УДК 621.39

ЗАЩИЩЕННАЯ СИСТЕМА РАДИОУПРАВЛЕНИЯ БЕСПИЛОТНЫМ ЛЕТАТЕЛЬНЫМ АППАРАТОМ С ПСЕВДОСЛУЧАЙНОЙ ПЕРЕСТРОЙКОЙ РАБОЧЕЙ ЧАСТОТЫ И КРИПТОГРАФИЧЕСКИМ ШИФРОВАНИЕМ

[1]Я.А. Мойсюк-Дранько, [2]И.А. Дубовик

[1]Учреждение образования «Национальный детский технопарк», г. Минск, Республика Беларусь

[2]Учреждение образования «Военная академия Республики Беларусь», г. Минск, Республика Беларусь

Аннотация. В статье рассматривается комплексный подход к обеспечению защищенности канала связи с беспилотными летательными аппаратами в условиях радиоэлектронного противодействия. Проведен анализ криптографических алгоритмов, обоснован выбор AES-256 для защиты командно-телеметрической информации. Представлена реализация метода псевдослучайной перестройки радиочастоты с использованием перемешанного конгруэнтного генератора. Разработанное решение обеспечивает высокий уровень криптографической стойкости и помехоустойчивости канала связи.
Ключевые слова: беспилотный летательный аппарат; радиосвязь; криптографическая защита; AES; псевдослучайная перестройка рабочей частоты; радиоэлектронное противодействие; перемешанный конгруэнтный генератор; помехозащищенность; перехват команд; телеметрия.

A SECURE RADIO CONTROL SYSTEM FOR AN UNMANNED AERIAL VEHICLE WITH FREQUENCY-HOPPING SPREAD SPECTRUM AND CRYPTOGRAHIC ENCRYPTION

[1]Y.A. Moisiuk-Dranko, [2]I.A. Dubovik
[1]Educational Institution "National Children's Technopark", Minsk, Republic of Belarus
[2]Educational Institution "Military academy the Republic of Belarus", Minsk, Republic of Belarus

Abstract. This article examines a comprehensive approach to ensuring the security of communications with unmanned aerial vehicles (UAV) in the face of electronic countermeasures. An analysis of cryptographic algorithms is conducted, substantiating the choice of AES-256 for protecting command and telemetry information. An implementation of a frequency hopping spread spectrum method using a permuted congruential generator is presented. The developed solution ensures a high level of cryptographic security and noise immunity for the communication channel.
Keywords: unmanned aerial vehicle; radio communication; cryptographic protection; AES; frequency hopping spread spectrum; electronic countermeasures; permuted congruential generator, interference immunity; command interception; telemetry.

Введение

Эффективность применения беспилотных летательных аппаратов (далее - БЛА) напрямую зависит от защищенности канала связи. В условиях интенсивного радиоэлектронного противодействия существующие системы управления БЛА сталкиваются с угрозами перехвата команд, постановки помех и захвата управления.

Основная часть

Для обеспечения конфиденциальности и целостности передаваемых данных был проведен сравнительный анализ алгоритмов симметричного шифрования: AES, 3DES и RC4.

Алгоритм AES-256 демонстрирует оптимальное сочетание криптографической стойкости и производительности. При использовании 256-битного ключа обеспечивается стойкость на уровне 2^{256} комбинаций, что делает атаки полным перебором практически невозможными. Высокая скорость шифрования критически важна для систем реального времени.

Алгоритм 3DES, представляющий собой трехкратное применение алгоритма DES, не гарантирует достаточную защиту БЛА.

Потоковый шифр RC4 был исключен вследствие выявленных критических уязвимостей в генерации ключевого потока и возможности статистических атак при определенных условиях использования.

На основе проведенного анализа выбран алгоритм AES-256 как оптимальное решение для защиты команд и телеметрии БЛА.

Для защиты от радиоэлектронного противодействия применен метод псевдослучайного переключения рабочей частоты (далее – ППРЧ), основанный на быстром переключении несущей частоты передатчика по псевдослучайному закону, известному обеим сторонам канала связи. Метод ППРЧ обладает рядом существенных преимуществ. Обеспечивается скрытность передачи: быстрое переключение частот создает сигнал, неразличимый для средств радиоразведки противника, что значительно затрудняет обнаружение и идентификацию канала связи. Достигается высокая помехозащищенность: для эффективного подавления сигнала с ППРЧ противнику необходимо создавать помеху в широкой рабочей полосе частот, что требует значительно большей мощности по сравнению с постановкой помех на фиксированной частоте. Система демонстрирует устойчивость к узкополосным помехам: даже при наличии мощной помехи на отдельных частотах общая пропускная способность канала снижается пропорционально отношению подавленных частот к общему числу используемых каналов.

Критически важным элементом системы ППРЧ является генератор псевдослучайных чисел, определяющий последовательность смены рабочих частот. Для генерации последовательности выбран перемешанный конгруэнтный генератор (далее - PCG). PCG сочетает преимущества линейных конгруэнтных генераторов с дополнительным этапом перемешивания выходных значений.

PCG обеспечивает минимальные корреляционные паттерны, что критически важно для предотвращения предсказания последовательности переключения частот противником. Высокая производительность генератора позволяет реализовать частоту переключения до нескольких тысяч скачков в секунду без создания значительной вычислительной нагрузки на микроконтроллер системы управления БЛА.

Синхронизация передающей и приемной сторон осуществляется путем использования общего начального значения (seed) для

PCG-генератора, передаваемого по защищенному каналу на этапе инициализации системы. Данный подход позволяет обеим сторонам независимо генерировать идентичную последовательность.

Заключение

Разработано комплексное решение по защите канала связи с БЛА, сочетающее криптографическую защиту AES-256 и радиочастотную защиту методом ППРЧ с PCG-генератором. Многоуровневая архитектура обеспечивает высокую стойкость к радиоэлектронному противодействию, требуя от противника одновременного преодоления криптографической и радиочастотной защиты.

Список использованных источников

1. Singh G., Supriya A. (2013) A Study of Encryption Algorithms for Information Security. *International Journal of Computer Applications*. 67 (19), 33-38.
2. O'Neill M. (2014) PCG: A Family of Simple Fast Space-Efficient Statistically Good Algorithms for Random Number Generation. *Technical Report HMC-CS-2014-0905, Harvey Mudd College.*
3. Daemen J., Rijmen V. (2002) *The Design of Rijndael: AES — The Advanced Encryption Standard.* Germany, Springer-Verlag.
4. Torrieri D. (2015) *Principles of Spread-Spectrum Communication Systems.* Germany, Springer.

References

1. Singh G., Supriya A. (2013) A Study of Encryption Algorithms for Information Security. *International Journal of Computer Applications*. 67 (19), 33-38.
2. O'Neill M. (2014) PCG: A Family of Simple Fast Space-Efficient Statistically Good Algorithms for Random Number Generation. *Technical Report HMC-CS-2014-0905, Harvey Mudd College.*
3. Daemen J., Rijmen V. (2002) *The Design of Rijndael: AES — The Advanced Encryption Standard.* Germany, Springer-Verlag.
4. Torrieri D. (2015) *Principles of Spread-Spectrum Communication Systems.* Germany, Springer.

Сведения об авторах

Мойсюк-Дранько Я.А., учащийся, учреждение образования «Национальный детский технопарк», jajaroslove@gmail.com.

Дубовик И.А., канд. техн. наук, доц., доц. каф. тактики и вооружения радиотехнических войск факультета противовоздушной обороны, учреждение образования «Военная академия Республики Беларусь», dubaiilia94@gmail.com.

Information about the authors

Moisiuk-Dranko Y.A., student, educational institution "National children's technopark", jajaroslove@gmail.com.

Dubovik I.A., Cand. Sci. (Tech.), Associate Professor, Associate Professor of the Department of Tactics and Armament of Radiotechnical Troops of the Faculty of Air Defense, educational institution "Military academy the Republic of Belarus", dubaiilia94@gmail.com.