Член-корреспондент Академии Связи Украины. Лауреат Государственной премии Украины в области науки и техники. Директор учебно-научного института компьютерных информационных технологий Национального авиационного университета.

Yudin Alexander, D. of Engineering, professor. Member of expert and scientifically-methodical advice of Department of education and science of Ukraine in an area "Informative security". Corresponding member of Academy of Connection of Ukraine. Laureate of the State bonus of Ukraine in area of SciTech. Director of Education and Research institute of computer information technologies the National Aviation University.

Бучик Сергій Степанович, кандидат технічних наук, доцент, начальник кафедри автоматизованих систем управління Житомирського військового інституту імені С. П. Корольова.
E-mail: s_stbu@ukr.net

Бучик Сергей Степанович, кандидат технических наук, доцент, начальник кафедры автоматизированных систем управления Житомирского военного института имени С.П. Королева.

Buchyk Sergii, PhD in Eng., chief of department of automated control the system the Zhitomir Military Institute of the name of S.P. Korolyova.

УДК 511.512

АЛГОРИТМ БАЙТ–ОРИЕНТИРОВАННОГО ПОТОЧНОГО ШИФРОВАНИЯ НА ОСНОВЕ РАВНОМЕРНО ПЛОТНЫХ БЛОКОВ НЕЛИНЕЙНОЙ ПОДСТАНОВКИ

Анатолий Белецкий, Денис Навроцкий, Александр Семенюк

В статье рассматриваются вопросы построения нового байт-ориентированного алгоритма синхронного поточного шифрования, в котором шифрующая гамма-последовательность стохастических битов формируется совокупностью равномерно плотных примитивов нелинейной подстановки (S-блоков). Равномерно плотными являются такие примитивы нелинейной подстановки, отклики которых равномерно распределены на поверхности диаграммы рассеяния примитива. Предложен вариант синтеза равномерно плотных S-блоков, диаграммы рассеяния которых превышают качественные характеристики соответствующих показателей диаграммы рассеяния блока нелинейной подстановки алгоритма Rijndael. Проведен сравнительный анализ эффективности разработанного криптопреобразования и наиболее популярного AES-алгоритма в режиме поточного шифрования. Обсуждаются направления применения предлагаемых шифров в различных приложениях.

Ключевые слова: *алгоритмы синхронного поточного шифрования, равномерно плотные блоки нелинейной подстановки, криптографическая защита информации.*

1. Введение и постановка задачи. Различают два основных класса алгоритмов шифрования: блочные и поточные. В *блочных шифрах* в результате криптопреобразования двух одинаковых блоков открытого текста образуются два одинаковых блока шифрованного текста. Избежать этого позволяют *поточные шифры* [1-2], в которых шифрующее преобразование «элемента» открытого текста меняется от одного элемента к другому. Такой эффект прослеживается, например, в блочных DES и AES шифрах, которые в режиме сцепления блоков фактически преобразуются в поточные шифры.

На практике термин поточный шифр используют, как правило, только в том случае, когда «элементы» открытого текста очень малы и составляют один бит или один байт. Если шифруемым элементом является бит, то такие поточные шифры называют *бит-ориентированными шифрами* [3]. Если же шифруемым элементом служит байт, то шифры называют *байт-ориентированными* [4]. Реже встречаются поточные шифры, размер шифруемых элементов в которых превышает байт [5].

Большинство поточных шифров могут быть названы *двоичными аддитивными шифрами* [6]. В таких шифрах $k-$битный секретный ключ K используется только для управления генератором, порождающего *псевдослучайную последовательность* (ПСП) битов $k_0, k_1, \ldots, k_{N-1}$, называемую *ключевым потоком* $\mathcal{K}$, где $N >> k$. Шифртекст C образуется путем сложения по модулю 2 битов T_i открытого текста T и битов k_i ключевого потока $\mathcal{K}$, в результате чего приходим к алгоритму шифрования

$$C_i = T_i \oplus k_i, \qquad i = 0,1,\ldots,N-1.$$

Дешифрование криптограммы C выполняется аналогично алгоритму шифрования открытого текста T, т. е. $T_i = C_i \oplus k_i$.

Поточные шифры находят применение в тех случаях, когда требуется высокая скорость передачи информации, например, при трансляции «живого» видео, в системах сотовой связи и др.,

или при передаче по каналам связи массивов данных большого объема.

В приложениях применяются два типа поточных шифров: синхронные и асинхронные шифры. В *синхронных поточных шифрах* (СПШ) ключевая (шифрующая) псевдослучайная последовательность (ПСП), называемая также *гаммирующей последовательностью* (или просто *гаммой*), формируется независимо как от входного текста T, так и шифртекста C.

В асинхронных поточных шифрах (АПШ), являющихся *самосинхронизирующимися шифрами*, ключевой поток $\mathcal{K}$ создаётся функцией ключа K и фиксированного числа знаков шифротекста C, за счет чего АПШ могут оказаться более устойчивыми к атакам, чем СПШ [2].

Основные требования, предъявляемые к шифрующим ПСП, таковы: большой *период гаммы*; «хорошие» *статистические свойства,* оцениваемые, в основном, пакетами тестов *NIST STS* [6] и *DIEHARD* [7]; соблюдение *постулатов Голомба* [8]; высокая *линейная сложность* последовательности [9] и др.

Одним из важнейших в перечисленных выше показателях поточных шифров является период шифрующей гаммы. Подлинно случайные ПСП должны быть бесконечными. Но величина периода никак не отображает характер распределения битов в последовательности. Поэтому, на данный момент, для определения свойств гаммирующей последовательности применяют пакеты статистического тестирования. При этом, как утверждает Д. Кнут, чем большим числом пакетов подтверждены успешные прохождения псевдослучайными последовательностями тестов, тем выше уверенность конструктора поточного шифра в качестве разработки [10].

Целью данной статьи является разработка новых байт-ориентированных синхронных алгоритмов поточного шифрования, в которых стохастическая гамма-последовательность шифрующих битов формируется группой равномерно плотных блоков нелинейной подстановки, осуществляющих преобразования «байт-в-байт».

Равномерно плотными примитивами нелинейной подстановки будем называть такие примитивы ($S-$блоки), отклики которых равномерно распределены на поверхности диаграммы рассеяния примитива.

2. Стохастический синтез равномерно плотных S-блоков. Классическим примитивом нелинейной подстановки (ПНП) может быть назван $S-$блок симметричного блочного шифра AES (алгоритм Rijndael) [11, 12], осуществляющий аффинное преобразование

$$y = x_f^{-1} \cdot A + b. \qquad (1)$$

Диаграмма рассеяния $S-$блока AES шифра представлена на рис. 1.

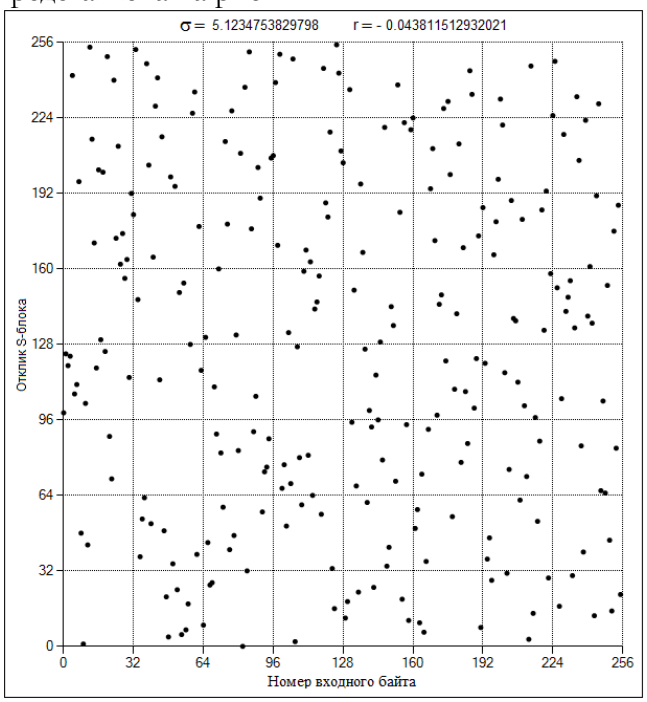

Рис. 1. Диаграмма рассеяния примитива нелнейной подстановки алгортма Rijndael

Как следует из визуального осмотра рис. 1, диаграмма рассеяния $S-$блока шифра AES далека от диаграммы с равномерной плотностью. При том, что среднее число точек $\overline{n}$ в элементах разбиения диаграммы рассеяния (порядок которых составляет 32x32) должно равняться четырем, фактически в элементы попадают от нуля до десяти точек. Среднее квадратическое отклонение σ числа точек, содержащихся в элементах диаграммы рассеяния, равно 5.12, а коэффициент корреляции составляет $r = -0.0438$.

Алгебраический метод описания $S-$блока шифра AES придает примитиву слабости, суть которых состоит в следующем. Аффинное преобразование (1) допускает возможность аппроксимации ПНП системой булевских уравнений, что, в свою очередь, ставит примитив под угрозу реализации алгебраической атаки [13]. С целью устранения уязвимости к алгебраическим атакам в последнее время переходят от детерминистских алгоритмов синтеза примитивов на основе аффинных преобразований к стохастическим методам построения $S-$блоков. Такой способ применен, в частности, при разработке $S-$блоков Украинского

национального стандарта симметричного блочного шифрования ДСТУ 7624:2014 [14] и в других шифрах.

Ниже кратко изложен один из вариантов стохастического синтеза равномерно плотных ПНП «байт-в-байт», который назовем *алгоритмом синтеза S-блоков с выбыванием*. Суть алгоритма состоит в следующем.

Пусть X и $Y-$ входной и выходной байты стохастического $S-$блока соответственно, десятичные эквиваленты которых лежат в диапазоне от 0 до 255. Разобьем шкалы диаграмм рассеяния X и Y, поименованные на рис. 1 как «Номер входного байта» и «Отклик $S-$блока», на восемь равномерных интервалов, каждый из которых содержит по 32 целочисленных отсчета. Стохастическое заполнение квадратов будем осуществлять таким способом, чтобы каждый квадрат разбиения $S_{k,l}$, $k,l=\overline{1,8}$, где $k-$ номер строки, а $l-$ номер столбца диаграммы рассеяния, содержал по четыре точки с координатами $(X,Y)\in S_{k,l}$, причем квадрат $S_{1,1}$ разместим в окрестности начала координат диаграммы.

Условимся считать, что если точка (X,Y) располагается на левой боковой грани квадрата $S_{k,l}$ или на его основании, то она принадлежит этому квадрату. Выберем, как наиболее простой, порядок заполнения диаграммы рассеяния по столбцам. Образуем два вспомогательных вектора длины 256 байт, а именно, вектор $\boldsymbol{X}$, в ячейки которого внесены восьмибитные числа от 0 до 255 и вектор $\boldsymbol{Y}$, все ячейки которого обнулены.

Сначала генерируют случайное равномерно распределенное в интервале от 0 до 1 число (РРЧ) x и вычисляют ординату $y_0=[x\cdot 256]$, где $[a]-$ целая часть значения a.

Байт числа y_0 размещается в нулевой ячейке вектора $\boldsymbol{Y}$, т.е. в ячейке $\boldsymbol{Y}(0)$, а ячейка $\boldsymbol{X}(y_0)$ исключается из вектора $\boldsymbol{X}$. Затем генерируется очередное РРЧ x и вычисляется ордината $y_1=[x\cdot 255]$. Число, содержащееся в ячейке $\boldsymbol{X}(y_1)$, размещается в ячейке $\boldsymbol{Y}(1)$, а ячейка $\boldsymbol{X}(y_1)$ исключается из вектора $\boldsymbol{X}$ и т.д. Следовательно, на $i-$м шаге генерации РРЧ x в $i-$ю ячейку вектора $\boldsymbol{Y}$ записывается байт числа $y_i=[x\cdot N_i]$, где $N_i=256-i$, а также исключается ячейка $\boldsymbol{X}(y_i)$ вектора $\boldsymbol{X}$.

Если на некотором $i-$м шаге генерации РРЧ x окажется, что в каком-либо квадрате первого столбца диаграммы рассеяния находятся четыре точки, то все оставшиеся 28 ячеек вектора $\boldsymbol{X}$ этого квадрата временно исключаются из рассмотрения.

Перед заполнением квадратов второго столбца таблицы рассеяния восстанавливаются 224 ячейки вектора $\boldsymbol{X}$, т.е. исходный вектор $\boldsymbol{X}$ за исключением тех 32 ячеек, которые были задействованы на этапе формирования первого столбца таблицы. Точно также переход к заполнению каждого очередного столбца диаграммы рассеяния предполагает исключение из вектора $\boldsymbol{X}$ 32 ячеек, использованных при формировании предыдущего столбца таблицы. Стартовое значение индекса i для квадратов второго столбца равно 32, для третьего – 64 и т.д.

Таким образом, после заполнения всех столбцов диаграммы рассеяния вектор $\boldsymbol{Y}$ будет содержать всю информацию относительно стохастически моделируемого примитива нелинейной подстановки. При этом номер ячейки $x=\overline{0,255}$ вектора $\boldsymbol{Y}$ является аргументом, а содержимое ячейки $\boldsymbol{Y}(x)=y\in[0,255]-$ функцией f нелинейного преобразования

$$y=f(x).$$

Пример результатов статистического моделирования равномерно плотного $S-$блока показан на рис. 2.

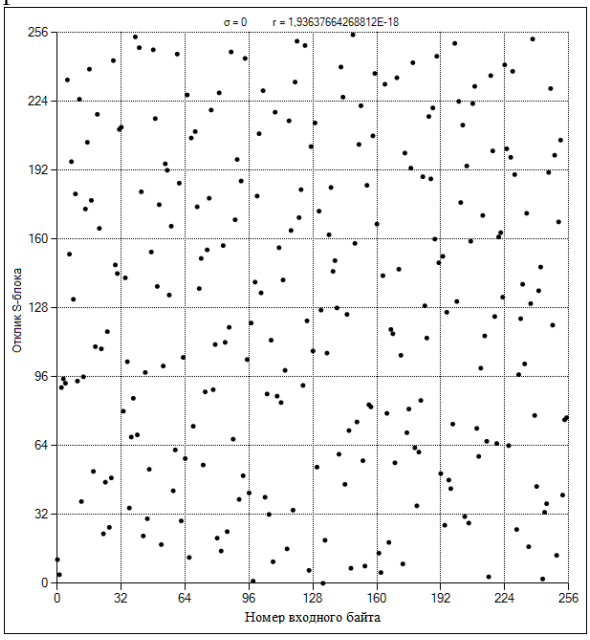

Рис. 2. Диаграмма рассеяния равномерно плотного примитива нелинейной подстановки

3. Блок преобразования байтов (БПБ), составленный из совокупности n равномерно плотных ПНП, является основным узлом предлагаемого

(п. 4) поточного шифра. На рис. 3 показана структурная схема БПБ, в состав которого входят четыре ПНП, обозначенные как $S-\text{box}i$, $i=\overline{0,3}$, типа «байт-в-байт».

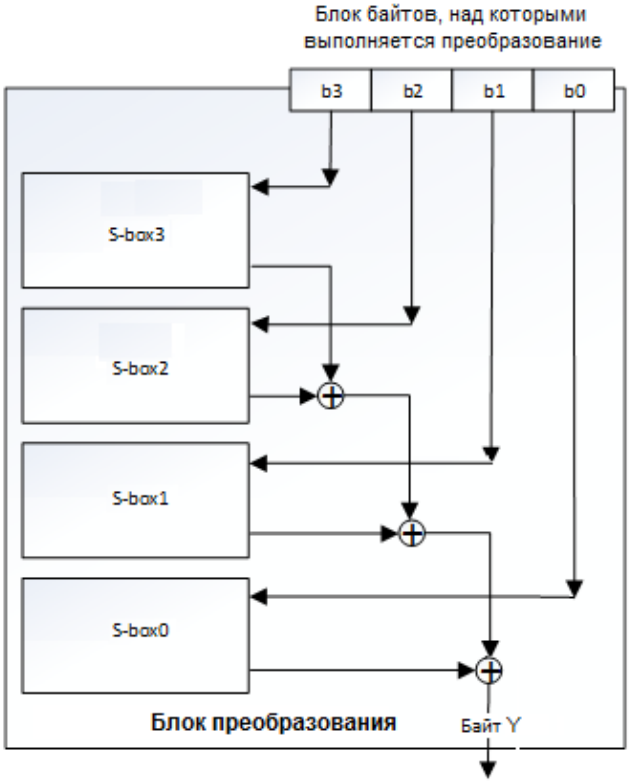

Рис. 3. Структурная схема четырехбайтного блока преобразования

Обобщенная формула преобразования байтов b_i, $i=\overline{0,n-1}$, реализуемая БПБ, такова

$$y=S_{n-1}(b_{n-1})\oplus S_{n-2}(b_{n-2})\oplus\ldots\oplus S_0(b_0),$$

где $S_i(b_i)-$ отклик $i-$го S-блока на входной байт b_i; $\oplus-$ оператор поразрядного сложения по модулю 2 (операция *XOR*).

Выходные байты $\boldsymbol{Y}$ БПБ (рис. 3) могут быть использованы для поточного шифрования последовательности байтов T открытого текста

$$C_i=T_i\oplus Y_i,\quad i=0,1,\ldots \qquad (2)$$

Соотношением (2) предполагается, что для каждого i соблюдается неравенство $Y_{i+1}\neq Y_i$.

Операция *XOR* является одной из наипростейших и (при правильном использовании) наиэффективнейших операций шифрования. Для взлома последовательности C_i третьей стороной необходимо знать:

1) Размерность m вектора байтов $\boldsymbol{B}=\{b_i\}$, над которым выполняется преобразование;

2) Непосредственно байты b_i, $i=\overline{0,m-1}$;

3) Стохастические таблицы $S-$блоков.

Допускается, что п. 1) и 2), т.е. размерность вектора n и сам вектор байтов $\boldsymbol{B}$, могут быть открытыми. Если таблицы $S-$блоков являются закрытыми, то шифрование (2) становится не взламываемым. В самом деле, по состоянию на 2016 год лобовая атака ключа длиною 128 бит (16 байт) по методу его последовательного перебора невозможна. Тем более бессмысленной является восстановление «вслепую» 256-байтного секретного ключа, не говоря уже о том, что как в блоках преобразования (рис. 3), так и в поточных шифраторах на их основе (п. 4), таких S-блоков может быть несколько, что значительно понижает вероятность взлома шифра.

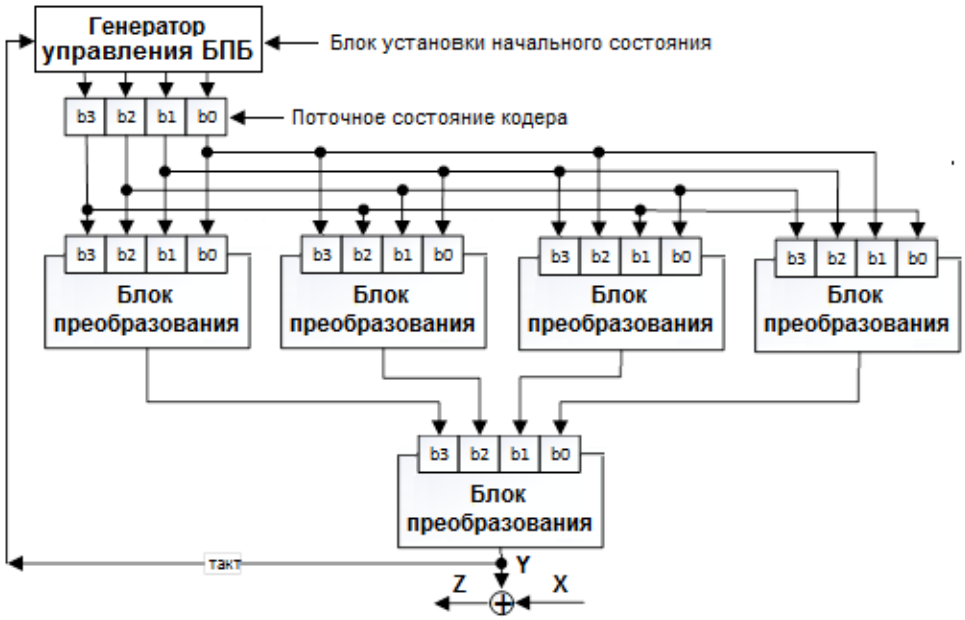

Рис. 4. Структурно-логическая схема алгоритма поточного шифрования на основе БПБ.

4. Алгоритм синхронного поточного шифрования строится на основе блоков преобразования байтов, рассмотренных в п. 3. Вариант такого шифра показан на рис. 4. На данной структурной схеме обозначено: $\boldsymbol{X}$ – Входной байт; $\boldsymbol{Y}$ – Байт гаммирования; и $\boldsymbol{Z}$ – Выходной байт.

В качестве *генераторов состояния шифраторов* (ГСШ) апробированы регистры сдвига с линейными обратными связями (РСЛОС) и двоичные счетчики. Как подтвердили результаты тестирования последовательностей шифрующих байтов $\boldsymbol{Y}$ пакетами *NIST STS* и *DIEHARD* ГСШ, образованные двоичными счетчиками, оказались более предпочтительными по сравнению с РСЛОС-генераторами.

Алгоритмы поточного шифрования, подобные тем, что изображены на рис. 4, ориентированы для использования в закрытых системах передачи данных, примерами которых могут быть системы: мобильной цифровой радиосвязи специального применения, передачи командно-телеметрической и видеоинформации в каналах связи между *наземным пунктом управления* (НПУ) и бортом *беспилотного летательного аппарата* (БПЛА) и ряд других систем.

5. Анализ эффективности БПБ-шифра. Наиважнейшим показателем качества поточных шифров является их способность генерировать псевдослучайную последовательность двоичных чисел, максимально приближенную по своим статистическим характеристикам к характеристикам «белого шума». Двоичная дискретная ПСП будет обладать свойствами «белого шума» при соблюдении, по крайней мере, следующих условий. Во-первых, последовательность должна быть *сбалансированной*, то есть число нулей и единиц в ней должно быть одинаковым. И, во-вторых, *автокорреляционная функция* потока, образованная ПСП нулей и единиц, описывается дельта-функцией Дирака [15]. Таким образом, двоичный дискретный «белый шум» - это просто сбалансированная последовательность независимых (т.е. статистически не связанных один с другим) чисел 0 и 1.

Существуют различные критерии и подходы оценки степени приближения ПСП, генерируемой поточным шифром, к «белому шуму». Простейший из них предполагает построение гистограммы *элементов* ПСП, которые составляются из фиксированного числа бит последовательности, и расчета на их основе энтропии генератора.

В качестве элемента ПСП выберем восьмибитные векторы (байты). Байты последовательности, формируемые генератором, могут находиться в одном из 256 состояний SB, начиная с $SB_0 = 00000000$ до $SB_{255} = 11111111$. Нижний индекс i в обозначении SB_i совпадает с десятичным значением состояния байта.

Пусть n_i – число SB_i байтов (частота) и $N = \sum_{i=0}^{255} n_i$ – общее число (объем) байтов ПСП. Энтропия H ПСП определяется формулой Шеннона

$$H = -\sum_{i=0}^{255} p_i \cdot \log_2 p_i ,$$

где $p_i = n_i / N$ – частость (статистическая вероятность) SB_i – байтов последовательности.

Для того чтобы перевести поточный шифр в режим генератора ПСП достаточно указать ключ шифрования, а на вход шифра подать «нулевой файл» некоторой фиксированной, но достаточно большой длины. *Нулевым* будем называть файл данных, далее обозначаемый как *nullFile*, каждый бит которого равен 0.

Программно рассчитанная табличная гистограмма ПСП байтов, формируемых БПБ поточным шифром (рис. 4), при подаче на его вход «нулевого файла» объемом 12,207 Мбайт, представлена табл. 1.

На пересечении строк [a] и столбцов [b] табл. 1 расположены частоты n_i шифрующих байтов SB_i, состояния i которых определяются значением $i = a + b$. Энтропия ПСП составляет величину $H = 0,999987$.

В табл. 2 сведены значения (результаты усреднения 10 компьютерных экспериментов) энтропии H и затрат машинного времени T на формирование ПСП объемом 1 Гбайт БПБ-генераторами, параметр m которых меняется в диапазоне от 2 до 8. В нижней строке таблицы приведены оценки H и T, обеспечиваемые шифром AES.

Таблица 1

Гистограмма шифрующей гаммы

dec	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]
[0]	49902	50189	50391	50142	50244	50128	50096	50033
[8]	50029	49896	49805	50077	50464	49945	50160	50016
[16]	50202	49922	49975	49995	50127	49845	49965	49862
[24]	50343	50208	49726	50173	50078	49873	50099	49977
[32]	49773	49865	49821	50104	49976	49738	50218	50070
[40]	49916	49768	50016	50081	49953	49671	49917	50048
[48]	50052	49981	50119	50169	50077	49867	49678	49723
[56]	49851	49994	50091	50063	50347	49893	50385	50268
[64]	49305	49837	50314	49823	49880	49968	50396	49763
[72]	50073	50092	49730	49993	49791	49883	50492	49624
[80]	50067	50363	50098	49979	50060	50180	50121	49926
[88]	49436	49958	49974	50140	49767	50079	49520	50003
[96]	49835	50348	49662	49827	50172	49918	50322	50098
[104]	49922	50160	49938	50178	50184	49674	50210	50182
[112]	50037	50119	50160	49962	50101	50133	49951	49837
[120]	50094	50146	50019	49866	50107	50423	49475	50012
[128]	49781	50055	49981	50200	50047	50045	49966	50016
[136]	50034	50233	49781	49966	49975	50134	49921	50181
[144]	49949	50245	49675	49779	50045	49873	49965	50132
[152]	49990	50042	50019	49862	50076	50135	49550	50124
[160]	49945	49685	49942	49663	49649	50118	49990	49786
[168]	49807	50031	50152	50082	49661	49829	49982	50180
[176]	50209	49938	49719	49728	49794	49860	49925	49533
[184]	50159	49953	49644	50054	50252	49896	49959	50230
[192]	50052	49646	50205	50015	50152	49684	49608	49716
[200]	49756	49978	49936	49883	50034	49796	50104	49644
[208]	50435	50147	50567	49838	50091	50122	49887	50076
[216]	50163	49906	49802	50144	50015	50331	49376	50717
[224]	50016	49912	50187	49917	49816	50310	50206	49962
[232]	50106	50001	49691	49671	49868	50159	50144	49862
[240]	50149	49929	50138	50296	50174	50255	49884	50054
[248]	50387	50262	50177	50255	50178	50215	49901	49840

Согласно данным табл. 2 оптимальным значением m (числа $S-$блоков, которые входят в блок преобразования байтов поточного шифра) равно четырем. При этом значении m энтропия H одногигабайтного файла, формируемого БПБ-шифром, и затраты машинного времени T программно реализованного алгоритма оказываются сопоставимыми с соответствующими характеристиками аппаратно-программного варианта шифра AES. Дальнейшее увеличение m практически не меняет величины H, в то же время значимо возрастают как затраты машинного времени T, так и число $S-$блоков $L=m\cdot(m+1)$, необходимых для построения поточного БПБ-шифра.

Таблица 2

Характеристики одногигабайтных БПБ-генераторов и шифра AES

m	H	T (сек.)	L
2	7.99671830	14.13	6
3	7.99999114	15.73	12
4	7.99999982	17.87	20
5	7.99999982	22.62	30
6	7.99999982	29.57	42
7	7.99999982	40.67	56
8	7.99999982	57.89	72
AES	7.99999982	17.38	—

6. Аппаратно-программный комплекс передачи командно-телеметрической информации (КТИ) в каналах «НПУ-БПЛА-НПУ».

Ниже приведены структурно-логические схемы обмена КТИ между наземным пунктом управления и бортом БПЛА (рис. 5), а также в канале «Борт БПЛА-НПУ» (рис. 6), в которых обозначены: ГПСП – генератор псевдослучайных последовательностей шифрующих байтов; МКВ (MKG) – микроконтроллер «Борта БПЛА» («Земли»).

Для обмена зашифрованными данными по каналам связи одного лишь шифрования недостаточно. Необходимо также решить задачу синхронизации ключей, которыми шифруются данные, а также задачу аутентификации, для того чтобы быть уверенным в том, что данные получены от конкретного «легализованного абонента», к которым будем относить аппаратно-программные средства «Земли» и «Борта», задействованные в обмене информации.

Разработанный криптографический протокол, краткое описание которого приведено в п. 7, как раз и предназначен для решения перечисленных выше проблем синхронизации ключей шифрования и аутентификации абонентов.

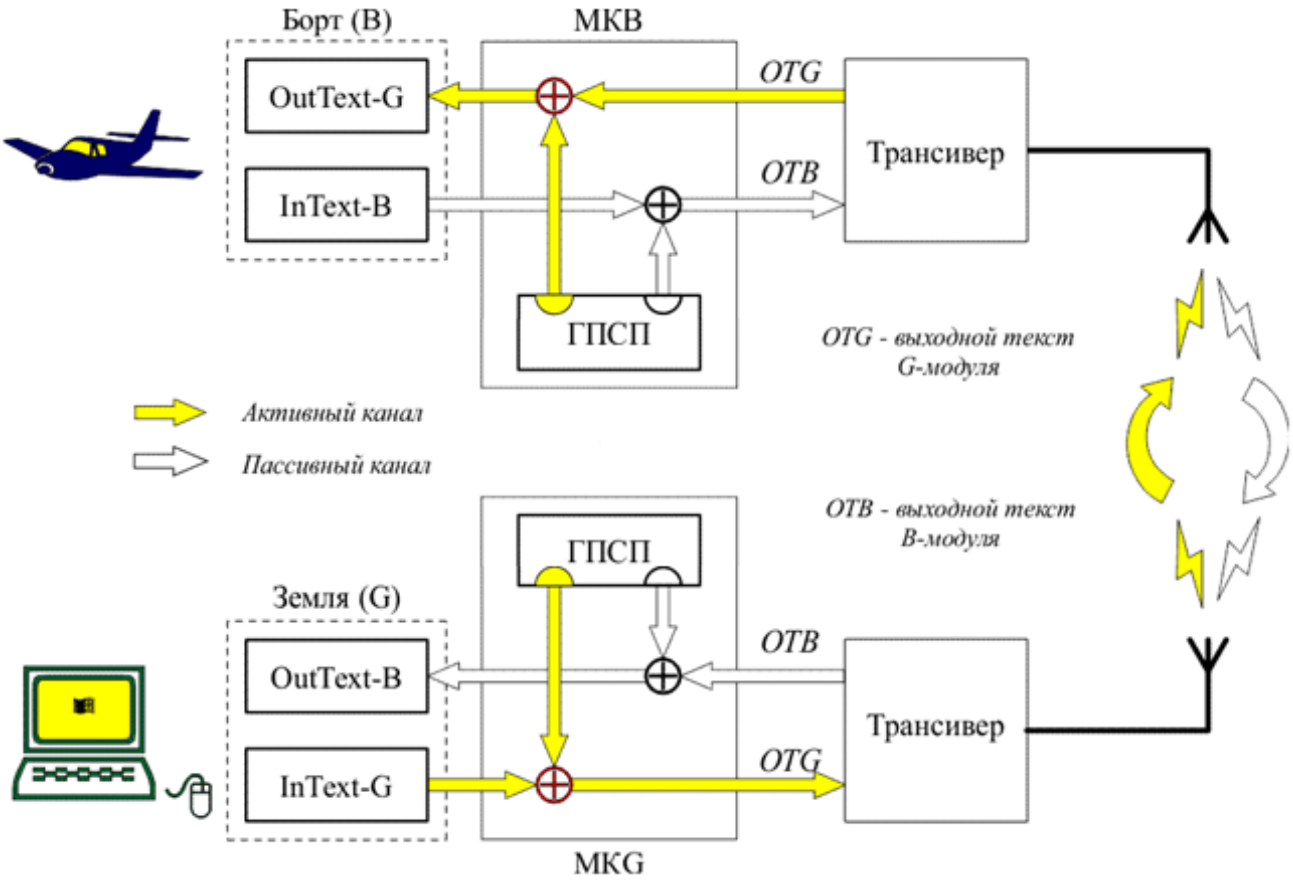

Рис. 5. Структурно-логическая схема передачи командной информации в канале «НПУ-Борт БПЛА»

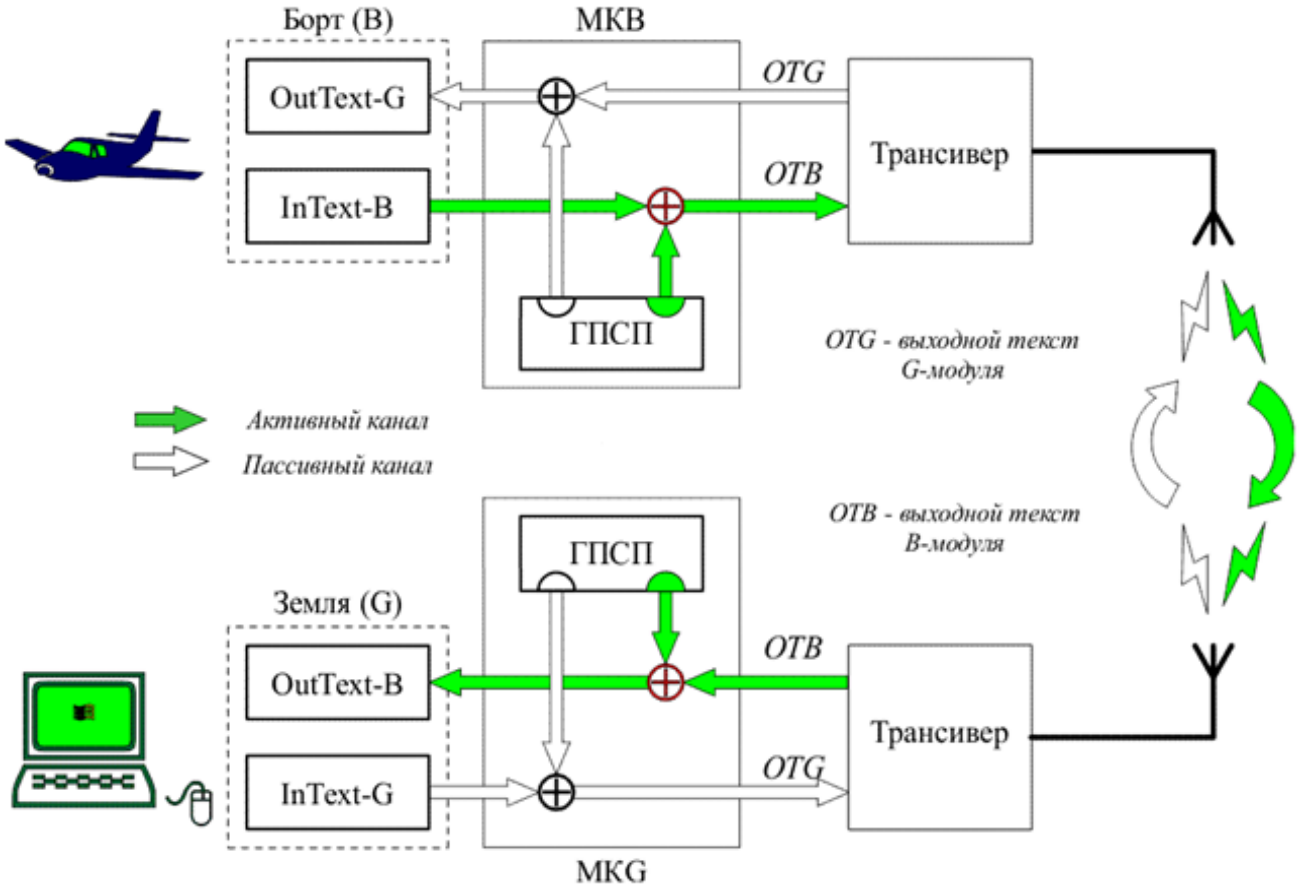

Рис. 6. Структурно-логическая схема передачи
телеметрической информации в канале «Борт БПЛА-НПУ»

7. Криптографические протоколы обмена данными. В основу протоколов положены правила, регламентирующие использование криптографических преобразований и алгоритмов в информационных процессах. Обобщенная схема построения криптографического *протокола зашифрования данных* приведена на рис. 7.

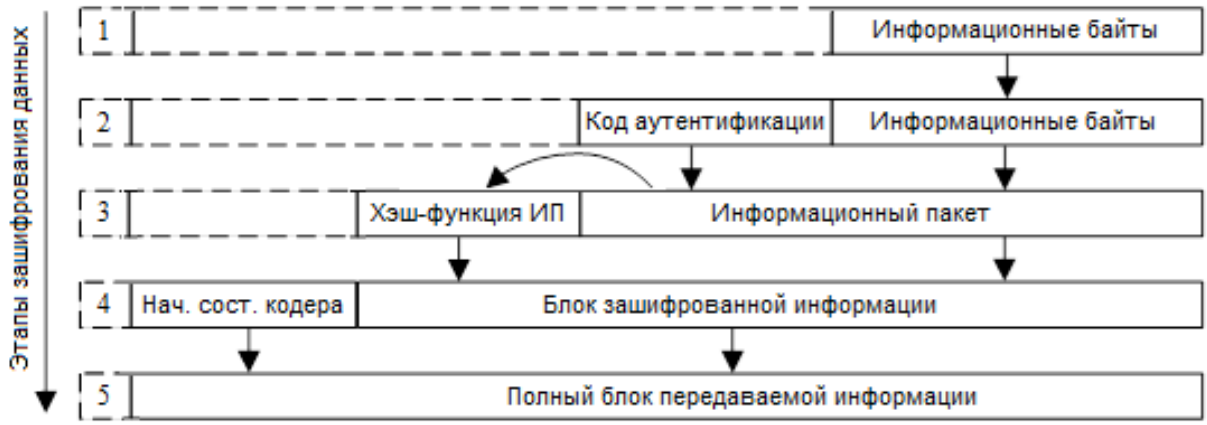

Рис. 7. Структурно-логическая схема протокола зашифрования данных

Протокол зашифрования решает следующие задачи:

- на этапе (1) формируется *блок информационных байтов*, который

- на этапе (2) дополняется секретным *кодом аутентификации* (в авиационной терминологии – индивидуальным кодом «свой-чужой»), совместно образуя *информационный пакет* (ИП);

- на этапе (3) вычисляется хэш-функция (ХФ) информационного пакета, а затем

- на этапе (4) объединенный блок ХФ + ИП подвергается криптографическому преобразованию поточным БПБ-шифром (рис. 4). К полученному *блоку зашифрованной информации* (БЗИ) присоединяется блок *начального состояния кодера* (НСК);

- на этапе (5) формируется полный *блок передачи информации* (БПИ) потребителю и, тем самым, завершается протокол зашифрования данных.

На приемной стороне этапы расшифрования данных выполняются в последовательности (рис. 8), обратной последовательности этапов зашифрования.

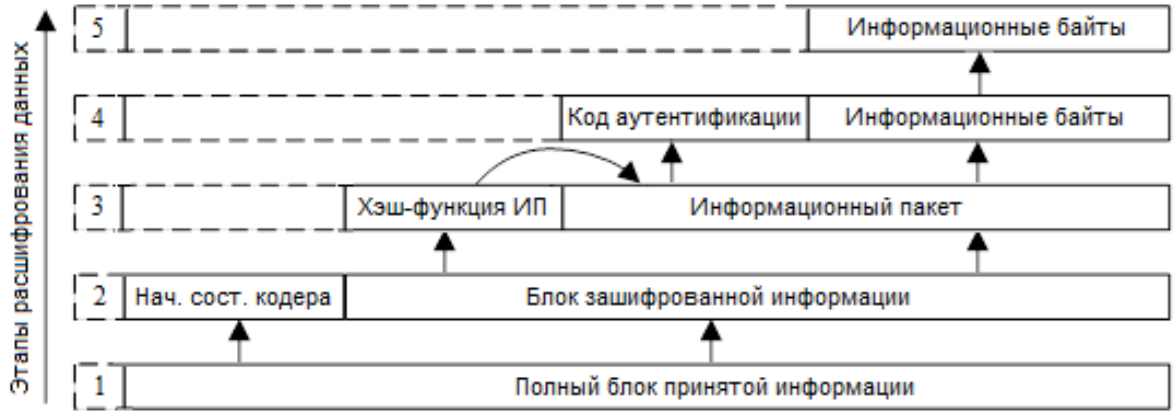

Рис. 8. Структурно-логическая схема протокола расшифрования данных

Протоколом расшифрования данных выполняются следующие преобразования:

- на этапе (1) в процессоре приемника размещается полный блок принятой информации, из которого

- на этапе (2) выделяются блоки НСК и БЗИ;

- на этапе (3) посредством блока НСК запускается процесс расшифровки данных по схеме, показанной на рис. 4, в результате которого из БЗИ выделяются ХФ и ИП. Затем вычисляется ХФ расшифрованного ИП. Если рассчитанная ХФ отличается от принятой, то ИП игнорируется. В случае совпадения ХФ

- на этапе (4) из ИП извлекаются код аутентификации и файл информационных байтов, а последний

- на этапе (5) размещается в регистре информационных байтов. На этом завершается протокол расшифрования данных.

Роль *синхронизирующего элемента* в протоколах обмена данными выполняет содержимое блока установки начального состояния генератора управления БПБ (рис. 4), которое передается по каналу связи в открытом виде, что не нарушает секретности передачи данных, так как третья сторона не в состоянии воспроизвести расшифровующую гамму, поскольку для него (противника) остаются закрытыми $S-$ блоки шифраторов.

Код (или ключ) аутентификации в составе хэш-функции информационного пакета обеспечивает возможность одному оператору НПУ поддерживать связь с целой группой БПЛА. С этой целью каждому аппарату выделяется индивидуальный код аутентификации. В то же время S-блоки шифраторов НПУ, как и всей группы беспилотников, могут быть одинаковыми, что снижает затраты на эксплуатацию системы.

Выводы. Отличительная особенность предлагаемого способа криптографических преобразований командно-телеметрической информации (КТИ) состоит в простоте алгоритмическо-программного обеспечения системы защиты КТИ. Есть все основания утверждать, что разработан новый, не имеющий отечественных и зарубежных аналогов, оригинальный алгоритм поточного шифрования данных, который по критериям быстродействия передачи информации и степени «отбеливания» исходного текста, оцениваемой энтропией шифрограммы, не уступает, а в отдельных машинных экспериментах и превышает, соответствующие показатели AES-шифра.

Технические решения, предлагаемые для организации криптографической защиты КТИ в каналах связи НТУ-БПЛА, могут быть адаптированы как для целей защиты видеоинформации, передаваемой с борта БПЛА на Землю, так и для криптографической защиты аудиоинформации в системах мобильной радиосвязи.

ЛИТЕРАТУРА

[1]. Асосков А. В. Поточные шифры / А. В. Асосков, М. А. Иванов, А. А. Мирский, А. А. Рузин и др. – М.: КУДИЦ-ОБРАЗ, 2003. – 336 с.

[2]. Поточные шифры. Результаты зарубежной открытой криптологии. [Электронный ресурс] – Режим доступа: http://www.ssl.stu.neva.ru/psw/crypto/potok/str_ciph.htm.

[3]. Поточный шифр A5. [Электронный ресурс] – Режим доступа: http://ru.wikipedia.org/wiki/A5

[4]. Поточный шифр RC4. [Электронный ресурс] – Режим доступа: http://ru.wikipedia. org/wiki/RC4

[5]. WEP шифрование в WI-FI сетях. [Электронный ресурс] – Режим доступа: http://kavayii.blogspot.com/2010/01/wep-wi-fi.html

[6]. Сушко С. А. Поточные шифры. Лекция 6. [Электронный ресурс] – Режим доступа: fitp.ifmo.ru/shared/files/201111/1_280.pdf.

[7]. A Statistical Test Suite for Random and Psevdorandom Number Generators for Cryptographic Applications. NIST Special Publication 800-22? Rev. 1a / Technology Administration, U.S. Department of Commerce. – Washington: NIST. – 2010. – P. 131.

[8]. Marsaglia G. DIEHARD Statistical Tests. [Электронный ресурс] – Режим доступа: http://stat.fsu.edu/~geo/diehard.html.

[9]. Golomb S. W. Shift Register Sequences. / S. W. Golomb. – San Francisco: Holden Day, 1967 (and also reprint: Aegan Park Press, 1982). – ISBN 978-3-540-44523-4.

[10]. Безверхая Г. С. Анализ перспективы развития поточного шифрования. / Г. С. Безверхая. // Системи обробки інформації, 2009, випуск. 7(81). – С. 54-55.

[11]. Белецкий А. А. Программно-моделирующий комплекс криптографических AES-подобных примитивов нелинейной подстановки. / А. А. Белецкий, А. Я. Белецкий, Д. А. Навроцкий, А. И. Семенюк. // Захист інформації. Том 16, № 4. – 2014. – С. 274-283.

[12]. National Institute of Standards and Technology (NIST), “Federal Information Processing Standard 197, The Advanced Encryption Standard (AES)”, http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf, 2001.

[13]. Долгов В. И. Подстановочные конструкции современных симметричных блочных шифров / В. И. Долгов, Р. В. Олейников, И. В. Лисицкая, Р. В. Сергиенко и др. // Радіоелектронні і комп’ютерні системи, 2009, № 6 (40). – С. 89-93.

[14]. Держспецзв'язку впроваджує нові стандарти криптографічного захисту інформації. [Электронный ресурс] – Режим доступа: http://www.kmu.gov.ua/control/publish/article?art_id=247952015

[15]. Белый шум и его характеристики. [Электронный ресурс] – Режим доступа: http://nauchebe.net/2012/03/belyj-shum-i-ego-xarakteristiki.

REFERENCES

[1]. Asoskov A. V. Stream ciphers / A. V. Asoskov, M. A. Ivanov, A. A. Mirskiy, A. A. Ruzyne etc.– M.: KUDITS-OBRAZ, 2003. – 336 p.

[2]. Stream ciphers. The results of foreign-covered cryptology. http://www.ssl.stu.neva.ru/psw/crypto/potok/str_ciph.htm.

[3]. Stream ciphers A5. http:// ru.wikipedia.org/wiki/A5.

[4]. Stream ciphers RC4. http:// ru.wikipedia.org/wiki/RC4.

[5]. WEP encryption in WI-FI networks. http:// kavayii.blogspot.com/2010/01/wep-wi-fi.html.
[6]. Sushco S. A. Stream ciphers. http://fitp.ifmo.ru/shared/files/201111/1_280.pdf.
[7]. A Statistical Test Suite for Random and Psevdorandom Number Generators for Cryptographic Applications. NIST Special Publication 800-22? Rev. 1a / Technology Administration, U.S. Department of Commerce. – Washington: NIST. – 2010. – P. 131.
[8]. Marsaglia G. DIEHARD Statistical Tests. http://stat.fsu.edu/~geo/diehard.html.
[9]. Golomb S. W. Shift Register Sequences. / S. W. Golomb. – San Francisco: Holden Day, 1967 (and also reprint: Aegan Park Press, 1982). – ISBN 978-3-540-44523-4.
[10]. Bezverhaja G. S. Analysis of the prospects for the development of in-line encryption. // Information processing systems, 2009. Vol. 7(81). – P. 54-55.
[11]. Beletsky A. A., Beletsky A. Ya., Navrotskyi D. A., Semenjuk A. I. Software modeling complex cryptographic AES-similar primitives nonlinear substitution, 2014. Vol. 16, # 4. – P. 274-283.
[12]. National Institute of Standards and Technology (NIST), "Federal Information Processing Standard 197 The Advanced Encryption Standard (AES)", http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf, 2001.
[13]. Dolgov V. I., Olejnikov R. V., Lisitskaja I. V., Sergienko R. V. Substitution Construction of modern symmetric block ciphers. // Radioelectronics and computer systems, 2009. Vol. 6(40). – P. 89-93.
[14]. State Special Communications introduces new standards for cryptographic protection of information. http://www.kmu.gov.ua/control/publish/article?art_id=247952015.
[15]. White noise and its characteristics http://nauchebe.net/2012/03/belyj-shum-i-ego-xarakteristiki.

АЛГОРИТМ БАЙТ-ОРІЄНТОВАНОГО ПОТОЧНОГО ШИФРУВАННЯ НА ОСНОВІ РІВНОМІРНО ЩІЛЬНОГО БЛОКУ НЕЛІНІЙНОЇ ПІДСТАНОВКИ

У статті розглядаються питання побудови нового байт-орієнтованого алгоритму синхронного поточного шифрування, в якому гамма-послідовність стохастичних бітів, що шифрує вхідний текст, формується сукупністю рівномірно щільних примітивів нелінійної підстановки (S – блоків). Рівномірно щільними є такі примітиви нелінійної підстановки, відгуки яких рівномірно розподілені на поверхні діаграми розсіювання примітиву. Запропоновано варіант синтезу рівномірно щільних S – блоків, діаграми розсіювання яких перевищують якісні характеристики відповідних показників діаграми розсіювання блоку нелінійної підстановки алгоритму Rijndael. Проведено порівняльний аналіз ефективності криптоперетворень розроблених і найбільш популярних алгоритмів поточного шифрування. Обговорюються можливості використання шифрів, що пропонуються, в різних напрямках застосування.

Ключові слова: алгоритми синхронного поточного шифрування, рівномірно щільні блоки нелінійної підстановки, криптографічний захист інформації.

ALGORITHM FOR BYTE-ORIENTED STREAM CIPHER ON BASED WITH A UNIFORM DENSITY THE NONLINEAR SUBSTITUTIONS

This article discusses the construction of a new byte-oriented synchronous stream encryption algorithm, which encrypts the gamma-stochastic sequence of bitsformed by a set of primitives uniformly dense nonlinear substitution S – blocks). Evenly dense are those entities nonlinear substitution reactions which are evenly distributed on the surface of the scattering diagram of the primitive. A variant of the synthesis of uniformly dense S – boxes, which scatterplot exceed the quality characteristics of the respective scatterplot indicators nonlinear substitution algorithm Rijndael block. A comparative analysis of the effectiveness of cryptographic transformations developed and most popular stream encryption algorithms. The directions of application of the proposed codes in various applications.
Keywords: synchronous stream encryption algorithms, uniformly dense blocks nonlinear substitution, cryptographic protection of information.

Білецький Анатолій Якович, доктор технічних наук, професор, заслужений діяч науки і техніки України, лауреат Державної премії України в галузі науки і техніки, професор кафедри електроніки Національного авіаційного університету.
E-mail: abelnau@ukr.net
Белецкий Анатолий Яковлевич, доктор технических наук, профессор, заслуженный деятель науки и техники Украины, лауреат Гос. премии Украины в области науки и техники, профессор кафедры электроники Национального авиационного ун-та.
Beletsky Anatoly, Doctor of Science, Professor, Honored Scientist of Ukraine, Laureate of the State Prize of Ukraine in Science and Technology, Professor of Department Electronics of National Aviation University.

Навроцкий Денис Александрович, ассистент кафедры электроники Национального авиационного университета. E-mail: sg6336@yandex.ua
Навроцький Денис Олександрович, асистент кафедри електроніки Національного авіаційного університету.
Navrotskyi Denys, Assistant of Department Electronics of National Aviation University.

Семенюк Александр Иванович, магистр кафедры электроники Национального авиационного университета. E-mail: sovist9@mail.ru
Семенюк Олександр Іванович, магистр кафедри електроніки Національного авіаційного університету.
Semenjuk Alexander, Magister of Department Electronics of National Aviation University.