УДК 004.056

Исследование современных инструментов обеспечения информационной безопасности

Насиров Фамиль Нурусланович
Баткенский государственный университет
соискатель

Аннотация
В связи с активным развитием информационных технологий растет многогранность и сложность проблем информационной безопасности, увеличиваются объемы передачи, обработки и хранения информации с ограниченным доступом. Известно, что наиболее эффективными средствами защиты конфиденциальных данных является кодирование и шифрование. Однако постоянное улучшение методов и средств криптоанализа и радиоразведки приводит систематическое повышение требований к коммуникационным системам. Современные телекоммуникационные сети используют известные и хорошо изученные сигналы (М-последовательности, коды Голда, последовательности Уолша, Баркера и др.), которые не могут обеспечить необходимую структурную скрытность и конфиденциальность процесса передачи информации. Формирования сигналов произвольной емкости является актуальным научно-практической задачей при разработке новых радиотехнических устройств. Повышение требований к кибербезопасности и электромагнитной совместимости требует развития новых областей исследования и разработки генераторов сигналов с большой информационной емкостью.
Ключевые слова: расширенный спектр, кибербезопасность, сигнал, информация, частота, тесты.

Research of modern instruments of information security support

Nasirov Famil Nuruslanovich
Batken State University
applicant

Abstract
In connection with the active development of information technology, the complexity and complexity of information security problems is increasing, the volumes of information transmission, processing and storage with limited access are increasing. It is known that the most effective means of protecting confidential data is encryption and encryption. However, the continuous improvement of methods and means of cryptanalysis and radio intelligence leads to a systematic increase in the requirements for communication systems. Modern telecommunications networks use well-known and well-studied signals (M-

sequences, Gold codes, Walsh, Barker sequences, etc.), which cannot provide the necessary structural secrecy and confidentiality of the information transfer process. Formation of signals of arbitrary capacity is an actual scientific and practical task in the development of new radio devices. Increasing requirements for cybersecurity and electromagnetic compatibility requires the development of new areas of research and development of signal generators with large information capacity.
Keywords: extended spectrum, cybersecurity, signal, information, frequency, tests.

В настоящее время одним из наиболее перспективных направлений исследований является системы связи с расширенным спектром [10; 21]. Расширение спектра делает увеличение базы сигнала и обеспечивает повышение эффективности передачи информации с помощью модулированных сигналов по каналу связи с сильными помехами. Сначала методы расширения спектра применялись для военных систем управления и связи и для борьбы с электромагнитными помехами. В дальнейшем развитие методов расширения спектра получило при разработке помехоустойчивых систем связи.

Суть методов расширенного спектра заключается в использовании полосы передачи сигнала, гораздо более шире минимально необходимой для передачи информации [25; 40].

Система связи называется системой с расширенным спектром в следующих случаях:

1. Использование полосы намного больше минимальной базы сигнала, необходимой для передачи информации.

2. Расширение спектра осуществляется с помощью сигнала расширения, который не зависит от информации.

3. Восстановление исходных данных приемником осуществляется путем сопоставления полученного сигнала и синхронизированной копии сигнала расширения.

В существующих сегодня системах связи с расширенным спектром используют следующие методы:

- псевдослучайные перенастройки рабочей частоты (frequency-hopping spread spectrum) [13; 38]. Суть метода заключается в периодической смене значения несущей частоты согласно алгоритму, известному принимающей и передающей стороне. Такой метод используются в Bluetooth. Преимуществом этого метода является простота реализации, а недостатком - задержка в потоке данных при каждой смене несущей частоты.

- расширение спектра методом прямой последовательности (direct sequence spread spectrum) [16; 34]. Суть метода заключается в повышении тактовой частоты модуляции, при этом каждому символу сообщения ставится в соответствие известная псевдослучайная последовательность. Метод используется в системах сотовой связи CDMA и Wi-Fi. По эффективности данный метод преобладает метод расширения спектра с помощью псевдослучайной перенастройки рабочей частоты.

- расширение спектра методом линейной частотной модуляции (chirp spread spectrum) [14; 39]. Суть метода заключается в перенастраивании несущей частоты по линейному закону. Данный метод используется в радиолокации.

Преимуществами систем с расширенным спектром являются:

- на сигнал слабо влияют помехи;
- расширение спектра позволяет скрывать и шифровать сигналы;
- несколько пользователей могут одновременно использовать одну полосу частот.

Системы связи с расширенным спектром с передачей опорного сигнала могут использовать случайные кодовые сигналы расширения и сжатия, поскольку кодовый и модулированный информационным кодом сигналы одновременно передаются в разные области спектра. Метод хранения опорного сигнала позволяет получать истинно случайные сигналы, поскольку кодовый сигнал должен храниться или генерироваться на приемной стороне.

Таким образом, расширяющие спектр последовательности современных систем связи с множеством доступов хорошо известны (М-последовательности, коды Голда, последовательности Уолша, Баркера и др.), но постепенно теряют свою актуальность для обеспечения надежного конфиденциальной связи. Растущие требования к электромагнитной совместимости, кибербезопасности, тенденция к уменьшению мощности источников электромагнитного излучения обуславливают целесообразность совмещения этапов кодирования и шифрования информации с использованием ППП. Источниками таких последовательностей могут быть непрерывные или дискретные НДС.

Для исследования статистических свойств генерируемых последовательностей на соответствие критериям псевдослучайности используют статистические тесты [2; 30]. К статистическим тестам относятся наборы тестов, разработанных Дональдом Кнутом, DIEHARD, NIST, FIPS и AIS.

Статистические тесты используют для проверки определенной нулевой гипотезы H_0 по случайности сложившейся последовательности. С гипотезой H_0 связана альтернативная гипотеза $H_{алт}$ о том, что последовательность не случайна. Для каждого теста, можно сделать вывод о принятии или отклонении нулевой гипотезы, исходя из сложившейся генератором последовательности. При этом для каждого теста и последовательности должна быть выбрана адекватная статистика случайности, на основе которой может быть принята или отклонена нулевая гипотеза. Теоретически для нулевой гипотезы распределения статистика определяется математическими методами. При проведении теста рассчитывается значение тестовой статистики, которое сравнивается с критическим. Если значение тестовой статистики превышает критическое, нулевая гипотеза отклоняется, в противном случае - принимается.

Обычно для тестирования последовательностей используют наборы статистических тестов FIPS и NIST SP 800-22. В подавляющем большинстве работ для комплексного тестирования последовательностей используется набор статистических тестов NIST SP 800-22. Такой выбор обусловлен тем, что данный набор предлагает критерии принятия решения относительно не только отдельной последовательности, но и в отношении всего ГПВП. Дополнительным фактором выбора этой методики является положительный опыт ее использования при исследовании статистических свойств криптоалгоритмов, что выдвигались на национальный стандарт государств НАТО.

Если последовательность проходит все тесты, тогда она считается криптографически стойкой. Приведем краткий обзор тестов.

1. Частотный (монобитный) тест [1; 32]. Целью этого теста является оценка пропорции нулей и единиц в заданной последовательности. В тесте осуществляется проверка, будет ли количество нулей и единиц в исследуемой последовательности примерно такое же, как у настоящей случайной последовательности. Тест оценивает количество единиц, блзких к ½. Вероятность отклонения в пропорции единиц оценивается с помощью критерия Пирсона (хи-квадрат статистики).

2. Частотный поблочный тест [4; 33]. Задачей теста является оценка соотношения различных бит в М-битных блоках. В тесте проверяется, будет ли количество единиц в середине каждого блока примерно равно М / 2, как это должно быть для настоящей случайной последовательности.

3. Тест серий [5; 31]. Серией называют непрерывную последовательность из одинаковых битов. В тесте осуществляется оценка количества различных серий во всей тестовой последовательности. Целью теста является сравнение, количества серий в исследуемой и случайной последовательности бит. Для прохождения теста имеющиеся отклонения должны находиться в допустимых пределах. Также можно сказать, что этот тест обнаруживает скорость и частоту колебаний между нулями и единицами в последовательности.

4. Поиск длинной серии из единиц [20; 36]. В тесте исследуются М-битные блоки, в каждом из которых ищется самая длинная серия из единиц. Результаты сравниваются с ожидаемыми для действительно случайной последовательности.

5. Тест ранга бинарных матриц [22; 27]. В тесте с заданной последовательностью формируются квадратные бинарные матрицы. Для каждой матрицы ищется ее ранг. Известно, что ранг матрицы является количественной оценкой линейной зависимости между ее строками. Если ранг матрицы меньше количества ее строк, тогда это значит, что отдельные строки зависимы между собой, а сама последовательность не случайна.

6. Тест на основе дискретного преобразования Фурье [8; 28]. В тесте выполняется быстрое преобразование Фурье над входной последовательностью. Наличие в спектре компонентов, значительно отличающихся по амплитуде говорит о признаках периодичности тестовой

последовательности.

7. Тест шаблонов без перекрытия [7; 26]. В этом тесте в последовательности ищется заранее заданный шаблон. Если последовательность битов соответствует шаблону, то анализируются следующие биты после него. Если шаблон отличается от текущей последовательности, то поиск сдвигается на один бит, и снова осуществляется сравнение и т.д. Подсчитанное количество совпадений сравнивается с аналогичным для случайной последовательности.

8. Тест шаблонов с перекрытием [9; 41]. От предыдущего этот тест отличается тем, что даже при совпадении шаблона окно сдвигается на один бит.

9. Универсальный тест Мауера [6; 35]. Целью теста является оценка возможности сжатия последовательности путем подсчета количества бит между совпадающими шаблонами. Если последовательность не случайна - она может быть значительно сжата без потерь.

10. Тест линейной сложности [11; 24]. В тесте осуществляется расчет длины линейного регистра сдвига, который может сгенерировать заданную последовательность. Если последовательность является сложной, то длина регистра будет большой.

11. Тест серий [17; 37]. В тесте серий исчисляется частота выпадения всех возможных m-битных шаблонов с перекрытием. Для случайной последовательности это количество будет примерно равно вероятной.

12. Тест энтропии [12; 42]. В тесте на энтропию подсчитывается частота выпадения всех возможных m и (m + 1) -битный шаблонов с перекрытием. Результаты сравниваются с ожидаемыми для настоящей случайной последовательности.

13. Тест накопленных сумм [3; 15]. В тесте начальная последовательность нулей и единиц превращается в последовательность «1» и «1». Далее рассчитывается, начиная с первого, сумма цифр и оказываются ее максимальные значения. Для случайной последовательности эти отклонения должны быть небольшими.

14. Тест случайных отклонений [18; 27]. Тест как предыдущий, с разницей в том, что вычисляется количество пересечений суммы уровней 4, 3, 2, 1, 1, 2, 3, 4 и сравнивается с ожидаемым для случайной последовательности.

15. Тест случайных отклонений – 2 [19; 34]. Все нули в тестовой последовательности заменяются на минус единицы. Интегральная сумма последовательности считается случайным отклонением. В тесте исчисляется количество достижений интегральной суммой состояний -9, -8 ..., 1, 1, 2, ..., 9 и сравнивается с ожидаемым для случайной последовательности.

Итак, ГПВП используются в телекоммуникационных системах для генерирования псевдослучайной гаммы в блочных и поточных методах шифрования, а также для формирования широкополосных сигналов.

Псевдослучайные последовательности современных телекоммуникационных систем формируются аппаратно реализованными схемами, основанные на:

- регистрах сдвига с линейной обратной связью,
- линейных конгруэнтных методах,
- методе Блюм-Блюм-Шуба,
- развязках системы нелинейных дифференциальных уравнений (схема Чуа, система Лоренца и т.д.);
- развязках системы одно- или многомерных рекуррентных отражений (логистическое отображение, тентовое, смещения и т.д.).

Хотя линейные конгруэнтные методы позволяют генерировать последовательности с хорошими псевдослучайными свойствами, однако, они не являются криптографически стойкими. Генераторы последовательностей на базе линейного конгруэнтного метода были сломаны Джимом Ридс и в последующем расширены на все типы линейных конгурентных методов.

Недавно показано [23; 29 и др.], что учет топологических свойств хаотических колебаний в фазовом пространстве при использовании методов нелинейного анализа (BDS- статистики, рекуррентный анализ, фрактальные размерности) для одномерных отображений делает различия хаотического сигнала и установления параметров системы.

Несмотря на разнообразие не все НДС могут быть использованы в качестве базы ГПВП, что обусловлено следующими требованиями:

- простота реализации для возможности использования на различных платформах. Например, полиномиальные отображения использовать для перевода в дробные степени нецелесообразно из-за наличия сложных арифметических операций;
- отсутствие начальных условий, которые со временем приводят к нулевой реализации выходного сигнала. Поэтому тентовое отображения и отображения смещения не рассматривались;
- нелинейные функции отражений должны быть взаимно неоднозначными;
- хаотические режимы должны быть устойчивыми и возникать в независимости от начальных условий.

Синтез аппаратных ГПВП на базе НДС и применение их для формирования псевдослучайных последовательностей является актуальной задачей в радиотехнических устройствах и средствах телекоммуникаций. На основе проведенного анализа научно-технических публикаций и результатов экспериментальных исследований можно сделать следующие выводы:

1. Из сравнительного анализа генераторов сигналов на базе НДС следует, что генераторы сигналов на базе НДС могут обеспечить синтез широкополосных сигналов с улучшенными статистическими характеристиками.

2. Большинство НДС не являются пригодными для использования в качестве базы ГПВП. Поэтому востребованным является синтез новых радиотехнических НДС для систем передачи информации.

3. Существуют существенные нерешенные проблемы практической реализации систем передачи информации на основе генераторов хаотических колебаний, которые связанны с технологической сложностью обеспечения идентичности параметров электронных компонент приемной и передающей части.

4. Последовательности, генерируемые регистрами сдвига с линейной обратной связью известны тем, что ограничивают их применение для телекоммуникационных систем.

5. Существует настоятельная потребность в синтезе высокоскоростных ГПВП и ГВС на базе многомерных НДС для генерирования ансамблей сигналов с повышенной информационной емкостью.

Библиографический список

1. Автономова С.А., Багновская Н.М., Веселов С.В., Грицук А.П., Давыдов Ю., Звегинцева И.А., Иванов А.В., Измайлова М.А., Кутыркина Л.В., Коро Н., Кутянская К.И., Киселев В.М., Ладогина А.Ю., Мелехова А.С., Музыкант В.Л., Музыкант П.В., Ромат Е.В., Пирогова Ю.К., Плющева Л.В., Почтарь Э.И. и др. Бренд-коммуникации. М., 2017.
2. Арасланова В.А. Теоретические аспекты исследования документа // Вестник Сургутского государственного педагогического университета. 2010. № 3 (10). С. 44-51.
3. Беловицкий К.Б., Николаев В.Г. Экономическая безопасность. - Москва, 2017.
4. Берсенева Е.А., Седов А.А. Создание автоматизированной системы формирования аналитической отчетности в городской клинической больнице с использованием olap-технологии // Врач и информационные технологии. 2010. № 4. С. 19-25.
5. Бондарев В.А., Волкогон В.А., Нечаев Ю.И. Концептуальный базис контроля морских катастроф в чрезвычайных ситуациях // Актуальные вопросы проектирования, постройки и эксплуатации морских судов и сооружений Труды региональной научно-практической конференции. Научный редактор В.И. Истомин. 2017. С. 28-46.
6. Вакуненков В.А., Жуков Л.В. К вопросу разработки новых конструктивно-технологических решений специальных фортификационных сооружений МО РФ // Строительные и дорожные машины. 2017. № 1. С. 54-56.
7. Валишин Н.Т., Давыдов Н.В. Метод v-функции: некоторые решения прямой задачи динамики в новой постановке // Вестник Казанского государственного технического университета им. А.Н. Туполева. 2008. № 1. С. 37-39.
8. Гейда А.С. Моделирование при исследовании технических систем: использование некоторых расширений теории графов // Труды СПИИРАН. 2011. № 2 (17). С. 234.
9. Гринчар Н. Методические аспекты управления рисками при внедрении

информационньж технологий на предприятии // РИСК: Ресурсы, информация, снабжение, конкуренция. 2012. № 2. С. 247-249.
10. Димов Э.М., Богданова Е.А., Горшкова Ю.С., Ольховая О.Н. Обобщенный алгоритм имитационного моделирования работы передающей части регионального радиотелевизионного центра // Телекоммуникации. 2007. № 6. С. 41-43.
11. Казиахмедов Т.Б.О проблемах интеллектуализации информационных систем // Вестник Нижневартовского государственного университета. 2013. № 1. С. 20-22.
12. Климов А.С., Емельянов Р.Т., Прокопьев А.П., Климов С.С., Авласевич А.И. Система автоматического управления асфальтоукладчика // патент на полезную модель RUS 105307 17.02.2011
13. Колесников А.А., Осипенко Л.П. Исследование методов факторизации // В сборнике: Сборник научных статей студентов Института информационных технологий и безопасности ФГБОУ ВПО «КубГТУ», Институт информационных технологий и безопасности. Краснодар, 2013. С. 78-84.
14. Лысенко И.В. Нечеткая оптимизация: новый подход к постановке и решению задач // Труды СПИИРАН. 2004. Т. 1. № 2. С. 90-118.
15. Маврин С.А., Путилова Е.В. Компьютерное моделирование как инструмент формирования навыков исследовательской деятельности у будущих учителей // Информационные технологии в социальной сфере Материалы IV международной заочной научно-практической конференции. 2016. С. 157-161.
16. Мастеренко Д.А. Повышение точности информационно-измерительных систем автоматизированного производства на основе методов статистической обработки сильно дискретизованных наблюдений // Диссертация на соискание ученой степени доктора технических наук. Москва, 2015.
17. Матющенко И.А. Работа в среде Microsoft Office Excel 2013. Saint-Louis, Missouri, 2016. 62 с.
18. Мещеряков А.В., Новоселов М.А., Скаржинская Е.Н. Активность регуляторных систем в компьютерных играх // Компьютерный спорт (киберспорт): проблемы и перспективы Материалы III Всероссийской научно-практической конференции (в формате интернет-конференции). РГУФКСМиТ. 2014. С. 37-44.
19. Михалёв Ю.А. Роль интернета в политике государств современного мира // Вестник Московского государственного лингвистического университета. Серия: Общественные науки. 2015. № 26 (737). С. 147-154.
20. Молодцов В.В. Расчет и конструирование направляющих и приводов подачи станков с ЧПУ. - Москва, 2006.
21. Нечаев Ю.Б., Борисов Д.Н., Климов А.И., Золотухин А.В. Исследование характеристик плоских антенных решеток вытекающей волны, рассчитанных для режима нормального излучения // Известия высших учебных заведений. Радиоэлектроника. 2013. Т. 56. № 10 (616). С. 3-12.

22. Пичугин В.Н., Федоров Р.В., Немкова М.П., Солдатов А.А. Компьютерная графика // Международный журнал экспериментального образования. 2017. № 2. С. 95-96.
23. Остах С.В. Концепция регионального аппаратно-программного комплекса экологического мониторинга и консалтинга // Интеграл. 2012. № 1. С. 37-39.
24. Пронькин Н.Н. Межвидовой моделирующий комплекс информационных и расчетных задач для сравнения боевых возможностей разнородных группировок войск сторон // Вестник академии военных наук. 2006. № 1 (14). С. 114-120.
25. Репинская Т.В. Исследование и разработка методов и устройств прогнозирования смены тенденции изменения параметров каналов систем радиосвязи: автореф. дисс. …. канд. техн. наук. - Москва, 2005
26. Садыкова О.В., Липчак А.А. Внедрение систем электронного документооборота и управления взаимодействием для повышения эффективности работы компании // В сборнике: Восемнадцатая всероссийская студенческая научно-практическая конференция Нижневартовского государственного университета Статьи докладов. ответственный редактор А.В. Коричко. 2016. С. 472-475.
27. Самарин И.В. О некоторых свойствах планового решения на проведение комплекса приоритетных фундаментальных, поисковых и прикладных исследований в задачах управления в социальных и экономических системах // Инновации и инвестиции. 2014. № 12. С. 173-177.
28. Сиразетдинов Р.Т., Порунов А.А., Тюрина М.М., Садыков А.А. Основные тенденции в разработке и исследовании систем измерения аэрометрических параметров подвижных объектов // В сборнике: XII всероссийское совещание по проблемам управления ВСПУ-2014 Институт проблем управления им. В.А. Трапезникова РАН. 2014. С. 7499-7510.
29. Стадник С.В. Современные решения по управлению рисками в области безопасности полетов // Вестник Московского университета МВД России. 2012. № 9. С. 197-200.
30. Старожилова О.В. Решение задач идентификации неоднородностей на изображениях с использованием нейронной сети // Международный научно-исследовательский журнал. 2015. № 2-1 (33). С. 83-84.
31. Степаненкова Л.Н. Оптимизация организации потоков в биореакторах непрерывного действия: автореф. дисс. … канд. тех. наук. - Москва, 2006.
32. Трубина М.А., Сакович В.М., Абанников В.Н., Григорьева Е.Г., Подгайский Э.В. Перспективы использования веб-технологий для повышения качества образования при подготовке профессиональных кадров в прикладной гидрометеорологии // В сборнике: Информационная среда вуза XXI века Материалы V Международной научно-практической конференции. 2011. С. 191-194.
33. Тураева Т.В. Применение метода анализа иерархий при проведении технико-экономического обоснования разработки радиоэлектронных устройств // T-Comm: Телекоммуникации и транспорт. 2009. № S3. С. 46-

48.
34. Шомахов А.Ю. Метод оптимальной оценки параметров логистической кривой // В сборнике: Статистические методы оценивания и проверки гипотез Межвузовский сборник научных трудов. Пермский государственный университет. Пермь, 1996. С. 105-110.
35. Шорохов Н.С. Эксплуатационные отказы изолирующих стыков // В сборнике: Актуальные проблемы развития железнодорожного транспорта материалы 2-й Международной научно-практической конференции. Самара, 2006. С. 196-197.
36. Юдин С.В., Румянцева И.И., Степанов В.Г., Степанова Т.В., Якушин Д.И. Опыт использования программ maxima и gretl в преподавании математики и эконометрики // Современные наукоемкие технологии. 2016. № 2-3. С. 447-452.
37. Gaĭnutdinov I.S., Nikitin A.S., Ivanov V.A., Borisov A.N., Nesmelov E.A. Cutoff and band-pass interference filters for the uv region // Journal of Optical Technology. 2002. Т. 69. № 12. С. 907-909.
38. Lipovka A.Y., Lipovka Yu.L. Application of "gradient" algorithm to modeling thermal pipeline networks with pumping stations // Журнал Сибирского федерального университета. Серия: Техника и технологии. 2013. Т. 6. № 1. С. 28-35.
39. Lukin V.P., Fortes B.V. Phase-correction of turbulent distortions of an optical wave propagating under conditions of strong intensity fluctuations // Applied Optics. 2002. Т. 41. № 27. С. 5616-5624.
40. Starkov A.N., Povitukhin S.A., Stashchuk P.V., Gallyamova M.S., Ganieva L.F., Romanova M.V., Storozheva E.V. Qualimetric model for comprehensive evaluation of E-business efficiency // Proceedings of the 2016 Conference on Information Technologies in Science, Management, Social Sphere and Medicine (ITSMSSM 2016) Сер. "ACSR: Advances in Computer Science Research" Editors: Olga Berestneva, Alexei Tikhomirov, Andrey Trufanov. 2016. С. 316-321.
41. Starostin V.S., Chernova V.Y. E-commerce development in Russia: trends and prospects // Journal of Internet Banking and Commerce. 2016. Т. 21. № S5. С. 010.
42. Vasileva I.V., Vasileva T.N. The role of brand in franchising system // Modern Science. 2017. № 4-1. С. 156-164.