Учреждение образования
«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ
ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Кафедра информационных систем и технологий

ЗАЩИТА ИНФОРМАЦИИ И НАДЕЖНОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ

**Методические указания и контрольные задания
для студентов специальности 1-40 01 02 (1-40 01 02-03)
«Информационные системы и технологии
(издательско-полиграфический комплекс)»
заочной формы обучения**

Часть 1

Минск 2012

УДК 004.056(075.8)
ББК 32.97я7
З69

Рассмотрены и рекомендованы редакционно-издательским советом университета.

Составители:
П. П. Урбанович, *Д. В. Шиман*

Рецензент
заведующий кафедрой полиграфического оборудования
и систем обработки информации
доцент, кандидат технических наук
М. С. Шмаков

По тематическому плану изданий учебно-методической литературы университета на 2012 год. Поз. 208.

Для студентов специальности 1-40 01 02 (1-40 01 02-03) «Информационные системы и технологии (издательско-полиграфический комплекс)» заочной формы обучения.

© УО «Белорусский государственный
технологический университет», 2012

ПРЕДИСЛОВИЕ

Настоящее пособие предназначено студентам специальности «Информационные системы и технологии» при изучении ими дисциплины «Защита информации и надежность информационных систем» по заочной форме обучения.

В соответствии с учебным планом дисциплины аудиторные занятия проводятся форме лекций – 18 ч (6 ч – в 8-м семестре, 6 ч – в 9-м, 6 ч – в 10-м) и лабораторных занятий – 18 ч (10 ч – в 9-м семестре, 8 ч – в 10-м). Промежуточный контроль знаний студентов осуществляется по результатам выполнения индивидуальных заданий в форме тестов на компьютере (по одному заданию в 9-м и 10-м семестрах).

Изучению дисциплины должно предшествовать усвоение базовых курсов высшей математики, физики, микропроцессорных и вычислительных устройств, базовых языков программирования, основ построения и функционирования реляционных баз данных.

В процессе изучения настоящей дисциплины студент должен освоить основы создания защищенных информационно-вычислительных систем, включающие анализ угроз, перечень атак, методов и средств защиты информации, методологию оценки надежности и информационной безопасности.

В результате изучения дисциплины студент должен знать и уметь реализовать на практике:

1) особенности информационных (информационно-вычислительных) систем ИС (ИВС) как объекта защиты;
2) правовые методы защиты ИС;
3) организационные методы защиты информации в ИС;
4) программно-технические средства преобразования и защиты информации в ИС;
5) методы криптографической защиты информации;
6) методы и средства повышения функциональной надежности программных, аппаратных и аппаратно-программных средств ИС (ИВС).

Весь учебный материал структурирован в виде шести разделов, поделенных на 18 тем (см. ниже раздел 1 данного пособия).

Первое контрольное задание (первый тест) охватывает вопросы, относящиеся к первым трем разделам учебного плана (точнее – к темам 1–7). Настоящее пособие призвано помочь студентам в овладении соответствующими знаниями и в подготовке к первому тесту.

1. СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

Раздел 1. ИНФОРМАЦИОННО-ВЫЧИСЛИТЕЛЬНЫЕ СИСТЕМЫ (ИВС) КАК ОБЪЕКТЫ ЗАЩИТЫ ИНФОРМАЦИИ И ПОВЫШЕНИЯ ФУНКЦИОНАЛЬНОЙ НАДЕЖНОСТИ

Тема 1. Фундаментальные понятия и определения из области информационной безопасности и надежности систем

Безопасность и надежность объекта и системы. Краткая историческая информация и тенденции развития ИВС. Общая характеристика факторов, влияющих на безопасность и надежность ИВС.

Тема 2. Потенциальные угрозы безопасности информации в ИВС. Объекты и методы защиты информации

Естественные и искусственные помехи. Ионизирующие излучения. Особенности их влияния на аппаратные и аппаратно-программные средства ИВС. Хакеры и кракеры. Особенности использования и угрозы со стороны деструктивных программных средств. Компьютерные преступления и ответственность нарушителей. Основные методы повышения безопасности и надежности ИС и ИВС.

Тема 3. Общая характеристика, структура и математическое описание каналов передачи и хранения информации

Описание и характеристика ИВС на структурно-функциональном уровне. Особенности и математическое описание каналов передачи и каналов хранения информации. Двоичные каналы.

Раздел 2. ОСНОВЫ ТЕОРИИ ИНФОРМАЦИИ

Тема 4. Понятие информации. Энтропия источника сообщений

Основы теории информации К. Шеннона. Понятие алфавита источника сообщения. Энтропия Шеннона и Хартли.

Тема 5. Количество информации. Энтропийная оценка потерь при передаче информации

Количество информации в сообщении. Информационная избыточность сообщений. Потери информации в зашумленных каналах. Условная энтропия и ее использование для оценки потерь информации в двоичных каналах передачи.

Раздел 3. БАЗОВЫЕ МЕТОДЫ ПРЕОБРАЗОВАНИЯ ИНФОРМАЦИИ С ЦЕЛЬЮ ПОВЫШЕНИЯ УРОВНЯ ЕЕ КОНФИДЕНЦИАЛЬНОСТИ И НАДЕЖНОСТИ ПЕРЕДАЧИ

Тема 6. Методы структурной, информационной и временной избыточности в ИВС

Характеристика базовых методов преобразования информации. Основные цели применения. Сущность методов структурной, ин-

формационной и временной избыточности в ИВС; комбинирование методов.

Помехоустойчивое кодирование информации. Классификация кодов и их граничные характеристики. Линейные и нелинейные коды. Коды Хемминга. Турбо-коды.

Циклические коды.

Методы кодирования и декодирования сообщений. Синдромное декодирование сообщений. Особенности аппаратной, программной и аппаратно-программной реализации кодеров и декодеров.

Методы и средства перемежения данных. Использование перемежителей/деперемежителей в системах передачи данных.

Тема 7. Сжатие информации как метод повышения ее безопасности и целостности

Классификация и цели использования методов сжатия сообщений. Словарные, вероятностные, арифметические и комбинированные методы сжатия.

Методы Берроуза – Уиллера, Шеннона – Фано, Хаффмана, Лемпеля – Зива. Алгоритмы и математическое описание. Особенности программной реализации методов.

Оценка эффективности методов сжатия (архивации) данных.

Особенности современных компьютерных архиваторов. Их применение для преобразования файлов различных форматов.

Тема 8. Криптографические методы повышения информационной безопасности

Математические основы шифрования данных. Проблема дискретного логарифма. Основы теории больших чисел. Модулярная арифметика в криптопреобразованиях данных.

Характеристика методов. Понятие криптостойкости шифра. Подстановочные и перестановочные шифры. Блочные и потоковые шифры. Симметричные и асимметричные криптосистемы. Алгоритм Диффи – Хеллмана. Стандарт шифрования ГОСТ 28147–89. Американский стандарт шифрования DES и его модификации.

Криптосистема RSA. Криптосистема ЭльГамаля.

Использование нейросетевых технологий в задачах обмена конфиденциальной информацией.

Электронная цифровая подпись (ЭЦП). Понятие хеш-функции и ее использование в ЭЦП. Особенности алгоритмов хеширования классов MD, SHA. Другие методы генерирования ЭЦП. Алгоритмы RSA, ЭльГамаля, DSA. Белорусский стандарт ЭЦП. ЭЦП на основе эллиптических кривых. Верификация подписи.

Криптоанализ. Атаки на шифры и ЭЦП.

Тема 9. Стеганографические методы преобразования информации

Сущность, особенности и классификация методов. Понятие контейнера.

Текстовая стеганография. Основные методы и особенности их программной реализации.

Стеганография на основе графических изображений и аудиоинформации.

Характеристики эффективности стеганографических методов. Особенности стегоанализа.

Раздел 4. ДЕСТРУКТИВНЫЕ КОМПЬЮТЕРНЫЕ ПРОГРАММЫ И ЗАЩИТА ОТ НИХ

Тема 10. Классификация и принципы действия деструктивных программ

Классификация вредоносных программ. Компьютерные вирусы и «троянские кони». Классификация и принципы действия. Методы защиты. Другие типы подобных программ. Спам.

Тема 11. Методы защиты ИВС от вредоносного ПО

Бреши в ПО. Их поиск и устранение. Использование анализаторов протоколов и портов ПК.

Антивирусное ПО. Особенности разработки и применения.

Раздел 5. МЕТОДЫ ИДЕНТИФИКАЦИИ И АВТОРИЗАЦИИ В ИВС

Тема 12. Идентификация и проверка подлинности

Программные и программно-технические методы идентификации и установления полномочий. Особенности биотехнических и антропометрических методов идентификации пользователя.

Парольная защита. Безопасное время и безопасная длина пароля. Формула Андерсена.

Взаимная проверка подлинности субъектов. Протоколы идентификации.

Тема 13. Разграничение доступа пользователей к ресурсам ИВС

Мандатный и избирательный методы разграничения доступа. Контроль доступа на основе ролей. Доступ пользователей к базам данных, особенности. «Красная» и «Оранжевая» книги. Международные стандарты в области безопасности ИС и доступа пользователей к ресурсам.

Тема 14. Защита операционных систем

Основы безопасности при работе с ОС Windows. Модель безопасности ОС Windows. Маркер безопасного доступа. Структура реестра и его роль в реализации политики безопасности.

Система Kerberos. Протокол Нидхема – Шредера. Типы используемых удостоверений.

Методы защиты прав интеллектуальной собственности на ПО. Водяные знаки и отпечатки пальцев в ПО.

Тема 15. Программно-технические методы и средства защиты ЛВС

Защита на основе сетевых протоколов. Протокол SSL. Межсетевые экраны. Источники бесперебойного питания.

Тема 16. Защита веб-ресурсов

Основные виды атак на серверы и веб-ресурсы. Атака SQL-injection на СУБД веб-приложений. XSS-атаки на локальные файлы. Атаки на HTML-ресурсы. Проблемы доверия в HTTP.

Раздел 6. МАТЕМАТИЧЕСКИЕ ОСНОВЫ ОПИСАНИЯ И МОДЕЛИРОВАНИЕ НАДЕЖНОСТИ ИВС

Тема 17. Факторы, влияющие на надежность ИВС

Климатические, вибрационные и иные типы факторов. Влияние ионизирующих излучений на полупроводниковые структуры, последствия.

Отказы и сбои. Распределение во времени. Равномерное и сгруппированное распределение.

Тема 18. Моделирование надежности цифровых устройств ИВС

Использование нормального закона распределения, смешанного пуассоновского и Г-распределения для описания статистических свойств сбоев и отказов в цифровых устройствах. Проверка параметрических гипотез.

Надежность резервируемых ИВС и систем с использованием помехоустойчивого кодирования.

2. УЧЕБНЫЕ МАТЕРИАЛЫ И МЕТОДИЧЕСКИЕ УКАЗАНИЯ К ИХ ОСВОЕНИЮ

Тема 1. Фундаментальные понятия и определения из области информационной безопасности и надежности систем

Основные понятия и определения

Информация – сведения (данные) о внутреннем и окружающем нас мире, событиях, процессах, явлениях и т. д., воспринимаемые и передаваемые людьми или техническими устройствами.

Информационная (*информационно-вычислительная*) *система* – организационно упорядоченная совокупность документов, технических средств и информационных технологий, реализующая информационные (информационно-вычислительные) процессы.

Информационные процессы – процессы сбора, накопления, хранения, обработки (переработки), передачи и использования информации.

Информационные ресурсы – отдельные документы или массивы документов в информационных системах.

Доступ – специальный тип взаимодействия между объектом и субъектом, в результате которого создается поток информации от одного к другому.

Несанкционированный доступ (НСД) – доступ к информации, устройствам ее хранения и обработки, а также к каналам передачи, реализуемый без ведома (санкции) владельца и нарушающий тем самым установленные правила доступа.

Объект – пассивный компонент системы, хранящий, перерабатывающий, передающий или принимающий информацию; примеры объектов: страницы, файлы, папки, директории, компьютерные программы, устройства (мониторы, диски, принтеры и т. д.).

Субъект – активный компонент системы, который может инициировать поток информации; примеры субъектов: пользователь, процесс либо устройство.

Безопасность ИВС – свойство системы, выражающееся в способности системы противодействовать попыткам несанкционированного доступа или нанесения ущерба владельцам и пользователям системы при различных умышленных и неумышленных воздействиях на нее.

Защита информации – организационные, правовые, программно-технические и иные меры по предотвращению угроз информационной безопасности и устранению их последствий.

Атака – попытка несанкционированного преодоления защиты системы.

Информационная безопасность систем – свойство информационной системы или реализуемого в ней процесса, характеризующее способность обеспечить необходимый уровень своей защиты.

Другое определение:

информационная безопасность – все аспекты, связанные с определением, достижением и поддержанием конфиденциальности, целостности, доступности информации или средств ее обработки:

конфиденциальность (confidentiality) – состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на нее право;

целостность (integrity) – избежание несанкционированной модификации информации;

доступность *(availability)* – избежание временного или постоянного сокрытия информации от пользователей, получивших права доступа.

Идентификация – процесс распознавания определенных компонентов системы (объектов или субъектов) с помощью уникальных идентификаторов.

Аутентификация – проверка идентификации пользователя или иного компонента ИС для принятия решения о разрешении доступа к ресурсам системы.

Надежность системы – характеристика способности программного, аппаратного, аппаратно-программного средства выполнить при определенных условиях требуемые функции в течение определенного периода времени.

Достоверность работы системы (устройства) – свойство, характеризующее истинность конечного (выходного) результата работы (выполнения программы), определяемое способностью средств контроля фиксировать правильность или ошибочность работы.

Ошибка устройства – неправильное значение сигнала (бита – в цифровом устройстве) на внешних выходах устройства или отдельного его узла, вызванное технической неисправностью, или воздействующими на него помехами (преднамеренными либо непреднамеренными), или иным способом.

Ошибка программы – проявляется в несоответствующем реальному (требуемому) промежуточному или конечному значению (результату) вследствие неправильно запрограммированного алгоритма или неправильно составленной программы.

Основные определения из предметной области можно найти в п. 1.1, 1.2, 1.5 пособия [1].

Краткая историческая информация

I этап – примерно до 1815/16 года – характеризуется использованием естественно возникавших средств информационных коммуникаций. Основная задача информационной безопасности – защита сведений о событиях, фактах, имуществе и т. д.

II этап – начиная с 1816 года – связан с началом использования технических средств электро- и радиосвязи. Характеризуется применением помехоустойчивого кодирования сообщения (сигнала) с последующим декодированием принятого сообщения (сигнала).

III этап – начиная с 1935 года – связан с появлением радиолокационных и гидроакустических средств. Обеспечение информационной безопасности основывалось на сочетании организационных и технических мер, направленных на повышение защищенности радиолокационных средств от воздействия на их приемные устройства активных и пассивных помех.

IV этап – начиная с 1946 года – связан с изобретением и внедрением в практическую деятельность электронно-вычислительных машин (компьютеров). Эру появления компьютерной техники связывают с разработкой в Пенсильванском университете (США) ЭВМ EN IAC (*Electronic Numerical Integrator And Computer* (*Calculator*)). Задачи информационной безопасности решались в основном методами и способами ограничения физического доступа к оборудованию средств сбора, переработки и передачи информации.

V этап – начиная с 1964/65 годов – обусловлен созданием и развитием локальных информационно-коммуникационных сетей. Задачи безопасности решались в основном методами и способами физической защиты средств, путем администрирования и управления доступом к сетевым ресурсам.

VI этап – начиная с 1973 года – связан с использованием мобильных коммуникационных устройств с широким спектром задач. В этот период созданы известные сейчас во всем мире фирмы Microsoft (Билл Гэйтс и Пол Ален) и Apple (Стив Джобс и Стэфан Возняк).

Образовались сообщества людей – *хакеров*, ставящих своей целью нанесение ущерба информационной безопасности отдельных пользователей, организаций и целых стран. Формируется *информационное право* – новая отрасль международной правовой системы.

VII этап – начиная примерно с 1985 года – связан с созданием и развитием глобальных информационно-коммуникационных сетей с использованием космических средств обеспечения.

Предусматривает комплексное использование мер и средств защиты.

VIII этап – примерно с конца XX – начала XXI в. – связан с повсеместным использованием сверхмобильных коммуникационных устройств с широким спектром задач и глобальным охватом в пространстве и времени, обеспечиваемым космическими информационно-коммуникационными системами. Характеризуется *«широким переходом на цифру»*. Предусматривает комплексное использование мер и средств защиты.

Общая характеристика факторов, влияющих на безопасность и надежность ИВС

Фактор, воздействующий на ИВС, – это явление, действие или процесс, результатом которых может быть утечка, искажение, уничтожение данных, блокировка доступа к ним, повреждение или уничтожение системы защиты.

Все многообразие дестабилизирующих факторов можно разделить на два класса: *внутренние* и *внешние*.

Внутренние дестабилизирующие факторы, влияющие:

1) на программные средства (ПС):
   а) некорректный исходный алгоритм;
   б) неправильно запрограммированный исходный алгоритм (первичные ошибки);
2) аппаратные средства (АС):
   а) системные ошибки при постановке задачи проектирования;
   б) отклонения от технологии изготовления комплектующих изделий и АС в целом;
   в) нарушение режима эксплуатации, вызванное внутренним состоянием АС.

Внешние дестабилизирующие факторы, влияющие:

1) на программные средства:
   а) неквалифицированные пользователи;
   б) несанкционированный доступ к ПС с целью модификации кода;
2) аппаратные средства:
   а) внешние климатические условия;
   б) электромагнитные и ионизирующие помехи;
   в) перебои в электроснабжении;
   г) недостаточная квалификация обслуживающего персонала;
   д) несанкционированный (в том числе – удаленный) доступ с целью нарушения работоспособности АС.

Вопросы для контроля и самоконтроля

1. Дать определение основных понятий и терминов, относящихся к области защиты информации и надежности информационных систем.
2. Чем отличается идентификация от авторизации?
3. Охарактеризовать основные этапы развития информационных технологий с точки зрения их безопасности.
4. Привести классификацию основных факторов, влияющих на ИВС.
5. К каким последствиям приводит влияние дестабилизирующих факторов на ИС или ИВС?
6. Дать характеристику внутренних факторов, дестабилизирующих работу ИС или ИВС.
7. Охарактеризовать внешние факторы, дестабилизирующие работу ИС или ИВС.
8. Как Вы понимаете «некорректный исходный алгоритм»?
9. Что такое «первичная ошибка» в программе?
10. Как влияют климатические условия на надежность аппаратных средств?

Тема 2. Потенциальные угрозы безопасности информации в ИВС. Объекты и методы защиты информации

Естественные и искусственные помехи

Одним из важнейших дестабилизирующих работу ИВС факторов являются *электромагнитные* и *ионизирующие* излучения. Источниками первых являются практически все средства, функционирование которых основано на использовании электроэнергии, и в особенности такие АС, которые целенаправленно излучают электромагнитные волны (к ним относится, например, приемо-передающие и иные подобные радиоэлектронные устройства). По большому счету любой проводник с током является источником электромагнитных помех. Такие источники относятся к классу *искусственных*, или *промышленно-бытовых*. В свою очередь, их можно подразделить на *непреднамеренные* и *преднамеренные*. Последние имеют место в ситуациях, похожих на эпизод в фильме о приключениях Шурика: профессор на экзамене включил генератор помех, который «забил» канал.

Ионизирующие излучения также могут иметь естественную (солнечная радиация) и искусственную (изотопы урана и тория излучают даже пластмассы) природу.

Основным последствием влияния помех на АС являются ошибки в хранящейся, передаваемой или обрабатываемой информации. Другими словами, помехи снижают функциональную надежность АС.

Для лучшего понимания сути и особенностей *угроз со стороны деструктивных программных средств*, а также физических лиц, использующих такие средства для организации НСД (хакеры и кракеры), на рис. 1 приведен пример периметра современной ИС, а на рис. 2 схематически показаны наиболее уязвимые места локальной сети.

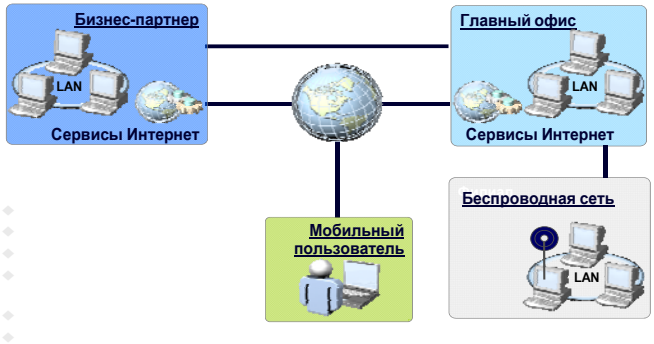

Рис. 1. Пример периметра современной ИС

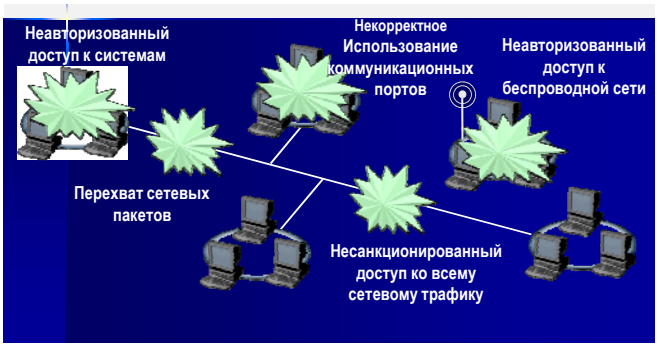

Рис. 2. Наиболее уязвимые места локальной сети

Основные факторы (угрозы):

1) действия злоумышленника;

2) наблюдение за источниками информации;

3) подслушивание конфиденциальных разговоров и акустических сигналов работающих механизмов;

4) перехват электрических, магнитных и электромагнитных полей, электрических сигналов и радиоактивных излучений;

5) несанкционированное распространение материальных носителей за пределами организации;

6) разглашение информации компетентными людьми;

7) утеря носителей информации;

8) несанкционированное распространение информации через поля и электрические сигналы, случайно возникшие в аппаратуре;

9) воздействие стихийных сил (наводнения, пожары и т. п.);

10) сбои и отказы в аппаратуре сбора, обработки и передачи информации;

11) отказы системы электроснабжения;

12) воздействие мощных электромагнитных и электрических помех (промышленных и природных).

Несанкционированный доступ с помощью *деструктивных программных средств* осуществляется, как правило, через компьютерные сети.

Классификацию вредоносного ПО можно представить следующим образом:

вирусы (viruses) – это программы, саморазмножающиеся путем дописывания собственных кодов к исполняемым файлам; вирусы могут содержать, а могут не содержать деструктивные функции;

черви (worms) – это программы, которые самостоятельно размножаются по сети и, в отличие от вирусов, не дописывают себя (как правило) к исполняемым файлам; все черви «съедают» ресурсы компьютера, «нагоняют» интернет-трафик и могут привести к утечке данных с вашего компьютера;

анализаторы клавиатуры, или *кейлоггеры* (keyloggers), – программы, которые регистрируют нажатия клавиш, делают снимки рабочего стола, отслеживают действия пользователя во время работы за компьютером и сохраняют эти данные в скрытый файл на диске, затем этот файл попадает к злоумышленнику;

трояны (trojans), или *«троянские кони»*, – собирают конфиденциальную информацию с компьютера пользователя (пароли, базы данных и пр.) и тайно по сети высылают их злоумышленнику (своему хозяину);

боты (bots) – распространенный в наше время вид зловредного ПО, который устанавливается на компьютерах пользователей (*сети botnet*) и используется для атак на другие компьютеры;

снифферы (sniffers) – это анализаторы сетевого трафика; могут использоваться в составе зловредного ПО, скрытно устанавливаться на компьютере пользователя и отслеживать данные, которые отправляет или получает пользователь по сети;

руткиты (rootkits) – сами по себе не являются зловредным ПО; назначение – скрывать работу других зловредных программ (кейлоггеров, троянов, червей и т. д.) как от пользователя, так и от программ и средств

обеспечения безопасности (антивирусов, файерволов (firewalls), систем обнаружения атак и пр.).

Важно отметить, что вирусы, трояны и иные деструктивные программы активизируются только после загрузки инфицированного файла в оперативную память компьютера (RAM).

Более подробно свойства и особенности деструктивных программ, как и методы борьбы с ними, будут проанализированы во второй части курса.

Основные методы повышения безопасности и надежности ИС и ИВС

В контексте сформулированной цели здесь кратко проанализируем методы и средства повышения информационной безопасности систем. Вопросы надежности будут рассмотрены во второй части (при подготовке ко второму тесту).

Политика информационной безопасности систем, как и во всех подобных случаях, должна строиться на основе *системного подхода*, предусматривающего всесторонний анализ причин и угроз безопасности, оценки их последствий, необходимости, экономической или иной целесообразности и адекватности принимаемых противодействий.

Все многообразие используемых методов и средств защиты можно разделить на три класса:

– законодательная, нормативно-правовая и научная база;

– организационно-технические и режимные меры и методы (политика информационной безопасности);

– аппаратные, программно-аппаратные и программные способы и средства обеспечения ИБ.

К ***первому классу*** относятся следующие:

1) акты национального законодательства:

а) международные договоры Республики Беларуси;

б) Конституция Республики Беларусь;

в) законы Республики Беларусь, например, *Закон Республики Беларусь от 10 ноября 2008 г. № 455-З* «Об информации, информатизации и защите информации»;

г) указы Президента Республики Беларусь, например, *Указ № 515 Президента Республики Беларусь от 30 сентября 2010 г.* «О некоторых мерах по развитию сети передачи данных в Республике Беларусь», *Указ № 60 Президента Республики Беларусь от 1 февраля 2010 г.* «О мерах по совершенствованию использования национального сегмента сети Интернет»;

д) постановления Правительства Республики Беларусь, например, *постановление Совета Министров Республики Беларусь от 11 февраля 2006 г. № 192* «Об утверждении Положения о сопровождении интернет-сайтов республиканских органов государственного управления, иных государственных организаций, подчиненных Правительству Республики Беларусь»; *постановление Совета Министров Республики Беларусь от 11 августа 2011 г. № 1084* «О внесении изменений и дополнений в Постановление Совета Министров Республики Беларусь от 29 апреля 2010 г. № 644»; *постановление Совета Министров Республики Беларусь от 26 мая 2009 г. № 675* «О некоторых вопросах защиты информации»; *постановление Совета Министров Республики Беларусь от 26 мая 2009 г. № 673* «О некоторых мерах по реализации Закона Республики Беларусь “Об информации, информатизации и защите информации” и о признании утратившими силу некоторых постановлений Совета Министров Республики Беларусь»;

е) нормативные правовые акты министерств и ведомств, например, постановление № 4/11 Оперативно-аналитического центра при Президенте Республики Беларусь и Министерства связи и информатизации Республики Беларусь от 29 июня 2010 г. «Об утверждении положения о порядке ограничения доступа пользователей интернет-услуг к информации, запрещенной к распространению в соответствии с законодательными актами», Приказ № 60 Оперативно-аналитического центра при Президенте Республики Беларусь от 2 августа 2010 г. «Об утверждении положения о порядке определения поставщиков интернет-услуг, уполномоченных оказывать интернет-услуги государственным органам и организациям, использующим в своей деятельности сведения, составляющие государственные секреты»;

ж) нормативные правовые акты субъектов, органов местного самоуправления и т. д.;

2) международные стандарты, например:

а) BS 7799-1:2005 – Британский стандарт BS 7799 Part 1 – *Code of Practice for Information Security Management* (Практические правила управления информационной безопасностью) описывает 127 механизмов контроля, необходимых для построения системы управления информационной безопасностью организации, определенных на основе лучших примеров мирового опыта в данной области. Этот документ служит практическим руководством по созданию СУИБ;

б) BS 7799-2:2005 – Британский стандарт BS 7799 Part 2 – *Information Security management* – specification for information security management systems (Спецификация системы управления информационной безопасностью) определяет спецификацию СУИБ. Вторая часть

стандарта используется в качестве критериев при проведении официальной процедуры сертификации СУИБ организации;

в) ISO/IEC 17799:2005 – «Информационные технологии – Технологии безопасности – Практические правила менеджмента информационной безопасности». Международный стандарт, базирующийся на BS 7799-1:2005;

г) ISO/IEC 27001:2005 – «Информационные технологии – Методы обеспечения безопасности – Системы управления информационной безопасностью – Требования». Международный стандарт, базирующийся на BS 7799-2:2005;

д) ISO/IEC 27002 – Сейчас: ISO/IEC 17799:2005. «Информационные технологии – Технологии безопасности – Практические правила менеджмента информационной безопасности». Дата выхода – 2007 год.

е) ISO/IEC 27005 – Сейчас: BS 7799-3:2006 – Руководство по менеджменту рисков ИБ.

Организационно-технические и режимные меры и методы

Для построения Политики ИБ рассматривают следующие направления защиты ИС:

– защита объектов ИС;
– защита процессов, процедур и программ обработки информации;
– защита каналов связи;
– подавление побочных электромагнитных излучений;
– управление системой защиты.

Организационная защита обеспечивает:

– организацию охраны, режима, работу с кадрами, с документами;
– использование технических средств безопасности (например, простейших дверных замков, магнитных или иных карт и др.), информационно-аналитическую деятельность по выявлению внутренних и внешних угроз.

Аппаратные, *программно-аппаратные и программные способы и средства обеспечения ИБ* условно можно классифицировать следующим образом:

1) средства защиты от несанкционированного доступа:
   а) средства авторизации;
   б) аудит;
2) системы мониторинга сетей:
   а) системы мониторинга сетей;
   б) анализаторы протоколов;
3) антивирусные средства:

а) антивирусные программы;
б) программные и иные антиспамовые средства;
в) межсетевые экраны;

4) криптографические средства:
а) шифрование данных;
б) электронная цифровая подпись;

5) системы бесперебойного питания;

6) системы аутентификации:
а) пароль;
б) ключ доступа (физический или электронный);
в) биометрия (анализаторы отпечатков пальцев, анализаторы сетчатки глаза, анализаторы голоса, анализаторы геометрии ладони и др.).

Вопросы систематизации методологии информационной безопасности достаточно подробно описаны в литературе [2].

Вопросы для контроля и самоконтроля

1. К чему приводят электромагнитные или ионизирующие излучения?
2. Привести пример источников электромагнитных или ионизирующих излучений.
3. Что такое «преднамеренная помеха», «непреднамеренная помеха»?
4. Из каких основных частей состоит периметр современной ИС?
5. Как можно осуществить неавторизованный доступ к сетевому трафику?
6. К каким последствиям могут привести отказы системы электроснабжения ИС?
7. Что такое «компьютерный вирус»? Чем он отличается от остальных деструктивных программ? Привести примеры известных вирусов.
8. Охарактеризовать известные Вам деструктивные программные средства.
9. В чем сущность системного подхода при проектировании политики безопасности?
10. Дать классификацию методов и средств защиты информации.
11. Перечислить основные направления реализации Политики информационной безопасности.
12. В чем назначение организационных методов защиты информации?
13. В чем назначение правовых методов защиты информации?
14. В чем назначение режимных методов защиты информации?

15. Какие национальные правовые акты, регламентирующие доступ к информационным ресурсам, Вы знаете?

16. Какие международные правовые акты, регламентирующие доступ к информационным ресурсам, Вы знаете?

17. В чем заключается назначение организационно-технических методов защиты информации?

18. Как можно защитить каналы связи?

19. Как можно защититься от мешающих электромагнитных излучений?

20. Перечислить известные методы и средства авторизации.

21. Назначение межсетевых экранов.

22. Назначение источников бесперебойного питания.

23. На чем основаны биометрические средства идентификации?

Тема 3. Общая характеристика, структура и математическое описание каналов передачи и хранения информации

В наиболее общем виде структуру ИС можно представить в виде трех соединенных блоков (модулей), как это показано на рис. 1.

Учитывая ограниченный объем настоящего пособия, авторы отсылают читателя для знакомства с более подробной информацией, касающейся данной темы, к пособию [1, п. 2.1 и 2.2].

Вопросы для контроля и самоконтроля

1. В каком наиболее общем виде можно представить структуру ИС?
2. Что такое «источник сообщения»? Привести примеры.
3. Что такое «получатель сообщения»? Привести примеры.
4. Что такое «канал передачи данных»? Привести примеры.
5. Привести примеры ИС, ИВС.
6. Что такое «двоичный симметричный канал»?
7. Почему «двоичный симметричный канал» относится к двоичным?
8. Почему «двоичный симметричный канал» относится к симметричным?

Тема 4. Понятие информации. Энтропия источника сообщений

Основы теории информации К. Шеннона.
Понятие алфавита источника сообщения.
Энтропия Шеннона и Хартли

Основную информацию по этой теме можно почерпнуть из [1, п. 2.1 и 2.2].

Вопросы для контроля и самоконтроля

1. Что такое «алфавит источника сообщения»?
2. Что такое «мощность алфавита источника сообщения»?
3. Какова мощность алфавита белорусского языка?
4. Какова мощность алфавита русского языка?
5. Какова мощность алфавита «компьютерного» языка?
6. Что такое «энтропия алфавита»?
7. От чего зависит энтропия алфавита?
8. Записать формулу для вычисления энтропии.
9. Что нужно знать для вычисления энтропии алфавита?
10. Вычислить энтропию белорусского (русского) языка.
11. Вычислить энтропию Шеннона бинарного алфавита, если вероятность появления в произвольном документе на основе этого алфавита одного из символов составляет 0.25, другого – 0.75; либо 0 и 1.0; либо 0.5 и 0.5.
12. Чем отличается энтропия Шеннона от энтропии Хартли?
13. Чему равна энтропия алфавита по Хартли, если мощность этого алфавита равна: а) 1 символ, б) 2 символа, в) 8 символов?

Тема 5. Количество информации. Энтропийная оценка потерь при передаче информации

Количество информации в сообщении.
Информационная избыточность сообщений

Выделенные полужирным прописным шрифтом вопросы также рассмотрены в необходимом объеме в п. 2.1 и 2.2 [1].

Потери информации в зашумленных каналах.
Условная энтропия и ее использование для оценки потерь информации в двоичных каналах передачи

Пусть в ИС сообщение $X_k = x_1, x_2, \ldots x_i, \ldots x_k$ на входе канала формируется на основе алфавита $A = \{a_i\}$, $i = 1 \ldots N$, где N – мощность алфавита.

Сообщение на выходе канала ($Y_k = y_1, y_2, \ldots y_j, \ldots y_k$) формируется на основе того же алфавита.

Если при передаче сообщений в двоичном канале с одинаковой вероятностью p появляются ошибки типа 0→1 (передан ноль, получена 1) либо 1→0, то такой *канал* называют *двоичным симметричным* (ДСК).

Здесь нужно вспомнить теорию вероятностей: *запись* $P(A \mid B)$ – *вероятность гипотезы A при наступлении события B* (*апостериорная вероятность*). В первом из вышеуказанных случаев появления ошибки

можем формально записать $p = P(x_i = 0 \mid y_j = 1)$ или более кратко $p = P(0 \mid 1)$; во втором случае – $p = P(x_i = 1 \mid y_j = 0)$ или более кратко $p = P(1 \mid 0)$. Обозначим символом q вероятность правильной передачи двоичного символа: $q = P(0 \mid 0) = P(1 \mid 1)$. Понятно, что $p + q = 1$.

Стоит задача: определить количественно потери информации, вызванные несовершенством ИС (канала), т. е. при $p > 0$. Задача относится к области *проверки гипотез и принятия статистических решений*. Математической основой ее решения является *теорема Байеса*: совместная вероятность случайных событий A и B:

$$P(A, B) = P(A \mid B) \cdot P(B) = P(B \mid A) \cdot P(A) \qquad (1)$$

или

$$P(A \mid B) = P(B \mid A) \cdot P(A) / P(B). \qquad (2)$$

В соответствии с (2) для ДСК можно записать (используя дискретную форму теоремы Байеса)

$$P(x_i \mid y_j) = P(y_j \mid x_i) \cdot P(x_i) / P(y_j), \qquad (3)$$

где

$$P(y_j) = \sum P(y_j \mid x_i) \cdot P(x_i). \qquad (4)$$

В общем случае i и j могут принимать различные значения в пределах от 1 до N. В соответствии с (3) и (4) для ДСК можем записать

$$P(x_i = 0 \mid y_j = 0) = [P(y_j = 0 \mid x_i = 0) \cdot P(x_i = 0)] / [P(y_j = 0 \mid x_i = 0) \times \times P(x_i = 0) + P(y_j = 0 \mid x_i = 1)\, P(x_i = 1)\,];$$

$$P(x_i = 1 \mid y_j = 0) = [P(y_j = 0 \mid x_i = 1) \cdot P(x_i = 1)] / [P(y_j = 0 \mid x_i = 0) \times \times P(x_i = 0) + P(y_j = 1 \mid x_i = 1) \cdot P(x_i = 1)\,];$$

$$P(x_i = 0 \mid y_j = 1) = [P(y_j = 1 \mid x_i = 0) \cdot P(x_i = 0)] / [P(y_j = 1 \mid x_i = 0) \times \times P(x_i = 0) + P(y_j = 1 \mid x_i = 1) \cdot P(x_i = 1)\,];$$

$$P(x_i = 1 \mid y_j = 1) = [P(y_j = 1 \mid x_i = 1) \cdot P(x_i = 1)] / [P(y_j = 1 \mid x_i = 0) \times \times P(x_i = 0) + P(y_j = 1 \mid x_i = 1) \cdot P(x_i = 1)\,].$$

Если $p > 0$, то это можно трактовать как *неоднозначность* (по Шеннону – equivocation) между переданным и принятым сообщениями. Эта неоднозначность определяется как *условная энтропия* сообщения X_k, обусловленная полученным сообщением Y_k:

$$H(x_i \mid y_j) = -\sum_{ij} P(x_i \mid y_j) \cdot \log P(x_i \mid y_j) = -\sum_{j} P(y_j) \cdot \sum_{i} P(x_i \mid y_j) \cdot \log P(x_i \mid y_j). \qquad (5)$$

В (5) и везде ниже логарифмирование ведется по основанию 2.

В соответствии с (5) можно определить, какому количеству информации соответствует один из символов сообщения X_k, если на выходе канала получен 0:

$$H(x_i \mid y_j = 0) = -P(x_i = 0 \mid y_j = 0) \cdot \log P(x_i = 0 \mid y_j = 0) - P(x_i = 1 \mid y_j = 0) \cdot \log P(x_i = 1 \mid y_j = 0) = -q \cdot \log q - p \cdot \log p.$$

То же, если на выходе получена 1:

$$H(x_i \mid y_j = 1) = -P(x_i = 0 \mid y_j = 1) \cdot \log P(x_i = 0 \mid y_j = 1) - P(x_i = 1 \mid y_j = 1) \cdot \log P(x_i = 1 \mid y_j = 1) = -p \cdot \log p - q \cdot \log q.$$

Определение. Условной энтропией источника дискретного сообщения X называем величину

$$H(x_i \mid y_j) = P(y_j = 0) \cdot H(x_i \mid y_j = 0) + P(y_j = 1) \cdot H(x_i \mid y_j = 1) = -p \log p - q \log q. \quad (6)$$

$H(x_i \mid y_j)$ означает среднее количество информации для входного символа относительно полученного сообщения Y, или *потерю информации на каждый символ переданного сообщения*.

Пример. Пусть известно, что $P(x = 0) = P(x = 1) = 0.5$ и $p = 0.01$. Нужно определить потерю информации на каждый символ переданного сообщения.

Из (6) определим

$$H(x \mid y) = -p \cdot \log p - q \cdot \log q = 0.01 \cdot \log 0.01 - 0.99 \cdot \log 0.99 = 0.081 \text{ бит}.$$

Это означает, что при указанных параметрах канала и источника сообщения при передаче каждого двоичного символа будет потеряно 0.081 бит информации.

Помним, что основанием логарифма является число 2.

К. Шеннон показал, что *эффективная информация* на выходе канала относительно входной в расчете на 1 символ (эффективная энтропия алфавита) составляет

$$H_e = H(X) - H(X \mid Y). \quad (7)$$

Для случая из примера $H_e = 0.919$ бит.

Если вероятность ошибки $p = 0$, то $H(X \mid Y) = 0$ и потерь информации при передаче нет.

Вопросы для контроля и самоконтроля

1. Что такое «количество информации»? В каких единицах оно выражается?

2. Записать формулу для подсчета количества информации.

3. Вычислить количество информации в сообщении, состоящем из ваших фамилии и имени.

4. Какое количество информации содержится в сообщении «information», если принять, что энтропия алфавита составляет 4.7 бит?

5. В чем сущность «информационной избыточности» сообщений?

6. Чем вызваны потери информации в каналах передачи?

7. Что характеризует «условная энтропия»?

8. Записать формулу для вычисления условной энтропии сообщения X_k, обусловленной полученным сообщением Y_k.

9. Известно, что $P(x = 0) = 0.2$, $P(x = 1) = 0.8$ и вероятность ошибки при передаче p составляет 0.01. Определить потерю информации на каждый символ переданного сообщения.

10. Известно, что $P(x = 0) = 0.2$, $P(x = 1) = 0.8$ и вероятность безошибочной передачи q составляет 0.01. Определить потерю информации на каждый символ переданного сообщения.

11. Для предыдущего условия определить количественно потерю информации в двоичном сообщении из 100 символов.

12. Какое количество информации будет передано по каналу связи за 1 час при скорости передачи 1 Мбит/с, если вероятность ошибки равна 0.5?

13. Что такое «эффективная информация», «эффективная энтропия»?

14. Определить эффективную энтропию алфавита для задач 9 и 10.

Тема 6. Методы структурной, информационной и временной избыточности в ИВС

Большинство вопросов, относящихся к этой теме (см. выше раздел 3 учебного материала), достаточно подробно рассмотрены в разделе 4 пособия [1].

Для лучшего понимания материала приведем общую классификацию кодов.

Блочные коды – каждое сообщение из k (X_k) символов (бит) сопоставляется с блоком нового сообщения (кодового слова) из n символов (кодовый вектор X_n длиной $n = k + r$), где k и r – длины информационного и проверочного слов соответственно.

Непрерывные (*рекуррентные, цепные, сверточные*) *коды* – непрерывная последовательность символов, не разделяемая на блоки. Передаваемая последовательность образуется путем *размещения в определенном порядке проверочных символов между информационными символами исходной последовательности*.

Систематические коды характеризуются тем, что сумма по модулю 2 *двух разрешенных кодовых комбинаций* снова дает разрешенную кодовую комбинацию.

Несистематические коды не обладают отмеченными выше свойствами (к ним относятся *итеративные* коды).

Линейные коды – проверочные (избыточные) символы вычисляются как *линейная комбинация информационных*; для кодов принимается обозначение [*n*, *k*] – *код*.

Циклические коды относятся к линейным систематическим.

Нелинейные коды являются противоположностью линейным.

Далее будет изложен материал, который необходимо усвоить и который отсутствует в упомянутом пособии [1].

Циклические коды (ЦК). Основные свойства:

– относятся к классу линейных, систематических;

– сумма по модулю 2 двух разрешенных кодовых комбинаций дает также разрешенную кодовую комбинацию;

– каждый вектор (кодовое слово), получаемый из исходного кодового вектора путем циклической перестановки его символов, также является разрешенным кодовым вектором;

– при циклической перестановке символы кодового слова перемещаются слева направо на одну позицию.

Пример 1. Если кодовое слово имеет следующий вид: 1101100, то разрешенной кодовой комбинацией будет и такая: 0110110.

Принято описывать ЦК при помощи порождающих полиномов $G(X)$ степени $r = n - k$, где r – число проверочных символов в кодовом слове.

Пример 2. Переведем кодовое слово X_n = 101100 в полиномиальный вид:

$$Bi(X) = 1 \cdot X^5 + 0 \cdot X^4 + 1 \cdot X^3 + 1 \cdot X^2 + 0 \cdot X^1 + 0 \cdot X^0 = X^5 + X^3 + X^2.$$

Операции кодирования и декодирования ЦК сводятся к известным процедурам умножения и деления полиномов. Действия с кодовыми словами в виде полиномов производятся по правилам арифметики по модулю 2 (вычитание равносильно сложению).

Из равенства $X^n - 1 = 0$ получаем $X^n = 1$. Прибавив к левой и правой частям по единице, имеем $X^n + 1 = 1 + 1 = 0$. Таким образом, вместо двучлена $X^n - 1$ можно ввести бином $X^n + 1$ или $1 + X^n$, из чего следует, что $X^n + X^n = X^n (1 + 1) = 0$.

Приведем далее порядок суммирования (вычитания), умножения и деления полиномов (по модулю 2). В примерах используем выше-

приведенные кодовые комбинации: $A_1(X) = X^5 + X^3 + X^2$ (101100) и $A_2(X) = X^4 + X^2 + X$ (10110).

Суммирование (вычитание):

$$A_1(X) + A_2(X) = A_1(X) - A_2(X) = X^5 + X^4 + X^3 + \underline{X}^2 + \underline{X}^2 + X = \\ = X^5 + X^4 + X^3 + X$$

$$\begin{array}{rl} & 101100 \\ \text{или} \quad \oplus & \underline{\ 10110} \\ & 111010 \end{array} = X^5 + X^4 + X^3 + X.$$

Помним, что $X^2 + X^2 = 0$.

Умножение:

$$A_1(X) \cdot A_2(X) = (X^5 + X^3 + X^2) \cdot (X^4 + X^2 + X) = \\ = X^9 + \underline{X}^7 + X^6 + \underline{X}^7 + X^5 + + \underline{\underline{X}}^4 + X^6 + \underline{\underline{X}}^4 + X^3 = \\ = X^9 + X^5 + X^3 = 1000101000.$$

Деление:

$$\begin{array}{l} X^5 + X^3 + X^2 \ \ | \underline{X^4 + X^2 + X} \\ \underline{X^5 + X^3 + X^2} \ \ | \ X \\ \ \ 0 \quad 0 \quad 0, \end{array}$$

остаток при делении – 000 или просто 0 ($R(X) = 0$).

Следует запомнить: *при циклическом сдвиге вправо на один разряд необходимо исходную кодовую комбинацию поделить на X, а умножение на X эквивалентно сдвигу влево на один символ.*

Порождающие полиномы циклических кодов. Формирование разрешенных кодовых комбинаций ЦК $B_j(X)$ основано на предварительном выборе порождающего (образующего) полинома $G(X)$, который обладает важным отличительным признаком: все комбинации $B_j(X)$ делятся на порождающий полином $G(X)$ без остатка:

$$B_j(X) / G(X) = A_j(X), \qquad (8)$$

где $B_j(X) = X_n$ – кодовое слово; $A_j(X) = X_k$ – информационное слово.

Степень порождающего полинома определяет число проверочных символов: $r = n - k$. Из этого свойства следует простой способ формирования разрешенных кодовых слов ЦК – умножение информационного слова на порождающий полином $G(X)$:

$$B(X) = A(X) \cdot G(X). \qquad (9)$$

Порождающими могут быть только такие полиномы, которые являются делителями двучлена (бинома) $X^n + 1$:

$$(X^n+1) / G(X) = H(X) \qquad (10)$$

при нулевом остатке $R(X) = 0$.

С увеличением максимальной степени порождающих полиномов r резко увеличивается их количество: при $r = 3$ имеется всего два полинома, а при $r = 10$ их уже несколько десятков. В табл. 1 приведены некоторые.

Таблица 1

Некоторые из известных кодов, описываемые с помощью полиномов

Степень полинома r	Полином $G(X)$	Двоичное представление полинома	n	k	Примечание
1	$X+1$	11	3	2	Код с проверкой на четность
2	X^2+X+1	111	3	1	Код с повторением
3	X^3+X^2+1	1101	7	4	Классический код Хемминга (7, 4)
	X^3+X+1	1011			
4	X^4+X^3+1	11001	15	11	Классический код Хемминга (15, 11)
	X^4+X+1	10011	15	11	Классический код Хемминга (15, 11)
	X^4+X^2+X+1	10111	7	3	Коды Файра – Абрамсона
	$X^4+X^3+X^2+1$	11101	7	3	Коды Файра – Абрамсона
5	X^5+X^2+1	100101	31	26	Классический код Хемминга (31, 26)
	X^5+X^3+1	101001			

Два варианта порождающих полиномов кода Хемминга (7, 4) с записью по модулю 2 в виде 1101 и 1011 представляют собой так называемые *двойственные многочлены* (полиномы): весовые коэффициенты одного полинома, зачитываемые слева направо, становятся весовыми коэффициентами двойственного полинома при считывании их справа налево.

Порождающие полиномы кода Хемминга (7, 4) являются не только двойственными, но и *неприводимыми*.

Неприводимые полиномы не делятся ни на какой другой полином степени меньше r, поэтому их называют еще *неразложимыми*, *простыми* и *примитивными*. Например, порождающий полином $G(X) = X^7 + 1$ раскладывается на три неприводимых полинома:

$$X^7 + 1 = (X + 1) \cdot (X^3 + X^2 + 1) \cdot (X^3 + X + 1) = G_1(X) \cdot G_2(X) \cdot G_3(X),$$

каждый из которых является порождающим для следующих кодов:
$G_1(X) = X + 1$ – код с проверкой на четность, КПЧ (7, 6);
$G_2(X) = X^3 + X^2 + 1$ – первый вариант кода Хемминга (7, 4);
$G_3(X) = X^3 + X + 1$ – двойственный $G_2(X)$, второй вариант кода Хемминга.

Различные вариации произведений $G_{1,2,3}(X)$ дают возможность получить остальные порождающие полиномы:

код Абрамсона (7, 3): $G_4(X) = G_1(X) \cdot G_2(X) = (X + 1) \cdot (X^3 + X^2 + 1) = X^4 + X^2 + X + 1,$

двойственный $G_4(X)$: $G_5(X) = G_1(X) \cdot G_3(X) = (X + 1) \cdot (X^3 + X + 1) = X^4 + X^3 + X^2 + 1,$

код с повторением (7, 1): $G_6(X) = G_2(X) \cdot G_3(X) = (X^3 + X^2 + 1) \cdot (X^3 + X + 1) = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1.$

Порождающая матрица G циклического кода имеет в качестве строк векторы $G(x)$, $xG(x)$, ..., $x^{k-1}G(x)$:

$$G = \begin{matrix} G(x) \\ xG(x) \\ \dots \\ x^{k-1}G(x) \end{matrix} = \begin{matrix} g_0\ g_1\ g_2 \dots g_r\ 0 \dots 0 \\ 0\ g_0\ g_1\ g_2 \dots g_r\ 0 \dots 0 \\ \dots \\ 0 \dots 0\ g_0\ g_1\ g_2 \dots g_r \end{matrix},$$

где g_0, ..., g_r – коэффициенты генераторного полинома.

Проверочная матрица H кода строится на основе полинома (см. (10)):

$$H(X) = (X^n + 1) / G(X) \qquad (11)$$

или

$$H = \begin{matrix} H(x) \\ xH(x) \\ \dots \\ x^{r-1}H(x) \end{matrix} = \begin{matrix} 0 \dots 0\ h_k \dots h_2\ h_1\ h_0 \\ 0 \dots h_k\ h_{k-1} \dots h_1\ h_0\ 0 \\ \dots \\ h_k \dots h_1\ h_0\ 0 \dots 0 \end{matrix},$$

где h_j – коэффициенты полинома $H(X)$.

Справедливо

$$G \cdot H^T = 0, \quad \text{или} \quad H \cdot G^T = 0, \qquad (12)$$

здесь индекс «Т» означает транспонирование матрицы.

Пример 3. Задан ЦК (7, 4) дуальными порождающими полиномами $G(7, 4) = X^3 + X + 1$ и $\underline{G}\ (7, 4) = X^3 + X^2 + 1$. Составить порождающие матрицы кодов.

Первой строкой в матрице записывается порождающий полином (в двоичном представлении) с умножением его на оператор сдвига X_r

для резервирования места под запись трех ($r = 3$) проверочных символов. Следующие $k - 1$ строк матриц получаются путем последовательного циклического сдвига базового кодового слова матриц G и $\underline{G}$ на одну позицию вправо:

$$G(7, 4) = \begin{matrix} 1011000 \\ 0101100, \\ 0010110 \\ 0001011 \end{matrix} \qquad \underline{G}(7, 4) = \begin{matrix} 1101000 \\ 0110100. \\ 0011010 \\ 0001101 \end{matrix}$$

Для построения порождающей матрицы, формирующей разделимый блочный код, необходимо матрицу привести к *каноническому* виду путем линейных операций над строками.

Каноническая матрица должна в левой части порождающей ЦК матрицы содержать единичную диагональную квадратную подматрицу порядка k для получения в итоге блочного ЦК.

Пример 4. Привести к каноническому виду матрицы из примера 3.

С этой целью для получения первой строки канонической матрицы Gк(7, 4) необходимо сложить по *модулю* 2 строки с номерами 1, 3 и 4 матрицы $G(7, 4)$, а для матрицы $\underline{G}$к (7, 4) – строки с номерами 1, 2 и 3 матрицы $\underline{G}(7, 4)$, оставшиеся строки – без изменений. В итоге имеем следующий вид первой из *дуальных канонических матриц*:

$$G\text{к}(7, 4) = \begin{matrix} 1000 & 101 & (1 + 3 + 4) \\ 0100 & 111 & (2 + 4). \\ 0010 & 110 & (3 = 3) \\ 0001 & 011 & (4 = 4) \end{matrix}$$

Запись (1 + 3 + 4) означает, что данная строка матрицы получена в результате суммы по модулю 2 первой, третьей и четвертой строк матрицы $G(7, 4)$.

Вторую матрицу постройте самостоятельно.

Проверочная матрица $H_{7,4}$ размерностью $n \times r$ может быть получена из порождающей матрицы канонического вида путем дополнения проверочной подматрицы единичной матрицей размерности $r \times r$:

$$H_{7,4} = \begin{matrix} 101 \\ 111 \\ 110 \\ \underline{011} \\ 100 \\ 010 \\ 001 \end{matrix}$$

или в каноническом виде

$$H_{7,4} = \begin{matrix} 1110 & 100 \\ 0111 & 010. \\ 1101 & 001 \end{matrix}$$

Вычисление проверочных символов X_r кодового слова X_n чаще всего основывается на методе деления полиномов. Метод позволяет представить разрешенные к передаче кодовые комбинации в виде разделенных информационных X_k и проверочных X_r символов, т. е. получить *блочный код*.

Поскольку число проверочных символов равно r, то для компактной их записи в последние младшие разряды кодового слова надо предварительно к X_k (соответствует $A_j(X)$ в формуле (8)) справа приписать r «нулей», что эквивалентно умножению X_k на оператор сдвига X_r. При этом имеется возможность представить кодовую комбинацию в виде последовательности информационных и проверочных символов:

$$X_n = X_k \cdot X_r \,||\, R(X), \qquad (13)$$

где $R(X)$ – остаток от деления $X_k \cdot X_r / G(X)$ (см. (9)).

В алгоритме на основе (13) можно выделить три этапа формирования разрешенных кодовых комбинаций в кодере:

1) к комбинации слова X_k дописывается справа r нулей, что эквивалентно умножению X_k на X_r;

2) произведение $X_k \cdot X_r$ делится на соответствующий порождающий полином $G(X)$ и определяется остаток $R(X)$, степень которого не превышает $r - 1$, этот остаток и дает группу проверочных символов (X_r);

3) вычисленный остаток присоединяется справа к X_k.

Пример 5. Рассмотрим процедуру кодирования для $X_k = 1001$, т. е. сформируем кодовое слово циклического кода (7, 4).

В заданном ЦК $n = 7$, $k = 4$, $r = 3$ выберем порождающий полином $G(X) = X^3 + X + 1$ (код Хемминга).

$X_k = 1001 \sim X^3 + 1$, (знак « ~ » – *тильда*, означает соответствие).

1. $X_k \cdot X_r = (X^3 + 1) \cdot X^3 = X^6 + X^3 \sim 1001000$, ($n = 7$).

2. $X_k \cdot X_r / G(X) = X^6 + X^3 \;\big|\; X^3 + X + 1$

$$\underline{X^6 + X^4 + X^3} \;\big|\; X^3 + X$$

$$X^4$$

$$\underline{X^4 + X^2 + X}$$

$$X^2 + X,$$

$X^2 + X$ – остаток; $R(X) = X^2 + X \sim 110$.

3. $X_n = X_k \cdot X_r \,||\, R(X) = 1001110$ – итоговая комбинация ЦК (кодовое слово).

Синдромный метод декодирования ЦК. Основная операция: принятое кодовое слово X_n нужно поделить на порождающий полином. Если X_n принадлежит коду, т. е. не искажено помехами, то остаток от деления (синдром) будет нулевым. Ненулевой остаток свидетельствует о наличии ошибок в принятой кодовой комбинации. Для исправления ошибки нужно определить вектор (полином) ошибки (обозначим его E_n).

После передачи по каналу с помехами принимается кодовое слово

$$Y_n = X_n + E_n, \qquad (14)$$

здесь также сумма по модулю 2.

При декодировании принятое кодовое слово делится на $G(X)$:

$$(Y_n) / (G(X)) = U,\ S_r, \qquad (15)$$

где S_r – остаток от деления $(Y_n) / (G(X))$ – синдром; U – результат деления.

Всякому ненулевому синдрому соответствует определенное расположение (конфигурация) ошибок: синдром для ЦК имеет те же свойства, что и для кода Хемминга (используются при декодировании синдрома).

Пример 6. Рассмотрим процедуру декодирования сообщения, сформированного в примере 5. Пусть Y_n =10<u>1</u>1110 (ошибочным является третий бит – подчеркнут).

Вспомним, что порождающая матрица имеет вид, показанный в примерах 3 и 4:

$$H_{7,4} = \begin{matrix} 1110 & 100 \\ 0111 & 010. \\ 1101 & 001 \end{matrix}$$

Для решения задачи последовательно выполняем следующие операции:

1) деление в соответствии с (15):

$$Y_n / G(X) = X^6 + X^4 + X^3 + X^2 + X \;\big|\; \underline{X^3 + X + 1}$$
$$\underline{X^6 + X^4 + X^3} \qquad\qquad\quad X^3$$
$$X^2 + X;$$

$X^2 + X$ – остаток, т. е. синдром $S_r = X^2 + X \sim 110$;

2) декодирование синдрома позволяет определить местоположение ошибки: по полученному синдрому 110 в анализаторе синдрома (дешифраторе синдрома) определяем вид вектора E_n = 0010000.

Здесь обратим внимание на важнейшую деталь: *синдром равен третьему вектор-столбцу в матрице $H_{7,4}$, поэтому единичный символ будет в третьем разряде вектора E_n*;

3) исправление ошибки: $Y_n + E_n$ = 10<u>1</u>1110 + 0010000 = 10<u>0</u>1110.

После исправления (исправленный бит подчеркнут двойной линией) получили такое же слово, которое было сформировано в источнике сообщения (см. п. 3 из примера 5).

Вопросы для контроля и самоконтроля

1. Что такое и для чего используются «структурная избыточность», «информационная избыточность» и «временная избыточность»?
2. В чем особенность перечисленных ниже кодов и в чем состоит отличие между кодами: а) блочным и непрерывным, б) систематическим и несистематическим, в) линейным и нелинейным?
3. К какому классу относится код Хемминга, циклический код?
4. Что такое «расстояние Хемминга», «вес Хемминга», «информационное слово», «кодовое слово», «избыточное слово», «информационный символ», «проверочный символ»?
5. Какое минимальное или максимальное число избыточных символов может содержать кодовое слово, принадлежащее коду?
6. Вычислите число и значение проверочных символов для кода простой четности, если информационное слово имеет вид: 1100; 1110; 101010; 11110000.
7. Какое число проверочных символов имеет кодовое слово кода Хемминга с минимальным кодовым расстоянием 3, если информационное слово имеет вид: 1100; 1110; 101010; 11110000; 1010111; 1111111100?
8. Построить проверочную матрицу кода Хемминга с минимальным кодовым расстоянием 3 (4) для вычисления проверочных символов, если информационное слово имеет вид из задания 7.
9. Вычислить проверочные символы кодового слова кода Хемминга с минимальным кодовым расстоянием 3 (4), если проверочная матрица H имеет вид

$$H = \begin{matrix} 0111 & 1 \\ 1011 & 1, \\ 1101 & 1 \end{matrix}$$

а информационное слово имеет вид: 1100, 1101, 0000, 1111.

10. Вычислить синдром ошибки для случая из задания 9, если ошибка при передаче кодового слова произошла: а) в первом бите этого слова, б) во втором, в) в пятом, г) в первом и в седьмом.
11. Как вычислить синдром ошибки?
12. Как определить вектор ошибки?
13. Какая конечная операция используется для исправления ошибки?

14. Чем характеризуется итеративный код?

15. Каково минимальное кодовое расстояние итеративного кода?

16. Какое число ошибок может исправить код с минимальным кодовым расстоянием: а) 3, б) 4, в) 7?

17. Вычислить минимальное количество и значения проверочных символов кодового слова итеративного кода, если информационное слово имеет вид: 1100, 0101, 101010101, 0000111100001111.

18. Если кодовое слово ЦК имеет вид 11011010, будут ли разрешенными кодовыми комбинациями следующие: 1101110, 01101011, 11011011?

19. Запишите в полиномиальном виде кодовое слово ЦК: 11011011, 1010101010, 0000000, 0000000001.

20. Чему равен результат операции по модулю 2 над полиномами ($X^6 + X^3 + X^2$) и ($X^4 + X^2 + X$), если такой операцией будет: сложение, вычитание, деление, умножение? Записать результат операции в двоичной форме.

21. Определить число и вычислить значения проверочных символов ЦК, если код задается полиномом $X^3 + X^2 + 1$, а информационное слово имеет вид: 1010, 1100.

22. Чему будет равен синдром ошибки, возникшей при передаче сообщения для условий из задачи 22, если ошибка произошла: а) в первом бите кодового слова, б) во втором, в) в пятом, г) в первом и в седьмом?

Методы и средства перемежения данных. Использование перемежителей/деперемежителей в системах передачи данных

Перемежителем называют такое устройство (реализовано аппаратно) или программное средство, которое определенным образом перемешивает (меняет местами) символы передаваемого сообщения (или кодового слова).

Основная причина разработки и использования перемежителей – желание разнести расположенные рядом (сгруппированные) ошибки в сообщении («размазать» ошибки по сообщению) с целью упрощения и сокращения во времени процедуры исправления таких ошибок сравнительно простыми кодами.

На рис. 3 показана структурная схема ИС, в которой наряду с помехоустойчивым кодом используется перемежение/деперемежение символов передаваемого сообщения.

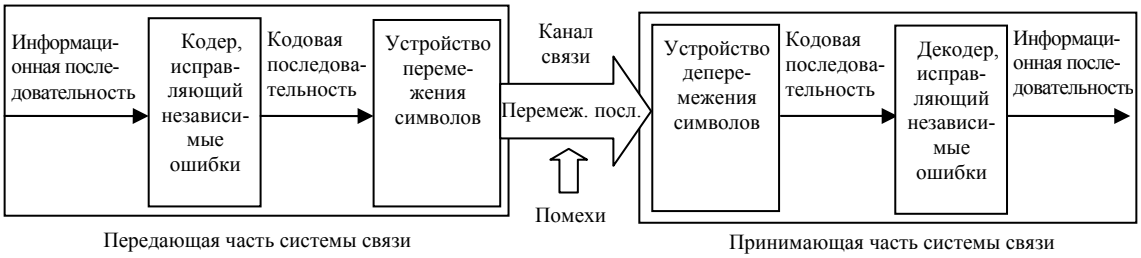

Рис. 3. Структурная схема ИС с перемежителем/деперемежителем

Выполнение операции декодирования в два этапа позволяет почти полностью избавиться от влияния помех. На первом этапе производится преобразование групп (пакетов) ошибок в группу случайных (обычно одиночных) ошибок (см. рис. 3). На втором этапе сигнал обрабатывается с помощью классических методов борьбы со случайными ошибками (линейные итеративные коды, сверточные коды, турбокоды), что должно приводить к полной коррекции ошибок.

Процедура перемежения/деперемежения состоит в перестановке символов кодового слова и восстановлении исходной последовательности после передачи ее по каналу. При перемежении обеспечивается преобразование бит входной последовательности в выходную последовательность без изменения ее длины. Однако чем больше *глубина перемежения* (минимальное расстояние – в битах, – на которое разносятся соседние символы входной последовательности), тем больше задержка.

В общем случае выбор глубины перемежения зависит от двух факторов. С одной стороны, чем больше расстояние между соседними символами, тем большей длины пакет ошибок может быть исправлен. С другой стороны, чем больше глубина перемежения, тем сложнее аппаратно-программная реализация оборудования и больше задержка сигнала.

В литературных источниках для сравнения перемежителей используют следующие характеристики: глубина перемежения; время перемежения; *рандомизация* бит (местоположение любого бита выходной последовательности должно отличаться от его местоположения в исходной последовательности). Однако основной характеристикой считают глубину перемежения.

Наиболее простым является метод блочного перемежения (рис. 4), основанный на принципе формирования прямоугольной матрицы (рис. 5), состоящей из n-разрядных строк (n – длина кодовой комбинации), с которой осуществляется поразрядное считывание каждого столбца через d разрядов.

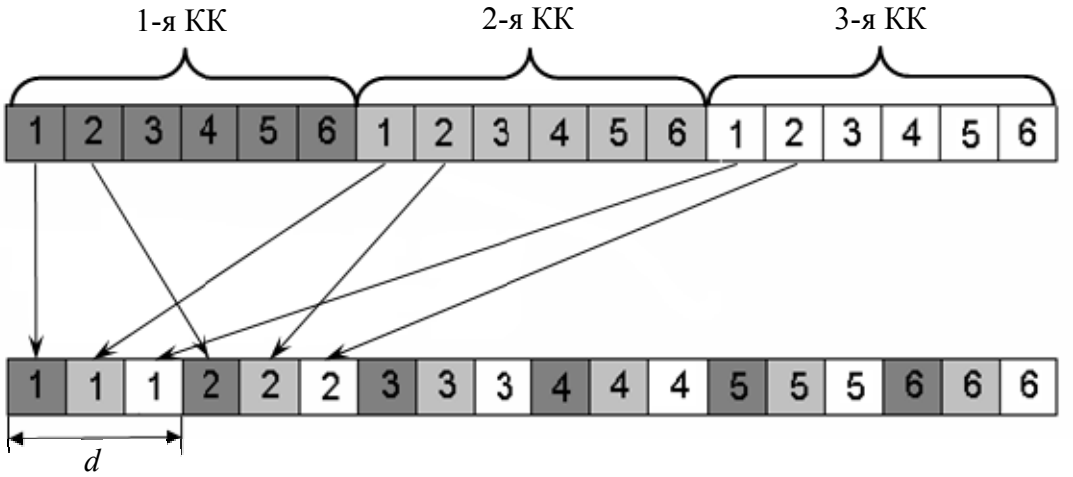

Рис. 4. Пояснение к алгоритму блочного перемежения,
где d – интервал декорреляции, КК – кодовая комбинация

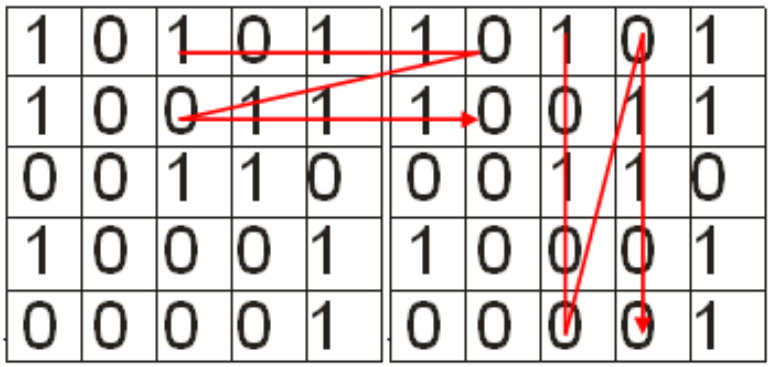

Рис. 5. Пояснение принципа блочного
перемежения

Пример 1. Рассмотрим процесс передачи информации с использованием кода Хемминга и блокового перемежителя. Информационный поток на входе кодера Хемминга (используется код 7, 4) имеет вид, как показано на рис. 6.

Информационная комбинация 1				Информационная комбинация 2				Информационная комбинация 3				Информационная комбинация 4				Информационная комбинация 5				Информационная комбинация 6				Информационная комбинация 7				…	Информационная комбинация *N*			
1	0	0	1	1	1	0	0	0	0	1	0	0	1	0	1	0	1	1	1	1	0	1	0	1	1	1	0	…	0	0	0	0

Рис. 6. Структура информационного потока на входе кодера

На выходе из кодера сообщение будет иметь вид, который можно понять из рис. 7.

Кодовая комбинация 1							Кодовая комбинация 2							Кодовая комбинация 3						
1	0	0	1	1	1	0	1	1	0	0	0	1	0	0	0	1	0	1	1	0

Кодовая комбинация 4							Кодовая комбинация 5							Кодовая комбинация 6						
0	1	0	1	1	0	0	0	1	1	1	0	1	0	1	0	1	0	0	1	1

Кодовая комбинация 7							…	Кодовая комбинация *N*						
1	1	1	0	1	0	0	…	0	0	0	0	0	0	0

Рис. 7. Последовательность символов сообщения на выходе из кодера

Матрица перемежения размером 7×7 будет иметь вид, как показано на рис. 8.

1	0	0	1	1	1	0
1	1	0	0	0	1	0
0	0	1	0	1	1	0
0	1	0	1	1	0	0
0	1	1	1	0	1	0
1	0	1	0	0	1	1
1	1	1	0	1	0	0

Рис. 8. Вид и содержание матрицы перемежения

После перемежения сообщение соответствует последовательности, изображенной на рис. 9.

Кодовая комбинация 1–7 после перемежения																				
1	1	0	0	0	1	1	0	1	0	1	1	0	1	0	0	1	0	1	1	1

Кодовая комбинация 1–7 после перемежения																				
1	0	0	1	1	0	0	1	0	1	1	0	0	1	1	1	1	0	1	1	0

Кодовая комбинация 1–7 после перемежения							Кодовая комбинация 8–14 после перемежения								
0	0	0	0	0	1	0	…	…	…	…	…	…	…	…	…

Рис. 9. Бинарная последовательность после перемежения

Предположим, что в процессе передачи информации по каналу возник пакет ошибок *P* (выделено черным) длиной 7 бит (рис. 10).

Рис. 10. Кодовое слово, содержащее группу ошибок

Сообщение на выходе канала связи записывается по столбцам в матрицу деперемежения (рис. 11).

1	0	0	0	1	1	0
1	1	1	0	0	1	0
0	0	0	0	1	1	0
0	1	1	1	1	0	0
0	1	0	1	0	1	0
1	0	0	0	0	1	1
1	1	0	0	1	0	0

Рис. 11. Вид и содержание
матрицы деперемежения

Из матрицы деперемежения двоичные символы сообщения считываются по строкам и поступают на декодер кода Хемминга (рис. 12).

Рис. 12. Ошибки разнесены по всему сообщению

После деперемежения пакет ошибок преобразован в независимые ошибки кратности 1 для каждой из кодовых комбинаций кода Хемминга. Как помним, такие ошибки код в состоянии исправить. Информационный поток на выходе из декодера кода Хемминга имеет вид в соответствии с рис. 13.

Информационная комбинация 1				Информационная комбинация 2				Информационная комбинация 3				Информационная комбинация 4				Информационная комбинация 5				Информационная комбинация 6				Информационная комбинация 7				…	Информационная комбинация N			
1	0	0	1	1	1	0	0	0	0	1	0	0	1	0	1	0	1	1	1	1	0	1	0	1	1	1	1	0	…	0	0	0	0

Рис. 13. Информационный поток на выходе из декодера кода Хемминга

Рассмотренный метод блочного перемежения применяется в GSM. К числу других используемых на практике относятся следующие методы перемежения/деперемежения: псевдослучайный, *S*-типа (применяется в турбо-кодировании, CDMA и др.), циклически-сдвиговый, случайный, диагональный, многошаговый.

Кратко охарактеризуем *метод S-случайного перемежения*.

Работа *S*-случайного перемежителя построена следующим образом. Имеется информационная последовательность длиной K символов. Предварительно устанавливается размер минимального расстояния разнесения группирующихся ошибок S. Данное значение показывает, что каждый символ в перемеженной последовательности должен иметь с каждым из предыдущих S символов разницу во входной последовательности минимум S позиций. При формировании перемеженной последовательности следующая позиция символа выбирается случайно из входной последовательности. Если данная позиция не находится в пределах $\pm S$ с предыдущими S символами выходной последовательности, то она добавляется в выходную последовательность и больше не участвует в выборе. В противном случае выбор позиции символа происходит еще раз. Процесс продолжается до тех пор, пока все K символов не будут выбраны.

Достоинство: минимальное расстояние составляет S.

Недостатки: время поиска алгоритма увеличивается с увеличением S, кроме того, нет гарантии сходимости алгоритма.

Пример 2. Пусть имеется кодовая последовательность, равная K = = 16 бит. Установим значение параметра $S = 3$. Сгенерируем позицию символа. Пусть она будет равна 0. Так как предыдущих позиций символов нет, то ее и записываем. Генерируем новую позицию. Пусть она будет равна 4. Сравниваем эту позицию с предыдущими тремя позициями новой последовательности на условии разницы каждой с сгенерированной. Если разница хотя бы с одной позицией меньше 3, то выбранная позиция на данном этапе не учитывается и выбирается новая из числа оставшихся. В противном случае данную позицию записываем в новую последовательность. Пусть в итоге получим сгенериро-

ванную последовательность позиций 0, 4, 8, 12, 1, 5, 9, 13, 2, 6, 10, 14, 3, 7, 11, 15. Перемежение будет выглядеть следующим образом.

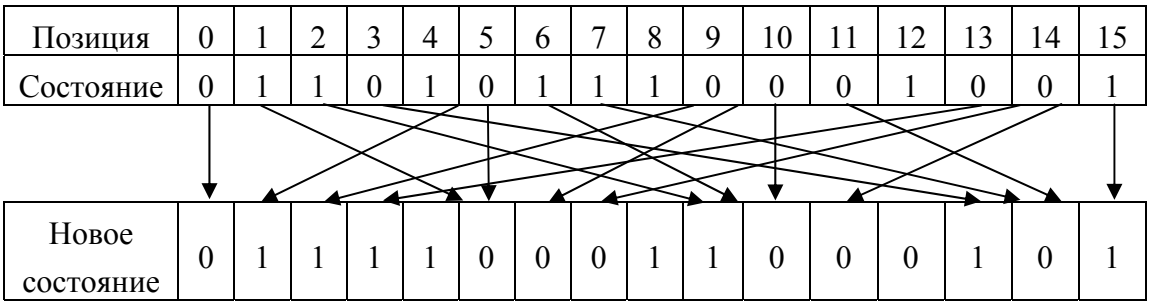

Рис. 14. Принцип *S*-случайного перемежения

Метод циклически-сдвигового перемежения описывается выражением

$$\pi(i) = (p \cdot i + s) \bmod K,$$

где s – размер сдвига; p – размер шага. Значение p выбирается взаимнопростым с K.

Достоинство: небольшое время перемежения битовых символов.

Недосток: небольшое расстояние разнесения бит.

Пример 3. Пусть имеется кодовая последовательность K, равная 16 бит (табл. 2).

Таблица 2

Кодовая последовательность для перемежения

Позиция	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Состояние	0	1	1	0	1	0	1	1	1	0	0	0	1	0	0	1

Установим размер сдвига $s = 2$, а размер шага $p = 5$. Определим новое местоположение каждого символа:

$$\pi(0) = (5 \cdot 0 + 2)\text{mod}16 = 2\text{mod}16 = 2;$$
$$\pi(1) = (5 \cdot 1 + 2)\text{mod}16 = 7\text{mod}16 = 7;$$
$$\pi(2) = (5 \cdot 2 + 2)\text{mod}16 = 12\text{mod}16 = 12;$$
$$\pi(3) = (5 \cdot 3 + 2)\text{mod}16 = 17\text{mod}16 = 1;$$
$$\pi(4) = (5 \cdot 4 + 2)\text{mod}16 = 22\text{mod}16 = 6;$$
$$\pi(5) = (5 \cdot 5 + 2)\text{mod}16 = 27\text{mod}16 = 11;$$
$$\pi(6) = (5 \cdot 6 + 2)\text{mod}16 = 32\text{mod}16 = 0;$$
$$\pi(7) = (5 \cdot 7 + 2)\text{mod}16 = 37\text{mod}16 = 5;$$
$$\pi(8) = (5 \cdot 8 + 2)\text{mod}16 = 42\text{mod}16 = 10;$$
$$\pi(9) = (5 \cdot 9 + 2)\text{mod}16 = 47\text{mod}16 = 15;$$

$$\pi(10) = (5 \cdot 10 + 2)\text{mod}16 = 52\text{mod}16 = 4;$$
$$\pi(11) = (5 \cdot 11 + 2)\text{mod}16 = 57\text{mod}16 = 9;$$
$$\pi(12) = (5 \cdot 12 + 2)\text{mod}16 = 62\text{mod}16 = 14;$$
$$\pi(13) = (5 \cdot 13 + 2)\text{mod}16 = 67\text{mod}16 = 3;$$
$$\pi(14) = (5 \cdot 14 + 2)\text{mod}16 = 72\text{mod}16 = 8;$$
$$\pi(15) = (5 \cdot 15 + 2)\text{mod}16 = 77\text{mod}16 = 13.$$

Перемеженная последовательность будет иметь вид в соответствии с табл. 3.

Таблица 3

Перемеженная последовательность

Позиция	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Состояние	1	1	1	1	1	0	0	0	0	1	1	0	0	0	1	0

Вопросы для контроля и самоконтроля

1. Основное назначение устройств перемежения.
2. Пояснить принцип работы устройств перемежения.
3. Перечислить основные характеристики методов перемежения.
4. Пояснить принцип работы блокового метода перемежения.
5. Какая последовательность получится на выходе из блокового перемежителя, если входная последовательность имеет вид 101110100?
6. Пояснить принцип работы *S*-случайного метода перемежения.
7. Пояснить принцип работы циклически-сдвигового метода перемежения.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Урбанович, П. П. Информационная безопасность и надежность систем / П. П. Урбанович, Д. М. Романенко, Е. В. Романцевич. – Минск: БГТУ, 2007. – 90 с.

2. Леонов, А. П. Безопасность автоматизированных банковских и офисных систем / А. П. Леонов, К. А. Леонов, Г. В. Фролов. – Минск: НКП Беларуси, 1996. – 280 с.

3. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей / В. Ф. Шаньгин. – М.: ИД «ФОРУС»: Инфра-М, 2008. – 416 с.

4. Скляр, Б. Цифровая связь. Теоретические основы и практическое применение / Б. Скляр; пер. с англ. – 2-е изд. – М.: ИД «Вильямс», 2003. – 1104 с.

5. Ипатов, В. П. Системы мобильной связи [Электронный ресурс] / В. П. Ипатов [и др.]. – Режим доступа: http://www.uftuit.uzpak.uz/Tatulib/book/sistemi_mob_svyazi/sistemi_mobilnoj_svyazi.htm. – Дата доступа: 05.02.12.

6. Гуров, И. П. Основы теории информации и передачи сигналов / И. П. Гуров. – СПб.: BHV-Санкт-Петербург, 2000. – 97 с.

ОГЛАВЛЕНИЕ

ЗАЩИТА ИНФОРМАЦИИ И НАДЕЖНОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ

Составители: **Урбанович** Павел Павлович
Шиман Дмитрий Васильевич

Редактор *Ю. А. Ирхина*
Компьютерная верстка *Е. Ю. Орлова*
Корректор *Ю. А. Ирхина*

Издатель:
УО «Белорусский государственный технологический университет».
ЛИ № 02330/0549423 от 08.04.2009.
ЛП № 02330/0150477 от 16.01.2009.
Ул. Свердлова, 13а, 220006, г. Минск.