

С.А.Осмоловский

Стохастическая информатика:

*инновации
в информационных
системах*

Москва
Горячая линия - Телеком
2012

УДК 519.72:621.391
ББК 32.811+22.18
О-74

Осмоловский С. А.

О-74 Стохастическая информатика: инновации в информационных системах. – М.: Горячая линия–Телеком, 2012. – 320 с.: ил.
ISBN 978-5-9912-0151-3.

Рассмотрены инновационные разработки в сфере информационных технологий и связи с использованием новых сигнальных конструкций, алгоритмов обработки информации и протоколов информационных систем (ИС). Разработки основаны на применении кодов восстановления целостности (КВЦ) информации, включающих элементы двоичного помехоустойчивого кодирования и криптографии Шеннона, и обеспечивающих сложность защиты информации от всех видов воздействия на нее в рамках единого алгоритма обработки информации при однократном введении избыточности. Протоколы ИС, использующих КВЦ, могут применять принципы адаптивного и робастного управления передачей в системе. Использование этих разработок расширяет функциональные возможности и улучшает характеристики информационных (информационно-телекоммуникационных) систем. В частности, системы приобретают свойство повышенной устойчивости к преднамеренным деструктивным воздействиям на систему (устойчивость к кибертерроризму).

Для руководителей и экспертов инновационных и венчурных компаний, «бизнес-ангелов»; разработчиков и научных работников, специализирующихся в области информационных технологий и систем, теории информации, помехоустойчивого кодирования, криптографии, информатики, теории управления; будет полезна студентам и аспирантам соответствующих специальностей.

ББК 32.811+22.18

Адрес издательства в Интернет WWW.TECHBOOK.RU

Научное издание

Осмоловский Станислав Антонович

**Стохастическая информатика:
инновации в информационных системах**

Редактор Ю. Н. Чернышов
Компьютерная верстка Ю. Н. Чернышова
Обложка художника В. Г. Ситникова

Подписано в печать 20.05.2012. Формат 60×88/16. Уч. изд. л. 20. Тираж 500 экз. (2-й завод 50 экз.)

ISBN 978-5-9912-0151-3

© С. А. Осмоловский, 2011, 2012
© Издательство НТИ «Горячая линия–Телеком», 2012

Введение и постановка задачи

В монографии рассматриваются вопросы создания и применения новых информационных технологий на основе оригинальных сигнальных конструкций и алгоритмов их обработки, созданных в России. Эти технологии основаны на идеях Клода Шеннона [1, 2] использования случайных сигналов в задачах защиты информации и могут дать в результате своего применения значительный технико-экономический эффект.

Цель монографии — показать на конкретном примере возможность и порядок доведения научной идеи до уровня инновационного проекта, способного принести как научные, так и практические результаты [3].

Ранее был проведен комплекс научно-исследовательских и экспериментальных работ [4], достаточных для перехода к промышленному этапу инновационного проекта.

В 2008 году начался финансовый кризис, быстро превратившийся в мировой экономический кризис, беспрецедентный по числу затронутых спадом производства стран и размеру спада. В период кризиса приходится объединять усилия руководителей всех стран мира и создаются условия для обновления базисных технологий, влияющих на состояние мировой экономики. Для скорейшего и эффективного применения новых информационных технологий требуются разработка, внедрение стандартов и согласованные действия ведущих мировых компаний при обязательной организующей роли России, где созданы эти инновационные технологии.

Для России это становится поводом начать выполнение объявленной программы по приданию экономике России инновационного характера, в том числе в сфере информационных технологий [5].

В современных информационных технологиях и системах просматривается тенденция применения сразу нескольких видов защиты информации, каждый из которых существенно необходим для эффективного выполнения функций информационных систем. Эта тенденция отражена в международных стандартах телекоммуникационных сетей, определяющих комплекс функций защиты информации: защита от ошибок в каналах связи с помощью помехоустойчивых кодов, аутентификация сообщений и контроль целостности информации (защита от навязывания ложной информации), рандомизация сигналов, защита от ознакомления с информацией (криптозащита).

В качестве примеров реализации этой тенденции можно привести стандарт 802.16 (WiMax) для широкополосных беспроводных сетей радиосвязи и европейский стандарт EN 300 744 (Digital Video Broadcasting (DVB); Framing structure, channel coding and modulation for terrestrial television) передачи данных для цифрового наземного телевидения.

Оглавление

Введение и постановка задачи	3
Глава 1. Содержание инновационных разработок	7
1.1. Основные принципы обновления информационных систем ...	7
1.2. Существо и порядок разработки инноваций, положенных в основу проекта	9
1.3. Последовательность и задачи создания новых информационных технологий	11
1.4. Инновационные разработки в России	12
1.5. Инновационный потенциал проекта	14
Глава 2. Защита информации в современных информационных системах	17
2.1. Основные понятия защиты информации	17
2.2. Модель уязвимости информации	18
2.3. Параметры для количественной оценки степени защиты информации	20
2.4. Защита от ошибок в современных телекоммуникационных системах	21
2.5. Защита средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации .	23
2.5.1. Основные принципы защиты от НСД	23
2.5.2. Классификация АС. Особенности различных классов защищенности АС	24
2.6. Криптографическая защита информации	25
2.6.1. Методы и средства криптографического преобразования информации	25
2.6.2. Криптографические методы контроля целостности информации	29
2.7. Традиции и мифы сегодняшнего дня	31
2.8. Постановка задачи на разработку метода универсальной защиты информации	32
Выводы по главе 2	44
Глава 3. Стохастическая информатика как составная часть общей информатики	39
3.1. Роль научного обоснования в инновационном развитии информационных технологий	39
3.2. Содержание общей информатики	40

3.3. Содержание и задачи стохастической информатики	42
3.4. Идеи стохастической информатики и порядок их реализации	43
Выводы по главе 3	44
Глава 4. Ансамбли случайных избыточных сигналов (криптокоды)	46
4.1. Общая идея совместного решения задач Клода Шеннона	46
4.2. Основные свойства случайного кодирования Шеннона	47
4.3. Описание и анализ алгоритмов декодирования случайных кодов	48
4.4. Принципы декодирования переменного случайного кода	51
4.5. Свойства переменных случайных кодов	54
4.6. Принципы построения переменного кода для обнаружения ошибок	58
4.6.1. Построение переменного кода на основе ансамбля ФСК	59
4.6.2. Построение переменного кода на основе ансамбля детерминированных кодов	60
4.7. Построение стохастического (n, k) -кода, обнаруживающего ошибки	61
4.8. Обнаружение ошибок корреляционным кодом	66
4.9. Принцип перехода к ансамблям случайных избыточных сигналов для обобщения и решения задач Шеннона	67
4.10. Стохастическое преобразование как ансамбль шифров	67
Выводы по главе 4	68
Глава 5. Коды восстановления целостности информации	69
5.1. Постановка задачи создания и декодирования кодов восстановления целостности для реальных каналов связи	69
5.2. Принципы исправления ошибок известными кодами	73
5.3. Принципы декодирования кода восстановления целостности информации (нанокода)	75
5.4. Построение и алгоритмы декодирования кодов с исправлением ошибок для реальных каналов связи	78
5.5. Алгоритм исправления стираний	87
5.6. Характеристики кода восстановления целостности (нанокода)	89
5.7. Свойства кодов восстановления целостности (нанокодов)	92
5.8. О необходимости стохастического преобразования для алгоритма единой системы ИТ обеспечения	94
5.9. Анализ вероятности ошибки при декодировании кода восстановления целостности (нанокода)	96
5.9.1. Вероятность ошибки после проверки одного соотношения	96
5.9.2. Верхняя граница для вероятности ошибки локализации	98
5.10. Построение и свойства расширенных стохастических кодов, исправляющих ошибки	99
5.10.1. Декодирование расширенных стохастических кодов	99

5.10.2. Свойства расширенных стохастических кодов	101
5.11. Исследование вероятности ошибки декодирования кода восстановления целостности (n, k, q) -кодов методом моделирования на ЭВМ	105
5.12. Сверточные стохастические коды	115
Выводы по главе 5	121
Глава 6. Сопоставление характеристик кодов	123
6.1. Сравнение КВЦ с алгоритмом СДХК и анализ степени оптимальности алгоритма декодирования нанокодов	124
6.2. Сравнение с турбокодами	126
6.3. Сравнение с кодами Рида–Соломона	131
6.4. Сопоставление кодов на основе двоичных кодов с перемежением	135
Выводы по главе 6	137
Глава 7. Стохастическая теория информации	138
7.1. Основные понятия классической теории информации	38
7.2. Понятие и особенности стохастической теории информации ..	139
7.3. Общие принципы защиты информации с помощью КВЦ	141
7.4. Основные теоремы для методов защиты информации КВЦ ..	143
7.5. Пропускная способность произвольного канала связи	144
7.6. Пути повышения устойчивости и безопасности информационных систем путем использования игровых методов и ансамблей кодов и шифров	145
Выводы по главе 7	147
Глава 8. Стохастическая криптография	148
8.1. Основные требования и определения К. Шеннона	148
8.2. Требования к операциям рандомизации	149
8.3. Создание искусственного q -ичного симметричного канала	151
8.4. Принципы построения алгоритма случайного шифрования ...	152
8.5. Построение метода стохастической защиты информации	154
8.6. Построение операций случайного (стохастического) криптографического преобразования	157
8.7. Построение датчика случайных чисел	160
8.8. Достигнутые характеристики ДСЧ и программы шифрования информации	163
8.9. Стохастическое преобразование q -ичных символов как операция шифрования информации	163
8.10. О криптографической стойкости q -ичных стохастических кодов	166
Выводы по главе 8	168
Глава 9. Алгоритмы каналов передачи данных, использующих стохастические коды с исправлением ошибок	169
9.1. Типы и характеристики алгоритмов каналов ПД	169

9.2. Пути повышения эффективности каналов ПД	170
9.3. Основные алгоритмы работы систем с обратной связью	172
9.4. Особенности q -ичных стохастических кодов, влияющих на построение и алгоритмы работы каналов ПД	174
9.5. Исследование потенциально достижимых характеристик дуплексных и симплексных каналов ПД, использующих (n, k, q) -коды	176
9.5.1. Порядок проведения моделирования и использования его результатов	176
9.5.2. Анализ результатов моделирования	179
9.5.3. Учет влияния сложности декодирования копии на потенциальные характеристики каналов ПД	181
9.6. Основные типы каналов ПД, использующих q -ичные стохастические коды	183
9.7. Опережающая коррекция при стохастическом кодировании ..	185
9.8. Методы сборки и обработки копий не декодированных блоков	187
9.9. Алгоритмы каналов ПД	189
9.10. Правила зачета q -ичных символов в алгоритмах, использующих декодирование копий	192
9.11. Алгоритм канала ПД с квити́рованием q -ичных символов	193
9.12. Вопросы унификации построения каналов ПД	195
9.12.1. Условия унификации каналов ПД	195
9.12.2. Задачи унификации	196
9.12.3. Построение унифицированного канала ПД и алгоритма защиты от ошибок на основе (n, k, q) -кодов	198
Выводы по главе 9	200
Глава 10. Анализ и синтез каналов передачи данных с обратной связью, использующих коды восстановления целостности	201
10.1. Сущность основных задач анализа и синтеза каналов ПД, использующих (n, k, q) -коды восстановления целостности	201
10.2. Порядок учета характеристик потока ошибок дискретного канала связи	202
10.3. Определение вероятности правильного приема кодового блока и сигналов обратной связи	205
10.4. Методы анализа характеристик каналов ПД с неограниченными объемами накопителей передатчика и приемника	206
10.4.1. Синхронный алгоритм адресного подтверждения	207
10.4.2. Асинхронный алгоритм адресного подтверждения	208
10.4.3. Алгоритм передачи нумерованных блоков с блокировкой	208
10.4.4. Алгоритм передачи нумерованных блоков с накоплением правильно принятых блоков в цикле блокировки .	209
10.5. Учет ограничений в объеме накопителей передатчика и приемника	209

10.6. Особенности расчета скорости передачи при использовании режима декодирования копий	212
10.7. Анализ режима опережающей коррекции	213
10.8. Методика и результаты расчета на ЭВМ характеристик каналов ПД, использующих q -ичные стохастические коды	214
10.9. Сопоставление характеристик каналов ПД, использующих стохастические коды с исправлением и обнаружением ошибок ..	215
10.10. Анализ темповых характеристик каналов ПД	221
10.11. Анализ условий целесообразного применения режима исправления ошибок в каналах ПД с обратной связью при ограниченной длине блока	223
10.12. Некоторые вопросы синтеза каналов ПД, использующих стохастические коды	225
Выводы по главе 10	228
Глава 11. Принципы построения и основные свойства информационных систем, использующих стохастические коды с универсальной защитой информации	229
11.1. Свойства стохастического q -ичного кода с исправлением и обнаружением ошибок	229
11.2. Анализ возможности универсальной защиты информации стохастическими кодами	230
11.3. Сферы и задачи применения стохастических средств защиты информации	233
11.4. Состояние разработки стохастических средств защиты информации при передаче и хранении	234
11.5. Построение и свойства средств передачи данных, использующих стохастические коды	235
11.6. Свойства стохастических средств криптографической защиты информации	237
Глава 12. Исследования на ЭВМ свойств метода стохастического шифрования и стохастического датчика	239
12.1. Постановка задачи на проведение исследований	239
12.2. Общие требования к генераторам псевдослучайных последовательностей	240
12.3. Результаты исследования периода стохастического генератора псевдослучайных последовательностей	244
12.4. Сравнение алгоритмов шифрования	246
Выводы по главе 12	248
Глава 13. Асимптотические свойства стохастических методов защиты информации	249
13.1. Стохастический код как ансамбль кодов	249
13.2. О возможности абсолютной секретности в постановке Шеннона	251
13.2.1. Случайность сигнала на выходе шифратора	252

13.2.2. Что такое ключ при абсолютно стойком шифровании...	253
13.2.3. Принципы построения алгоритма случайного шифрования с позиций обеспечения абсолютной стойкости	254
13.2.4. Обсуждение результатов	255
13.3. Достижение ненулевой скорости передачи кодами с обнаружением ошибок при вероятности ошибки, стремящейся к нулю..	255
13.4. Построение адаптивных КПД при гарантированной достоверности в произвольном канале связи	256
Выводы по главе 13	258
Глава 14. Универсальность и комплексность защиты информации кодами восстановления целостности	259
14.1. Организационные и математические аспекты решения задач защиты информации в рамках одного алгоритма при однократном введении избыточности	259
14.2. Вопросы технической реализации протоколов для универсальной защиты	261
14.3. Способы достижения свойств универсальной защиты информации	265
Выводы по главе 14	276
Глава 15. Надежные и конкурентоспособные информационные и ИТ системы на основе нанокодов	277
15.1. Надежные информационные системы	277
15.2. Принципы построения надежных информационных систем ..	278
15.3. Применение нанокодов в сфере информационных технологий и разработки ИТС	279
15.4. Условия и проблемы реализации сигнальных конструкций (помехоустойчивых кодов)	284
15.5. Преимущества, достигаемые применением нанокодов	289
15.6. Средства обеспечения конкурентоспособности продукции и создания единой системы ИТ обеспечения	290
15.7. Основное содержание защищенных объектов интеллектуальной собственности	291
Выводы по главе 15	293
Глава 16. Обсуждение результатов	294
16.1. Задачи модернизации отечественных ИС	294
16.2. Основные особенности и свойства нанокодов	294
16.3. Ожидаемый выигрыш от применения нанокодов	297
16.4. Результаты технической реализации	299
Выводы по главе 16	301
Литература	302
Приложения	309