© Navrotskyi D. Cryptographic system of protection UAVs communication channels against illegal intrusion // Ukrainian Scientific Journal of Information Security, 2014, vol. 20, issue 3, p. 248-252.

КРИПТОГРАФІЧНА СИСТЕМА ЗАХИСТУ РАДІОКАНАЛІВ БПЛА ВІД НЕСАНКЦІОНОВАНОГО ВТРУЧАННЯ

Денис Навроцький

Національний авіаційний університет, Україна

НАВРОЦЬКИЙ Денис Олександрович

Рік та місце народження: 1982 рік, м. Київ, Україна.
Освіта: Національний технічний університет України «Київський політехнічний інститут», 2007 рік; Національний авіаційний університет, 2009 рік.
Посада: асистент кафедри електроніки з 2013 року.
Наукові інтереси: інформаційна безпека, криптографія, стеганографія.
Публікації: більше 14 наукових публікацій, серед яких наукові статті, тези доповідей та патенти на винаходи.
E-mail: sg6336@yandex.ua

Анотація. *В статті наведено інформацію про ефективний криптографічний захист радіоканалу зв'язку «Земля – БПЛА – Земля». Розглянуті основні загрози для БПЛА і несанкціоновані методи втручання в канал зв'язку. Приведено приклад несанкціонованого втручання в канал зв'язку «Земля – БПЛА – Земля». Запропоновано рішення захисту командно-телеметричної інформації БПЛА. Відображено спосіб і апаратно-програмна реалізація «навісного» захисту БПЛА за допомогою розробленого шифратору. Надано схему під'єднання шифратора до наземної і бортової апаратури. Розглянуто механізм синхронізації шифраторів БПЛА. Наведено результати досліджень захисту каналу зв'язку для БПЛА. Надано опис апаратно-програмної реалізації захисту. Приведені технічні характеристики апаратної реалізації шифратора. Отримані результати дозволяють підвищити ефективність роботи систем захисту інформації БПЛА та створюють підґрунтя для подальших досліджень щодо розробки нових ефективних систем захисту інформації з використанням «навісного» захисту, що не вносить змін в роботу БПЛА.*

Ключові слова: *захист інформації, криптографія, перехоплення інформації, криптоаналіз, БПЛА.*

Вступ

Ринок БПЛА досить різноманітний за своїм асортиментом, цінами і доступністю. Зараз зібрати багатофункціональний БПЛА можна вже в домашніх умовах. Якщо, воєнні і дорогі БПЛА (які не доступні пересічному користувачу) оснащенні надійними системами захисту, то у «бюджетних» БПЛА цей захист досить часто відсутній. В той же час, досить поширене явище, коли саме дешеві БПЛА використовуються для відповідальних задач, таких як спостереження за місцевістю, або доставкою вантажу та інше. Іноді готові БПЛА можуть забороняти до продажу, але окремі деталі (з яких можна зібрати БПЛА) представлені в широкому асортименті на ринку, їх може купити будь хто і самостійно зібрати або модифікувати потрібний БПЛА. Оскільки модельний ряд «бюджетних» і власноруч зроблених БПЛА досить великий, то постає питання про створення універсальної системи захисту, яку можна адаптувати під різні моделі БПЛА і яка б не впливала на функціонування БПЛА. У користувача зазвичай відсутня можливість вносити зміни в прошивку мікроконтролера (МК), що керує БПЛА, тому вирішення проблеми захисту БПЛА тільки програмним шляхом ускладняється закритістю коду. Розробка потребує апаратно-програмної реалізації, що під'єднується до апаратури БПЛА не впливаючи на її функціонування («навісний» захист).

Останні дослідження та публікації

Ідея була взята з програмування, де використовується захист навісного типу (протектор) для захищення програм в яких не передбачений захист [1,2]. Подібна система була недавно розроблена Intel і має назву Data Protection Technology for Transactions, вона представляє собою перше в галузі рішення для наскрізного шифрування користувальницьких і фінансових даних [3].

Рис. 1. Ізраїльська розробка самозахисту БПЛА SPS-65V5 при радіоелектронній боротьбі

Також до уваги слід взяти ізраїльську розробку захисту БПЛА SPS-65V5 (див. рис. 1), що була продемонстрована на паризькій авіаційній виставці (Paris Air Show 2013) фірмами Elbit Systems

EW і Sigint – Elisra's («Elisra»), як система самозахисту при радіоелектронній боротьбі (a self protection Electronic Warfare system) [4].

Формулювання цілей статті (постановка завдання)

Дослідити захищеність каналу зв'язку БПЛА. Розробити криптографічну систему захисту БПЛА. Продемонструвати основні вузли і способи підключення шифратору до бортової і наземної апаратури. Надати пояснення щодо апаратно-програмної реалізації шифратора.

Основна частина

Способи несанкціонованого втручання в роботу БПЛА

Існує три основні способи несанкціонованого втручання в роботу БПЛА. Перший з них це механічний вплив, можна збити БПЛА. Другий спосіб – це використання «глушилок», пристроїв які пригнічують будь-які радіоканали, пов'язані з роботою БПЛА, шляхом генерації на заданих частотах дуже потужного пригнічуючого сигналу. Третій спосіб полягає в перехваті і підміні передаваємих/нриймаємих пакетів даних БПЛА.

Розглянемо більш детально останній з цих способів. Відомі випадки, коли БПЛА вдавалось посадити шляхом підміни одного сигналу іншим. Наприклад, описано випадок, коли спеціальна наземна станція генерувала більш потужний (ніж у супутника) GPS сигнал з хибними координатами. В такому випадку БПЛА, який орієнтується за допомогою GPS, приймав рішення що він знаходиться в іншій місцевості і виконував запрограмовані для цієї місцевості дії (міг кружляти на місці або приземлитись, якщо із-за хибних координат він «думав», що вже долетів до точки приземлення). Також описані і інші випадки. Ще один приклад описує несанкціоноване проникнення до каналу зв'язку і підміну пакетів даних для командної і телеметричної інформації. Був випадок, коли підміною пакетів даних в каналі зв'язку командно-телеметричної інформації вдалось примусить БПЛА скинути бомбу не в указаному місці, а в точці повернення на базу. Захист командно-телеметричної інформації в БПЛА це актуальна задача.

Спосіб захисту від несанкціонованого втручання в командно-телеметричну інформацію БПЛА

У дешевих БПЛА не передбачений криптографічний захист каналу зв'язку. Тобто *одним і тим же командам, що надходять з землі на борт і з борта на землю відповідають одні і ті ж сигнали*. Що дає можливість зловмиснику перехопити керування БПЛА і використати його на свій розсуд (як саме це робиться буде показано далі).

На ринку представлена продукція фірм, що спеціалізуються на різних модулях БПЛА (трансивери, автопілоти, корпуси, …). Ці модулі обмінюються даними між собою використовуючи стандартні протоколи обміну даних. Наприклад, один із самих відомих і простих способів передачі даних реалізується в БПЛА за допомогою універсального асинхронного прийомпередатчика (УАПП, англ. Universal Asynchronous Receiver-Transmitter, UART).

Передача даних в UART виконується по одному біту в рівні проміжки часу. Цей часовий проміжок визначається заданою швидкістю UART і для певного з'єднання вказується в бодах (що в даному випадку відповідає бітам за секунду). Існують загальноприйняті значення швидкостей:
300; 600; 1200; 2400; 4800; 9600; 19200; 38400; 57600; 115200; 230400; 460800; 921600 бод. Швидкість (*S*, бод) і тривалість біта (*T*, секунд) пов'язані співвідношенням:

$$T = 1 / S.$$

Швидкість в бодах іноді називають сленговим словом *бітрейт*.

Як правило, всі пристрої працюють на трьох стандартних швидкостях: 9600, 19200, 115200. Також можливі й інші варіанти, навіть використання нестандартних швидкостей, що змінюються з часом.

Зазвичай, UART що використовується в БПЛА складається з двох каналів передачі даних TXD (transmit) – передаючий і RXD (receive) – приймаючий, живлення (+5V) і землі (GND), всі інші дроти допоміжні (рис. 2).

Рис. 2. Зовнішній вигляд роз'єму UART

Слід пам'ятати, про таку послідовність з'єднання:

TX1 → RX2. RX1 ← TX2.

Це значить, що при з'єднанні пристроїв за допомогою UART треба під'єднати передаючий провід до приймаючого, а приймаючий до передаючого (рис. 3).

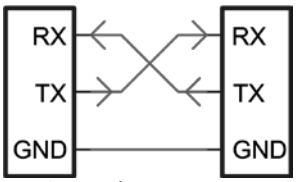

Рис. 3. Схема з'єднання двох UART

На рис. 4-6 показано підключення шифратора, у якого два UART. Один з UART підключається до апаратури, інший до трансиверу. Трансивер (англ. Transceiver — приймодавач) — пристрій для передачі і прийому сигналу між двома фізично різними середовищами системи зв'язку, саме слово утворено з часток англійських слів *trans*mitter (передавач) та r*eceiver* (приймач) [5]. Шифратор реалізовано на мікроконтролері (МКВ для борту і МКG для землі). Уся командно-телеметрична інформація перед відправкою в ефір проходить скрізь шифратор. Таким чином, перед відправленням в ефір будь яких даних, шифратор їх

попередньо зашифровує. При прийомі даних, шифратор їх розшифровує.

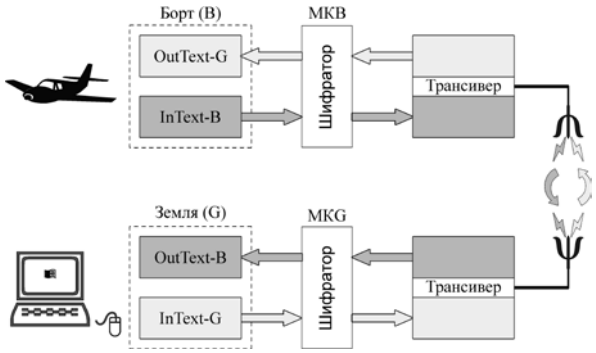

Рис. 4. Схематичне зображення включення шифратора (навісна система криптографічного захисту даних)

Рис. 5. Схематичне зображення підключення шифратора в розрив між наземною станцією і трансивером

Рис. 6. Схематичне зображення підключення шифратора в розрив між автопілотом і трансивером

Оскільки в більшості випадків користувач не має можливості вносити зміни в програму керування БПЛА, то був запропонований варіант навісного захисту. Суть полягає в тому, що шифратор включається в розрив після бортової/наземної апаратури і перед трансивером. Таким чином між трансиверами (радіоканал) завжди передається криптографічно захищені дані.

Опис алгоритму шифрування

Ядро алгоритму – поточний шифратор, що складається з генератора гами.

Криптографічні примітиви генерують псевдовипадкову послідовність бітів k_i, яка об'єднується з відкритим текстом m_i за допомогою складання за модулем два. Так формується шифрограма c_i:

$$c_i = m_i \oplus k_i .$$

Розшифрування відбувається за допомогою регенерації ключового потоку k_i і складання з шифрограмою c_i за модулем два. В наслідок властивостей складання за модулем два на виході ми отримуємо початковий незашифрований текст m_i:

$$m_i = c_i \oplus k_i = (m_i \oplus k_i) \oplus k_i .$$

Ініціалізація шифру складається з двох частин:

1. Ініціалізація ключів;
2. Генерація псевдо-випадкового слова.

Механізм синхронізація і ініціалізація шифраторів Земля – БПЛА – Земля

Оскільки за синхронізацію передачі даних в радіоканалі «Земля - БПЛА – Земля» відповідають трансивери на землі і на борту (рис. 4-6), то постає задача тільки синхронізувати ключі в шифраторах. Кожна пара шифраторів (земля і борт) містить в собі однакові стартові статичні унікальні ключі для цієї пари шифраторів. Також кожен сеанс зв'язку передається випадковий сеансовий ключ. Шифратор після отримання сеансового ключа і за допомогою алгоритму формування ключів, що має вхідним параметром стартовий статичний ключ, формує вектор ініціалізації (ключ), який вже безпосередньо впливає на генератор гамми.

Таким чином, кожна пара шифраторів містить унікальний статичний стартовий ключ, що встановлюється виробником шифратора. А всі сеансові ключі генеруються ПЗ користувача і пересилаються радіоканалом.

Такий підхід дозволяє шифрувати данні по різному для різних пар шифраторів БПЛА.

На випадок різних завад, шифратором періодично відправляється радіоканалом сигнал-мітка. Якщо в каналі зв'язку відбулись втрати, чи спотворення (щось завадило трансиверам вірно передати чи прийняти сигнал і як наслідок відбулась десинхронізація формування гамм в шифраторах), то шифратори запускають механізм синхронізації для встановлення однакових ключів шифрування для формування однакових гамм.

Для звичайних умов використання БПЛА достатньо механізму синхронізації даних між трансиверами. Періодична перевірка синхронності формування однакових гамм в шифраторах є підстраховка на всяк випадок, якщо БПЛА будуть використовувати в несприятливих умовах.

Дослідження захищеності каналу зв'язку БПЛА

Були проведені дослідження які виявили, що якщо не використовувати шифратор, то завжди одній і тій самій команді будуть відповідати одні її ті самі пересилаємі дані (як було описано вище, це дає змогу перехопити керування БПЛА третій особі).

Для перехоплення сигналу БПЛА, були автором розроблені спеціальні пристрої і програмне забезпечення (ПЗ) до них, схематичний принцип дії яких зображено на рис. 7 і рис. 8. Суть у тому, що пристрій «Приймач 2» під'єднується паралельно до каналу зв'язку після чого за допомогою спеціального ПЗ фіксуємо всі дані, що курсують каналом зв'язку між землею і бортом. Наприклад, прошу оператора надіслати команду «поворот вліво», він надсилає цю команду з землі на борт (від «Передавач» до «Приймач 1»). В той же час «Приймач 2» перехоплює цю команду і зберігає в пам'яті. Таким чином створюється таблиця відповідностей «команда – інформаційна послідовність». Тобто ми вже знаємо який сигнал відповідає якій командній інформації. Так само робиться і з телеметричною інформацією. Створюємо таблицю відповідностей в якій вказані показники БПЛА і інформаційна послідовність, що

надходить в цей час від БПЛА. Слід зазначити, що в ході експерименту було помічено, що структура командної і телеметричної інформації відмінна.

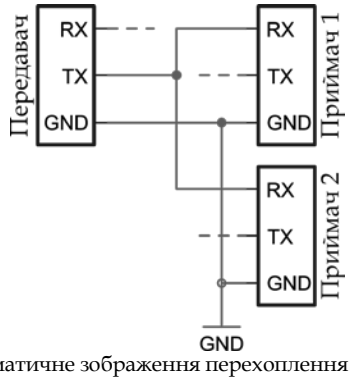

Рис. 7. Схематичне зображення перехоплення сигналу що надходить через UART

Після того, як сформована таблиця відповідностей (за допомогою пристрою, що працює як показано на рис. 7), стає можливим несанкціоноване втручання в керування БПЛА. Внесення змін відбувається як показано на рис. 8.

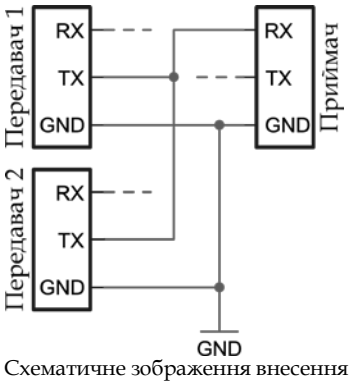

Рис. 8. Схематичне зображення внесення змін в надсилаємий сигнал що надходить через UART

При використанні шифратора (рис. 4, рис. 9, рис. 10) одній і тій самій команді будуть відповідати зовсім різні інформаційні послідовності. Оскільки шифратор побудовано на криптографічних примітивах, що генерують псевдовипадкову послідовність довільної довжини [6], за допомогою якої відбувається шифрування даних. Фактично, між шифраторами курсують криптографічно захищені дані. І їх перехоплення без знання відповідних ключів мало чим буде корисним зловмиснику. Оскільки криптоаналіз, це принципово більш складана задача, і швидко вона не виконується. Таким чином принципово ускладнюється для зловмисника задача перехоплення керуванням БПЛА.

Рис. 9. Зовнішній вигляд модуля шифрування (шифратора)

Рис. 10. Підключення модуля шифрування (шифратора) до бортової і наземної апаратури

Деякі характеристики шифратора

Автором були розроблені (спроектовані і реалізовані) шифратори для БПЛА (див. рис. 6 і рис. 7). Шифратори основані на мікроконтролері Atmega64 в якому запрограмований авторський алгоритм шифрування даних [6]. Живлення мікроконтролера співпадає з живленням бортової і наземної апаратури +5В. Тому шифратор можна під'єднати в розрив проводу без використання перетворювачів живлення. Була використана швидкість передачі даних 19200 бод. Отримано акт лабораторних випробувань, оформлено два патенти.

Слід зазначити, що шифратор може працювати на всіх доступних швидкостях UART, а не тільки 19200 бод (ця швидкість була в UART між модулями досліджуваного БПЛА, але в інших моделях БПЛА вона може бути іншою). Також слід зазначити, що не має значення який трансивер встановлено на бортовій і наземній апаратурі, він може передавати/приймати в діапазоні 30МГц – 6ГГц. Це обумовлене тим, що бортова і наземна апаратура приєднується до трансиверів через UART і шифратору не має значення на якій частоті трансивер передає дані далі в ефір. Трансивер отримує вже зашифровані дані і передає зашифровані дані далі. Шифратори до і після трансиверів займаються зашифровуванням і розшифровуванням даних, щоб ті були «зрозумілі» бортовій і наземній апаратурі.

Висновки

Розглянуті основні види загроз для БПЛА. Запропонований криптографічний захист командно-телеметричної інформації БПЛА. Описано принцип передачі даних між наземною або бортовою апаратурою і трансивером за допомогою UART. Показано спосіб несанкціонованого доступу до каналу зв'язку і захист від нього за допомогою розробленого шифратора. Наведено реалізацію навісної системи захисту для БПЛА, яка пройшла лабораторні випробування що підтверджено відповідним актом. Отримані результати дозволяють підвищити ефективність систем захисту БПЛА та створюють підґрунтя для подальших досліджень щодо розробки нових ефективних систем захисту інформації з використанням навісного захисту, що не вносить змін в роботу БПЛА.

Література

[1] Мельников В.П. Информационная безопасность и защита информации: Учебное пособие для вузов по спец. «Информационные системы и технологи» / В.П. Мельников, С.А. Клейменов,

А.М. Петраков; Под ред. С.А. Клейменова. — 5-е изд., стер. — М. : Academia, 2011. — 331 с. : ил. — (Высшее профессиональное образование). — Библиогр.: с. 327-328

[2] Фленов М. Компьютер глазами хакера / М.Е. Фленов. — 3-е изд., перераб. и доп. — СПб. : БХВ — Петербург, 2012. — 264 с. : ил. — Библиогр.: с. 260.

[3] Електронний ресурс. — Режим доступу: http://www.intelsecurity.com/solutions/intel-data-protection-technology.html

[4] Електронний ресурс. — Режим доступу: http://www.elbitsystems.com

[5] Електронний ресурс]. — Режим доступу: uk.wikipedia.org/wiki/Трансивер

[6] Патент UA №94189 «Спосіб криптографічного перетворення інформації».

УДК 003.26:004.056.55 (045)

Навроцкий Д.А. Криптографическая система защиты радиоканалов БПЛА от несанкционированного доступа

Аннотация. *В статье представлена информация об эффективной криптографической защите радиоканала связи «Земля – БПЛА – Земля». Рассмотрены основные угрозы для БПЛА и несанкционированные методы вмешательства в канал связи. Описан пример несанкционированного вмешательства в канал связи «Земля – БПЛА – Земля». Предложено решение защиты командно-телеметрической информации БПЛА. Показан способ и аппаратно-программная реализация «навесной» защиты БПЛА с помощью разработанного шифратора. Приведена схема подсоединения шифратора к наземной и бортовой аппаратуре. Рассмотрен механизм синхронизации шифраторов БПЛА. Приведено описание аппаратно-программной реализации защиты. Показаны технические характеристики аппаратной реализации шифратора. Полученные результаты позволяют увеличить эффективность работы систем защиты информации БПЛА и создают основание для дальнейших исследований, касающихся разработки новых эффективных систем защиты информации с использованием «навесной» защиты, которая не вносит изменений в работы БПЛА.*

Ключевые слова: *защита информации, криптография, перехват информации, криптоанализ, БПЛА.*

Navrotskyi D. Cryptographic system of protection UAVs communication channels against illegal intrusion

Abstract. *The article provides information on effective cryptographic protection of radio communication «Ground – UAV – Ground». The main threats to UAVs and illegal intrusion methods in communication channel are considered. An example of illegal intrusion into communication channel «Ground – UAV – Ground» is provided. A suggested approach to protect UAVs control telemetry data. The way and hardware-software implementation of «on-board» UAVs protection using the developed encoder is shown. The circuit of connection an encoder to ground and on-board equipment is available. The mechanism of synchronization UAVs with an encoder is considered. The investigation results of protection UAVs communication channel are offered. A description of hardware-software implementation of protection is given. Technical characteristics of hardware implementation of an encoder are presented. The obtained results can improve the efficiency of UAVs information security systems and create the basis for further researches in the field of development new effective information security systems using "on-board" protection that does not change the operation of UAVs.*

Key words: *information security, cryptography, information interception, cryptanalysis, UAV.*

Отримано *18 вересня 2014 року*, затверджено редколегією *3 жовтня 2014 року*