахунків.

Список використаних джерел

1. Fuller S. H., Gaschnig J. G., Gillogly J. J. An analysis of the alpha–beta pruning algorithm. Department of Computer Science Report, Carnegie-Mellon University, Pittsburgh, Pennsylvania, 1973, 51 p.

2. Felstiner C. Alpha-Beta Pruning, Whitman College, 2019.

3. Wang J. J., Liu M. S., Zhao G. D. Design of Military Chess System Based on Alpha-Beta Pruning Algorithm. *36th Chinese Control and Decision Conference (CCDC).* IEEE, 2024. P. 3092–3097.

УДК 004.08

Рудь О. С., здобувачка вищої освіти,
Юстименко Є. А., здобувач вищої освіти,
Ніколюк П. К., д-р фіз.-мат. наук, професор
кафедри інформаційних технологій

АЛГОРИТМИ ШИФРУВАННЯ ДЛЯ ЗАХИСТУ РАДІОЗВ'ЯЗКУ В УМОВАХ БОЙОВИХ ДІЙ

Донецький національний університет імені Василя Стуса, м. Вінниця

Сучасні воєнні операції все більше залежать від швидкої та безпечної передачі інформації. Радіозв'язок є надважливим засобом комунікації на полі бою, проте він залишається вразливим до перехоплення та глушіння з боку супротивника. Розробка ефективних алгоритмів шифрування має велике значення для забезпечення конфіденційності та достовірності переданих даних.

Ця тема є надзвичайно актуальною в умовах воєнного стану і в час, коли технологічні засоби ведення бойових дій постійно вдосконалюються. Під час бойових дій інформаційна безпека особливо важлива та безпосередньо впливає на успішне виконання військових завдань. Забезпечення захищеної передачі даних допомагає запобігти перехопленню ворогом стратегічно важливої інформації та зберегти життя військовослужбовців.

Радіозв'язок є одним із ключових елементів забезпечення військових операцій, адже через нього передаються накази, координати, розвідувальні дані та інша критично важлива інформація. Одним із найпоширеніших методів захисту даних є шифрування. Проте розробка алгоритмів шифрування для військових потреб має враховувати специфічні вимоги до швидкості, безпеки та енергоефективності [1].

Процес безпечної передачі даних включає кілька етапів: шифрування даних на стороні передавача, передача зашифрованих даних через радіоканал і розшифрування даних на стороні приймача. На рисунку 1 зображено етапи безпечної передачі даних між передавачем і приймачем у радіозв'язку.

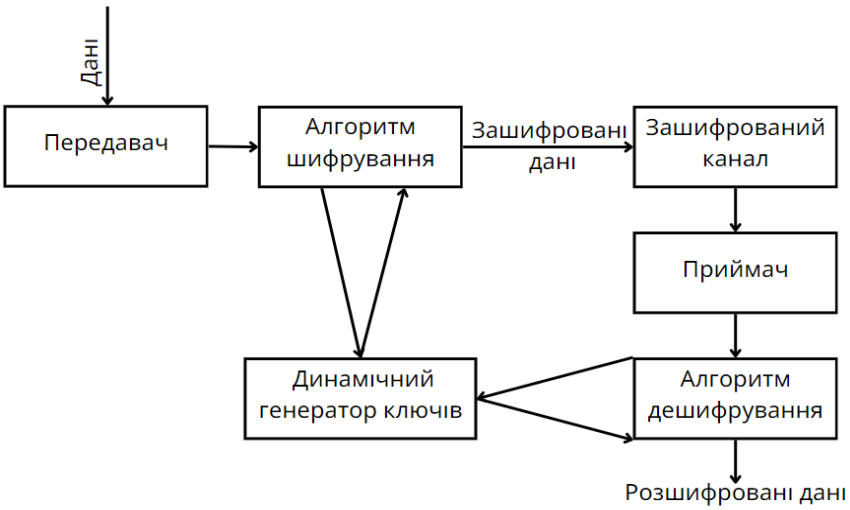

Рисунок 1 – Процес безпечної передачі даних між передавачем і приймачем у радіозв'язку

Опис зв'язків між елементами схеми:

1. Передавач:

- Передавач отримує дані, які потрібно передати, і надсилає їх у блок алгоритму шифрування.
- Для виконання шифрування цей блок взаємодіє з динамічним генератором ключів, який генерує унікальний ключ для кожного повідомлення чи пакету даних.
- Зашифровані дані надсилаються через зашифрований канал до приймача.

2. Зашифрований канал:

- Канал передачі (радіосигнал) слугує середовищем для пересилання зашифрованих даних від передавача до приймача.

3. Приймач:

- Приймач отримує зашифровані дані через зашифрований канал.
- Зашифровані дані передаються до блоку алгоритму дешифрування, який відновлює вихідні дані.
- Блок дешифрування також використовує динамічний генератор ключів, щоб створити той самий ключ, що й на передавачі, синхронізований за допомогою попередньо узгодженого секрету або параметрів радіоканалу.

4. Динамічний генератор ключів:

- У передавачі й приймачі генератори працюють синхронно, створюючи однакові ключі в реальному часі. Це дає змогу уникнути передачі ключів через канал зв'язку, що знижує ризик їх перехоплення [2].

Перехоплення радіосигналу є звичною практикою на полі бою. Тому алгоритми шифрування повинні бути максимально стійкими до криптоаналізу, навіть якщо противник має доступ до значних обчислювальних ресурсів. Класичні алгоритми, як-от AES (Advanced Encryption Standard), хоча і забезпечують високий рівень безпеки, часто виявляються непридатними для використання у військових пристроях, як-от портативні радіостанції чи дрони. Ці пристрої мають обмежену обчислювальну потужність, що робить ресурсомісткі алгоритми неприйнятними.

Легковагові шифри, наприклад, SPECK або SIMON, є перспективними для таких умов. Вони спеціально розроблені для роботи в обмежених апаратних середовищах і мають оптимізовану структуру, що знижує енерговитрати. Ці шифри використовують прості математичні операції, які виконуються швидко навіть на пристроях із низькою продуктивністю, водночас забезпечуючи захист від базових атак.

Ще одним важливим елементом у військовому зв'язку є динамічне управління ключами. Традиційні підходи до генерації і зберігання ключів не враховують специфіку бойових умов, де радіосигнал може бути перехоплений або заглушений. Для уникнення таких ризиків сучасні алгоритми пропонують генерувати ключі у реальному часі. Наприклад, можна використовувати псевдовипадкові генератори, які створюють унікальний ключ для кожного пакету даних. Початковий секрет, відомий лише сторонам комунікації, дає змогу синхронізувати генерацію ключів без їх передачі через радіоканал.

Особливої уваги заслуговують інноваційні методи генерації ключів, що базуються на фізичних параметрах середовища, як-от шум радіоканалу, фазові зміщення чи затримка сигналу. Такі параметри є унікальними для кожної ситуації, що ускладнює їх прогнозування або підробку супротивником.

Для підвищення загальної безпеки ефективним є використання гібридних підходів, які поєднують симетричне і асиметричне шифрування. У таких системах асиметричне шифрування використовується для захищеної передачі ключів, а симетричне – для шифрування великих обсягів даних. Така комбінація дає змогу досягти високої швидкості передачі за збереження надійності захисту.

Енергоефективність також є критичним параметром для алгоритмів шифрування. Військові пристрої часто працюють на батарейках чи інших автономних джерелах енергії, і їх ресурс може бути обмеженим. Оптимізація алгоритмів із використанням менш енерговитратних операцій, як-от додавання чи побітові зсуви замість множення або експоненціювання, дає змогу продовжити час роботи пристрою без заміни або заряджання батареї.

Важливо також враховувати стійкість алгоритмів до атак «людина посередині» (MITM) та глушіння сигналу. Використання технік, як-от зміна частоти передачі та додаткове шифрування контрольних пакетів, ускладнює роботу супротивника і підвищує загальну надійність системи

Захист радіозв'язку в умовах бойових дій є не лише технічною, але й стратегічною проблемою, адже ворог завжди намагається використовувати інформаційні слабкості для отримання переваги. Також важливо враховувати необхідність інтеграції розроблених алгоритмів у вже наявну військову інфраструктуру без значних витрат на її модернізацію. Використання динамічних шифрів з підтримкою адаптації до змін умов середовища дасть змогу мінімізувати ризики перехоплення або глушіння сигналу. До того ж приділяти увагу розвитку систем резервного зв'язку, які автоматично перемикаються на альтернативні канали в разі атак. Надійне шифрування відіграє значну роль не лише у захисті інформації, а й у збереженні життя військових, адже перехоплення даних може розкрити позиції підрозділів. Подальші дослідження у цій сфері мають зосередитися на спрощенні апаратної реалізації складних алгоритмів, щоб вони стали доступними навіть для малих мобільних пристроїв [3].

Отже, для захисту радіозв'язку у бойових умовах необхідно враховувати широкий спектр факторів, від апаратних обмежень до криптографічних загроз. Легковагові шифри, динамічне управління ключами та адаптивність до параметрів середовища є основними компонентами сучасних алгоритмів, які забезпечують швидку, надійну та захищену передачу інформації.

Список використаних джерел

1. Шолудько В. Г., Єсаулов М. Ю. Організація військового зв'язку: навч. посіб. Київ: 2017. 112 с.
2. Кутень Р. Б., Синявський О. Ю. Методи і засоби забезпечення стабільності та захисту радіозв'язку в умовах складної електромагнітної обстановки: наукова стаття. Львів: 2024.
3. Головін Ю. О. Основи радіозв'язку з рухомими об'єктами: навч. посіб. Київ: 2016. 14 с.

УДК 004.75:004.021

Ярошенко Б. М., здобувач вищої освіти,
Хмелівський Ю. С., асистент кафедри
інформаційних технологій

РОЛЬ АЛГОРИТМІВ У БЛОКЧЕЙН-ТЕХНОЛОГІЯХ

Донецький національний університет імені Василя Стуса, м. Вінниця

Блокчейн-технології є ключовим елементом сучасної цифрової економіки, забезпечуючи децентралізацію, прозорість і безпеку. Ці технології стали основою для інновацій, як-от криптовалюти, смарт-контракти та децентралізовані додатки (DApps). Алгоритми відіграють вирішальну роль у функціонуванні блокчейнів, забезпечуючи узгодженість даних, безпеку і масштабованість системи. Основні типи алгоритмів у блокчейні можна розділити на такі категорії:

1. Алгоритми консенсусу – це механізм, за допомогою якого блокчейн досягає узгодженості даних серед усіх учасників мережі без необхідності централізованих регуляторів. Оскільки мережа є одноранговою, процес перевірки транзакцій має бути автоматизованим. Алгоритми консенсусу забезпечують, щоб усі учасники мережі дотримувалися правил і здійснювали транзакції в належний спосіб. Вони також запобігають спробам подвійного витрачання цифрових валют, що є важливим для забезпечення безпеки. Серед найбільш відомих алгоритмів консенсусу – Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS) [1].

2. Алгоритми хешування – це математична операція, яка приймає вхідні дані будь-якого розміру, обробляє їх і створює вихідні дані фіксованого розміру, відомі як хеш. У блокчейн-технологіях основними функціями цього алгоритму є підвищення безпеки, оскільки будь-яка зміна даних змінює хеш блоку, роблячи втручання очевидним. Це забезпечує цілісність даних, оскільки наступний блок містить хеш попереднього, і зміна даних у попередньому блоці робить ланцюг недійсним. Хешування також допомагає перевіряти дані – порівнюючи хеш блоку з хешем, на який посилається наступний блок, можна підтвердити, що дані не були змінені [2].