Макаревич Олег Борисович
Технологический институт Федерального государственного образовательного учреждения высшего профессионального образования «Южный федеральный университет» в г. Таганроге.
E-mail: mak@tsure.ru.
347928, г. Таганрог, ул. Чехова, 2.
Тел.: 8 (8634) 371-905.
Кафедра безопасности информационных технологий; заведующий кафедрой; профессор.

Makarevich Oleg Borisovich
Taganrog Institute of Technology – Federal State-Owned Educational Establishment of Higher Vocational Education "Southern Federal University".
E-mail: mak@tsure.ru.
2, Chekhova str., Taganrog, 347928, Russia.
Phone: 8 (8634) 371-905.
Department of IT-Security; Head of Department; professor.

Федоров Владимир Михайлович
Технологический институт Федерального государственного образовательного учреждения высшего профессионального образования «Южный федеральный университет» в г. Таганроге.
E-mail: vladmih@rambler.ru.
347928, г. Таганрог, ул. Чехова, 2.
Тел.: 8 (8634) 371-905.
Кафедра безопасности информационных технологий; доцент.

Fedorov Vladimir Mikhailovich
Taganrog Institute of Technology – Federal State-Owned Educational Establishment of Higher Vocational Education "Southern Federal University".
E-mail: vladmih@rambler.ru.
2, Chekhova str., Taganrog, 347928, Russia.
Phone: 8 (8634) 371-905.
Department of IT-Security; associate professor.

УДК 004.056.053

А.Ф. Чипига

ПОДХОД К РЕШЕНИЮ ПРОБЛЕМЫ СОХРАНЕНИЯ ДАННЫХ ПРИ РАСКРЫТИИ КЛЮЧА ДЕШИФРОВАНИЯ НА ПРИЕМЕ

Раскрыт подход к решению проблемы сохранения данных при компрометации ключа на приеме в одноключевых системах за счет использования физического уровня эталонной модели взаимосвязи открытых систем.

Блочные шифры; размножение ошибок; математическая модель ионосферы; электромагнитная доступность; помехоустойчивость.

A.F. Chipiga

THE APPROACH TO THE DATA RETENTION PROBLEM WITH DECRYPTION KEY DISCLOSING AT THE RECEIVING SIDE

The approach to the data retention problem with compromised key at the receiving side of the one key system in OSI Physical Layer was exposed.

Block ciphers; error propagation; mathematic ionosphere model; electromagnetic accessibility; noise immunity.

Существующая статистика взлома противником зашифрованных данных свидетельствует о том, что в большинстве случаев это происходит за счет определения противодействующей стороной ключа дешифрования [1].

Для зашифрования информации с использованием блочных шифров выработан и одобрен NIST ряд специальных режимов обработки различных объемов данных. Основными или базовыми режимами являются Electronic Code Book (ECB), Cipher Block Chaining (CBC), Output Feedback (OFB), Cipher Feedback (CFB). Новые более эффективные решения шифрования базируются на перечисленных выше, связаны с конкретной областью применения и гарантируют определенную степень защиты от той или иной криптоаналитической угрозы [2].

Во всех режимах происходит размножение ошибок при дешифровании принятого с ошибкой блока криптограммы. Принципы рассеивания и перемешивания, положенные в основу при построении произвольных блочных шифров, обуславливают, что любая ошибка канала при передаче блока криптограммы, в зависимости от режима, как минимум, приведет к искажению порядка $n/2$ бит очередного дешифрованного блока сообщения, где n – длина блока [3].

В режимах ECB и OFB искажение при передаче одного 64-битового блока шифротекста C_i, где i – номер блока, приводит к искажению после расшифрования соответствующего блока M_i открытого текста, но не влияет на следующие блоки.

В режимах CBC и CFB искажение при передаче одного блока шифротекста C_i приводит к искажению на приеме не более двух блоков открытого текста M_i и M_{i+1}.

Поэтому проблема размножения ошибок при передаче шифрованной информации по каналам с ошибками в настоящее время рассматривается как негативный фактор и требует применения либо мер повышения достоверности, либо каналов с малыми значениями вероятности ошибочного приема $P_{ош.}$ Однако тот факт, что искажения в канале приводят к искажению дешифрованного текста и существенно затрудняют работу криптоаналитика, может быть использован для решения проблемы сохранения данных в секрете даже в том случае, если на приёмной стороне противнику будет известен ключ дешифрования, и усложнить работу криптоаналитика.

Проблема может быть решена при использовании следующего предлагаемого способа функционирования системы обмена данными между корреспондентами:

1. Применение одного из алгоритмов зашифрования данных на передающей стороне.
2. Применение одного из режимов использования блочных шифров.
3. Использование для передачи данных такого канала, который обеспечил бы на приёме большое значение вероятности ошибочного приёма $P_{ош}$, такое, что без

применения специальных мер повышения достоверности гарантированно в блоке зашифрованного текста разрядностью n бит содержались бы ошибочные разряды.

4. Применение специальных мер повышения достоверности, понижающих значение $P_{ош}$ до допустимого значения, позволяющего дешифровать принятые зашифрованные блоки данных. Канал связи и меры повышения достоверности должны быть такими, что противник, пытающийся получить передаваемую информацию, либо не в состоянии был сделать это, либо при попытке выполнения мер повышения достоверности явно обнаруживал бы себя.

5. Дешифрование «очищенного» от ошибок приема блока криптограммы.

Предложенный способ функционирования в значительной мере позволит решить две проблемы. Во-первых, выявить противника, во-вторых, даже при наличии ключа дешифрования исключить похищение противником дешифрованной информации. Максимальная эффективность предложенного алгоритма будет достигаться в режимах CBC и CFB, в которых искажение при передаче одного блока шифротекста гарантированно приводит к искажению двух блоков открытого текста.

Кроме того, работа криптоаналитика будет существенно затруднена, так как он вынужден работать с шифротекстом, содержащим ошибки. Покажем вариант решения проблемы на примере систем спутниковой связи (ССС).

В настоящее время защита информации в системах спутниковой связи (ССС) осуществляется на втором (канальном), третьем (сетевом) и более высоких уровнях семиуровневой эталонной модели взаимосвязи открытых систем (ЭМВОС). С этой целью используются традиционные методы шифрования, кодирования и т. д. Поиск дополнительных резервов защиты информации приводит к очевидному выводу о целесообразности использования и первого (физического) уровня модели ЭМВОС. Однако до настоящего времени мероприятия по защите информации на физическом уровне ЭМВОС никем не предлагались. Для ССС решение этой задачи представляется возможным в силу следующих причин.

Основным достоинством ССС является высокое качество передачи информации, а основным недостатком – высокая электромагнитная доступность (ЭМД) радиоизлучения ССС для приемника несанкционированного пользователя. Указанные достоинство и недостаток обусловлены одной причиной: хорошими условиями распространения радиоволн для традиционно используемых в ССС несущих частот 1…10 ГГц. Если понизить частоту до 30…100 МГц, то существенно возрастет поглощение, рефракция, фазовая дисперсия и рассеяние волны в ионосфере, что приведет к значительному (на порядки) снижению как показателей качества передачи информации в ССС, так и ее ЭМД [4].

Есть основания полагать, что на частотах выше 60…70 МГц превалирующее влияние на снижение этих показателей будет оказывать рассеяние радиоволн на неоднородностях ионосферы. Однако для повышения качества передачи информации в каналах с ионосферным рассеянием можно использовать различные методы разнесенного (на несколько антенн) приема (внедрение которых для несанкционированных пользователей затруднено). Следовательно, применение в ССС пониженных несущих частот с одновременным внедрением методов разнесенного приема сигналов можно рассматривать как новый способ защиты информации ССС от несанкционированного использования, позволяющего обеспечить высокое качество передачи информации при низкой ЭМД радиоизлучения ССС. Отсюда следует вывод о наличии крупной научно-технической проблемы уменьшения электромагнитной доступности излучения (повышения скрытности) систем спутниковой связи для несанкционированных пользователей без снижения качества

передачи информации за счет одновременного понижения несущей частоты до $f_0 = 60...70\,\text{МГц}$ и внедрения пространственно-разнесенного приема на несколько антенн [5].

Предлагаемые меры одновременно приводят к уменьшению электромагнитной доступности (повышению скрытности) излучения систем спутниковой связи от несанкционированных пользователей на 3-4 порядка (без снижения качества передачи информации) за счет понижения несущих частот до $f_0 = 60...70\,\text{МГц}$ и внедрения разнесенного приема сигналов на несколько антенн [6].

Таким образом, существует реальный способ решения проблемы сохранения данных при раскрытии ключа дешифрования на приеме.

Концептуальные подходы к решению проблемы сводятся к применению физического уровня ЭМВОС, а пути и методы решения сводятся к следующему.

1. Разработка математической модели ионосферы для оценки факторов трансионосферного распространения радиоволн (поглощения, рассеяния, дисперсии и т.д.).

2. Разработка основ теории построения структурно-физических моделей трансионосферных радиоканалов (с общими или частотно-селективными замираниями и дисперсионными искажениями) на базе комплексного применения методов статистической теории связи (построения многолучевых моделей каналов связи) и статистической радиофизики (фазового экрана, параболического уравнения).

3. Разработка методов построения структурно-физических моделей пространственно-временных трансионосферных радиоканалов (с учетом пространственно-селективных замираний).

4. Теоретическое обобщение методов анализа помехоустойчивости ССС при одновременном проявлении замираний (общих или селективных по частоте и пространству), межсимвольной интерференции и дисперсионных искажений.

5. Прогнозирование показателей качества (помехоустойчивости и электромагнитной доступности) систем спутниковой связи при использовании пониженных частот.

6. Разработка методики энергетического расчета радиолиний ССС на пониженных частотах и оценки их электромагнитной доступности.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Ярочкин В.И.* Информационная безопасность : учебник для вузов / В.И. Ярочкин. – М. : Академический Проспект ; фонд «Мир», 2003. – 640 с.

2. *Соколов А.В.* Защита информации в распределенных корпоративных сетях и системах / А.В. Соколов, В.Ф. Шаньгин. – М. : ДМК Пресс, 2002. – 656 с.

3. *Алферов А.П.* Основы криптографии : учебное пособие / А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. – 2-е изд., испр. и доп. – М. : Гелиос АРВ, 2002. – 480 с.

4. *Сенокосова А.В.* Математическая модель ионосферы для оценки поглощения радиоволн в системах космической связи / А.В. Сенокосова, М.Э. Солчатов, А.В. Стрекалов, А.Ф. Чипига // Инфокоммуникационные технологии. – 2006. – Т. 4. – № 1. – С. 77-82.

5. *Чипига А.Ф.* Защита информации в системах космической связи за счет изменения условий распространения радиоволн / А.Ф. Чипига, А.В. Сенокосова // Космические исследования. – 2007. – Т. 45. – № 1. – С. 59-66.

6. *Чипига А.Ф.* Способ обеспечения энергетической скрытности систем спутниковой связи / А.Ф. Чипига, А.В. Сенокосова // Космические исследования. – 2009. – Т. 47. – № 5. – С. 428 – 433.

Чипига Александр Федорович
Северо-Кавказский государственный технический университет
E-mail: zik@ncstu.ru.
355003, Ставрополь, ул. Морозова, 105, кв. 15.
Тел.: 8 (9624) 44-10-70.
Заведующий кафедрой информационной безопасности.

Chipiga Alexander Fedorovich
North Caucasus State Technical University.
E-mail: zik@ncstu.ru.
App. 15, 105, Morozova str., Stavropol, Russia.
Phone: 8 (9624) 44-10-70.
head of Information Security department

УДК 681.3

И.А. Калмыков, А.А. Чипига, А.В. Барильская, О.А. Кихтенко

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ДАННЫХ В ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЯХ НА БАЗЕ НЕПОЗИЦИОННЫХ ПОЛИНОМИАЛЬНЫХ СИСТЕМ

Рассмотрен алгоритм нелинейного шифрования потока данных с операцией возведения в степень элементов расширенных полей Галуа $GF(p^v)$. Представлена структура устройства для вычисления индекса элемента поля Галуа.

Нелинейное шифрование; расширенные поля Галуа; элементы полей Галуа; полиномиальная система классов вычетов; индекс.

I.A. Kalmikov, A.A. Chipiga, A.V. Baril'skaya, O.A.Kikhtenko

CRYPTOGRAPHIC PROTECTION OF DATA IN INFORMATION TECHNOLOGY ON BASE NEPOZICIONNYH POLYNOMIAL SYSTEMS

Algorithm for non-linear encryption of a data flow with elements of extended Galois $GF(p^v)$ fields involution operation. Device structure for Galois field element index calculation is offered.

Non-linear encryption; extended Galois $GF(q^v)$; elements of extended Galois $GF(q^v)$ polynomial system of residue classes; index.

В стратегии развития Российского государства в качестве одного из приоритетов определена национальная безопасность, одним из важнейших элементов последней является информационная безопасность. Именно поэтому разработка безопасных и эффективных информационных систем является одним из приоритетных направлений развития РФ. Решая задачи создания новых технологий информационной безопасности, необходимо сочетать, с одной стороны, высокую скорость обработки и передачи больших объемов информации, а с другой – ограничения доступа к ней, обеспечивая требуемый уровень защиты информации.

Проведенный анализ работ [1,2] показал, что современные системы криптографической защиты информации не позволяют в полной мере решить данную