θ, *f*, δ) вида (9), определяемой для данных простого числа *p* и примитивного элемент *a* поля ***GF***(*p*) с помощью следующих соотношений:

$$X = \mathbf{GF}(p),\ K = U = \mathbf{GF}(p)^*,\ L = (\mathbf{Z}_{p-1})^*,\ Y = \mathbf{GF}(p)^* \times \mathbf{Z}_{p-1},$$

$$\theta: K \to U,\ f: X \times K \times L \to Y,\ \delta: X \times Y \times U \to \{0, 1\},$$

$$\theta(k) = a^k \pmod p,\ f(x, u, l) = (y_1, y_2),$$

$$y_1 = a^l \pmod p,\ y_2 = (x - k\,y_1)\,l^{-1} \bmod (p-1), \qquad (15)$$

$$\delta(x, (y_1, y_2), u) = 1 \Leftrightarrow u^{y_1} y_1^{y_2} \equiv a^x \pmod p,$$

где $k \in K$, $x \in X$, $l \in L$, $(y_1, y_2) = y \in Y$. Следует обратить внимание на определенное сходство систем Эль-Гамаля $\wp$ (открытого шифрования) и Γ (цифровой подписи). Так, множества *X*, *K*, *U* и *L* соответственно подписываемых сообщений, секретных ключей, открытых ключей и параметров системы Γ совпадают с аналогичными множествами криптосистемы $\wp$ (см. пример 2). Кроме того, в обеих системах используются одинаковые алгоритмы вычисления открытых ключей по секретным (совпадают отображения θ). Также равны первые координаты y_1 значений функций шифрования и подписывания соответственно. Наиболее существенное различие между системами открытого шифрования и цифровой подписи Эль-Гамаля заключается в способе формирования координаты y_2 подписи и соответственно шифрованного сообщения (см. соотношения (15) и (7)).

IV Выводы

Предложенный подход к формализации понятий системы открытого шифрования и системы цифровой подписи, очевидно, не является единственно возможным. Вместе с тем, построенные выше алгебраические модели несимметричных криптосистем составляют формальную теоретическую основу исследований общих критографических свойств различных систем с открытым ключом. Основная задача в области анализа несимметричных криптосистем, представленных в виде многоосновных универсальных алгебр, состоит в конструктивном описании таких алгебр, допускающих простую реализацию и обеспечивающих приемлемую вычислительную стойкость шифрования (цифровой подписи). Важной задачей дальнейших исследований является также определение условий эквивалентности (в том или ином смысле) несимметричных криптосистем или сводимости их друг к другу.

Литература: 1. Diffie W., Hellman M. E. New directions in cryptography // IEEE Trans. on Inf. Theory. – 1976. – IT-22. – P. 644-654. 2. Артамонов В. А., Ященко В. В. Многоосновные алгебры в системах открытого шифрования // Успехи матем. наук. – 1994. – Т. 49. – С. 149-150. 3. Сидельников В. М., Черепнев М. А., Ященко В. В. Системы открытого распределения ключей на основе некоммутативных полугрупп // Доклады РАН. – 1993. – Т. 332. – № 5. – С. 566-567. 4. Schneier B. Applied Cryptography. – John Wille & Sons, Inc. – N-Y. – 1996. 5. Горчинский Ю. Н. О гомоморфизмах многоосновных универсальных алгебр в связи с криптографическими применениями // Труды по дискретной математике – 1997. – Т. 1. – С. 43-66. 6. Шапошников И. Г. О конгруэнциях конечных многоосновных универсальных алгебр // Дискретная математика. – 1999. – Т. 11. – В. 3. – С. 48-62. 7. Шеннон К. Теория связи в секретных системах // Работы по теории информации и кибернетике. – М.: Изд-во иностр. литературы, 1963. – С. 333- 402. 8. El Gamal T. A public-key cryptosystem and signature scheme based on discrete logarithms // IEEE Trans. on Inf. Theory. – 1985. – IT-31. – № 4.

УДК 681.3.06: 519.248.681

СТОЙКОСТЬ ГОСТ 28147-89 ПРИ ИСПОЛЬЗОВАНИИ ТАБЛИЦЫ ПОДСТАНОВОК ИЗ ГОСТ 34.311-95

Роман Олейников
Харьковский Национальный Университет Радиоэлектроники

Анотація: **Розглядається стійкість ГОСТ 28147-89 при використанні довгострокового ключа, що наведений у стандарті хешування ГОСТ 34.311-95. Наводяться приклади побудови диференційних характеристик та доводиться неможливість диференційної та лінійної атаки на ГОСТ 28147-89 з**

цією таблицею підстановок. Пропонується використовувати довгостроковий ключ як стандартний для ГОСТ 28147-89.
Summary: **The resistance of the GOST 28147-89 encryption algorithm with the S-boxes from the hash function standard GOST 34.311-95 is considered. The examples of the differential characteristics are given and the invulnerableness of the cipher with these S-boxes to the differential and linear cryptanalysis is proved. The S-boxes from the GOST 34.311-95 are proposed as a standard for the GOST 28147-89.**
Ключевые слова: **ГОСТ 28147-89, ГОСТ 34-311-95, дифференциальный криптоанализ, линейный криптоанализ.**

В стандарте ГОСТ 28147-89 не определён один из основных элементов шифра, влияющих на его стойкость – заполнение узлов замены. Можно предположить, что при разработке шифра предполагалась генерация отдельного секретного долговременного ключа для каждой сети абонентов. Использование секретных подстановок значительно повышает стойкость алгоритма, однако возможна умышленная генерация таблиц подстановок, ослабленных для дифференциального и линейного криптоанализа. При криптографической защите информации в открытых глобальных сетях с большим количеством абонентов принципиально невозможно применение единой секретной подстановки, неизвестной злоумышленнику. Кроме того, для систем криптографической защиты информации (СКЗИ) в открытых сетях обязательно выполнение правила Кирхгофа, в соответствии с которым противник располагает полной информацией о системе защиты, за исключением текущих ключей шифрования. Долговременный ключ является частью СКЗИ, следовательно, известен атакующему.

Поэтому при использовании ГОСТ 28147-89 для защиты информации в открытых сетях необходим единый несекретный долговременный ключ, оптимизированный против дифференциального и линейного криптоанализа. Существуют различные методики генерации таблиц подстановок для ГОСТа, в том числе с оптимизацией против дифференциального и линейного криптоанализа [1]. Однако наиболее широко распространённым и доступным всем разработчикам СКЗИ является долговременный ключ, опубликованный в ГОСТ 34.311-95. Он сформирован разработчиками алгоритма шифрования, располагающими наиболее полной информацией о свойствах ГОСТ 28147-89. Кроме того, в некоторых источниках этот долговременный ключ упоминается как «стандартный», и приводится пример его использования Центральным Банком РФ [2].

Существуют различные мнения о существовании возможных уязвимостей, встроенных разработчиками в ГОСТ 28147-89 в целом и в таблицу подстановок ГОСТ 34.311-95 в частности. Из известных в настоящее время криптоаналитических атак против ГОСТ 28147-89 могут быть эффективны лишь дифференциальный криптоанализ и, отчасти, линейный криптоанализ. В настоящем докладе производится анализ дифференциальных и линейных свойств подстановок долговременного ключа ГОСТ 34.311-95, затем приводятся примеры построения дифференциальных характеристик, после чего делаются выводы об общей стойкости ГОСТ 28147-89 при применении таблицы подстановок из ГОСТ 34.311-95.

Основными элементами ГОСТ 28147-89, влияющими на его стойкость к линейному криптоанализу, являются ключевой сумматор и долговременный ключ. При проведении атаки линейного криптоанализа используются переходы с максимальной вероятностью. По их значению можно делать предположения о проведенной оптимизации таблиц против выбранного метода криптоанализа.

Максимальные, минимальные и средние значения (без учёта нулевых входных и выходных масок) элементов таблиц линейной аппроксимации для долговременного ключа из ГОСТ 34.311-95 приведены в таблице 1.

Как следует из полученных данных, для подстановки, соответствующей S1, максимальное значение модуля элемента таблицы линейной аппроксимации равно 4, среднее значение ненулевых элементов равно 2.55, минимальное значение равно 2. Для остальных подстановок максимальным модулем элемента является 6, однако, эти значения встречаются крайне редко (от 1 до 4 раз для одной подстановки). Соответствующие вероятности являются низкими для построения эффективных линейных аппроксимаций при выполнении атаки на все 32 цикла шифрования даже при малом количестве переносов, возникающих на ключевом сумматоре.

Таблица 1– Максимальные, минимальные и средние значения элементов таблиц линейной аппроксимации для долговременного ключа из ГОСТ 34.311-95

Номер подстановки	1	2	3	4	5	6	7	8
Максимальное значение	4	6	6	6	6	6	6	6
Минимальное значение	2	2	2	2	2	2	2	2
Среднее значение	2.55	2.41	2.42	2.46	2.41	2.41	2.46	2.47

Для сравнения, в таблице 2 приводятся средние значения для модуля элемента таблицы линейной аппроксимации после обработки 30000 случайно сгенерированных подстановок. Среднее значение модуля элемента таблицы линейной аппроксимации примерно равно тому же параметру для подстановок из ГОСТ 34.311-95.

Таблица 2 – Максимальные, минимальные и средние значения элементов таблиц линейной аппроксимации для случайных подстановок

Максимальное значение	5.87
Минимальное значение	2
Среднее значение	2.46

Кроме того, возможна специальная генерация подстановок, уязвимых для линейного криптоанализа, однако для исследуемых подстановок этого не наблюдается. Поэтому можно сделать вывод о линейных свойствах, близким к свойствам случайных подстановок, или существовании достаточно «мягкого» критерия линейной оптимизации при генерации заполнения узлов замены, обеспечивающего при этом стойкость к линейному криптоанализу. Отсюда следует, что даже при использовании сеансовых ключей шифрования с малым количеством единиц и низкой вероятностью возникновения переноса построение высоковероятных линейных аппроксимаций для ГОСТ 28147-89 невозможно, и известный как долговременный ключ обеспечивает стойкость шифра к линейному криптоанализу.

Как было показано в [3] при неудачном выборе (умышленной генерации) слабого долговременного ключа ГОСТ 28147-89 может быть уязвимым для дифференциального криптоанализа. Поскольку правила генерации заполнения узлов замены из ГОСТ 34.311-95 в открытой печати не опубликованы, необходимо проведение исследований дифференциальных свойств известного долговременного ключа. Для вычисления разности между входными значениями, как и в [3], использовалась операция сложения по модулю 2. Максимальная вероятность перехода равна 8/16 для $S7$ и $S8$, 6/16 для $S1$, $S2$, $S3$, $S4$ и $S6$, 4/16 для $S5$. Для таблиц, в которых присутствуют переходы с вероятностью 8/16 и 6/16, более 94% переходов имеют вероятность 2/16 и 4/16 (для переходов с вероятностью выше 0). Кроме того, входные и выходные разности для переходов с вероятностями 8/16 и 6/16 имеют несколько активных (ненулевых) битов, что уменьшает их вероятность прохождения через сумматор без искажения. Отсутствие переходов с вероятностью 1 (кроме $0h \rightarrow 0h$) и 12/16 позволяет утверждать об отсутствии «закладок», уменьшающих стойкость шифра к дифференциальному криптоанализу, а малое количество переходов с вероятностями 8/16 и 6/16, а также вид их входных и выходных разностей позволяет утверждать о существовании критериев оптимизации против дифференциального криптоанализа при генерации таких таблиц.

Следует отметить, что критерии отбора таблиц являются достаточно мягкими и возможна генерация всех 8 подстановок с максимальной вероятностью перехода 4/16 (как для $S5$). Этот факт был обнаружен при проведении исследований, результаты которых отражены в [1].

Приведенные факты позволяют утверждать об отсутствии закладок, и, более того, оптимизации подстановок из ГОСТ 34.311-95 против дифференциального криптоанализа. Недостатком этого долговременного ключа является наличие переходов с вероятностями 8/16 и 6/16, которых можно было бы достаточно просто избежать путём выбора более жёстких критериев генерации таблиц подстановок. Влияние этих переходов на вероятность дифференциальных характеристик в ГОСТ 28147-89 с долговременным ключом из ГОСТ 34.311-95 будет рассмотрено ниже.

Дифференциальные свойства отдельных подстановок имеют большое значение, однако, для эффективного проведения криптоанализа очень важным является возможность объединения разностей подстановок для построения многоцикловых характеристик. К примеру, попытка замены стандартных *S*-блоков DES другими, имеющими лучшие дифференциальные свойства (каждого предложенного *S*-блока, по сравнению со стандартными) дала возможность более эффективного объединения входных и выходных разностей и соответствующего увеличения вероятностей эффективных характеристик, что привело к значительному уменьшению стойкости шифра [4]. Поэтому после изучения дифференциальных свойств подстановок следующим этапом оценки стойкости к дифференциальному криптоанализу является исследование наиболее эффективных характеристик.

Как показывает проведенный анализ источников в настоящее время не существует общей методики, позволяющей находить наиболее эффективные характеристики (по крайней мере, в открытой литературе). На основании проведенных исследований возможные методы поиска характеристик можно разделить на 4 класса.

1. Эвристический выбор.

Этот метод фактически основан на интуиции исследователя, выбирающего наиболее вероятные, с его точки зрения, варианты. Имеет низкую эффективность, как и любой неупорядоченный поиск с малыми вычислительными ресурсами. Однако при отсутствии эффективной формализованной методики имеет некоторые преимущества перед вариантом 2, в некоторых случаях позволяя лучшие решения, не входящие в область автоматизированного решения.

2. Перебор значений на входе одной подстановки, активизирующих переходы с максимальной вероятностью.

   В этом случае при построении характеристики на входе алгоритма активизируется одна подстановка, для которой перебираются все наиболее вероятные переходы. Метод эффективен для шифров, не обеспечивающих значительного перемешивания на одном цикле шифрования, например, ГОСТ 28147-89. Для алгоритмов шифрования со значительным перемешиванием на одном цикле, таких как DES или SAFER+, он неэффективен. Преимуществом метода является возможность нахождения подмножества или полного множества наиболее эффективных характеристик при использовании ограниченных вычислительных ресурсов.

3. Эвристический выбор множества активных подстановок и входных значений для них.

   Этот метод позволяет объединить положительные свойства двух предыдущих, избавившись от их недостатков. При выполнении поиска анализируется значительное количество вариантов входных разностей и их преобразований, ведущих к построению наиболее вероятных характеристик. Является самым эффективным, если вычислительных ресурсов недостаточно для проведения полного перебора всех вариантов входных разностей (метод 4). Следует отметить, что при проведении исследований стойкости DES к дифференциальному криптоанализу и возможности модификации стандартных *S*-блоков [ЗащDES, SG] авторами использовался именно этот метод.

4. Полный перебор входных значений разности на входе алгоритма и вариантов их преобразования.

   В этом случае анализируются все возможные варианты активизации входных разностей и возможности их преобразования. Достоинством метода является гарантированное нахождение лучшей характеристики, недостатком – необходимость использования значительных вычислительных ресурсов, что в ряде случаев не позволяет провести вычислительный эксперимент, и, соответственно, воспользоваться этим методом.

При поиске характеристик для ГОСТ 28147-89 методы 2 и 3 примерно равнозначны, поскольку, на наш взгляд, наиболее эффективный метод поиска – активизация одной подстановки на входе 1-го цикла. Сразу следует отметить, что ни одной характеристики, которую можно было бы использовать на все 32 цикла шифрования, обнаружено не было (и, скорее всего, они вообще не существуют). Поэтому критерием оценки характеристики было количество циклов, после которого её вероятность становится ниже порогового значения 2^{-64}. Соответственно, чем большее количество циклов алгоритма шифрования может охватить характеристика до достижения порогового значения, тем она эффективнее.

Кроме того, при проведении вычислительного эксперимента было сделано предположение об отсутствии искажения разностей (XOR) на ключевом сумматоре. В общем случае, это утверждение верно только лишь для нулевого ключа шифрования. Однако, поскольку проводится доказательство стойкости шифра, а не разработка эффективной атаки, то предположение в пользу криптоаналитика не будет опровергать доказательство стойкости. Для ключей шифрования, в которых присутствуют единичные биты, эмпирическая вероятность характеристики будет ниже рассмотренных далее из-за возникновения искажений на ключевом сумматоре.

При поиске характеристик проводилась активизация разности для одной подстановки на входе первого цикла шифрования. Значения входной разности выбирались с учётом возможности активизации перехода с вероятностью 4/16, 6/16 и 8/16. Поскольку одно значение входной разности дает несколько вариантов перехода для подстановок ГОСТ 34.311-95 (за исключением нулевой входной разности), все возможные значения обрабатывались последовательно (в порядке возрастания значений разности). Выходные значения разности на выходе подстановок объединялись в целое выходное значение разности цикловой функции, которое после сложения по модулю 2 с разностью левой половины на входе текущего цикла формировало разность для входа цикловой функции следующего цикла. При выборе переходов соответствующим образом производился учёт вероятностей переходов, формирующих вероятность характеристики. Переходы с вероятностью 2/16 не рассматривались, поскольку пороговой вероятностью преобразования на S-блоке является 4/16: при наличии одной активной подстановки в каждом цикле шифрования (для характеристик ГОСТ 28147-89 в некоторых циклах обязательно присутствует более одной активной подстановки) вероятность характеристики для 32 циклов равна $\left(\frac{4}{16}\right)^{32} = 2^{-64}$. Для некоторых характеристик возможны

промежуточные циклы с нулевой входной разностью (примеры для DES можно увидеть, например, в [5]), однако они обязательно требуют несколько активных подстановок на предыдущих циклах и для рассматриваемого случая эффект увеличения вероятности полностью нивелируется.

Первоначальный вариант поиска характеристики предполагал активизацию всех возможных комбинаций входных разностей, активизирующих на первом цикле переходы с вероятностями 6/16 и 8/16 (а не только одной подстановки). Поскольку теоретически оценить сложность получаемого дерева характеристик не представляется возможным, был проведен вычислительный эксперимент. За 25 часов работы ПЭВМ Celeron-633 было обработано порядка $67 \cdot 10^9$ характеристик (учитывались только переходы с вероятностью 4/16 и выше), что составляет примерно 2,5% от общего количества. Полученные результаты приведены в таблице 3 (количество циклов характеристики, после которого её вероятность становится менее 2^{-64}, и соответственно количество найденных характеристик).

Таблица 3 – Количество найденных характеристик в зависимости от цикла шифрования

Количество циклов характеристики	Количество найденных характеристик	Количество циклов характеристики	Количество найденных характеристик
5	409933849	15	68627
6	28974550012	16	15965
7	30711528470	17	2456
8	4955798938	18	186
9	756928135	19	0
10	143620531	20	0
11	41575739	21	52
12	3455345	22	300
13	2052011	23	69
14	469360	24	20

Характеристик с количеством циклов менее 5 и более 24 не обнаружено. Соответственно среднее количество циклов, после которого вероятность характеристики становится менее 2^{-64}, равно 6.65615. Из таблицы 3 можно заметить, что с возрастанием количества циклов (после 7-го) количество характеристик экспоненциально убывает, а наибольшее количество характеристик переходит порог вероятности на 6 или 7 цикле.

Пример преобразования разностей для одной из найденных 24-цикловых характеристик приведен в таблице 4 (значения разностей приведены в шестнадцатеричной системе счисления).

Таблица 4 – Преобразования разностей для 24-цикловой характеристики

Номер цикла	Левая половина входной разности	Правая половина входной разности	Номер цикла	Левая половина входной разности	Правая половина входной разности
1	0	800000	13	807000	7
2	800000	7	14	7	800000
3	7	807000	15	800000	0
4	807000	800000	16	0	800000
5	800000	807007	17	800000	7
6	807007	7007	18	7	807000
7	7007	7	19	807000	800000
8	7	7	20	800000	807007
9	7	7007	21	807007	7007
10	7007	807007	22	7007	7
11	807007	800000	23	7	7
12	800000	807000	24	7	5007

В основе этой характеристики лежит преобразование разностей с вероятностями 4/16 $\rightarrow$ 8/16 и наоборот. Отсюда следует, что если бы разработчики таблиц не допускали бы переходы с вероятностью 8/16, такое большое количество циклов характеристики было бы недостижимо. Тем не менее, атаковать весь 32-цикловый шифр с помощью 24-цикловой характеристики невозможно (см. ниже).

При проведении вычислительного эксперимента за 25 часов работы компьютера было обработано порядка 2,5% возможных входных значений разности, активизирующих переходы с вероятностями 6/16 и 8/16. Отсюда следует, что на проведение полного перебора входных разностей потребовалось бы более 40 суток работы. Для переходов с такими вероятностями существует 31104 вариантов входной разности для правого полублока (левый всегда принимается равным нулю). Если к этим комбинациям добавить переходы с вероятностью 4/16, то всего получится $1{,}04 \cdot 10^{11}$ входных комбинаций. Требуемый объём вычислений не позволяет провести экспериментальный расчёт. Тем не менее, случайная генерация входных разностей с активизацией переходов с вероятностью 4/16 и выше даёт статистические результаты, схожие с уже полученными (см. табл. 3).

Однако анализ показал, что характеристики с максимальным количеством циклов (для данного вида входной разности, без рассмотрения дополнительного первого цикла) имеют во входной разности на первом цикле всего одну активную подстановку. Это позволило выполнить полный перебор входных разностей с одной активной подстановкой для переходов с вероятностями 4/16 и выше для всех 8 *S*-блоков. В результате после обработки $1{,}28 \cdot 10^{10}$ характеристик (переходы с вероятностью 2/16 опять игнорировались) было найдено 16 характеристик, для которых вероятность становилась менее 2^{-64} после 25 циклов шифрования.

Для сравнения можно привести результаты работы [6], где использовалась похожая методика дифференциального криптоанализа. Авторы сообщают о нахождении только лишь 12-цикловой характеристики с вероятностью 2^{-68}.

Основываясь на том, что характеристики с наибольшим количеством циклов формируются входными разностями, активизирующими одну подстановку, можно сделать вывод, что 25 циклов является предельным значением для характеристик подстановок ГОСТ 34.311-95, хотя провести полный вычислительный эксперимент или привести строгое теоретическое доказательство не представляется возможным.

Таким образом, при использовании в ГОСТ 28147-89 подстановок из ГОСТ 34.311-95 для существующей методики дифференциального криптоанализа ГОСТа [3], существуют характеристики, эффективные не более чем для 24-х циклов шифрования.

При проведении дифференциальной атаки для увеличения количества охватываемых циклов возможно использование дополнительного первого цикла и 2*R*-атаки после характеристики. Однако даже эта методика позволяет атаковать не более $24 + 1 + 2 = 27$ циклов шифрования ГОСТ 28147-89. Кроме того, при построении характеристик было сделано предположение об отсутствии искажений на ключевом сумматоре. При использовании ключа шифрования, в котором присутствуют единичные биты, сумматор будет вносить дополнительные искажения, что уменьшит количество циклов эффективной характеристики.

Ещё одним из вариантов увеличения количества охватываемых циклов шифрования может стать бумеранг-атака. Она может эффективно применяться против шифров, в которых вероятность p характеристики для всего алгоритма не позволяет провести эффективную атаку, однако вероятность q для характеристики на половину циклов шифрования позволяет провести атаку со сложностью $O(q^{-4})$ отобранных открытых текстов. Однако для подстановок из ГОСТ 34.311-95 вероятность характеристик для 16 циклов (с рассмотрением частей 24-цикловых характеристик) величина $O(q^{-4})$ значительно превосходит 2^{64}, что делает атаку на 32 цикла невозможной.

При использовании в ГОСТ 28147-89 подстановок из ГОСТ 34.311-95 эффективные характеристики могут быть использованы против 24 циклов шифрования и менее. Методы увеличения количества атакуемых циклов, такие как дополнительный первый цикл, 2*R*-атака и бумеранг-атака не позволяют атаковать полный вариант шифра. Хотя создатели таблиц могли уменьшить количество циклов в наиболее эффективных характеристиках, используемые ими критерии позволили полностью защитить шифр от атак дифференциального криптоанализа.

Выше было отмечено, что из всех аналитических атак против ГОСТа могут эффективно использоваться только дифференциальный и линейный криптоанализ. Стойкость шифра к этим нападениям в значительной степени определяется свойствами долговременного ключа, который не задаётся стандартом. В ГОСТ 34.311-95 приведен один из вариантов таблицы подстановок, который наиболее широко распространён и может быть использован в качестве единого долговременного ключа. При его генерации использовались критерии оптимизации против дифференциального и линейного криптоанализа. Из-за линейных свойств подстановок и наличия переносов в ключевом сумматоре линейный криптоанализ неэффективен против ГОСТ 28147-89 с подстановками из ГОСТ 34.311-95. Дифференциальный криптоанализ не может быть эффективно использован против более 27 циклов шифрования, т. е. полный вариант алгоритма защищён и от этого вида криптонападения.

Отсюда следует, что при использовании подстановок ГОСТ 34.311-95 первые три режима работы ГОСТ 28147-89 (простой замены, гаммирования и гаммирования с обратной связью) защищены от

дифференциальных и линейных атак. 4-й режим (выработки имитовставки) потенциально уязвим для дифференциального криптоанализа, поскольку использует только 16 циклов шифрования вместо 32. Однако если сообщение с имитовставкой зашифровывается перед передачей, то в этом случае дифференциальная атака на 4-й режим невозможна (поскольку дифференциальный криптоанализ относится к атакам с выбранными открытыми текстами и для его проведения необходимо знание открытых и зашифрованных сообщений). Даже при использовании 4-го режима работы алгоритма шифрования для передачи незашифрованной имитовставки необходимость выбора большого количества открытых текстов и получения соответствующих им зашифрованных делает дифференциальную атаку на этот режим практически неосуществимой в реальных СЗИ. При разработке новых систем для обеспечения имитозащиты можно рекомендовать применение функции хеширования ГОСТ 34.311-95 (с соответствующим добавлением ключевых данных) вместо 4-го режима ГОСТ 28147-89.

При разработке СЗИ следует обеспечивать защиту от атак на реализацию, таких как временная атака, анализ энергопотребления, дифференциальный анализ сбоев, поскольку ни один шифр не может быть защищён от этого вида нападений исключительно математическими методами.

Анализ свойств таблицы подстановок ГОСТ 34.311-95 показал, что в них отсутствуют закладки, делающие шифр уязвимым для известных видов криптоанализа. Более того, проведена оптимизация против дифференциального и линейного криптоанализа. В принципе, существует возможность генерации более стойких таблиц с дополнительными критериями для защиты от дифференциального и линейного криптоанализа, однако и рассмотренная обеспечивает максимальную стойкость трёх режимов ГОСТ 28147-89 и практическую стойкость режима выработки имитовставки. Поэтому можно рекомендовать использование долговременного ключа из ГОСТ 34.311-95 в качестве стандартного для ГОСТ 28147-89 при обеспечении криптографической защиты информации в открытых системах.

Литература: 1. В. И. Долгов, И. В. Лисицкая, Р. В. Олейников, С. А. Головашич, А. С. Коряк. Дополнительные требования к отбору таблиц подстановок для ГОСТ 28147-89. Материалы научно-практической конференции по вопросам криптографической и технической защиты информации. Департамент специальных телекоммуникационных систем и защиты информации Службы Безопасности Украины, Центр Банковских Информационных Технологий. Киев, 2000. 2. B. Schneier. Applied Cryptography. Addison Wesley and Sons, New York, 1996. 3. Р. В. Олейников. Дифференциальный криптоанализ алгоритма шифрования ГОСТ 28147-89. Радиотехника, 119. 2001 г. С. 146-152. 4. K. Kim, S. Lee, S. Park and D. Lee. How to strength DES against two robust attacks. Joint Workshop on Information Security and Cryptology. Inuyata, Japan, January 24-25, 1995. 5. В. И. Долгов, И. В. Лисицкая, С. А. Головашич, Р. В. Олейников. Принципы защиты алгоритма DES от атак дифференциального криптоанализа. Радиотехника, 113. 2000 г. С. 148–157. 6. J. Kelsey, B. Schneier, D. Wagner. Key-Schedule Cryptanalysis of IDEA, G-DES, GOST, SAFER and Triple-DES. Advances in Cryptology – CRYPTO'96, Springer-Verlag, Berlin 1996.

УДК 681.3.06

ПРИНЦИПЫ ПОСТРОЕНИЯ И ИСПОЛЬЗОВАНИЯ МНОГОУРОВНЕВЫХ ЦЕНТРОВ УПРАВЛЕНИЯ И СЕРТИФИКАЦИИ КЛЮЧЕЙ

Иван Горбенко, Александр Волощук*, Елена Качко*, Андрей Свинарев*, Павел Колесников, Татьяна Гриненко

Харьковский национальный университет радиоэлектроники

**АТ "Институт информационных технологий"*

Анотація: **Розглядаються основні положення створення багаторівневого центру сертифікації. Визначаються основні функції центру. Розглядаються проблеми, що з'являються під час розробки багаторівневого центру.**

Summary: **In the proposed report we consider the main statements of multilevel certification center development. Main functions of such centers are: generation, distribution and support of common parameters and keys for whole multilevel network, developing of open key base. It is considered a number of problems, which appears during of key transitions.**

Ключові слова: **Ключі, управління ключами, сертифікація ключів, бази даних ключів, паролів, фіскальний контроль.**