ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РЕСПУБЛИКИ КАЗАХСТАН
MINISTRY OF EDUCATION AND SCIENCE
OF THE REPUBLIC OF KAZAKHSTAN

Л.Н. ГУМИЛЕВ АТЫНДАҒЫ
ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ
ЕВРАЗИЙСКИЙ НАЦИОНАЛЬНЫЙ
УНИВЕРСИТЕТ ИМ. Л.Н. ГУМИЛЕВА
GUMILYOV EURASIAN
NATIONAL UNIVERSITY

ЖАС ҒАЛЫМДАР КЕҢЕСІ

Студенттер мен жас ғалымдардың «Ғылым және білім - 2015» атты X Халықаралық ғылыми конференциясының БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ X Международной научной конференции студентов и молодых ученых «Наука и образование - 2015»

PROCEEDINGS of the X International Scientific Conference for students and young scholars «Science and education - 2015»

УДК 001:37.0
ББК72+74.04
Ғ 96

Ғ96
«Ғылым және білім – 2015» атты студенттер мен жас ғалымдардың X Халық. ғыл. конф. = X Межд. науч. конф. студентов и молодых ученых «Наука и образование - 2015» = The X International Scientific Conference for students and young scholars «Science and education - 2015». – Астана: http://www.enu.kz/ru/nauka/nauka-i-obrazovanie-2015/, 2015. – 7419 стр. қазақша, орысша, ағылшынша.

ISBN 978-9965-31-695-1

Жинаққа студенттердің, магистранттардың, докоранттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.

В сборник вошли доклады студентов, магистрантов, докторантов и молодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 001:37.0
ББК 72+74.04

ISBN 978-9965-31-695-1

мониторинга, а также для выявления зависимости прохождения СВЧ волны от диэлектрической проницаемости среды распространения [4].

В итоге измерения и сравнительный анализ позволили прийти к выводу о том, что крупный гранит и большие компоненты грунта являются главными факторами, оказывающим решающее воздействие на затухание сигнала.

Список использованных источников

1. Кочумеев В.А., Мирманов А.Б., Стукач О.В. Изучение проблемных ситуаций в разработке перспективных геофизических информационно-измерительных систем // Вестник науки Сибири. - Т. 4. - N 3. - 2012. - С. 99-102.

2. Мирманов А.Б., Стукач О.В. Сегментация вмещающей среды в геофизической системе передачи данных // Комп'ютерна графіка та розпізнавання зображень / Збірник наукових праць науково-практичної Інтернет-конференції / Кол.авт./ - Вінниця: Вінницький обласний інститут післядипломної освіти педагогічних працівників, травень 2012 року. - с. 108-120.

3. Харвей А.Ф. Техника сверхвысоких частот. М.: СОВЕТСКОЕ РАДИО, 1965. – 759 с.

4. Мирманов А.Б., Сарсембиева Э.К, Байгуаныш С., Алимбаев А. Возможности технологических применений мощных импульсных СВЧ сигналов в передаче телеметрической информации // Международная конференция «Радиоэлектронные устройства и системы для инфокоммуникационных технологий» (REDS-2014) – Москва, 21 - 23 мая 2014г. с. 183-1864

УДК 681.3.06

ГИБРИДНАЯ КРИПГРАФИЧЕСКАЯ ЗАЩИТА ТЕЛЕКОММУНИКАЦИОННЫХ КАНАЛОВ

Молдамурат Хуралай
moldamurat@yandex.kz
к.т.н., доценткафедры РЭТ, ЕНУ им. Л.Н.Гумилева, Астана, Казахстан

Одной из самых слабых сторон телекоммуникационных каналов нашего время стала низкая защищенность от перехвата информации. Радиоэфир в целом открытая неоднородная нелинейная среда для электромагнитных волн с пере отражениями, рефракциями и использования антенн с узкой диаграммой направленности не защищает канал от перехвата информации. Рост объемов конфиденциальной информации, передаваемой по незащищенным каналам связи, привел к широкому применению криптографических методов защиты. При этом предполагается, что криптография должна обеспечить такую защиту конфиденциальной информации, что даже в случае ее перехвата противником и обработки любыми способами с использованием современных и перспективных средств вычислительной техники она не должна быть дешифрована в течение нескольких десятилетий.

Таким образом, повышение уровня криптографической защиты космических телекоммуникационных каналов это актуальнейшая задача современной IT-технологий и касается она и нашей страны, где практически все телекоммуникационные каналы (телевидение, сотовая и проводная связь, Интернет и др.) реализованы через оборудование и каналы стран ближнего и дальнего зарубежья, это касается и наших космических спутников серии KazSat, разработанных и созданных зарубежными производителями.

Процесс передачи информации по каналам связи содержит два основных этапа, это кодирование и шифрование, и соответственно процесс приема - декодирование и дешифрование, а также сжатие. Архивация (сжатие) информации служит уменьшению объеме через уменьшение избыточности и использует для этого специальные алгоритмы.

Для того, чтобы предупредить потерю целостности информации применяют помехоустойчивое кодирование, целью которого является контроль целостности данных и возможность их полного или частичного восстановления. Целью кодирования информации является лишь предотвращение ее повреждения и кодирование, как правило, не меняет статистических характеристик информации.

Последнее десятилетие создало условия для достижения в реальной каналообразующей аппаратуре систем связи пропускной способности близкого к теоретическим пределам для каналов космической и спутниковой связи. Так в области кодирования перспективно активно развиваются многопороговое декодирование (МПД). Данные алгоритмы характеризуются небольшой сложностью реализации и при этом обладают достаточно высокой энергетической эффективностью. МПД позволяют обеспечить высокую достоверность передачи данных в каналах при весьма высоком уровне шума и практически неограниченном быстродействии[1].

Самым актуальным и криптографически гарантированными методом защиты информациииостаётся симметричное шифрование. В симметричном шифровании, основанном на использовании составных ключей, идея состоит в том, что секретный ключ делится на две части, хранящиеся отдельно. Преимуществом данных алгоритмов с симметричными ключами является высокая производительность и при прочих равных условиях стойкость определяется длиной ключа. Так как для шифрования и дешифрования используется один и тот же ключ, при использовании таких алгоритмов требуются высоко надежные механизмы для распределения ключей. Для эффективного симметричного шифрования используют ключи не очень большой длины что позволяет быстро шифровать большие объемы данных.

Участившееся возникновение нежелательного ПО, использующего новые уязвимости, повысило требования к современным системам информационной безопасности и привело использованию систем искусственного интеллекта [2]. Интеллектуальные средства находят активное применение для решения задач защиты информации. Классификация и кластеризация являются основными задачами, решаемыми интеллектуальными средствами обеспечения информационной безопасности (ИБ) телекоммуникационных каналов в условиях космической связи, т. к. необходим постоянный мониторинг уязвимостей системы и поля угроз каналам [3, 4]. Известные средства обеспечения ИБ компьютерных сетей, такие как: детекторы уязвимостей, детекторы вторжений, антивирусное ПО, межсетевые экраны [5] не применимы в полном объеме для космических каналов в связи с отсутствием мощных вычислительных средств на спутниках, тем более на микроспутниках.К примеру на рисунке 1а приведен реализации в общем виде взлома криптографический защищенного канала связи с открытым ключом нарушителем посередине (Е) - казалось бы одной из самых защищенных систем. Ещё одна форма атаки, теперь уже пассивной, вычисление закрытого ключа по известному открытому ключу (рисунок 1б). Этот процесс упрощается, если криптоаналитик (Е) перехватил несколько криптотекстов, посланных лицом А лицу В.

а) б)

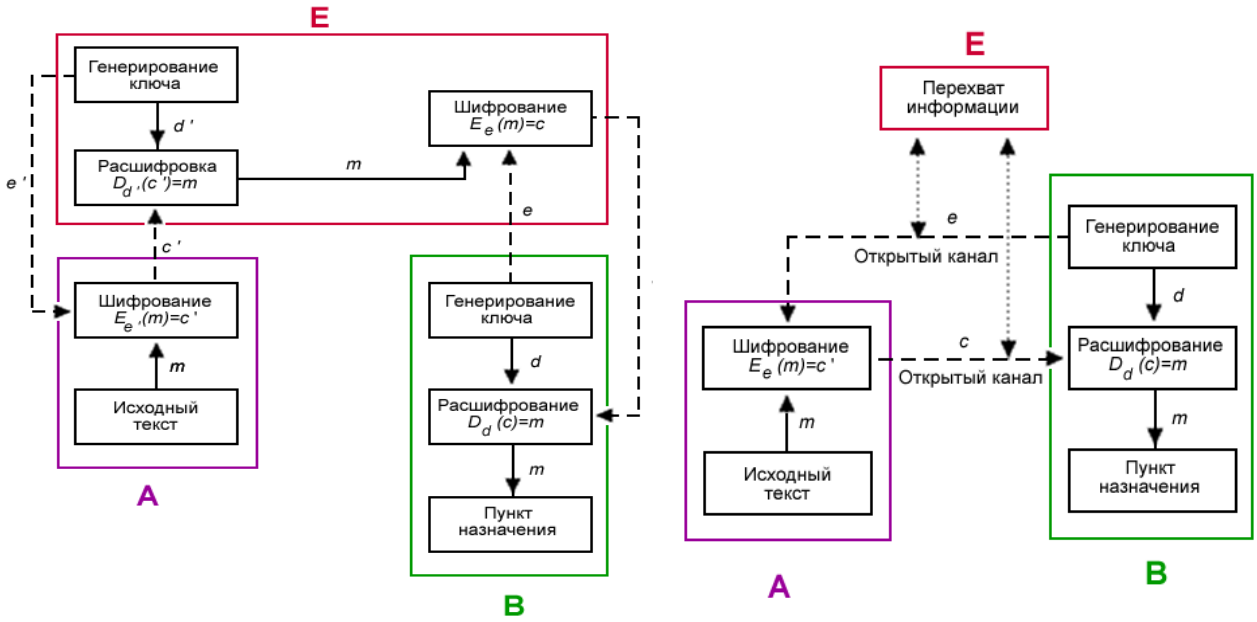

Рисунок 1 Способы взлома криптозащищенного канала

Что же касается защиты информации, то большинство современных системы информационной безопасности не обладают возможностью самообучения и используют только определенные правила, заложенные в них программно или аппаратно. Создание перспективных систем защиты информации (СЗИ) в последнее время отождествляют с использованием интеллектуальных средств, таких как: экспертные системы, системы нечеткой логики, нейронные сети, генетические алгоритмы, реализующих в СЗИ эволюционные свойства адаптации, самоорганизации, обучения, возможности наследования и представления опыта экспертов информационной безопасностив виде доступной для анализа системы нечетких правил If-Then.

Основная задача предлагаемой концепции гибридной защиты - создание адаптивной программно-аппаратной защиты канала связи, реализующей максимально эффективную обработку сигнала этапах кодирования шифрования. В данном исследовании предлагается использовать гибридную архитектуру:

- аппаратную часть выполнить на высокопроизводительной ПЛИС (раундовые операции Фейстеля в шифраторе и регистровые операции в многопороговом кодере);

- в программной части использовать многоядерный сигнальный процессор (интеллектуальный анализ попыток вторжения и модификаций защиты).

Реализация на современных ПЛИС алгоритма многопорогового декодирования сигнала [6] обеспечит высокую скорость и достоверность передачи данных в каналах даже при весьма высоком уровне шума. Рассмотрим предлагаемую архитектуру защиты на примере канала передачи исследовательского микроспутника. Адаптивная защита реализована на основе искусственного интеллекта с многопороговым декодером каналов космической связи (рис. 2).

Аппаратная реализация отличается существенно большей стоимостью. но ей присущи такие преимущества как высокая производительность, простота, защищенность. Программная реализация более просто реализуема и допускает высокую алгоритмическую гибкость.

Процесс криптографического закрытия данных в данном исследовании предполагается осуществляться как программно, так и аппаратно, что обеспечивает данному подходу максимальную вычислительную эффективность при сохранении гибкости архитектуры. Использование многоядерного сигнального микропроцессора позволит

реализовать гибкую и самоорганизующуюся интеллектуальную защиту канала с одновременным распаралеливанием процессов и разными стандартами шифрования, к примеру на рисунке 2 -это ГОСТ 28147-89 и AES.

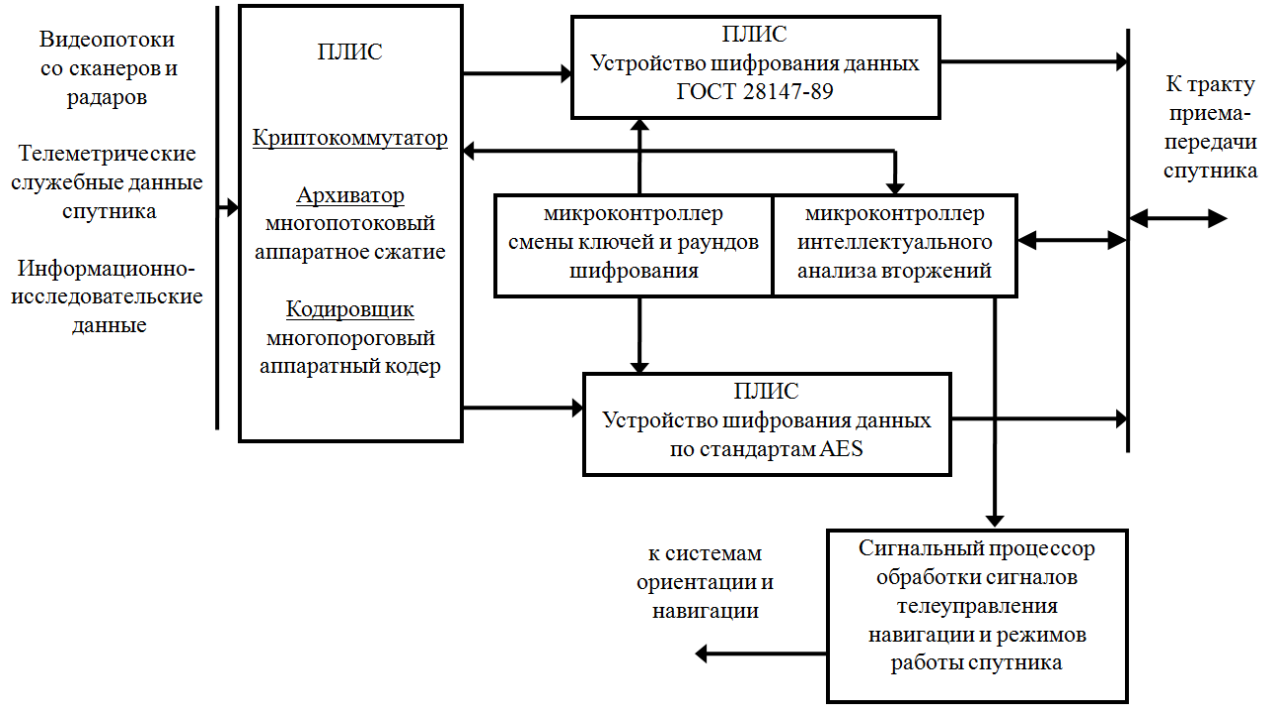

Рисунок 2 - Гибридная адаптивная защита канала передачи информации

Таким образом, предлагаемый подход дает возможностьпроектирования аппаратного шифратора с помощью HDL на базе микросхемы ПЛИС и с возможностью последующего практического использования для улучшения стойкости шифрования, быстродействия и других параметров телекоммуникационных систем.

Список использованных источников

1. http://vpk-news.ru/news/14276
2. www.bbc.co.uk/ukrainian/science/2014/05/140518_space_russia_usa_troubles_ms.shtml
3. Нестерук Г. Ф., Молдовян А. А., Костин А. А., Нестерук Ф. Г., Воскресенский С. И. Организация иерархической защиты информации на основе интеллектуальных средств нейро-нечеткой классификации // Вопросы защиты информации. 2005, № 3. С.16 – 26.
4. Satellite Communications in the Global Internet: Issues, Pitfalls, and Potential
5. Золотарев В.В. Теория и алгоритмы многопорогового декодирования . – М.: Радио и связь, Горячая линия – Телеком, 2006.-276 с.
6. Асимметричная криптосистема с пассивным перехватчиком, Лабанкова Е. https://ru.wikipedia.org/wiki8

УДК 621

ИЗМЕРЕНИЕ ДИАГРАММЫ НАПРАВЛЕННОСТИ ДИФРАКЦИОННОЙ АНТЕННЫ

Мусаханов Досымхан Абитханович
Dos_f@mail.ru
Старший преподаватель кафедры радиотехники, электроники и телекоммуникаций
ЕНУ им. Л.Н.Гумилева, Астана, Казахстан