УДК 623.746.-519:004.056.55

А.Н.Давиденко, С.Я.Гильгурт, А.С.Потенко, А.К.Евдина, г. Киев

АНАЛИЗ ВОПРОСОВ ЗАКРЫТИЯ ИНФОРМАЦИОННОГО КАНАЛА СВЯЗИ С БЕСПИЛОТНЫМ ЛЕТАТЕЛЬНЫМ АППАРАТОМ

Abstract. The questions of cryptographic protection of communication interface to an unmanned flying vehicle using symmetric block encryption algorithms are analyzed. A solution based on reconfigurable computing to overcome found problems is proposed.

Введение. В настоящее время беспилотные летательные аппараты (БПЛА) находят широкое применение не только в военном деле, но и в гражданском секторе. Их все чаще применяют для решения таких народнохозяйственных задач, как аэрофотосъемка, метеорологические измерения, контроль состояния трубопроводов, линий электропередач и др. Наблюдаемый в мире бум использования беспилотной авиации в последнее время объясняется очевидными преимуществами таких устройств – низкой стоимостью, экономичностью, простотой эксплуатации и безопасностью обслуживающего персонала.

Вместе с тем становится актуальным ряд проблем, связанных с интенсивным развитием данного направления, как организационных и нормативно-правовых, так и технических. В том числе особую остроту приобретают вопросы информационной безопасности, в частности, закрытие телекоммуникационных каналов связи с БПЛА.

Анализ последних исследований и публикаций показывает, что актуальные вопросы закрытия информации в каналах связи наземных пунктов управления с беспилотными летательными аппаратами недостаточно полно освещены в литературе.

Целью настоящей работы является исследование проблем и технических сложностей, возникающих при использовании в данной области наиболее известных интерфейсов и алгоритмов шифрования, а также поиск путей их решения.

1. История развития. Беспилотные летательные аппараты появились в связи с необходимостью эффективного решения военных задач – тактической разведки, доставки боеприпасов к месту назначения, управления боевыми действиями и др. [1].

Первым применением беспилотных воздушных средств можно считать доставку австрийскими войсками бомб к осажденной Венеции с помощью воздушных шаров в 1849 году [2]. Мощным импульсом к развитию БПЛА послужило появление радиотелеграфа и авиации, что позволило существенно улучшить их автономность и управляемость.

В целом историю беспилотных летательных аппаратов можно условно разделить на четыре временных этапа [3]:

- с 1849-го года по начало XX века – попытки и экспериментальные опыты по созданию БПЛА, формирование теоретических основ аэродинамики, теории полета и расчета самолета в работах ученых;
- с начала XX века по 1945-й год – разработка БПЛА военного назначения (самолетов-снарядов с небольшой дальностью и продолжительностью полета);
- с 1945-го по 1960-е годы – период расширения классификации БПЛА по назначению и создание их преимущественно для разведывательных операций;
- с 1960-х годов по наши дни – расширение классификации и усовершенствование БПЛА, начало массового использования для решения задач невоенного характера.

2. Классификация. Гражданские БПЛА можно классифицировать по ряду признаков. Так, по дальности действия можно различить аппараты [4]:

- ближнего действия – до 25 км;
- малой дальности – до 100 км;
- средней дальности – до 500 км;
- большой дальности – более 500 км.

По взлетной массе различают следующие классы БПЛА:

- класс микро – до 5 кг;
- малый класс – 5-25 кг;
- легкий класс – 25-150 кг;
- средний класс – 150-750 кг;
- тяжелый класс – 750-15000 кг.

По типу БПЛА могут быть построены по самолетной либо по вертолетной схеме (мультикоптеры).

По кратности применения различают одноразовые и многоразовые БПЛА.

По способу старта и посадки "беспилотники" бывают:

- запускаемые с руки;
- запускаемые с пусковой установки;
- запускаемые "по-самолетному";
- вертикального взлета;
- воздушного старта;
- парашютной посадки;
- с посадкой "по-самолетному";
- с посадкой в сеть;
- с подхватом в воздухе.

По высоте полетов беспилотные летательные аппараты можно разделить на [5]:

• низковысотные – до 300 м;
• маловысотные – до 3000 м;
• средневысотные – до 8000 м;
• высотные – свыше 8000 м.

Силовая установка БПЛА может быть бензиновой или электрической. Бензиновый двигатель способен обеспечить намного более продолжительный полет, но сложнее в эксплуатации, менее надежен, требует большего времени при подготовке БПЛА к старту.

3. Технические проблемы. В настоящее время существует ряд технических проблем, сдерживающих развитие БПЛА. Наиболее существенной является задача обеспечения передачи информации по каналам связи между "беспилотником" и наземным пунктом управления в требуемом объеме, с заданной скоростью и без искажения. Данная задача решается путем увеличения пропускной способности и помехоустойчивости каналов передачи информации.

Проблема уязвимости каналов передачи данных между БПЛА и наземным комплексом управления (НКУ), в качестве которого чаще всего используется планшетный компьютер или ноутбук, решается одним из следующих способов [6]:

• применение автономных БПЛА;
• использование спутниковых ретрансляторов;
• закрытие линии связи криптографическими средствами.

В большинстве применений наиболее приемлемым и экономичным является последний из перечисленных вариантов.

Из приведенной выше классификации видно, что круг задач, решаемых БПЛА довольно широк. Требования, предъявляемые к каналам связи в целом, включая средства закрытия информации, также варьируются в широких пределах.

При оценивании требований, предъявляемых к системе защиты канала связи (СЗКС) криптографическими методами, можно выделить такие аспекты как: быстродействие, надежность шифрования, массогабаритные показатели бортовой части СЗКС. Данные факторы вступают в противоречие между собой, особенно при повышенных требованиях к пропускной способности канала и небольшой массе БПЛА.

На выбор алгоритма шифрования влияет ряд факторов, как организационных (в частности, вопросы сертификации), так и технических, среди которых важным моментом является реализуемость на имеющейся элементной базе.

Применение наиболее стойких алгоритмов шифрования, принятых в качестве государственных стандартов (AES, ГОСТ 28147-89), для закрытия коммуникационных каналов, которые основаны преимущественно на последовательном способе передачи данных (бит за битом), наталкивается на принципиальное ограничение, связанное с тем, что упомянутые шифры

относятся к классу алгоритмов так называемого блочного симметричного шифрования (БСШ).

Ниже данная проблема рассмотрена на примере закрытия алгоритмом ГОСТ 28147-89 одного наиболее распространенных коммуникационных интерфейсов RS-232.

4. Шифрование интерфейса RS-232 алгоритмом ГОСТ 28147-89. Коммуникационный пакет, передаваемый по протоколу RS-232 в зависимости от настроек может иметь длину от 9 до 11 битов. Из них 8 битов (в большинстве приложений) являются информационными, то есть несущими полезную нагрузку, остальные – служебные [7].

В соответствии с алгоритмом ГОСТ 28147-89 подлежащая закрытию информация группируется по 8 байтов (64 бита). Такой же размер имеет на выходе зашифрованный блок [8]. Следовательно, принимаемые по последовательному каналу биты необходимо сохранить в буферном запоминающем устройстве, а после обработки криптоалгоритмом снова преобразовать в последовательную форму. Как следствие, в тракт передачи информации схемой шифрования вносится задержка, зависящая от заданного алгоритма, быстродействия шифрующего устройства и выбранной скорости передачи коммуникационного канала. Оценим ее величину.

Полная задержка, возникающая в результате выполнения процедуры закрытия информации при передачи данных в одну сторону, включая операции зашифрования и расшифрования, в случае использования произвольного алгоритма БСШ определяется по формуле:

$$T_п = T_з + T_р,$$

где $T_з$ и $T_р$ – соответственно задержки зашифрования и расшифрования, равные:

$$T_з = T_р = (2\ T_{пр} + T_ш),$$

где $T_{пр}$ – время преобразования блока данных из последовательного в параллельный код либо обратно; $T_ш$ – время зашифрования/расшифрования (одинаковое в случае БСШ).

Время преобразования определяется как:

$$T_{пр} = N_б * (N_п + N_с) * T_с,$$

где $N_б$ – количество байтов в блоке для заданного алгоритма БСШ;

$N_п$ – количество полезных (информационных) битов в коммуникационном пакете;

$N_с$ – количество служебных битов в коммуникационном пакете (стартовый, стоповый, бит четности);

$T_с$ – период тактовой частоты, обратно пропорциональный выбранной скорости передачи.

Выполнив все подстановки, получаем:

$T_п = 2 \cdot (2 \cdot (N_б \cdot (N_п + N_с) \cdot T_с) + T_ш)$.

В случае использования в протоколе RS-232 восьми информационных битов, одного стартового, одного стопового, без контроля четности, скорости передачи 9600 бит/сек и алгоритма шифрования ГОСТ 28147-89 (размер блока – 8 байтов), величина полной задержки при передаче информации в одну сторону равна:

$T_п = 2 \cdot (2 \cdot (8 \cdot 10 \cdot 1/9600) + T_ш) = 2 \cdot (0{,}0167 + T_ш)$.

Следовательно, даже если время шифрования будет пренебрежимо малым, неустранимая задержка в коммуникационном канале для заданной скорости и выбранного алгоритма составит не менее 33 мс.

Следует заметить, что применение алгоритма AES приведет к вдвое большей неустранимой задержке, поскольку длина блока в этом случае составит 16 байтов (128 битов).

5. Предлагаемое решение. На основе вышеизложенного сформулируем требования, предъявляемые к системе защиты канала связи.

Аппаратная часть СЗКС должна состоять, как минимум, из двух частей – наземной и бортовой.

Для снижения задержки должно обеспечиваться максимально возможное быстродействие реализации криптоалгоритма.

Бортовая часть должна обладать минимальной массой и габаритами, потреблять минимум энергии.

Наземная часть должна удобно стыковаться с НКУ, обеспечивать функции конфигурации и контроля.

В целом система должна отличаться невысокой стоимостью разработки, изготовления и эксплуатации.

Создавать системы СЗКС, удовлетворяющие перечисленным требованиям, дает возможность использование реконфигурируемых унифицированных вычислителей (РУВ) на базе программируемых интегральных сем (ПЛИС). Данные устройства, а также многие вопросы, связанные с их разработкой и использованием, подробно рассмотрены в работах [9 - 14].

Согласно изложенным в данных публикациях сведениях о РУВ для решения рассматриваемой задачи следует использовать вычислители, оснащенные входным и выходным портом коммуникационного канала, который задействован для управления конкретного БПЛА, например, RS-232. Наличие интерфейса связи с ПК по универсальной шине USB позволит максимально полно удовлетворить требованиям по гибкости и удобству эксплуатации.

Отдельно следует остановиться на путях решения рассмотренной выше проблемы большой задержки, которая вносится в тракт управления СЗКС в случае использования алгоритмов БСШ. Для сокращения этой задержки можно применять либо потоковое шифрование, либо нестандартные алгоритмы БСШ с меньшим размером блока. Снижение криптостойкости при

этом можно компенсировать путем применения различных способов усиления криптографической защиты. Такие способы усиления включают в себя комбинирование нескольких алгоритмов шифрования и/или их динамическую модификацию во времени [15]. Существенно облегчить создание конфигураций для ПЛИС реконфигурируемых вычислителей, а также сократить сроки разработки СЗКС при использовании предложенного подхода позволяет Методика создания реконфигурируемых процессоров, реализующих усиленные алгоритмы закрытия информации, недавно разработанная в Институте проблем моделирования в энергетике им. Г.Е.Пухова НАН Украины [16].

Выводы. В настоящем исследовании проанализированы вопросы закрытия канала связи с беспилотным летательным аппаратом криптографическими средствами. Сформулированы требования, предъявляемые к таким средствам.

Выявлена проблема, связанная с возникновением в канале последовательной передачи данных временной задержки, величину которой невозможно сделать меньше определенного значения в случае применения наиболее известных и проверенных временем алгоритмов блочного симметричного шифрования.

В качестве решения предлагается использование реконфигурируемых вычислителей, которые позволяют создавать системы защиты канала связи, удовлетворяющие сформулированным требованиям. Определены возможные пути решения выявленной проблемы.

1. *Иноземцев Д.П.* Беспилотные летательные аппараты: теория и практика // ООО «ПЛАЗ» [Электронный ресурс]. – Санкт-Петербург. – Режим доступа: http://www.credo-dialogue.com/getattachment/6cf5bf18-cf53-4532-b5bd-1ed04dabc234/Bespilotnue-letatelnue-apparatu.aspx – Загл. с экрана. – (Дата обращения: 26.07.2014).
2. *Павлушенко М., Евстафьев Г., Макаренко И.* БПЛА: история, применение, угроза распространения и перспективы развития. М., «Права человека», 2005.
3. *Цепляева Т.П., Морозова О.В.* Этапы развития беспилотных летательных аппаратов // Открытые информационные и компьютерные интегрированные технологии. – №42 . – М.: 2009.
4. *Козлов Д.* Беспилотники сертифицируют // АвиаПорт.Ru. [Электронный ресурс]. – 30.10.2012. – Режим доступа: http://vpk.name/news/77892_bespilotniki_sertificiruyut.html – Загл. с экрана. – (Дата обращения: 26.07.2014).
5. *Мосов С.* Беспилотная разведывательная авиация стран мира: история создания, опыт боевого применения, современное состояние, перспективы развития: Монография. – К.: Изд. дом. "Румб", 2008. – 160 с.
6. *Галушко С.В.* Беспилотные летательные аппараты кардинально изменят облик авиации будущего // Наука и жизнь, - 2001. - No9. - С.18-20.
7. *ГукМ.* Аппаратные интерфейсы ПК. Энциклопедия. – СПб.: Питер, 2002. – 528 с.
8. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования: ГОСТ 28147-89. – М.: Госстандарт СССР, 1989. – 26 с.

9. *Гильгурт С.Я.* Применение типовых устройств на базе программируемой логики для решения вычислительных задач // Тез. докл. II международной конф. «Параллельные вычисления и задачи управления», 4–6 окт. 2004 г. – М.: Институт проблем управления им. В.А. Трапезникова РАН, 2004. – С. 514–530.
10. *Гильгурт С.Я., Гиранова А.К.* Некоторые вопросы обмена данными между персональным компьютером и реконфигурируемым устройством // Моделювання та інформаційні технології. Зб. наук. пр. ІПМЕ НАН України. – Вип. 43. – Київ: 2007. – С. 86–94.
11. *Гильгурт С.Я.* Анализ существующих унифицированных вычислителей для выполнения ресурсоемких расчетов // Моделювання та інформаційні технології. Зб. наук. пр. ІПМЕ НАН України. – Вип. 48. – Київ: 2008. – С. 115-120.
12. *Гильгурт С.Я.* Анализ применения унифицированных вычислителей в интеллектуальных системах // Искусственный интеллект. – Донецк: НАН Украины – институт проблем ИИ. – 2009. – №1. – С. 144–148.
13. *Гильгурт С.Я.* Анализ типовых режимов обмена данными с реконфигурируемыми вычислителями // Зб. наук. пр. ІПМЕ НАН України. – Київ, 2011. – Вип. 59. – С. 113–121.
14. *Гильгурт С.Я.* Реконфигурируемые вычислители. Аналитический обзор // Электронное моделирование. – 2013. – Т.35, № 4. – С. 49–72.
15. *Гиранова А.К.* Анализ подходов к повышению эффективности закрытия информации и вопросы их реализации на унифицированных вычислителях / А.К. Гиранова // Зб. наук. праць _ІПМЕ _м. Г.Є. Пухова НАНУ. - Київ, 2009. -Вип. 52. - С.78-83.
16. *Гильгурт С.Я., Гиранова А.К.* Методика создания реконфигурируемых процессоров, реализующих усиленные алгоритмы закрытия информации // Зб. наук. пр. ІПМЕ НАН України. – Київ, 2011. – Вип. 61. – С. 69–78.

Поступила 31.03.2014р.

УДК 66.045

О. А. Голік, І. А. Владимирський, м. Київ.

ВИЗНАЧЕННЯ ФАКТИЧНИХ ТЕПЛОФІЗИЧНИХ ХАРАКТЕРИСТИК ТЕПЛОІЗОЛЮЮЧИХ МАТЕРІАЛІВ ДЛЯ ЇХ ОБГРУНТОВАНОГО ВИБОРУ

The task of choosing heat and hydro insulation (insulating coatings) for protection of steel pipelines from the negative effects of condensate is considered.
Keywords: dew point, thermal conductivity, relative humidity.

Постановка задачі.

В роботі представлено вирішення практичного питання, пов’язаного з утворенням конденсату при експлуатації стальних трубопроводів на різних об’єктах енергетичної сфери, що характеризуються низькою температурою

