Министерство образования и науки Украины
Севастопольский национальный технический университет

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

к выполнению контрольной работы
по дисциплине

«РАДИОЭЛЕКТРОННЫЕ СИСТЕМЫ ЗАЩИТЫ ОБЪЕКТОВ И ИНФОРМАЦИИ»

для студентов заочной формы обучения
специальности 7.090701 — Радиотехника

Севастополь
2007

УДК 004.056

Методические указания к выполнению контрольной работы по дисциплине «Радиоэлектронные системы защиты объектов и информации» для студентов заочной формы обучения специальности 7.090701 Радиотехника / Сост. И.В.Лащенко.— Севастополь: Изд-во СевНТУ, 2007.— 20с.

Целью методических указаний является оказание помощи студентам заочной формы обучения при самостоятельном изучении дисциплины «Радиоэлектронные системы защиты объектов и информации» и при выполнении и оформлении контрольной работы по указанной дисциплине. Изложены основные темы дисциплины и дана их краткая характеристика. Приведены контрольные задания, а также указания по выполнению и оформлению контрольной работы.

Методические указания рассмотрены и утверждены на заседании кафедры радиотехники (протокол № 12 от " 29 " июня 2007 г.).

Допущено учебно-методическим центром СевНТУ в качестве методических указаний.

Рецензенты: Иськив В.М., старший преподаватель кафедры радиотехники; Савочкин А.А., к.т.н., доцент кафедры радиотехники.

Ответственный за выпуск: Гимпилевич Ю.Б., доктор техн. наук, профессор, заведующий кафедрой радиотехники.

СОДЕРЖАНИЕ

1. ЦЕЛЬ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ

Целью изучения дисциплины «Радиоэлектронные системы защиты объектов и информации» является приобретение знаний по вопросам правовых аспектов защиты информации, принципов построения систем охраны объектов и защиты информации, формирование у студентов навыков и умений решения задач обнаружения и блокировки устройств несанкционированного доступа к информации, ознакомление с принципами криптографической защиты информации.

2. КРАТКОЕ СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

2.1. Свойства информации. Правовые вопросы защиты информации

Понятие “информация”, ее свойства. Виды представления информации. Угрозы информации. Преднамеренные и непреднамеренные источники угроз. Деятельность подразделений по технической защите информации.

Основные понятия и определения

Понятие “информация” — многозначное, встречается во многих областях деятельности человека. В соответствии с действующим законодательством “...к **информации** относятся сведения о лицах, предметах и фактах, событиях и процессах,

независимо от формы их представления...” Виды представления информации: устная; рукописная; печатная (в нескольких экземплярах или массовая); на магнитных, оптических, электронных носителях, в другом виде. Информация делится по режиму доступа на открытую информацию и информацию с ограниченным доступом (секретная, конфиденциальная).

Защита информации — это комплекс мероприятий, направленных на обеспечение информационной безопасности. Эффективная защита информации включает следующие меры: законодательные; административные; организациионные; морально-этические; физические; технические; программные; криптографические и др. Должны быть обеспечены доступность, целостность и конфиденциальность информации. **Доступность** — это возможность за приемлемое время получить требуемую информационную услугу. Под **целостностью** подразумевается актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения. **Конфиденциальность** — это защита от несанкционированного доступа к информации.

Вопросы для самопроверки

1. Виды представления информации.
2. Какие свойства информации должны быть обеспечены при ее защите?
2. Какие сведения относятся к государственной тайне? Какие сведения относятся к коммерческой тайне?
3. Перечислите основные угрозы для информации, источники непреднамеренных и преднамеренных угроз.
4. Основные направления деятельности подразделений по технической защите информации.

2.2. Физические средства защиты объектов и информации

Технические средства охраны. Системы охранно-пожарной сигнализации. Принцип действия электромагнитных, электромеханических, акустических, фотоэлектрических, пассивных, инфракрасных, емкостных, ультразвуковых, микроволновых, радиолучевых датчиков. Средства технической укрепленности. Системы наблюдения. Системы контроля доступа и досмотра. Системы «интеллектуального здания». Автомобильная сигнализация, навигационные системы поиска автомобилей.

Основные понятия и определения

Технические средства охраны — устройства, системы и сооружения, предназначенные для создания физических препятствий нарушителю, своевременного обнаружения и блокирования его действий.

Системы охранной сигнализации составляют охранные извещатели (датчики) различных типов, приемно-контрольные приборы, оповещатели, шлейфы охранной сигнализации. Эти системы часто применяются совместно с системами пожарной сигнализации и пожаротушения.

Средства технической укрепленности выполняют роль преград при попытке нарушителя проникнуть на объект — это механические и строительные конструкции; замки различных видов; сейфы, металлические шкафы и тайники.

Системы наблюдения предназначены для визуального контроля состояния защищаемого объекта. В их состав могут входить телекамеры, телемониторы, видеокоммутаторы, видеомультиплексеры, видеообнаружители движения, видеомагнитофоны либо цифровые камеры с компьютерными системами обработки и управления процессом наблюдения.

Системы контроля доступа (СКД) могут основываться на трех различных принципах. Основанные на знаниях СКД — используют различаемую информацию (жесты, символы…) или хранимую информацию (личные номера, коды, пароли…). Атрибутивные СКД — используют документы (пропуска, удостоверения с фотографиями…), различные карты (магнитные, смарткарты, проксимити- и виганд-карты), другие предметы (ключи, жетоны…). Персональные СКД — основаны на уникальных характеристиках человека, присущих непосредственно субъекту доступа: квазистатические (биометрические) системы используют информацию об отпечатках пальцев, строении лица, форме черепа, ушной раковины, геометрии руки, рисунке на сетчатке глаз и других постоянных признаках, а квазидинамические системы используют информацию об интегральных параметрах речи, подчерка, стиле печатания, пульсе, кардиограмме…

Системы охраны объектов и информации часто координируются одним центром. Автоматизированные технические системы «**Интеллектуальное здание**», предназначенны для обеспечения максимального достижимого комфорта и безопасности обитателей здания, состоят из подсистем управления зданием, безопасности, жизнеобеспечения, информатизации, объединенной кабельной сети.

Вопросы для самопроверки

1. Что такое технические средства охраны? Какие технические средства относятся к средствам охранной сигнализации?
2. Для чего предназначены системы наблюдения, из каких устройств они состоят?
3. Опишите назначение и состав систем контроля доступа и досмотра персонала и посетителей.
4. Дайте развернутую классификацию существующих принципов опознавания.
5. Для чего предназначено «интеллектуальное здание», из каких систем состоит?

2.3. Технические каналы утечки информации

Классификация, источники, способы скрытия. Заходовые и беззаходовые методы, средства проникновения и маскировки. Физические преобразователи акустической информации, устройства прослушивания помещений. Радиомикрофоны, диктофоны, средства подключения к линиям связи. Паразитные связи и наводки, перехват электромагнитных излучений. Системы скрытого видеонаблюдения. Методы и средства разрушения информации.

Основные понятия и определения

Технический канал утечки информации — система связи, состоящая из источника утечки информации, среды распространения и злоумышленной принимающей стороны (средства разведки).

Выделяют акустический, визуальный, электромагнитный, электрический, материально-вещественный каналы утечки информации.

Анализ возможных каналов утечки и несанкционированного доступа к информации показывает, что существенную их часть составляют технические каналы утечки **акустической** информации.

В зависимости от среды распространения акустических колебаний, способов их перехвата и физической природы возникновения информационных сигналов можно рассматривать воздушный, вибрационный, электроакустический, оптико-электронный и параметрический каналы утечки акустической информации.

Утечки информации могут происходить как по специально организованным каналам, так и непреднамеренно. Специально внедренные устройства несанкционированного получения информации называют **закладными устройствами**. Существуют различные средства получения акустической информации (обычные, лазерные, узконаправленные микрофоны, диктофоны, стетоскопы, резонаторы и др.). Чаще всего они выполняются в малогабаритном или камуфлированном варианте исполнения.

Вопросы для самопроверки

1. Перечислите виды технических каналов утечки информации.
2. Охарактеризуйте акустический технический канал утечки информации.
3. Охарактеризуйте электромагнитный канал утечки информации.
4. Охарактеризуйте электрический канал утечки информации.
5. Охарактеризуйте визуально-оптический канал утечки информации.
6. Охарактеризуйте материально-вещественный канал утечки информации.
7. Опишите принципы действия устройств несанкционированного получения информации.

2.4. Технические средства предотвращения несанкционированного доступа к информации

Устройства, контролирующие радиоэфир (индикаторы поля, сканеры). Устройства, контролирующие параметры телефонных линий. Средства, исключающие распространение по проводным линиям непредусмотренных низкочастотных сигналов (акустическое подслушивание); средства, исключающие распространение непредусмотренных высокочастотных сигналов (ВЧ навязывание). Устройства активной защиты (постановщики помех, маскираторы, нейтрализаторы). Нелинейные локаторы.

Основные понятия и определения

Системы защиты можно разделить на пассивные и активные.

Активные средства защиты формируют специальный электромагнитный или акустический, вибрационный сигнал (помеху), препятствующий передаче информационного сигнала из защищаемого помещения.

С помощью пассивных средств проводят обнаружение существующих закладок различных типов, а также предотвращают случайную утечку информации по техническим каналам.

Индикаторы поля (специальные широкополосные приемники) и сканеры (специальные перестраиваемые приемники) предназначены для поиска устройств передачи информации по радиоканалу.

Методы контроля проводных линий, как слаботочных (телефонных линий, систем охранной и пожарной сигнализации), так и силовых, основаны на выявлении в них информационных сигналов (низкочастотных и высокочастотных) и измерении параметров линии, которые изменяются при несанкционированном подключении.

Для устранения наводок от технических средств передачи и обработки информации, необходимо не только подавить их в выходящих из помещения проводниках, но и ограничить сферу действия электромагнитного поля, создаваемого в непосредственной близости от источников. Эта задача решается применением экранирования.

С помощью нелинейных локаторов можно обнаружить внедренные технические средства разведки, даже находящиеся в отключенном состоянии. Принцип действия нелинейного локатора основан на переизлучении гармоник исходного сигнала элементом с нелинейной характеристикой (любым полупроводниковым прибором) при его облучении.

Вопросы для самопроверки

1. Опишите назначение, принцип действия и характеристики индикаторов поля.
2. Опишите назначение, принцип действия и характеристики сканеров.
3. Опишите назначение, принцип действия и характеристики нелинейных локаторов.
4. Рассмотрите экранирование как способ предотвращения утечки информации по электромагнитному каналу.
5. Опишите применение средств активной защиты.

2.5. Системы закрытия речи

Аналоговые и цифровые системы закрытия речи. Временное и частотное аналоговое скремблирование. Статические и динамические скремблеры. Широкополосные и узкополосные цифровые системы закрытия речи. Виды вокодеров.

Основные понятия и определения

Для смыслового закрытия речи телефонного сообщения применяют специальные устройства — **скремблеры**. Под аналоговым скремблированием понимают изменение характеристик речевого сигнала, таким образом, чтобы полученный сигнал, обладая свойствами неразборчивости и неузнаваемости, занимал ту же полосу частот, что и исходный. Выделяют временно́е и частотное скемблирование.

В системах временно́го скремблирования речь дробится на определенные равные информационные участки, которые до передачи в линию связи запоминаются, затем «перемешиваются» по определенному закону. Чем меньше длительность элементарных отрезков, на которые разбивается входной сигнал и чем больше элементов участвует в перестановке, тем сложнее восстановить перехваченный сигнал.

В системах частотного скремблирования с помощью системы фильтров вся полоса частот стандартного телефонного канала делится на некоторое число полос, которые перемешиваются по определенному закону, иногда добавляется инвертирование некоторых или всех полос.

Цифровые системы закрытия речи подразделяются на широкополосные и узкополосные. В широкополосных цифровых системах закрытия речи исходный сигнал дискретизируется, шифруется и передается только по специально выделенным широкополосным каналам связи.

В узкополосных цифровых системах закрытия речи используется снижение информационной избыточности речи. В таких системах устройство кодирования речи (**вокодер**), анализируя форму речевого сигнала, производит оценку параметров переменных компонент речи и передает эти параметры в цифровой форме по обычному каналу связи на синтезатор, где согласно принятой модели синтезируется речевое сообщение.

Вопросы для самопроверки

1. Поясните принципы работы временных аналоговых скремблеров.
2. Поясните принципы работы различных частотных аналоговых скремблеров.
3. Поясните принцип работы вокодеров.
4. Сравните степень защиты и качество восстановленной речи для различных систем закрытия речи.

2.6. Программные методы защиты информации

Виды угроз информации. Общие принципы построения систем защиты информации в компьютеризированных системах. Политика безопасности. Способы организации процедуры разграничения доступа. Методы аутентификации пользователей, виды паролей. Программные средства контроля программ, антивирусные сканеры, сетевые фильтры.

Основные понятия н определения

Основными **источниками угроз** информации в компьютеризированных системах являются :

— случайные или некорректные действия недостаточно квалифицированных пользователей;

— преднамеренное воздействие на программные средства (с помощью программных закладок или со стороны несанкционированных пользователей — непосредственно у компьютера или с удаленным доступом);

— воздействие компьютерных вирусов;

— утечка незащищенных данных по техническим каналам (например, электромагнитное излучение).

Программные закладки — преднамеренные дефекты программного обеспечения, которые служат для целенаправленного скрытого воздействия на информационную систему.

Компьютерным вирусом называется программа, которая может «инфицировать» другие программы, включая в них свою (возможно модифицированную) копию, способную к дальнейшему размножению. После размножения или вместо него в определенных случаях вирус совершает различные деструктивные действия. Для защиты информации применяют специальное антивирусное программное обеспечение.

Политика безопасности — набор законов, правил и норм поведения, определяющих методы защиты, обработки и распространения информации. Одним из первых средств защиты информации является разграничение доступа. Существуют различные способы организации процедуры разграничения доступа. Рассмотрим матричное разграничение: права пользователей задаются в виде таблицы, в строках которой представлен список пользователей, а в столбцах — перечень объектов (файлы, базы данных, прикладные, системные программы и т.д.) В клетках таблицы описаны допустимые действия субъекта по отношению к объекту (только чтение, запись, выполнение, возможность передачи прав другому субъекту и т.п.) Таким образом, каждому субъекту предоставляются права в соответствии с уровнем его полномочий. Каждый пользователь, прежде чем совершать какие-либо действия в системе, должен идентифицировать себя, то есть назвать, и его имя должно быть зарегистрировано в имеющейся базе данных. Система должна проверить подлинность личности пользователя (аутентификация), то есть установить — является ли он именно тем, за кого себя выдает. Наиболее широко применяется парольная система аутентификации.

Защита внутренних ресурсов сетей от внешних атак решается **сетевыми фильтрами** (брандмауерами) — с помощью централизации доступа к сети и контроля за ним программно-аппаратными средствами.

Надежная система обязана фиксировать все события, касающиеся безопасности. К числу таких событий относятся — вход в систему; выход из системы; обращение к удаленной системе; обращение к программам, попытка их изменения, операции с файлами (открыть, закрыть, переименовать, удалить, изменить…), смена атрибутов безопасности. Ведение протоколов должно дополняться **аудитом**, то есть анализом регистрируемой информации и принятием конкретных мер по отношению к субъектам, совершающим подозрительные действия.

Вопросы для самопроверки

1. Охарактеризуйте основные принципы политики безопасности.
2. Опишите виды компьютерных вирусов и меры борьбы с ними.
3. Перечислите способы организации процедуры разграничения доступа.
4. Опишите процессы аутентификации с помощью различных видов паролей.

2.7. Основы криптографической защиты информации

Классификация основных криптографических методов защиты информации. Стандарты шифрования данных. Методы ассиметричной криптонрафии. Электрон-

ная цифровая подпись. Стеганографические методы защиты информации. Понятия практической и теоретической стойкости криптосистем.

Основные понятия и определения

Криптография (от греч. «тайнопись») — наука о методах преобразования информации в целях ее защиты от незаконных пользователей. **Шифр** — алгоритм преобразования информации, **ключ** — сменяемый элемент шифра.

Можно выделить симметричные и несимметричные методы криптографии. При использовании **симметричных методов** шифрование исходного сообщения и дешифрация криптограммы происходит по определенным алгоритмам с использованием одного и того же ключа. К симметричным методам относят:

- **перестановочные шифры —** знаки исходного сообщения переставляются по определенному алгоритму. Алгоритм перестановок может определяться аналитическим путем, либо могут использоваться специальные механические приспособления;
- **подстановочные шифры —** знаки исходного алфавита замещаются любыми знаками: буквами, цифрами, символами. Подстановка может быть однозначной либо многозначной;
- **гамма шифры —** символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности случайных чисел, которая называется **гаммой**. Может выполняться не сложение, а другие математические, логические операции. Используются конечные либо бесконечные гаммы;
- **метод аналитических преобразований —** над преобразованными в математическую форму символами исходного сообщения и ключа проводят аналитические операции, например, умножение матрицы (ключа) на вектор (исходное сообщение);
- **комбинированные методы** — последовательное шифрование блоков исходного текста с помощью двух и более методов (подстановка, замена и гаммирование).

В **несимметричных системах** формируются два ключа: открытый ключ, доступный многим, и закрытый — секретный. Шифрование исходных сообщений и дешифрация криптограмм проводится с использованием различных ключей.

Криптографическая защита информации находит широкое применение для хранения и передачи конфиденциальных сообщений, данных, подтверждения подлинности электронных документов. **Электронная цифровая подпись** — дополняющее текст документа математическое преобразование, гарантирующее неизменный вид текста.

Стеганография — совокупность методов, обеспечивающих сокрытие самого факта существования секретной информации, а также средств реализации этих методов. Большинство методов компьютерной стеганографии базируется на двух принципах: а) файлы, не требующие абсолютной точности могут быть видоизменены без потери функциональности; б) органы чувств человека неспособны надежно различать незначительные изменения в таких исходных файлах.

Вопросы для самопроверки

1. Перечислите основные методы шифрования.
2. Поясните принцип, положенный в основу шифров "подстановка", недостатки и методы модификации.
3. Поясните принцип, положенный в основу шифров "перестановка", недостатки и методы модификации.
4. Поясните суть метода гаммирования.
5. Поясните понятие «электронная цифровая подпись».
7. Дайте определение понятий «криптография», «стеганография».

3. ПЕРЕЧЕНЬ ЛАБОРАТОРНЫХ РАБОТ

1. Изучение датчиков охранной сигнализации.
2. Изучение электронных металлодетекторов.
3. Изучение устройств несанкционированного доступа к аудиоинформации.
4. Изучение средств противодействия несанкционированному доступу к информации.
5. Изучение средств закрытия речи.

4. КОНТРОЛЬНАЯ РАБОТА

4.1. Общие положения

По дисциплине «Радиоэлектронные системы защиты объектов и информации» выполняется одна контрольная работа в 11 семестре.

Цель выполнения контрольной работы — формирование у студентов комплексного подхода к решению задач создания систем охраны объектов и информации, практическое закрепление и систематизация изученного материала.

Задачи сгруппированы по вариантам. Вариант задачи выбирается по последней цифре (***n***) номера зачетной книжки.

Контрольная работа выполняется на листах формата А4. На титульном листе указываются: фамилия, имя, отчество студента; номер учебной группы; номер зачетной книжки; название дисциплины; адрес студента, если контрольная отсылается по почте.

Контрольная работа оформляется в соответствии с требованиями, изложенными в методических указаниях [7]. Ответы на теоретические вопросы должны быть полными, отражающими суть излагаемого материала. Расчеты обязательно должны сопровождаться пояснениями выполняемых операций. Необходимые рисунки, графики, диаграммы выполняются с применением чертежных принадлежностей либо персональной ЭВМ.

Обязательны ссылки на используемую литературу. Перечень ссылок, оформленный в соответствии с требованиями, приводится в конце выполненной контрольной работы.

В конце работы должны быть подпись и дата отправления выполненного задания.

4.2. Задание 1

Вариант 1

1) Предложить мероприятия по обеспечению комплексной защиты объекта и информации в офисе предприятия, занимающего один из этажей многоэтажного здания.

2) Описать способы противодействия утечке акустической информации.

Вариант 2

1) Предложить мероприятия по обеспечению комплексной защиты объекта и информации в офисе предприятия, занимающего отдельное строение, без прилегающей территории.

2) Описать виды, состав и назначение средств защиты телефонных линий.

Вариант 3

1) Предложить мероприятия по обеспечению комплексной защиты объекта и информации на предприятии, обладающем обширной прилегающей территорией.

2) Описать состав и назначение систем охранной сигнализации, типы датчиков, применяемых для защиты внешнего рубежа охраны.

Вариант 4

1) Предложить мероприятия по обеспечению комплексной защиты объекта и информации в кабинете руководителя предприятия.

2) Описать назначение и принцип действия нелинейного локатора.

Вариант 5

1) Предложить мероприятия по обеспечению комплексной защиты объекта и информации в личном доме руководителя предприятия.

2) Описать состав и назначение системы «интеллектуальное здание».

Вариант 6

1) Предложить мероприятия по обеспечению комплексной защиты объекта и информации в производственных помещениях.

2) Описать виды, состав и назначение систем контроля доступа.

Вариант 7

1) Предложить мероприятия по обеспечению комплексной защиты объекта и информации в торговом центре.

2) Описать состав и назначение системы видеонаблюдения.

Вариант 8

1) Предложить мероприятия по обеспечению комплексной защиты объекта и информации в вычислительном центре предприятия.

2) Описать основные принципы создания «политики безопасности».

Вариант 9

1) Предложить мероприятия по обеспечению комплексной защиты объекта и информации в лабораториях учебного заведения.

2) Описать состав и назначение систем охранной сигнализации, типы датчиков, применяемых для защиты внутреннего объема помещения.

Вариант 0

1) Предложить мероприятия по обеспечению комплексной защиты объекта и информации в зале совещаний.

2) Описать виды, состав и назначение средств радиомониторинга.

Примечание. По согласованию с преподавателем тема этого задания может быть заменена, с учетом места работы студента.

4.3. Задание 2

Зашифруйте свои фамилию, имя и отчество различными способами, укажите выбранный ключ.

Для четных ***n***

— с помощью метода перестановки (маршрутная транспозиция);

— с помощью метода подстановки (метод Виженера);

— с помощью метода гаммирования;

— с помощьюнесимметричного метода с открытым ключом.

Для нечетных ***n***

— с помощью метода перестановки (метод Кардано);

— с помощью метода подстановки (шифрование по книге);

— с помощью метода гаммирования;

— с помощью несимметричного метода с открытым ключом.

4.4. Указания к выполнению контрольной работы

4.4.1. При выполнении первого задания необходимо:

— самостоятельно выделить защищаемые объекты и информацию, определить необходимость защиты людей;

— определить, какие угрозы наиболее существенны;

— описать комплекс возможных мероприятий по защите объекта и информации. Необходимо привести состав и краткое описание выбранных систем охранной и пожарной сигнализации, контроля доступа, видеонаблюдения, контроля линий связи и эфира, средств закрытия речи, если они применены. Желательно предусмотреть возможность контроля рабочего времени и интеллектуальное управление системами жизнеобеспечения здания.

Одну из систем (вопрос 2) рассмотреть более продробно, с указанием применяемых видов датчиков, средств аутентификации, средств мониторинга и т.п. Описать принцип действия. Желательно привести примеры конкретных моделей оборудования.

Ориентировочный объем каждого задания — 2…3 стр.

4.4.2. При выполнении второго задания опирайтесь на следующие сведения.

Разбиение сообщения на слова облегчает процесс дешифровки, поэтому свои фамилию, имя, отчество надо представить без пробелов; оставшиеся пустыми клетки таблиц, как правило, заполняют произвольными знаками. При выполнении каждого задания контрольной работы ключ может выбираться произвольно, он **должен быть** приведен в тексте работы.

Тип шифра — перестановка

а) Маршрутная транспозиция

Сообщение последовательно побуквенно записывается в прямоугольную таблицу, столбцы которой затем переставляются заданным образом. Количество столбцов и порядок перестановок определяется ключом — например, алфавитным порядком следования букв в некотором слове. Выберем в качестве ключа слово "шифр". Это слово содержит 4 буквы, значит, в таблице должно быть 4 столбца. Алфавитный порядок следования букв: 4132.

Расшифруйте: ПКИРРТГОЯАИФ.

б) Метод Кардано

Сообщение побуквенно записывается в открытые ячейки прямоугольной таблицы, форма которой определяется специальной карточкой с отверстиями — решеткой Кардано (см. Приложение А) При поворачивании карточки в определенной последовательности, закрываются все клетки поля, кроме тех, в которых просматривается очередной отрывок сообщения.

Расшифруйте: СШПОИВТЕКФРАЕАНР.

Тип шифра — подстановка

а) Шифр Виженера (полиалфавитная замена)

Над буквами сообщения записывают повторяющееся слово или словосочетание — ключ. По буквам верхней строки определяют столбец в таблице Виженера (Приложение Б), по букве нижней строки — строку этой таблицы. В криптограмму записывают букву, стоящую на пересечении выбранных столбца и строки. Например, выбираем ключ «ВИЖЕНЕР».

Расшифруйте: ГЫКААКТПРТЕАКЫЭХК.

б) Шифрование по книге (гомофоническая замена)

Ключом может служить известный текст — достаточно объемное стихотворение, заданная страница в книге. Каждой букве текста ключа соответствует пара цифр (строка, столбец). Часто встречающимся буквам соответствует много пар, из которых выбирается любая. Например, выбираем ключ — отрывок стихотворения, приведенный в приложении В.

Расшифруйте: 4,1 3,4 1,16 9,9 3,8 6,4 2,1 1,8 7,8 2,8 3,18 4,5 4,9.

Тип шифра — гаммирование

Открытый текст предварительно преобразуют в двоичный код. С помощью датчика псевдослучайных чисел формируют гамму, числа которой последовательно складываются по модулю 2 с числами исходного текста.

Пример:

В соответствии с приложением Г преобразуем текст «УРА» в двоичный код: 10011 10000 00001.

Выберем гамму (произвольно): 1 3 5 , также преобразуем в двоичный код: 00001 00011 00101

Выполним поэлементное логическое сложение.

Криптограмма: 10010 10011 00100.

Расшифруйте: 00101 00010 01001 01101 00010

При выполнении этого задания выберете в качестве гаммы последовательность цифр, определяющих дату Вашего рождения: 8 цифр: ДДММГГГГ. (Например: «29071980» для 29 июля 1980 года).

Шифрование с открытым ключом (метод *RSA*)

При выполнении этого задания зашифруйте только свою фамилию.

Сначала необходимо сформировать открытый и закрытый ключи:

— выберем два простых числа p и q, так чтобы их произведение $s = p \cdot q$ было больше, чем число знаков алфавита исходного сообщения. Реально используются очень большие числа порядка 10^{150} … 10^{200};

— выберем число d — взаимно простое с результатом умножения $(p-1)(q-1)$;

— определим такое число e, для которого является истинным соотношение

$$e \cdot d \bmod (p-1)(q-1) = 1.$$

Открытым ключом являются числа e и s, а закрытым — числа d и s.

Чтобы зашифровать данные по известному открытому ключу $\{e; s\}$, необходимо

— разбить исходный текст на блоки, каждый из которых представить в виде чисел

$$M(i) = 0,1,2\ldots;$$

— вычислить*

$$C(i) = M(i)^e \bmod(s).$$

Чтобы расшифровать эти данные, необходимо, используя закрытый ключ, выполнить преобразование:

$$M(i) = C(i)^d \bmod(s).$$

Пример.

— Выбираем простые числа p=3 и q=11, тогда s= 33.

— $(p-1)(q-1) = 20 = 2 \cdot 2 \cdot 5$.

— Выбираем $d = 3$.

— Определим число e из условия $e \cdot 3 \bmod(20) = 1$.

$$e = 7.$$

Например, исходному тексту «ЕДА» соответствует «651», если буквы алфавита заменить целыми числами,

$$M(i) = \{6,5,1\}.$$

Вычислим зашифрованные значения каждого символа по формуле

$$C(i) = M(i)^7 \bmod(33).$$

Подставим

$$C(0) = 6^7 \bmod(33) = 30;$$

$$C(1) = 5^7 \bmod(33) = 14;$$

$$C(2) = 1^7 \bmod(33) = 1.$$

Криптограмма «301401».

Примечание*:

За результат операции ($A \bmod B$) принимается остаток от целочисленного деления A на B (вычет).

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Хорошко В. А. Методы и средства защиты информации/ В. А. Хорошко, А. А. Чекатков; Под ред. Ю. С. Ковтанюк. — К.: ЮНИОР, 2003. — 505 с.

2. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты/ В.В. Домарев. — М.; СПб.; К.: ДиаСофт , 2002. — 671с.

3. Пазизин С. В. Основы защиты информации в компьютерных системах: учеб. пособие для студ. вузов/ С. В. Пазизин. — М.: Науч. изд - во "ТВП", 2003. — 178 с.

4. Баричев С. Г. Основы современной криптографии: учеб. курс/ С. Г. Баричев, В. В. Гончаров, Р. Е. Серов. — 2-е изд., перераб. и доп. — М.: Горячая линия — Телеком, 2002. — 176 с.

5. Петраков А.В. Основы практической защиты информации: учеб. пособие / А.В. Петраков. — 3-е изд. — М.: Радио и связь, 2001. — 360 с.

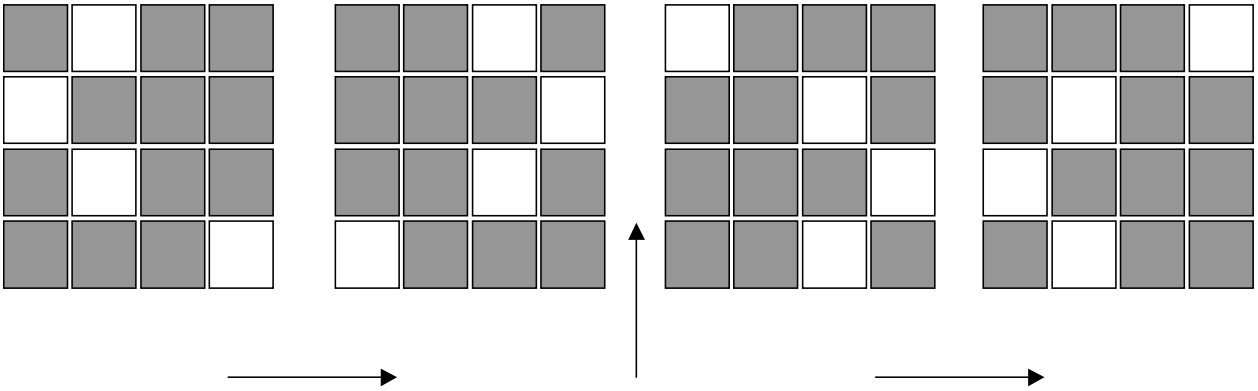
6. Технические методы и средства защиты информации/ Ю.Н. Максимов, В.Г., В.Г. Петров; Под ред. В.Г. Сонникова. — СПб.: Полигон, 2000. — 314 с.

7. Методические указания по оформлению студенческих работ для студентов дневной и заочной форм обучения направления 7.090701 — «Радиотехника» / В.Г. Слезкин. — Севастополь: Изд-во СевНТУ, 2006. — 15 с.

ПРИЛОЖЕНИЕ А

Карта к методу Кардано

Решетка Кардано — это прямоугольная карточка с отверстиями, чаще квадратная, которая при наложении на лист бумаги оставляет открытыми лишь некоторые его части. При последовательном ее поворачивании каждая клетка лежащей под ней таблицы окажется открытой по одному разу.



ПРИЛОЖЕНИЕ Б

Таблица Вижинера к методу полиалфавитной замены

В первой строке **таблицы Виженера** записан весь используемый алфавит, в каждой последующей осуществляется циклический сдвиг на одну букву.

А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я
Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я	А
В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я	А	Б
Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я	А	Б	В
Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я	А	Б	В	Г
Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я	А	Б	В	Г	Д
Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е
З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж
И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З
Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И
К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й
Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К
М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л
Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М
О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н
П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О
Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П
С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р
Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С
У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т
Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У
Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф
Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х
Ч	Ш	Щ	Ь	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц
Ш	Щ	Ь	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч
Щ	Ь	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш
Ь	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ
Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь
Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы
Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э
Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю

ПРИЛОЖЕНИЕ В

Ключ к методу шифрования по книге

Отрывок из поэмы Н. А. Некрасова «Кому на Руси жить хорошо»

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	
1	**В**	**к**	**а**	**к**	**о**	**м**	**г**	**о**	**д**	**у**	**р**	**а**	**с**	**с**	**ч**	**и**	**т**	**ы**	**в**	**а**	**й**	1
2	**В**	**к**	**а**	**к**	**о**	**й**	**з**	**е**	**м**	**л**	**е**	**у**	**г**	**а**	**д**	**ы**	**в**	**а**	**й**			2
3	**Н**	**а**	**с**	**т**	**о**	**л**	**б**	**о**	**в**	**о**	**й**	**д**	**о**	**р**	**о**	**ж**	**е**	**н**	**ь**	**к**	**е**	3
4	**С**	**о**	**ш**	**л**	**и**	**с**	**ь**	**с**	**е**	**м**	**ь**	**м**	**у**	**ж**	**и**	**к**	**о**	**в**				4
5	**С**	**е**	**м**	**ь**	**в**	**р**	**е**	**м**	**е**	**н**	**н**	**о**	**о**	**б**	**я**	**з**	**а**	**н**	**н**	**ы**	**х**	5
6	**П**	**о**	**д**	**т**	**я**	**н**	**у**	**т**	**о**	**й**	**г**	**у**	**б**	**е**	**р**	**н**	**и**	**и**				6
7	**У**	**е**	**з**	**д**	**а**	**Т**	**е**	**р**	**п**	**и**	**г**	**о**	**р**	**е**	**в**	**а**						7
8	**П**	**у**	**с**	**т**	**о**	**п**	**о**	**р**	**о**	**ж**	**н**	**е**	**й**	**в**	**о**	**л**	**о**	**с**	**т**	**и**		8
9	**И**	**з**	**с**	**м**	**е**	**ж**	**н**	**ы**	**х**	**д**	**е**	**р**	**е**	**в**	**е**	**н**	**ь**					9
10	**З**	**а**	**п**	**л**	**а**	**т**	**о**	**в**	**а**	**Д**	**ы**	**р**	**я**	**в**	**и**	**н**	**а**					10
11	**Р**	**а**	**з**	**у**	**т**	**о**	**в**	**а**	**З**	**н**	**о**	**б**	**и**	**ш**	**и**	**н**	**а**					11
12	**Г**	**о**	**р**	**е**	**л**	**о**	**в**	**а**	**Н**	**е**	**е**	**л**	**о**	**в**	**а**							12
13	**Н**	**е**	**у**	**р**	**о**	**ж**	**а**	**й**	**к**	**а**	**т**	**о**	**ж**									13
14	**С**	**о**	**ш**	**л**	**и**	**с**	**я**	**и**	**з**	**а**	**с**	**п**	**о**	**р**	**и**	**л**	**и**					14
15	**К**	**о**	**м**	**у**	**ж**	**и**	**в**	**е**	**т**	**с**	**я**	**в**	**е**	**с**	**е**	**л**	**о**					15
16	**В**	**о**	**л**	**ь**	**г**	**о**	**т**	**н**	**о**	**н**	**а**	**Р**	**у**	**с**	**и**							16
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	

ПРИЛОЖЕНИЕ Г

Русский алфавит в двоичном представлении

А – 1 – 00001	Б – 2 – 00010	В – 3 – 00011
Г – 4 – 00100	Д – 5 – 00101	Е – 6 – 00110
Ж – 7 – 00111	З – 8 – 01000	И – 9 – 01001
К – 10 – 01010	Л – 11– 01011	М – 12 – 01100
Н – 13 – 01101	О – 14 – 01110	П – 15 – 01111
Р – 16 – 10000	С – 17 – 10001	Т – 18 – 10010
У – 19 – 10011	Ф – 20 – 10100	Х – 21 – 10101
Ц – 22 – 10110	Ч – 23 –10111	Ш – 24 – 11000
Щ – 25 –11001	ь – 26 – 11010	ы – 27 – 11011
ъ – 28 – 11100	Э – 29 – 11101	Ю – 30 – 11110
	Я – 31 – 11111	