УДК 62-50:519.7(045)

В.В. Кириченко[1], канд. физ.-мат. наук, доц.,
Е.В. Лесина[2], канд. физ.-мат. наук, доц.
[1]Национальный авиационный университет, г.Киев
[2] Красноармейский индустриальный институт ГВУЗ "ДонНТУ",
lesina17@gmail.com

Особенности информационной системы управления БПЛА

В данной работе исследуются особенности функционирования информационного канала беспилотного летательного аппарата и принципы закрытия канала связи с БПЛА криптографическими средствами. Сформулированы требования, предъявляемые к таким средствам. Рассматривается способ шифрования информации, использующий прямую и обратную динамические системы. С помощью программы шифрования - дешифрования произведен ряд экспериментов по преобразованию информации, результаты которых демонстрируют определенные особенности алгоритмов, основанных на вышеуказанных системах.

Ключевые слова: информационный канал БПЛА, обратимые динамические системы, конечномерное кольцо целых чисел, генераторы псевдослучайных последовательностей.

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 – таких, как аэрофотосъемка, метеорологические измерения, контроль состояния трубопроводов, линий электропередач и т.д. Наблюдаемый в последние годы мировой бум использования беспилотной авиации 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.

На сегодняшний день большинство существующих беспилотных летательных аппаратов пилотируются вручную, с помощью пультов дистанционного управления, работающих на радиоканалах. При ручном управлении БПЛА возникают трудности, связанные с подготовкой пилотов, недостаточной рабочей дальностью, ограничениями, которые вызваны погодными условиями. Однако наиболее существенной является задача обеспечения передачи информации по каналам связи между летательным аппаратом, именуемым для краткости «Борт», и наземным пунктом управления (НПУ), который будем обозначать термином «Земля», в требуемом объеме, с заданной скоростью и без искажения. Данная задача решается путем увеличения пропускной способности и помехоустойчивости каналов передачи информации [1].

БПЛА как объект управления представляет собой сложную динамическую систему ввиду наличия большого количества связанных между собой параметров и сложных перекрестных взаимодействий между ними. Сложное движение часто разбивают на простейшие виды: угловые движения и движения центра масс, продольное и боковое движение.

Подобное деление органов управления является условным, так как можно привести режимы полета, в которых органы управления оказывают перекрестные воздействия на другие движения. В то же время такой подход позволяет выделить главные функции конкретных органов и каналов управления и независимо решать множество относительно простых и имеющих практическую ценность задач.

Информация о движении БПЛА поступает в соответствующие каналы, где формируются команды на рули, элероны и рычаг управления двигателем, которые обеспечивают заданное управление полетом. Стабильное управление полетом невозможно без создания приемлемой по качеству системы автоматического управления. Система управления самолетом служит для обеспечения полета по заданной траектории путем создания на крыле и оперении требуемых аэродинамических сил и моментов [2]. Возможны три типа систем управления – ручная, полуавтоматическая и автоматическая.

В ручной системе управления пилот-оператор, оценивая обстановку, обеспечивает выработку управляющих импульсов и с помо-

щью командных рычагов через пульты управления отклоняет рулевые поверхности, удерживая их в нужном положении.

В полуавтоматической системе управляющие сигналы пилота-оператора преобразуются и усиливаются различного рода автоматами и усилителями, обеспечивая оптимальные характеристики устойчивости и управляемости самолета.

Автоматические системы обеспечивают полную автоматизацию отдельных этапов полета, освобождая пилота-оператора от непосредственного участия в управлении самолетом.

К важнейшим видам информации, которыми обмениваются Борт и Земля, относятся командная, телеметрическая и видеоинформация [1, 3].

Командная информация представляет собой цифровые блоки (пакеты) фиксированной длины, которые поступают по радиоканалу с Земли на Борт для корректировки положения органов управления аппарата с целью выполнения маневров, задаваемых оператором НПУ.

Телеметрическая информация, передаваемая с Борта на Землю также в виде цифровых пакетов, содержит сведения о положении органов управления БПЛА.

Видеоинформация представляет собой широкополосные сигналы, снимаемые с бортовых цифровых видеокамер (или тепловизоров).

Бортовые видеокамеры необходимы для формирования панорамы в «поле зрения» БПЛА с целью обнаружения различных объектов на местности и определения их координат, разведки районов лесных и торфяных пожаров, крупных техногенных катастроф, экологического мониторинга и др. Отдельные тактические задачи, решаемые на основе бортовой видеоинформации, носят закрытый характер и подлежат защите от несанкционированного доступа. Простое решение проблемы криптографической защиты информации в широкополосных системах передачи видеосигналов состоит в применении для этих целей поточных шифров.

Проблема уязвимости каналов передачи данных между БПЛА и наземным комплексом управления, в качестве которого чаще всего используется планшетный компьютер или ноутбук, решается одним из следующих способов [1]:

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

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

При оценивании требований, предъявляемых к системе защиты канала связи криптографическими методами, можно выделить такие аспекты как: быстродействие, надежность шифрования, массогабаритные показатели бортовой части системы. 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.

Данная работа посвящена разработке программно-моделирующего алгоритма шифра, обеспечивающего скоростное поточное криптографическое преобразование широкополосных сигналов, передаваемых с борта БПЛА.

Математическая модель

В последнее время формируется новое направление в криптологии, которое связано с использованием динамических систем с хаотическим поведением [4,5]. Один из основных подходов в данной области базируется на использовании обратных систем управления для построения криптографических алгоритмов [6].

Динамические системы, обладающие хаотичным поведением, в настоящее время интенсивно используются и применяются в различных областях, в частности, для криптографической защиты информации [7]. На основе таких систем могут быть построены генераторы псевдослучайных последовательностей, которые в дальнейшем используются для кодирования открытого текста. С другой стороны, всякая динамическая система, имеющая структуру вход-выход, может использоваться непосредственно для преобразования информации. На основе таких систем создается шифратор. Входом в систему служит оцифрованное сообщение, а выходом является зашифрованный сигнал, направленный в телекоммуникационные сети. Необходимым условием для однозначной дешифровки является существование обратной системы.

В работе реализована система, общая схема которой представлена на рис. 1.

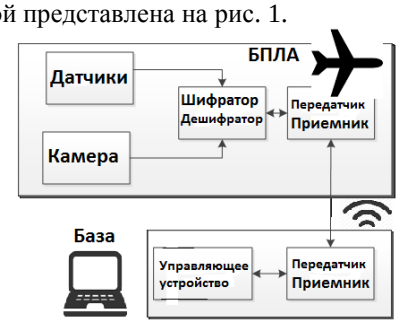

Рисунок 1 – Схема защиты канала связи с БПЛА

Любая информация, обрабатываемая различными дискретными вычислителями, в конечном итоге может быть представлена последователь-

ностью битов (0 или 1). Это представление, собственно, и используется при ее преобразовании с помощью различных динамических хаотических систем. Однако в вычислительных системах для представления различных типов данных используются более крупные единицы – байты (8 бит), машинные слова обычно в зависимости от разрядности машины – от 16 до 64. Чаще всего применяется побайтовое представление информации. Так, кодовые таблицы в вычислительных системах для представления текстовой информации указывают соответствие между 256 байтами и символами разных алфавитов.

Оперирование побайтно представленной информацией во многих случаях упрощает и алгоритмы ее обработки вычислительными системами. Поэтому будем считать дальше единицей информации байт, а информацию, обрабатываемую в компьютерной среде, представлять как последовательность различных байтов.

В качестве способа шифрования информации выберем способ ее непосредственного преобразования с помощью динамической хаотической системы, использующей прямую и обратную системы.

Отметим, что традиционными примерами динамических систем с хаотическим поведением выступают системы Чуа, Лоренца и Ресслера [8].

1) Система Чуа:

Прямая:

$$\begin{cases} \dot{x}_1 = A_1(A_2(x_2 - x_1) - (x_1 + 1)), \\ \dot{x}_2 = A_3(A_2(x_1 - x_2) - x_3 + Av_{in}), \\ \dot{x}_3 = A_4(x_2 - A_5 x_3). \end{cases}$$

Обратная:

$$\begin{cases} \dot{x}'_1 = A_1(A_2(x'_2 - x'_1) - (x'_1 + 1), \\ v_{out} = \dfrac{1}{A}(\dfrac{1}{A_3}\dot{x}_2 - A_2(x'_1 - x'_2) + x'_3, \\ \dot{x}'_3 = A_4(x'_2 - A_5 x'_3). \end{cases}$$

Здесь и далее v_{in} и v_{out} – входные сигналы прямой и обратной систем соответственно.

2) Система Лоренца:

Прямая:

$$\begin{cases} \dot{x}_1 = A_1(x_2 - x_3), \\ \dot{x}_2 = A_2 x_1 - x_2 - x_1 x_3 + Av_{in}, \\ \dot{x}_3 = x_1 x_2 - A_3 x_3. \end{cases}$$

Обратная:

$$\begin{cases} \dot{x}'_1 = A_1(x'_2 - x'_3), \\ v_{out} = \dfrac{1}{A}(\dot{x}_2 - A_2 x'_1 + x'_2 + x'_1 x_3), \\ \dot{x}'_3 = x'_1 x'_2 - A_3 x'_3. \end{cases}$$

3) Система Ресслера:

Прямая:

$$\begin{cases} \dot{x}_1 = -(x_2 + x_3), \\ \dot{x}_2 = x_1 + A_1 x_2 + Av_{in}, \\ \dot{x}_3 = A_3 + x_3(x_1 - A_2). \end{cases}$$

Обратная:

$$\begin{cases} \dot{x}'_1 = -(x'_2 + x'_3), \\ v_{out} = \dfrac{1}{A}(\dot{x}_2 - x'_1 - A_1 x'_2), \\ \dot{x}'_3 = A_3 + x'_3(x'_1 - A_2). \end{cases}$$

Выходы всех прямых систем и входы обратных равны $\dot{x}_2$.

Дискретизируя дифференциальные уравнения с шагом 1, получим:

1) Система Чуа:

Прямая:

$$\begin{cases} x_1(t+1) = x_1(t) + A_1[A_2(x_2(t) - x_1(t)) - (x_1(t) + 1)], \\ x_2(t+1) = x_2(t) + A_3[A_2[x_1(t) - x_2(t)] - x_3(t) + Av_{in}(t)], \\ x_3(t+1) = x_3(t) + A_4[x_2(t) - A_5 x_3(t)]. \end{cases}$$

Здесь и далее выход системы $v_{out}(t)=x_2(t)$.

Обратная:

$$\begin{cases} x_1(t+1) = x_1(t) + A_1[A_2(x_2(t) - x_1(t)) - (x_1(t) + 1)], \\ v_{out}(t+1) = \dfrac{1}{A}\left(\dfrac{x_2(t+1) - x_2(t)}{A_3} - A_2[x_1(t) - x_2(t)] + x_3(t)\right), \\ x_3(t+1) = x_3(t) + A_4[x_2(t) - A_5 x_3(t)]. \end{cases}$$

2) Система Лоренца:

Прямая:

$$\begin{cases} x_1(t+1) = x_1(t) + A_1[x_2(t) - x_3(t)], \\ x_2(t+1) = x_2(t) + A_2 x_1(t) - x_2(t) - x_1(t)x_3(t) + Av_{in}(t), \\ x_3(t+1) = x_3(t) + x_1(t)x_2(t) - A_3 x_3(t). \end{cases}$$

Обратная:

$$\begin{cases} x_1(t+1) = x_1(t) + A_1[x_2(t) - x_3(t)], \\ v_{out}(t+1) = \dfrac{1}{A}[x_2(t+1) - x_2(t) - A_2 x_1(t) + x_2(t) + x_1(t)x_3(t)], \\ x_3(t+1) = x_3(t) + x_1(t)x_2(t) - A_3 x_3(t). \end{cases}$$

3) Система Ресслера:

Прямая:

$$\begin{cases} x_1(t+1) = x_1(t) - x_2(t) - x_3(t), \\ x_2(t+1) = x_2(t) + x_1(t) + A_1 x_2(t) + Av_{in}(t), \\ x_3(t+1) = x_3(t) + A_3 + x_3(t)x_1(t) - A_2 x_3(t). \end{cases}$$

Обратная:

$$\begin{cases} x_1(t+1) = x_1(t) - x_2(t) - x_3(t), \\ v_{out}(t+1) = \dfrac{1}{A}[x_2(t+1) - x_2(t) - x_1(t) - A_1 x_2(t)], \\ x_3(t+1) = x_3(t) + A_3 + x_3(t)x_1(t) - A_2 x_3(t). \end{cases}$$

В значительной мере степень криптографической стойкости, конфиденциальность определяются параметрической и функциональной сложностью, связанной с построением обратной системы.

Множества входных и выходных символов, компоненты $x_i(t)$, $i = 1,2,3$, понимаются как

элементы конечного поля $GF(q)$ или кольца $Z(q)$, а операции сложения и умножения есть соответствующие операции в этом поле или кольце.

Для цифровой обработки информации применяются, как правило, поля или кольца характеристики 2, то есть $q = 2^n, n \in N$. Учитывая особенности представления информации в памяти компьютера, в программе используются поля $GF(2^{8k})$, или кольца $Z(2^{8k})$, k=1,2,3,4. Это связано с тем, что информационный файл сохраняется в памяти компьютера как последовательность байтов. Существует несколько типов представления поля Галуа. В программе использованы два из них: целочисленное представление, и векторное. Неявно при разработке алгоритмов вычисления в полях используется также полиномиальное представление.

Расшифровка осуществляется обратным автоматом Лоренца, который существует для любого $A \in GF(q)$ или же $A \in Z(q)$, $A \neq 0$.

Ключом системы шифрования являются коэффициенты системы A_i и исходное состояние автомата. При необходимости ключевым параметром может быть также величина k, которая задает размер обрабатываемого блока информации (квант информации) в k байт.

Основные этапы алгоритма шифрования следующие:

1) инициализация (настройка) автомата – задаются его коэффициенты и входное состояние по ключу шифрования и размер кванта;

2) обработка очередного кванта информации в соответствии с системой, которая находится в текущем состоянии, с выдачей зашифрованного кванта и переходом в новое состояние. Этот шаг повторяется до конца файла, который обрабатывается.

При реализации пересчета значений состояний S_i автомата, вычисления происходят в поле $GF(2^p)$ или кольце $Z(2^p)$.

Система шифрования автоматом Лоренца является симметричной. Это означает, что при расшифровке файла используется тот же ключ, что и при шифровании.

Пересчет коэффициентов обратного автомата происходит во время настройки системы для расшифровки файла.

В результате работы шифратора выходом будет некоторая последовательность, которая должна иметь свойства псевдослучайной.

Мощность кольца может быть легко увеличена, что усложнит или сделает невозможным взлом методом перебора значений ключа.

Результаты

Для исследования псевдослучайной последовательности чисел есть две группы тестов.

Графические тесты. Статистические свойства последовательностей отображаются в виде графических зависимостей, по виду которых делают выводы о свойствах исследуемой последовательности.

Оценочные тесты. Статистические свойства последовательностей определяются числовыми характеристиками. На основе оценочных критериев делаются выводы о степени близости свойств анализируемой и истинно случайной последовательностей. Для оценки псевдослучайной последовательности чисел, генерируемых с помощью системы Лоренца, используется пакет статистических тестов NIST [9].

На рисунках 2-5 показаны результаты шифрования периодического и постоянного сигналов с использованием автомата Лоренца в конечном кольце $Z(2^8)$ при условиях: A_1=9, A_2=99, A_3=113, x_{10}=116, x_{20}=47, x_{30}=38.

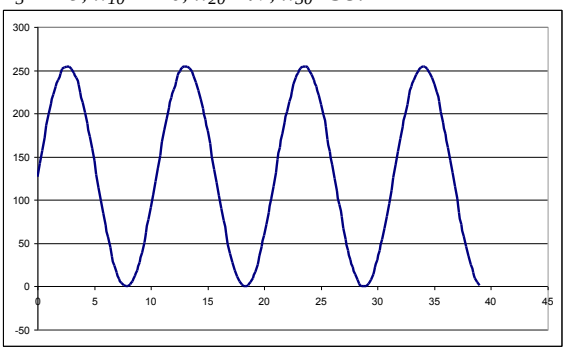

Рисунок 2 – Периодический сигнал

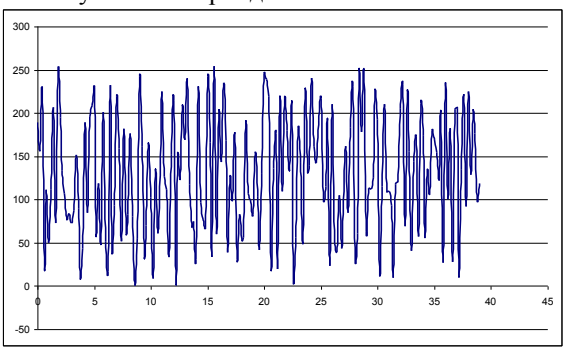

Рисунок 3 – Преобразованный периодический сигнал с помощью автомата Лоренца

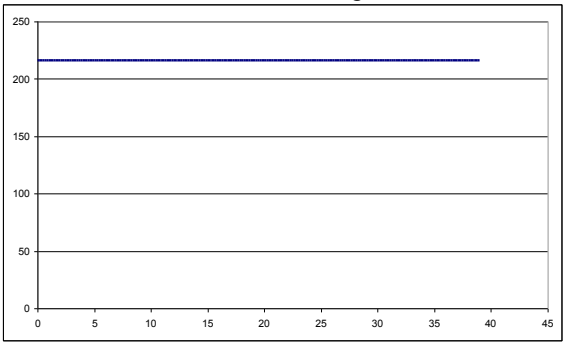

Рисунок 4 – Постоянный сигнал

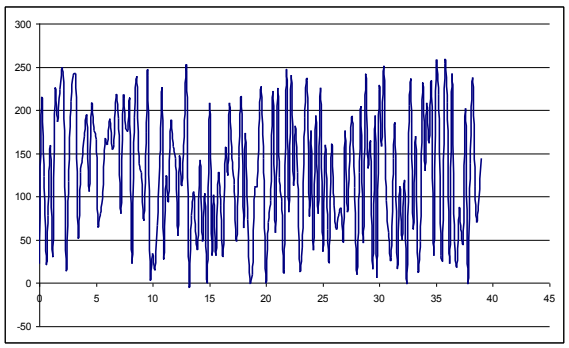

Рисунок 5 – Преобразованный постоянный сигнал с помощью автомата Лоренца

Использование тестов NIST показало, что при шифровании системой Лоренца в кольце Z_8 получается неудовлетворительный результат. С увеличением мощности кольца результат улучшается, и время работы тестов уменьшается. При добавлении в систему предиката наблюдается небольшое улучшение результата. Выполнение всех операций в полях $GF(2^p)$ заметно улучшает результаты.

Для сравнения был реализован алгоритм A5 [10], который используется для получения псевдослучайной последовательности из трех линейных регистров сдвига с обратной связью, и алгоритм RC4 [10], специально предназначенный для потоковых шифров. Алгоритм A5 используется для шифрования сеанса между телефонными абонентами телефонной трубки и базовой станцией в европейской цифровой системе мобильной связи GSM (Group Special Mobile). В результате было установлено, что шифры, использующие обратную динамическую систему для преобразования и передачи информации в поле $GF(2^{16})$ или в кольце Z_{32}, не уступают по эффективности известным алгоритмам и имеют высокую скорость передачи. Таким образом, новый алгоритм имеет высокую степень защиты и может быть использован для безопасной передачи данных через информационные каналы БПЛА или с помощью других средств.

Заключение

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

Разработанный программный комплекс реализует один из возможных алгоритмов криптографически защищенной передачи широкополосных видеосигналов с борта БПЛА на Землю.

Любую управляемую динамическую систему, имеющую структуру вход-выход, можно использовать непосредственно для преобразования информации. Идея применения обратных систем управления со сложным поведением траекторий лежит в основе задачи синтеза новых эффективных алгоритмов защиты информации, в первую очередь, от несанкционированного доступа.

Проведенные исследования и их оценка позволяют утверждать, что получены новые результаты, расширяющие теоретическую базу современной криптологии и являющиеся перспективными для создания эффективных криптографических алгоритмов. В то же время открытым остается ряд вопросов, связанных с влиянием динамических параметров на устойчивость криптоалгоритмов к атакам, устойчивость к искажениям информации, появлению инвариантных многообразий.

Список использованной литературы

1. Программно-моделирующий комплекс ВРС алгоритма поточного шифрования и помехоустойчивого кодирования видеосигналов, передаваемых с борта БПЛА / А. Белецкий, А. Максименко, Д. Навроцкий и др. // Захист інформації. – Т. 16. – №3. – С. 184-191
2. Моисеев В.С. Прикладная теория управления беспилотными летательными аппаратами: моногр. / В.С. Моисеев. – Казань: ГБУ «Республиканский центр мониторинга качества образования» (Серия «Современная прикладная математика и информатика»). – 768 с.
3. Слюсар В. Передача данных с борта БПЛА: стандарты НАТО / В. Слюсар // Электроника: НТБ. – 2010. – №. 3. – С. 80–86. http:// www.slyusar.kiev.ua /UAV-1.pdf
4. Kirichenko V.V. Information security of communication channel with UAV / V.V. Kirichenko // Electronics and control systems. – 2015. – N 3(45). – P. 23-27
5. Кириченко В.В. Эффективность использования обратных систем управления для преобразования и передачи информации / В.В. Кириченко // Моделирование, идентификация, синтез систем управления: тез. докл. 11-й межд. науч.-технич. конф. (14-21 сентября 2008 г., Москва). – С. 46-47
6. Кириченко В.В. Використання обернених систем управління при кодуванні та передачі інформації / В.В. Кириченко // Тези доповідей науково-технічної конференції "Проблеми розвитку глобальної системи зв'язку, навігації, спостереження та організації повітряного руху CNS/ATM". – К., 2014, 139 с.

7. Обобщенная обратимость динамических систем в задачах шифрования / А.М. Ковалев, В.А. Козловский, В.Ф. Щербак. – ПДМ, 2009, приложение № 1. – С. 20–21.
8. Sobhy M.J. and Shehata A. Secure computer communication using haotic algorithms. Int. J. of Bifurcation and Chaos. vol. 10, no. 12, 2000, pp. 2831–2839.
9. A statistical test suite for random and pseudorandom number generators for cryptographic applications / Rukhin A., Soto J., Nechvatal J., Smid M., Barker E., Leigh S., Levenson M., Vangel M., Banks D., Heckert A., Dray J., San Vo. National Institute of Standards and Technology Special Publication 800-22 revision 1a, April 2010. 131 p. http://csrc.nist.gov/groups/ST/toolkit/rng /documents/SP800-22rev1a.pdf
10. Рябко Б.Я. Криптографические методы защиты информации / Б.Я. Рябко, А.Н. Фионов. – М: Горячая линия-Телеком, 2005. – 232 с.

Надійшла до редакції 20.03.2016

В.В. КИРИЧЕНКО[1], Є.В. ЛЕСІНА[2]
[1] Національний авіаційний університет
[2] Красноармійський індустріальний інститут ДВНЗ "ДонНТУ"

ОСОБЛИВОСТІ ІНФОРМАЦІЙНОЇ СИСТЕМИ КЕРУВАННЯ БПЛА

У даній роботі розглянуто особливості функціонування інформаційного каналу безпілотного літального апарату та проаналізовано питання закриття каналу зв'язку з БПЛА криптографічними засобами. Сформульовано вимоги до таких засобів. Розглянуто спосіб шифрування інформації, що використовує прямі і зворотні динамічні системи. За допомогою програми шифрування - дешифрування виконаний ряд експериментів з перетворення інформації, які показали певні особливості алгоритмів, заснованих на вищевказаних системах.

Ключові слова: інформаційний канал БПЛА, зворотні динамічні системи, кінцевовимірне кільце цілих чисел, генератори псевдовипадкових послідовностей.

V.V. KIRICHENKO[1], Ye.V. LESINA[2]
[1] National Aviation University
[2] Krasnoarmeysk industrial institute of DonNTU

FEATURES OF INFORMATION UAV CONTROL SYSTEM

The present study has analyzed the issues of closing the communication channel with unmanned aerial vehicles by cryptographic means. The requirements applicable to such means have been defined. The developed software package realizes one of the possible algorithms of cryptographically secured transmission of broadband video signals from the UAV board to the Ground. Any controlled dynamic system with the input-output structure can be used directly for conversion of information. The idea of using inverse control systems with complex behavior of trajectories is at the heart of the objective to synthesize new efficient algorithms of information protection, primarily from the unauthorized access. The researches carried out and their evaluation allows us to suggest that we obtained new results that extend the theoretical basis of the modern cryptology and seem to be efficient for developing efficient cryptographic algorithms. At the same time, there is a number of open issues related to the impact of dynamic parameters on the stability of cryptographic algorithms to attacks, resistance to information distortion and appearance of invariant varieties. This work analyses the issues of closing the communication channel with an unmanned aerial vehicle by using cryptographic means. Requirements applicable to such means are formulated. The method of information encryption envisaging use of direct and reverse dynamical systems is considered. There has been carried out a series of experiments on information conversion with the encryption-decryption system that showed some algorithm features based on the above mentioned systems.

Keywords: information UAV channels, inverse dynamic system, finite-dimensional ring of integers, generators of pseudo-random sequences.