МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ

«БРАТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Кафедра управления в технических системах

УТВЕРЖДАЮ:
Проректор по учебной работе
_____ Е.И. Луковникова
«_____» _____ 201__ г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ ИНФОКОММУНИКАЦИОННЫЕ СИСТЕМЫ В ИНТЕРНЕТЕ

Б1.В.ДВ.07.02

НАПРАВЛЕНИЕ ПОДГОТОВКИ

11.03.02 Инфокоммуникационные технологии и системы связи

ПРОФИЛЬ ПОДГОТОВКИ
Многоканальные телекоммуникационные системы

Программа академического бакалавриата

Квалификация (степень) выпускника: бакалавр

СОДЕРЖАНИЕ ПРОГРАММЫ Стр.

1. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Вид деятельности выпускника

Дисциплина охватывает круг вопросов, относящихся к экспериментально-исследовательскому виду профессиональной деятельности выпускника в соответствии с компетенциями и видами деятельности, указанными в учебном плане.

Цель дисциплины

Формирование у обучающихся профессиональных компетенций в области построения и функционирования сетей передачи данных, базовых технологий организации локальных и территориальных компьютерных сетей.

Задачи дисциплины

Формирование знаний, умений и навыков, позволяющих проводить самостоятельный анализ сетевых технологий глобальных сетей,

Код компетенции	Содержание компетенций	Перечень планируемых результатов обучения по дисциплине
1	2	3
ПК-9	умение проводить расчеты по проекту сетей, сооружений и средств инфокоммуникаций в соответствии с техническим заданием с использованием как стандартных методов, приемов и средств автоматизации проектирования, так и самостоятельно создаваемых оригинальных	**знать:** - основы цифровой вычислительной техники, структуры и функционирование локальных вычислительных сетей и глобальной сети Интернет, основные закономерности передачи информации в инфокоммуникационных системах, основные виды сигналов, используемых в телекоммуникационных системах, особенности передачи различных сигналов по каналам и тракам телекоммуникационных систем; **уметь:** - формулировать основные технические требования к телекоммуникационным сетям и систем, оценивать основные проблемы, связанные с эксплуатацией и внедрением новой телекоммуникационной техники; **владеть:** - начальными навыками разработки и отладки с использованием соответствующих отладочных средств программного обеспечения сигнальных процессов и микроконтроллеров.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина Б1.В.ДВ.07.02 Инфокоммуникационные системы в интернете относится к дисциплинам по выбору

Дисциплина Инфокоммуникационные системы в интернете базируется на знаниях, полученных при изучении дисциплин Основы построения инфокоммуникационных систем и сетей, Моделирование сетей связи, Вычислительная техника и информационные технологии.

Основываясь на изучении перечисленных дисциплин, Инфокоммуникационные системы в интернете представляет основу для производственной (преддипломная) практики и подготовки к государственной итоговой аттестации.

Такое системное междисциплинарное изучение направлено на достижение требуемого ФГОС уровня подготовки по квалификации бакалавр.

3. РАСПРЕДЕЛЕНИЕ ОБЪЕМА ДИСЦИПЛИНЫ

3.1. Распределение объема дисциплины по формам обучения

Форма обучения	*Курс*	*Семестр*	*Трудоемкость дисциплины в часах*						*Контрольная работа*	*Вид промежуточной аттестации*
			Всего часов (с экз.)	*Аудиторных часов*	*Лекции*	*Лабораторные работы*	*Практические занятия*	*Самостоятельная работа*		
1	2	3	4	5	6	7	8	9	10	11
Очная	4	7	144	51	17	17	17	39	-	Экзамен
Заочная	-	-	-	-	-	-	-	-	-	-
Заочная(ускоренное обучение)	-	-	-	-	-	-	-	-	-	-
Очно-заочная	-	-	-	-	-	-	-	-	-	-

3.2. Распределение объема дисциплины по видам учебных занятийи трудоемкости

Вид учебных занятий	*Трудо-емкость (час.)*	*в т.ч. в интерактивной, активной, иннова-ционнойформах, (час.)*	*Распределение по семестрам, час*
			7
1	2	3	4
I. Контактная работа обучающихся с преподавателем (всего)	51	12	51
Лекции (Лк)	17	4	17
Лабораторные работы (ЛР)	17	4	17
Практические занятия (ПЗ)	17	4	17
Консультации	+	-	+
II.Самостоятельная работа обучающихся (СР)	39	-	39
Подготовка к лабораторным работам	10	-	10
Подготовка к практическим занятиям	10	-	10
Подготовка к экзамену в течение семестра	19	-	19
III. Промежуточная аттестация экзамен	54	-	54
Общая трудоемкость дисциплины час.	144	-	144
зач. ед.	4	-	4

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1. Распределение разделов дисциплины по видам учебных занятий - для очной формы обучения:

№ раз-дела и темы	*Наименование раздела и тема дисциплины*	*Трудоем-кость, (час.)*	*Виды учебных занятий, включая самостоятельную работу обучающихся и трудоемкость; (час.)*			
			учебные занятия			*самостоя тельная работа обучаю-щихся*
			лекции	*лабораторные работы*	*практиче ские работы*	
1	2	3	4	5	6	7
1.	**Информационная безопасность**	**13**	**4**	**-**	**-**	**9**
1.1.	Введение в информационную безопасность	6	2	-	-	4
1.2.	Модель сетевой безопасности .Классификация сетевых атак	7	2	-	-	5
2.	**Защита информации при помощи криптографии**	**23**	**4**	**9**	**-**	**10**
2.1.	Защита передаваемых и хранимых секретных данных от разглашения и искажения	11,5	2	4.5	-	5
2.2.	Задача подтверждения авторства сообщения	11,5	2	4.5	-	5
3.	**Классификация шифров**	**17**	**4**	**3**		**10**
3.1.	Перестановочные шифры	8	2	1		5
3.2.	Классификация методов дешифрования. Модель предполагаемого противника. Правила Керкхоффа	9	2	2		5
4.	**Криптосистемы**	**37**	**5**	**5**	**17**	**10**
4.1.	Устройство шифров	8	2	-	4	2
4.2.	Поточные шифры	13	2	5	4	2
4.3.	Алгоритм DES	7,5	0.5	-	4	3
4.4.	Алгоритм ГОСТ 28147	8.5	0.5	-	5	3
	ИТОГО	**90**	**17**	**17**	**17**	**39**

4.2. Содержание дисциплины, структурированное по разделам и темам

1. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ.

Введение в информационную безопасность

За несколько последних десятилетий требования к информационной безопасности существенно изменились. До начала широкого использования автоматизированных систем обработки данных безопасность информации достигалась исключительно физическими и административными мерами. С появлением компьютеров стала очевидной необходимость использования автоматических средств защиты файлов данных и программной среды. Следующий этап развития автоматических средств защиты связан с появлением распределенных систем обработки данных и компьютерных сетей, в которых средства сетевой безопасности используются в первую очередь для защиты передаваемых по сетям данных. В наиболее полной трактовке под средствами сетевой безопасности мы будем иметь в виду меры предотвращения нарушений безопасности, которые возникают при передаче информации по сетям, а также меры, позволяющие определять, что такие нарушения безопасности имели место. Именно изучение средств сетевой безопасности и связанных с ними теоретических и прикладных проблем, составляет основной материал книги.

Термины "безопасность информации" и "защита информации" отнюдь не являются синонимами. Термин "безопасность" включает в себя не только понятие защиты, но также и *аутентификацию*, аудит, обнаружение проникновения.

Перечислим некоторые характерные проблемы, связанные с безопасностью, которые возникают при использовании компьютерных сетей:

1. Фирма имеет несколько офисов, расположенных на достаточно большом расстоянии друг от друга. При пересылке конфиденциальной информации по общедоступной сети (например, Internet) необходимо быть уверенным, что никто не сможет ни подсмотреть, ни изменить эту информацию.
2. Сетевой администратор осуществляет удаленное управление компьютером. Пользователь перехватывает управляющее сообщение, изменяет его содержание и отправляет сообщение на данный компьютер.
3. Пользователь несанкционированно получает доступ к удаленному компьютеру с правами законного пользователя, либо, имея право доступа к компьютеру, получает доступ с гораздо большими правами.
4. Фирма открывает *Internet*-магазин, который принимает оплату в электронном виде. В этом случае продавец должен быть уверен, что он отпускает товар, который действительно оплачен, а покупатель должен иметь гарантии, что он, во-первых, получит оплаченный товар, а во-вторых, номер его кредитной карточки не станет никому известен.
5. Фирма открывает свой сайт в *Internet*. В какой-то момент содержимое сайта заменяется новым, либо возникает такой поток и такой способ обращений к сайту, что сервер не справляется с обработкой запросов. В результате обычные посетители сайта либо видят информацию, не имеющую к фирме никакого отношения, либо просто не могут попасть на сайт фирмы.

Рассмотрим основные понятия, относящиеся к информационной безопасности, и их взаимосвязь.

Собственник определяет множество **информационных ценностей**, которые должны быть защищены от различного рода *атак*. *Атаки* осуществляются *противниками* или *оппонентами*, использующими различные *уязвимости* в защищаемых ценностях. Основными нарушениями безопасности являются раскрытие информационных ценностей (потеря *конфиденциальности*), их неавторизованная модификация (потеря *целостности*) или неавторизованная потеря доступа к этим ценностям (потеря *доступности*).

Собственники информационных ценностей анализируют *уязвимости* защищаемых ресурсов и возможные *атаки*, которые могут иметь место в конкретном окружении. В результате такого анализа определяются *риски* для данного набора информационных ценностей. Этот анализ определяет выбор контрмер, который задается политикой безопасности и обеспечивается с помощью *механизмов* и *сервисов безопасности*. Следует

учитывать, что отдельные *уязвимости* могут сохраниться и после применения *механизмов* и *сервисов безопасности*. ***Политика безопасности*** определяет согласованную совокупность *механизмов* и *сервисов безопасности*, адекватную защищаемым ценностям и окружению, в котором они используются.

На рис.1.1 показана взаимосвязь рассмотренных выше понятий информационной безопасности. Дадим следующие определения:

Уязвимость - слабое место в системе, с использованием которого может быть осуществлена *атака*.

Риск - вероятность того, что конкретная *атака* будет осуществлена с использованием конкретной *уязвимости*. В конечном счете, каждая организация должна принять решение о допустимом для нее уровне *риска*. Это решение должно найти отражение в политике безопасности, принятой в организации.

Политика безопасности - правила, директивы и практические навыки, которые определяют то, как информационные ценности обрабатываются, защищаются и распространяются в организации и между информационными системами; набор критериев для предоставления *сервисов безопасности*.

Атака - любое действие, нарушающее безопасность информационной системы. Более формально можно сказать, что *атака* - это действие или последовательность связанных между собой действий, использующих *уязвимости* данной информационной системы и приводящих к нарушению политики безопасности.

Рис. 1.1. Взаимосвязь основных понятий безопасности информационных систем

Механизм безопасности - программное и/или аппаратное средство, которое определяет и/или предотвращает *атаку*.

Сервис безопасности - сервис, который обеспечивает задаваемую политикой безопасность систем и/или передаваемых данных, либо определяет осуществление *атаки*. *Сервис* использует один или более механизмов безопасности.

Рассмотрим модель сетевой безопасности и основные типы *атак*, которые могут осуществляться в этом случае. Затем рассмотрим основные типы *сервисов* и *механизмов безопасности*, предотвращающих такие *атаки*.

Модель сетевой безопасности .Классификация сетевых атак

В общем случае существует информационный поток от отправителя (файл, пользователь, компьютер) к получателю (файл, пользователь, компьютер):

Все *атаки* можно разделить на два класса: *пассивные* и *активные*.

I. Пассивная атака

Пассивной называется такая ***атака***, при которой *противник* не имеет возможности модифицировать передаваемые сообщения и вставлять в информационный канал между отправителем и получателем свои сообщения. Целью *пассивной атаки* может быть только прослушивание передаваемых сообщений и анализ трафика.

Активной называется такая ***атака***, при которой *противник* имеет возможность модифицировать передаваемые сообщения и вставлять свои сообщения. Различают следующие типы *активных атак*:

II. Активная атака

Отказ в обслуживании - *DoS-атака (DenialofService)*

Отказ в обслуживании нарушает нормальное функционирование сетевых сервисов. *Противник* может перехватывать все сообщения, направляемые определенному адресату. Другим примером подобной *атаки* является создание значительного трафика, в результате чего сетевой сервис не сможет обрабатывать запросы законных клиентов. Классическим примером такой *атаки* в сетях TCP/IP является SYN-атака, при которой нарушитель посылает пакеты, инициирующие установление TCP-соединения, но не посылает пакеты, завершающие установление этого соединения. В результате может произойти переполнение памяти на сервере, и серверу не удастся установить соединение с законными пользователями.

Модификация потока данных - *атака "maninthemiddle"*

Модификация потока данных означает либо изменение содержимого пересылаемого сообщения, либо изменение порядка сообщений.

1. **Создание ложного потока (фальсификация)**

Фальсификация (нарушение аутентичности) означает попытку одного субъекта выдать себя за другого.

Повторное использование

Повторное использование означает пассивный захват данных с последующей их пересылкой для получения несанкционированного доступа - это так называемая***replay-атака***. На самом деле *replay-атаки* являются одним из вариантов фальсификации, но в силу того, что это один из наиболее распространенных вариантов *атаки* для получения несанкционированного доступа, его часто рассматривают как отдельный тип *атаки*.

Перечисленные *атаки* могут существовать в любых типах сетей, а не только в сетях, использующих в качестве транспорта протоколы TCP/IP, и на любом уровне модели OSI. Но в сетях, построенных на основе TCP/IP, *атаки* встречаются чаще всего, потому что, во-первых, Internet стал самой распространенной сетью, а во-вторых, при разработке протоколов TCP/IP требования безопасности никак не учитывались.

Сервисы безопасности

Основными *сервисами безопасности* являются следующие:

Конфиденциальность - предотвращение *пассивных атак* для передаваемых или хранимых данных.

Аутентификация - подтверждение того, что информация получена из законного источника, и получатель действительно является тем, за кого себя выдает. В случае передачи единственного сообщения *аутентификация* должна гарантировать, что получателем сообщения является тот, кто нужно, и сообщение получено из заявленного источника. В случае установления соединения имеют место два аспекта. Во-первых, при инициализации соединения *сервис* должен гарантировать, что оба участника являются требуемыми. Во-вторых, *сервис* должен гарантировать, что на соединение не воздействуют таким образом, что *третья сторона* сможет маскироваться под одну из легальных сторон уже после установления соединения.

Целостность - *сервис*, гарантирующий, что информация при хранении или передаче не изменилась. Может применяться к потоку сообщений, единственному сообщению или отдельным полям в сообщении, а также к хранимым файлам и отдельным записям файлов.

Невозможность отказа - невозможность, как для получателя, так и для отправителя, отказаться от факта передачи. Таким образом, когда сообщение отправлено, получатель может убедиться, что это сделал легальный отправитель. Аналогично, когда сообщение пришло, отправитель может убедиться, что оно получено легальным получателем.

Контроль доступа - возможность ограничить и контролировать доступ к системам и приложениям по коммуникационным линиям.

Доступность - результатом *атак* может быть потеря или снижение доступности того или иного сервиса. Данный *сервис* предназначен для того, чтобы минимизировать возможность осуществления *DoS-атак*.

Механизмы безопасности

Перечислим основные *механизмы безопасности*:

Алгоритмы симметричного шифрования - алгоритмы шифрования, в которых для шифрования и дешифрования используется один и тот же ключ или ключ дешифрования легко может быть получен из ключа шифрования.

Алгоритмы асимметричного шифрования - алгоритмы шифрования, в которых для шифрования и дешифрования используются два разных ключа, называемые открытым и закрытым ключами, причем, зная один из ключей, вычислить другой невозможно.

Хэш-функции - функции, входным значением которых является сообщение произвольной длины, а выходным значением - сообщение фиксированной длины. *Хэш-функции* обладают рядом свойств, которые позволяют с высокой долей вероятности определять изменение входного сообщения.

Модель сетевого взаимодействия

Модель безопасного сетевого взаимодействия в общем виде можно представить следующим образом:

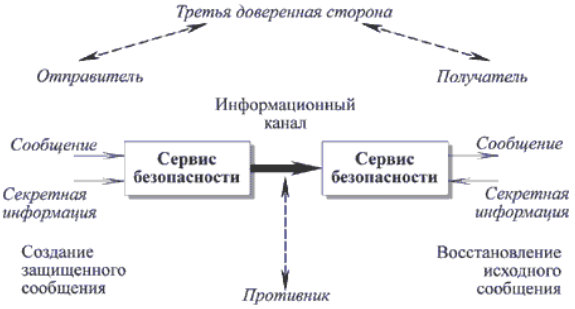

Рис. 1.8. Модель сетевой безопасности

Сообщение, которое передается от одного участника другому, проходит черезразличного рода сети. При этом будем считать, что устанавливается логический информационный канал от отправителя к получателю с использованием различных коммуникационных протоколов (например, TCP/IP).

Средства безопасности необходимы, если требуется защитить передаваемую информацию от *противника*, который может представлять угрозу *конфиденциальности*, *аутентификации*, *целостности* и т.п. Все технологии повышения безопасности имеют два компонента:

1. Относительно безопасная передача информации. Примером является шифрование, когда сообщение изменяется таким образом, что становится нечитаемым для *противника*, и, возможно, дополняется кодом, который основан на содержимом сообщения и может использоваться для *аутентификации* отправителя и обеспечения *целостности* сообщения.
2. Некоторая секретная информация, разделяемая обоими участниками и неизвестная *противнику*. Примером является ключ шифрования.

Кроме того, в некоторых случаях для обеспечения безопасной передачи бывает необходима *третья доверенная сторона* (thirdtrustedparty - TTP). Например, *третья сторона* может быть ответственной за распределение между двумя участниками секретной информации, которая не стала бы доступна *противнику*. Либо *третья сторона* может использоваться для решения споров между двумя участниками относительно достоверности передаваемого сообщения.

Из данной общей модели вытекают три основные задачи, которые необходимо решить при разработке конкретного *сервиса безопасности*:

1. Разработать алгоритм шифрования/дешифрования для выполнения безопасной передачи информации. Алгоритм должен быть таким, чтобы *противник* не мог расшифровать перехваченное сообщение, не зная секретную информацию.
2. Создать секретную информацию, используемую алгоритмом шифрования.

3. Разработать протокол обмена сообщениями для распределения разделяемой секретной информации таким образом, чтобы она не стала известна *противнику*.

Модель безопасности информационной системы

Существуют и другие относящиеся к безопасности ситуации, которые не соответствуют описанной выше модели сетевой безопасности. Общую модель этих ситуаций можно проиллюстрировать следующим образом:

Данная модель иллюстрирует концепцию безопасности информационной системы, с помощью которой предотвращается нежелательный доступ. Хакер, который пытается осуществить незаконное проникновение в системы, доступные по сети, может просто получать удовольствие от взлома, а может стараться повредить информационную систему и/или внедрить в нее что-нибудь для своих целей. Например, целью хакера может быть получение номеров кредитных карточек, хранящихся в системе.

Другим типом нежелательного доступа является размещение в вычислительной системе чего-либо, что воздействует на прикладные программы и программные утилиты, такие как редакторы, компиляторы и т.п. Таким образом, существует два типа *атак*:

1. Доступ к информации с целью получения или модификации хранящихся в системе данных.
2. *Атака* на сервисы, чтобы помешать использовать их.

Вирусы и черви - примеры подобных *атак*. Такие *атаки* могут осуществляться как с помощью дискет, так и по сети.

Сервисы безопасности, которые предотвращают нежелательный доступ, можно разбить на две категории:

1. Первая категория определяется в терминах сторожевой функции. Эти *механизмы* включают процедуры входа, основанные, например, на использовании пароля, что позволяет разрешить доступ только авторизованным пользователям. Эти *механизмы* также включают различные защитные экраны (firewalls), которые предотвращают *атаки* на различных уровнях стека протоколов TCP/IP, и, в частности, позволяют предупреждать проникновение червей, вирусов, а также предотвращать другие подобные *атаки*.
2. Вторая линия обороны состоит из различных внутренних мониторов, контролирующих доступ и анализирующих деятельность пользователей.

Одним из основных понятий при обеспечении безопасности информационной системы является понятие ***авторизации*** - определение и предоставление прав доступа к конкретным ресурсам и/или объектам.

В основу безопасности информационной системы должны быть положены следующие основные принципы:

1. Безопасность информационной системы должна соответствовать роли и целям организации, в которой данная система установлена.
2. Обеспечение информационной безопасности требует комплексного и целостного подхода.
3. Информационная безопасность должна быть неотъемлемой частью системы управления в данной организации.
4. Информационная безопасность должна быть экономически оправданной.
5. Ответственность за обеспечение безопасности должна быть четко определена.
6. Безопасность информационной системы должна периодически переоцениваться.
7. Большое значение для обеспечения безопасности информационной системы имеют социальные факторы, а также меры административной, организационной и физической безопасности.

Интерактив 2 часа (фильма + обсуждение)

2. ЗАЩИТА ИНФОРМАЦИИ ПРИ ПОМОЩИ КРИПТОГРАФИИ

Как было отмечено ранее, злоумышленник в криптографии есть персонифицированный набор целей по отклонению информационного процесса от его штатного протекания, и возможностей по достижению этих целей. Рассмотрение проблемы ведется в предположении, что злоумышленник действует наилучшим возможным в его ситуации образом. В качестве злоумышленников могут выступать:

- законные участники процесса;
- субъекты, не являющиеся законными участниками процесса, но имеющие доступ к информации, передаваемой и обрабатываемой в ходе осуществления информационного взаимодействия и могущие повлиять на его протекание.

Если законные участники процесса не могут выступать в качестве злоумышленников, такой процесс называется "**информационным взаимодействием со взаимным доверием сторон друг другу**", понятно, что в противном имеет место "**процесс информационного взаимодействия в условии отсутствия взаимного доверия сторон**". Классы методов защиты процессов обоих типов существенно отличаются друг от друга, вторая задача сложнее - общеизвестно, что практически любую систему намного легче защитить от проникновения извне, чем от злоумышленных действий со стороны ее законных пользователей.

Надо отметить, что когда речь идет о **взаимном доверии сторон**, имеется в виду нечто большее, чем просто отношение субъектов информационного взаимодействия друг к другу. При определении этого должны рассматриваться многие факторы, например среда и окружение, в которых они работают. Для иллюстрации сказанного рассмотрим задачу защиты программного обеспечения компьютерных систем от несанкционированной модификации, которая обычно решается следующим образом:
1. При инсталляции и "легальной" модификации программ для каждой защищаемой единицы (обычно это исполняемый файл) вырабатывается контрольный код, являющийся "дальним родственником" обыкновенной контрольной суммы.

3. В соответствии с некоторым регламентом (например, при каждой загрузке системы, или один раз в определенный промежуток времени, или перед запуском программы на выполнение) проверяется соответствие защищаемой единицы контрольному коду.

Если компьютер действительно персональный, то оба эти действия выполняет один и тот же человек, но требования к "чистоте" среды совершенно различные. Первое действие выполняется при добавлении в систему нового программного обеспечения или перенастройке уже существующего, что в большинстве реальных узкоспециализированных систем происходит достаточно редко. Необходимым условием выполнения этой операции является отсутствие "закладок" в п/о, вырабатывающем контрольный код. "Чистая" среда обычно создается загрузкой операционной системы с носителя, физически защищенного от записи - единожды сформированного и выверенного, и с тех пор остающегося неизменным.

Второе действие осуществляется значительно чаще, и по определению, может выполняться в не столь "чистой" среде. Поэтому, даже если обе процедуры выполняет один и тот же человек, с точки зрения задачи это все равно два различных субъекта, и пользователь-создатель контрольного кода не должен доверять пользователю-проверяющему. В силу вышеизложенного для решения данной задачи больше подходят схемы, основанные на электронно-цифровой подписи, эффективно работающие в условиях отсутствия взаимного доверия сторон, нежели использование криптографической контрольной комбинации на основе симметричных шифров.

Задачи, решаемые криптографическими методами, отличаются друг от друга следующим:
- характером защищаемого информационного взаимодействия;
- целями злоумышленников;
- возможностями злоумышленников.

Простейший случай информационного взаимодействия - это передача данных от одного субъекта другому. Соответственно, самая распространенная задача из сферы защиты - защита передаваемой по каналам связи или хранимой в компьютерной системе информации, она исторически самая первая и до сих пор наиболее важная. Впрочем, необходимо добавить, что в последнее время в связи с проникновением электронных технологий во многие сферы жизни человека и общества возникают и принципиально новые проблемы. Одни из них первичны, такие, как уже упомянутая проблема защиты данных в каналах связи. Другие вторичны и существуют только в рамках конкретного решения той или иной первичной задачи. Например, "открытое распределение ключей" - совместная выработка двумя субъектами в ходе сеанса связи по открытому каналу общего секретного ключа таким образом, чтобы злоумышленники, "прослушивающие" канал, не смогли получить тот же

самый ключ.

Рассмотрение задач из сферы криптографии начнем с задачи защиты данных, передаваемых по открытым каналам связи в наиболее полной постановке: В системе имеются две легальные стороны - "отправитель" и "получатель". Информационный процесс заключается в передаче сообщения от первого второму и считается протекающим нормально, если получатель получит сообщение без искажений, кроме него никто не ознакомится с содержанием сообщения, и если стороны не будут выставлять претензий друг другу. В задаче также присутствует злоумышленник, имеющий доступ к каналу передачи данных и стремящийся добиться отклонений от нормального течения процесса. Кроме того, каждая из легальных сторон может предпринять злоумышленные действия в отношении другой стороны. Перечислим возможные угрозы:

1. **Угрозы со стороны злоумышленника.**
1.1. Ознакомление с содержанием переданного сообщения.
1.2. Навязывание получателю ложного сообщения - как полная его фабрикация, так и внесение искажений в действительно переданное сообщение.
1.3. Изъятие переданного отправителем сообщения из системы таким образом, чтобы получатель не узнал о факте передачи сообщения;
1.4. Создание помех для нормальной работы канала передачи связи, то есть нарушение работоспособности канала связи.
2. **Угрозы со стороны законного отправителя сообщения:**
2.1. Разглашение переданного сообщения.
2.2. Отказ от авторства в действительности переданного им сообщения.
2.3. Утверждение, что некоторое сообщение отправлено получателю когда в действительности отправка не производилась.
3. **Угрозы со стороны законного получателя сообщения:**
3.1. Разглашение полученного сообщения.
3.2. Отказ от факта получения некоторого сообщения когда в действительности оно было им получено.
3.3. Утверждение, что некоторое сообщение получено от отправителя когда в действительности предъявленное сообщение сфабриковано самим получателем.

Как правило, угроза работоспособности канала связи (угроза 1.4) наиболее эффективно достигается нарушением физической среды передачи данных (разрушение линий передачи и узлов обработки данных) или созданием помех ("глушение" радиосигнала, бомбардировка системы большим количеством ложных сообщений - "спам", и т.д.). Близко к ней находится угроза 1.3 - изъятие сообщения из канала связи. Эффективной защиты криптографическими средствами от этих угроз не существует, поэтому они обычно не рассматривается в работах по криптографии, проблема решается другими методами. Так, для устранения угрозы 1.3 обычно используется квитирование - высылка получателем отправителю квитанции (подтверждения) на полученное сообщение. Также в рамках криптографии отсутствует решение, которое бы устранило угрозы 2.1 и 3.1 - разглашение секретных данных одной из легальных сторон со "списыванием" этого на другую сторону или на ненадежность канала связи.
Оказалось, что сформулированная выше задача за вычетом угроз 1.3, 1.4, 2.1, 3.1 может быть разделена на три подзадачи, которые решаются независимо друг от друга и характеризуются собственными наборами угроз из приведенного списка:

- "классическая задача криптографии" - защита данных от разглашения и искажения при передаче по открытому каналу связи;
- "подпись электронного документа" - защита от отказа от авторства сообщения;
- "вручение заказного письма" - защита от отказа от факта получения сообщения;

Ниже все три задачи рассмотрены с необходимой степенью подробности.

Защита передаваемых и хранимых секретных данных от разглашения и искажения

Это исторически первая и до сих пор наиболее важная задача криптографии, в ней учитываются угрозы 1.1 и 1.2 из приведенного выше списка. "Классическая" задача возникает, если создание и использование массивов данных разделены во времени и/или в пространстве, и на своей пространственно-временной "линии жизни" информация оказывается в зоне досягаемости злоумышленника. В первом случае говорят о защите данных при хранении, во втором - при передаче. При достаточной общности каждый из вариантов задачи имеет свои особенности, соответственно и методы решения также могут отличаться. В задаче присутствуют две легальные стороны:

- отправитель или источник сообщения (О, назовем его Олегом, чтобы избежать фраз типа "отправитель отправляет, а получатель получает");
- получатель или приемник сообщения (П, назовем его Петром);

Между отправителем и получателем сообщения есть взаимное доверие, поэтому в качестве злоумышленника может выступать только субъект, отличный от них обоих (З, назовем его Захаром). Олег отправляет Петру сообщение, при этом Захар может попытаться выполнить одного или нескольких следующих действий:

(1) чтение сообщений;
(2) внесение изменений в реальное переданное сообщение "на лету";
(3) создание нового сообщения и отправка его Петру от имени Олега;
(4) повторная передача ранее переданного сообщения;
(5) уничтожение переданного сообщения.

Каждое из перечисленных выше действий является **атакой** на наш информационный процесс. Возможности по доступу к каналу передачи, необходимые для их выполнения, различны, и в реальной ситуации может оказаться, что одни атаки осуществимы, а другие - нет. Для реализации атаки №1 необходим доступ к каналу передачи данных на чтение, для атаки №3 - на запись, для атаки №4 - на чтение и запись. Для осуществления атак №№2 и 5 необходим полный контроль над каналом, то есть возможность разорвать его и встроить туда собственные узлы обработки данных, или получить контроль над существующем узлом обработки. Какие из атак доступны злоумышленнику, зависит от конкретных условий протекания информационного процесса - от среды передачи данных, от аппаратуры, которой он располагает, и т.д.. Так, если средой передачи информации служит радиоэфир, осуществление атак №2 и частично №5 (если не рассматривать "глушение") невозможно, доступны только атаки №№1,3,4. При использовании оптоволоконной линии связи злоумышленнику может быть доступна только атака №1 - незаметно "врезаться" в оптоволоконную линию практически невозможно. Некоторые атаки из приведенного списка могут рассматриваться как последовательное осуществление других из того же списка. Так, атака №2 может рассматриваться как последовательное исполнение атак №№1,5,3, а атака № 4 - как исполнение атак №1 и 3, разнесенное по времени.

Подведем итог, постановка "классической" задачи криптографии следующая:

1. Законные стороны информационного процесса - отправитель и получатель сообщения. Задача первого отправить, а второго получить сообщение и понять его содержание. 2. Процесс считается нормально идущим, если к получателю придет именно то сообщение, которое отправил отправитель, и кроме него никто не сможет ознакомиться с его содержанием. Возможны следующие отклонения от его нормального течения:

- передаваемые данные станут известны кому либо еще помимо законного получателя;
- передаваемые данные будут искажены, то есть получатель получит не то или не в точности то, что отправлено отправителем.

4. Между отправителем и получателем есть взаимное доверие и ни один из них не осуществляет злоумышленных действий, злоумышленником является третья сторона, которая ставит перед собой цели ознакомиться с содержанием переданного сообщения или навязать получателю ложное сообщение, полностью сфабриковав его самостоятельно или исказив переданное отправителем сообщение. Злоумышленник имеет доступ к каналу связи и для осуществления своей цели может "слушать" канал или передавать в него свои данные. В наилучшей для себя ситуации злоумышленник может захватить полный контроль над каналом и ему станут доступны любые манипуляции с переданными данными.

Задача подтверждения авторства сообщения.

В этой задаче принимаются во внимание угрозы 2.2 и 3.3 из приведенного выше списка - между отправителем и получателем сообщения отсутствует взаимное доверие и возможно возникновение конфликта по поводу переданных данных. Каждый из них может совершать злоумышленные действия, направленные против другой стороны, и по этой причине в системе необходимо наличие инстанции, которая выполняет "арбитражные" функции, то есть в случае конфликта между абонентами решает, кто из них прав, а кто нет - эта сторона по вполне понятным причинам называется в криптографии "независимым арбитражем". Вместе с тем, злоумышленник как отдельный субъект информационного процесса здесь отсутствует. Опишем задачу по той же схеме:

1. Законные стороны информационного процесса - отправитель и получатель сообщения.
   - отправитель или источник сообщения (О, Олег);
   - получатель или приемник сообщения (П, Петр);
   - независимый арбитр (А, Антон), разрешающий конфликт между Олегом и Петром в случае его возникновения.

Задача первого отправить, а второго получить сообщение и понять его содержание, задача последнего - вынести суждение о том, кто из двух предыдущих участников прав в случае возникновения конфликта между ними.

2. Процесс считается проходящим нормально, если Петр получит именно то сообщение, которое отправил Олег, и стороны не будут предъявлять претензий друг другу касательно переданных данных. Возможны следующие отклонения от нормального течения процесса:
   - отправитель откажется от авторства переданного им сообщения;
   - получатель будет утверждать, что некоторое сообщение получено им от отправителя, хотя в действительности тот его не передавал.

3. Между отправителем и получателем отсутствует взаимное доверие, каждый из них может осуществить злоумышленные действия в отношении другого: Олег может попытаться убедить Антона, что он не отправлял сообщения, которое в действительности отправил Петру. Петр, в свою очередь, может попытаться убедить Антона в том, что он получил некоторое сообщение от Олега, хотя тот его в действительности не отправлял.

Вручение сообщения под расписку.

В этой задаче принимаются во внимание угрозы 2.3 и 3.2 из приведенного выше списка - между отправителем и получателем сообщения отсутствует взаимное доверие и возможно возникновение конфликта по поводу переданных данных. Каждый из них может совершать злоумышленные действия, направленные против другой стороны, злоумышленник как отдельный субъект информационного процесса здесь также отсутствует. Охарактеризуем задачу по нашей схеме:

1. Законные стороны информационного процесса - отправитель и получатель сообщения.
   - отправитель или источник сообщения (О, Олег);
   - получатель или приемник сообщения (П, Петр);

Задача первого отправить, а второго получить сообщение и понять его содержание.

2. Процесс считается проходящим нормально, если получатель ознакомится с содержанием полученного сообщения и стороны не будут предъявлять претензий друг другу касательно переданных данных. Возможны следующие отклонения от нормального течения процесса:
   - отправитель будет утверждать, что передал получателю сообщение, хотя в действительности не отправлял его;
   - получатель ознакомится с содержанием сообщения, но будет утверждать, что никакого сообщения не получал.

3. Между отправителем и получателем отсутствует взаимное доверие, каждый из них может осуществить злоумышленные действия в отношении другого, Петр может утверждать, что он не получал сообщения, которое в действительности получил и прочитал, а Олег, в свою очередь, может утверждать, что Петр прочитал сообщение, хотя в действительности он его не передавал Петру.

Решением этой задачи может являться такая схема информационного взаимодействия,

которая группирует в одну транзакцию два следующих действия, не позволяя ни одному из них осуществиться без другого:

- Олег получает и читает сообщение;
- Петр получает подтверждение о том, что Олег получил сообщение.

Две следующие задачи касаются проблемы обмена ключевой информацией. Для защиты передаваемых по открытым каналам связи данных обычно применяется шифрование, одним из наиболее распространенных вариантов является использование симметричных шифров, то есть шифров с секретным ключом. В таких системах возникает проблема распределения ключевой информации, так как для ее передачи участникам информационного обмена нужен защищенный канал связи. В системах с большим числом абонентов эта проблема превращается в серьезную головную боль администраторов. Способов ее обойти всего два:

- использовать асимметричные алгоритмы шифрования, в которых для процедуры за- и расшифрования используются различные ключи и знание ключа зашифрования не позволяет определить соответствующий ключ расшифрования, поэтому он может быть несекретным и передаваться по открытым каналам связи;
- вырабатывать общий секретный ключ в ходе некоторого сеанса информационного взаимодействия по открытому каналу, организованного таким образом, чтобы ключ было невозможно выработать на основе только перехваченных в канале данных.

Первый подход получил название **асимметричного** или **двухключевого шифрования**, второй - **открытого распределения ключей.**
Вот, пожалуй и все наиболее популярные задачи практической криптографии. Конечно, есть и другие, но они или менее известны, или отсутствует их удовлетворительное решение, или это решение есть, но оно не получило заметного практического применения. Кратко перечислим наиболее известные из этих "теоретических" задач:

1. Синхронный обмен сообщениями. Требуется организовать обмен двух субъектов сообщениями таким образом, чтобы ни один из них, получив сообщение другой стороны, не смог отказаться от передачи своего и не смог сформировать свое сообщение в зависимости от сведений из сообщения другой стороны. В качестве дополнительного условия иногда требуется, чтобы передаваемые сообщения удовлетворяли определенным заранее критериям.

Как вариант предыдущей задачи - проблема "подписи контракта": есть два документа в электронной форме и есть процедура выработки цифровой подписи под документами. Требуется организовать обмен подписанными документами между двумя субъектами таким образом, чтобы ни один из них не смог отказаться передавать "свой" подписанный документ, получив подписанный документ от другой стороны. Очевидно, что это вариант предыдущей задачи, в котором "определенный критерий" - это корректность подписи документа, то есть соответствие подписи содержанию.
3. "Передача с забыванием" - организовать передачу сообщения одним субъектом другому таким образом, чтобы вероятность получения сообщения была ровно 0.5 и чтобы на эту вероятность никто не мог повлиять.
4. "Бросание монеты по телефону" - организовать такое взаимодействие не доверяющих друг другу субъектов через канал передачи данных, которое позволит выработать один бит информации (значение 0 или 1) таким образом, чтобы он был случайным, несмещенным (вероятность каждого исхода равна 0.5), чтобы на исход "бросания монеты" не мог повлиять никто извне ("третьи лица"), и чтобы в исходе "бросания" можно было убедить независимый арбитраж при возникновении у участников разногласий о результате.
5. "Сравнение с нулевым разглашением" или "проблема двух миллионеров" - два миллионера хотят узнать, кто из них богаче, но при этом никто из них не хочет сообщить другой стороне истинную величину своего состояния. В более общей постановке задача формулируется следующим образом: есть два субъекта, каждый из которых располагает некоторым элементом данных - соответственно **a** и **b**, и которые желают совместно вычислить значение некоторой согласованной функции **f(a,b)**. Требуется организовать процедуру вычисления таким образом, чтобы никто из субъектов не узнал значения параметра другого.

6. "**(n,k)**-пороговая схема" - имеется некоторый ресурс, например - зашифрованный набор данных (файл), также есть **n** субъектов. Необходимо построить процедуру, разрешающую

доступ к ресурсу (дающую возможность расшифровать файл), только если его запросят одновременно не менее **k** субъектов.

7. "Тайное голосование по телефону" - имеется **n** субъектов, взаимодействующих по линиям связи, некоторый вопрос ставится им на голосование, каждый из субъектов может проголосовать либо "за", либо "против". Требуется организовать процедуру голосования таким образом, чтобы можно было вычислить ее исход - подсчитать, сколько подано голосов "за" или, в более простом случае, выяснить, что "за" было подано достаточное (большее или равное некоторой величине), или недостаточное (меньшее этой величины) число голосов, и чтобы при этом результаты голосования каждого из субъектов оставались в тайне.

Конечно, это далеко не все задачи, рассматриваемые криптографией. Но, как сказал классик, "никто не может объять необъятного", поэтому автор вынужден поставить точку в данном выпуске. Следующий выпуск будет посвящен алгоритмам шифрования.

3. КЛАССИФИКАЦИЯ ШИФРОВ

Симметричные алгоритмы представляют собой алгоритмы, в которых ключ шифрования может бать рассчитан по ключу дешифрирования и наоборот. В большинстве симметричных систем ключи шифрования и дешифрирования одни и те же. Эти алгоритмы также называют алгоритмами с секретным ключом или алгоритмами с одним ключом. Для работы такой системы требуется, чтобы отправитель и получатель согласовали используемый ключ перед началом безопасной передачи сообщения (имели защищенный канал для передачи ключа). Безопасность симметричного алгоритма определяется ключом, т.о. раскрытие ключа дает возможность злоумышленнику шифровать и дешифрировать все сообщения.

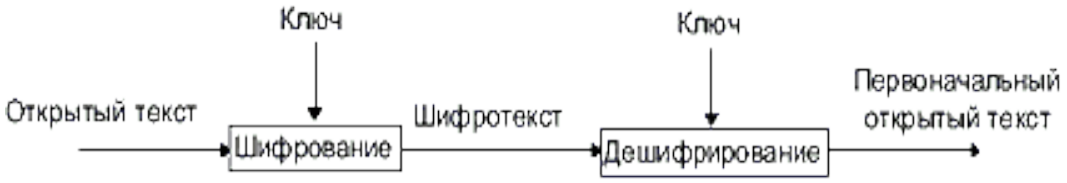

Рис. 3.1 Схема канала защищенной связи.

Из-за большой избыточности естественных языков в зашифрованное сообщение трудно внести осмысленные изменения, поэтому помимо защиты информации обеспечивается защита от навязывания ложных данных. Если же естественная избыточность недостаточна, то используется специальная контрольная комбинация - имитовставка.

Так как используется один ключ, то каждый из участников обмена может зашифровывать и дешифрировать сообщения, поэтому данная схема шифрования работает на взаимном доверии. Если его нет, то могут возникать различные коллизии, так как при возникновении какого-либо спора по поводу достоверности сообщения, независимый наблюдатель не может сказать кем из участников было отправлено сообщение.

Симметричные алгоритмы делятся на две категории. Одни из них обрабатывают текст побитно(иногда побайтно) и называются *потоковыми алгоритмами* или *потоковыми шифрами*. Те же, которые работают с группами битов открытого текста называются*блочными алгоритмами (шифрами).*

Перестановочные шифры

Простой столбцевой перестановочный шифр

В данном виде шифра текст пишется на горизонтально разграфленном листе бумаги фиксированной ширины, а шифротекст считывается по вертикали. Дешифрирование заключается в записи шифротекста вертикально на листе разграфленной бумаги фиксированной ширины и затем считывании открытого текста горизонтально.

Перестановочный шифр с ключевым словом

Буквы открытого текста записываются в клетки прямоугольной таблицы по ее строчкам. Буквы ключевого слова пишутся над столбцами и указывают порядок этих столбцов (по возрастанию номеров букв в алфавите). Чтобы получить зашифрованный текст, надо выписывать буквы по столбцам с учетом их нумерации:

Открытый текст: Прикладная математика Ключ: Шифр

Ш	и

ф р
4 1 3 2
П р и к л а д н а я м а т е м а т и к а

Криптограмма: Раяеикнаааидммкплатт

Ключевое слово(последовательность столбцов) известно адресату, который легко сможет расшифровать сообщение.

Так как символы криптотекста те же, что и в открытом тексте, то частотный анализ покажет, что каждая буква встречается приблизительно с той же частотой, что и обычно. Это дает криптоаналитику информацию о том, что это перестановочный шифр. Применение к криптотексту второго перестановочного фильтра значительно повысит безопасность. Существуют и еще более сложные перестановочные шифры, но с применением компьютера можно раскрыть почти все из них.

Хотя многие современные алгоритмы используют перестановку, с этим связана проблема использования большого объема памяти, а также иногда требуется работа с сообщениями определенного размера. Поэтому чаще используют подстановочные шифры.

Подстановочные шифры

В подстановочных шифрах буквы исходного сообщения заменяются на подстановки. Замены в криптотексте расположены в том же порядке, что и в оригинале. Если использование замен постоянно на протяжение всего текста, то криптосистема называется *одноалфавитной (моноалфавитной).* В *многоалфавитных*системах использование подстановок меняется в различных частях текста.

Шифр Цезаря

Юлий Цезарь повествует о посылке зашифрованного сообщения Цицерону. Используемая при этом система подстановок была одноалфавитной, но не являлась системой Цезаря: латинские буквы заменялись на греческие способом, который не был ясен из рассказа Цезаря. Информация о том, что Цезарь действительно использовал систем у Цезаря, пришла от Светония.

В шифре Цезаря каждая буква замещается на букву, находящуюся **k** символами правее по модулю равному количеству букв в алфавите. (Согласно Светонию у Цезаря k=3 n=50)

$C_k(j)=(j+k)(\mathrm{mod}\ n)$, n - количество букв в алфавите

Очевидно, что обратной подстановкой является

$C_k^{-1}(j)=C_{n-k}=(j+n-k)(\mathrm{mod} n)$

Шифр Цезаря с ключевым словом

В данной разновидности шифра Цезаря ключ задается числом **k (0<=k<=n-1)** и коротким ключевым словом или предложением. Выписывается алфавит, а под ним, начиная с **k**-й позиции, ключевое слово. Оставшиеся буквы записываются в алфавитном порядке после ключевого слова. В итоге мы получаем подстановку для каждой буквы. Требование, чтобы все буквы ключевого слова были различными не обязательно - можно записывать ключевое слово без повторения одинаковых букв. Количество ключей в системе Цезаря с ключевым словом равно **n!**.

Многоалфавитные системы

Полиалфавитные подстановочные шифры были изобретены ЛиномБаттистой (LeanBattista) в 1568 году. Основная идея многоалфавитных систем состоит в том, что на протяжении всего текста одна и та же буква может быть зашифрована по-разному. Т.е. замены для буквы выбираются *из многих алфавитов* в зависимости от положения в тексте. Это является хорошей защитой от простого подсчета частот, так как не существует единой маскировки для каждой буквы в криптотексте. В данных шифрах используются

множественные однобуквенные ключи, каждый из которых используется для шифрования одного символа открытого текста. Первым ключом шифруется первый символ открытого текста, вторым - второй, и т.д. После использования всех ключей они повторяются циклически.

Шифр Вернама

Шифр Вернама, или *одноразовый блокнот*, был изобретен в 1917 году Мейджором Джозефом Моборном (MajorJosephMauborn) и Гильбертом Вернамом (GilbertVernam) из AT&T (AmericanTelephone&Telegraph). В классическом понимании одноразовый блокнот является большой неповторяющейся последовательностью символов ключа, распределенных случайным образом. Первоначально это была одноразовая лента для телетайпов. Отправитель использовал каждый символ ключа для шифрования только одного символа открытого текста. Шифрование представляет собой сложение по модулю **n** (мощность алфавита) символа открытого текста и символа ключа из одноразового блокнота. Каждый символ ключа используется только один раз и для единственного сообщения, иначе даже если использовать блокнот размером в несколько гигабайт, при получении криптоаналитиком нескольких текстов с перекрывающимися ключами он сможет восстановить исходный текст. Он сдвинет каждую пару шифротекстов относительно друг друга и подсчитает число совпадений в каждой позиции.если шифротексты смещены правильно, соотношение совпадений резко возрастет. С этой точки зрения криптоанализ не составит труда. Если же ключ не повторяется и случаен, то криптоаналитик, перехватывает он тексты или нет, всегда имеет одинаковые знания. Случайная ключевая последовательность, сложенная с неслучайным открытым текстом, дает совершенно случайныйкриптотекст, и никакие вычислительные мощности не смогут это изменить.

Рис. 3.1 схема шифра Вернама.

В реальных системах сначала подготавливают две одинаковые ленты со случайными цифрами ключа. Одна остается у отправителя, а другая передается "неперехватываемым" образом например, курьером с охраной, законному получателю. Когда отправитель хочет передать сообщение, он сначала преобразует его в двоичную форму и помещает в устройство, которое к каждой цифре сообщения прибавляет по модулю два цифры, считанные с ключевой ленты. На принимающей стороне кодированное сообщение записывается и пропускается через машину, похожую на устройство, использованное для шифрования, которое к каждой двоичной цифре сообщения прибавляет (вычитает, так как сложение и вычитание по модулю два эквивалентны) по модулю два цифры, считанные с ключевой ленты, получая таким образом открытый текст. При этом, естественно, ключевая лента должна продвигаться абсолютно синхронно со своим дубликатом, используемым для зашифрования.

Главным недостатком данной системы является то, что для каждого бита переданной информации должен быть заранее подготовлен бит ключевой информации, причем эти биты должны быть случайными. При шифровании большого объема данных это является серьезным ограничением. Поэтому данная система используется только для передачи сообщений наивысшей секретности. По слухам "горячая линия" между США и СССР шифровалась с помощью одноразового блокнота. Многие сообщения советских шпионов были зашифрованы с использованием одноразовых блокнотов. Эти сообщения нераскрыты сегодня, и не будут раскрыты никогда (если не найдется способа вернуться в прошлое и достать эти блокноты :)

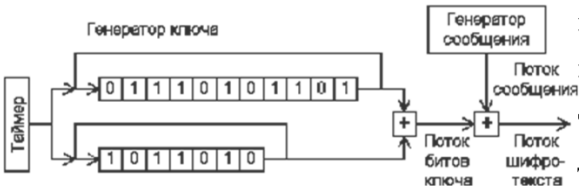

Рис. 3.2 Шифр гаммированияпсевдослучайнойпоследовательносью.

Чтобы обойти проблему предварительной передачи секретного ключа большого объема, инженеры и изобретатели придумали много остроумных схем генерации очень длинных потоков псевдослучайных цифр из нескольких коротких потоков в соответствии с некоторым алгоритмом. Получателя шифрованного сообщения при этом необходимо снабдить точно таким же генератором, как и у отправителя. Но такие алгоритмы добавляющих регулярности в шифротекст, обнаружение которых может помочь аналитику дешифровать сообщение. Один из основных методов построения подобных генераторов заключается в использовании двух или более битовых лент, считанные с которых данные побитно складываются для получения "смешанного" потока. Например, простая одноразовая лента может быть заменена двумя циклическими лентами, длины которых являются простыми или взаимно простыми числами. Так как в этом случае длины лент не имеют общих множителей, полученный из них поток имеет период повторения, равный произведению их длин: две ленты, имеющие длину 1000 и 1001 соответственно, дают в результате составной поток с периодом 1000x1001=1001000 цифр. Ленты циркулируют через сумматор, который складывает по модулю два считанные с них цифры. Выход сумматора служит ключом, используемым для зашифрования сообщения. Поэтому важно, чтобы составной поток превышал по длине все вместе взятые сообщения, которые могут быть переданы за разумный период времени. Поскольку побитовый сумматор является линейным устройством, он изначально криптографически слаб, но может быть усилен большим количеством различных способов. Другой способ - указание местонахождения ключа как места в книге, например, *Дональд Э. Кнут Искусство Программирования Том 2. Получисленные алгоритмы. Третье издание. стр 83, 3-й абзац.* Все символы, входящие в алфавит, начиная с этого места используются как одноразовый ключ для какого-либо сообщения. Но в данном случае *ключ не будет случайным* и может быть использована информация о частотах распределения букв.

Как не удивительно, но класс шифров Вернама - единственный класс шифров, для которого может быть доказана (и была доказана Шенноном) невскрываемость в абсолютном смысле этого термина.

Шифр Виженера

Одной из старейших и наиболее известных многоалфавитных криптосистем является система Виженера, названная в честь французского криптографаБлейзаВиженера(Vigenere), в *М.Н.Аршинов, Л.Е.Садовский Коды и математика* данный шифр назван шифром Тритемиуса. Этот метод был впервые опубликован в 1586 году. В данном шифре ключ задается набором из **d** букв. Такие наборы подписываются с повторением под сообщением, а, затем, полученную последовательность складывают с открытым текстом по модулю **n**(мощность алфавита). Т.е. получается следующая формула:$Vig_d(m_i)=(m_i+k_{imod\ d})(mod\ n)$

Также букву шифротекста можно находить из следующей таблицы, как пересечение столбца, определяемого буквой открытого текста, и строки, определяемой буквой ключа:

В частном случае, при **d=1**, получаем шифр Цезаря. обратная подстановка легко определяется из квадрата, или по формулам

$Vig_d^{-1}(m_i)=(m_i-k_{imodd})(modn)$ и$Bof_d^{-1}(m_i)=Bof_d(m_i)=(k_i-m_{imodd})(modn)$

соответственно.

Повторное применение двух или более шифров Виженера будет называться *составным шифром Виженера*. Он имеет уравнение

$Vig^*(m_i)=(m_i + k_{imoddk} + l_{imoddl} + ... + s_{i\ mod\ ds})\ (mod\ n)$

где $k_i + l_i + ... + s_i$ вообще говоря, имеют различные периоды dk, dl, ..., ds соответственно. Период их суммы $k_i + l_i + ... + s_i$ будет наименьшим общим кратным отдельных периодов.

Если ключ k не повторяется, то получится шифр Вернама. Если в качестве ключа используется текст, имеющий смысл, то имеем *шифр "бегущего ключа"*.

Шифр Виженера с перемешанным один раз алфавитом.

Такой шифр представляет собой простую подстановку с последующим применением шифра Виженера:

$Vig\hat{}(m_i)=f(m_i) + k_{i \bmod d}$, $Vig\hat{}^{-1}(m_i)=f^{-1}(m_i - k_{i \bmod d})$.

Шифр с автоключом

Дальнейшей модификацией системы Виженера является система шифров с *автоключом(auto-key),* приписываемая математику XVIв. Дж. Кардано, AUTOCLAVE. Шифрование начинается с помощью "первичного ключа" (который является настоящим ключом в нашем смысле) и продолжается с помощью сообщения или криптограммы, смещенной на длину первичного ключа, затем производится сложение по модулю, равному мощности алфавита. Например:

Сообщение	П Р И В Е Т П Р И М А Т У
Первичный ключ	В Г П У
Автоключ	П Р И В Е Т П Р И
Шифротекст	С У Ч Х Ф В Ч Т Н Ю П В Ы

Легальная расшифровка не представляет труда: по первичному ключу получается начало сообщения, после чего найденная часть исходного сообщения используется в качестве ключа. В другом варианте данной системы в качестве ключа служит текст сообщения, зашифрованный с помощью ключа по системе Виженера. Но данныйкриптоалгоритм слабее оригинального.

Методы анализа многоалфавитных систем

Если ключ повторяется периодически и период известен, то криптоанализ данных систем может быть сведен к криптоанализуодноалфавитных систем. Пусть период равен 5. Буквы упорядочиваются по столбцам следующим образом:

0

1 2 3 4 5

.. ..

Два появления одной буквы в одном столбце представляют одну букву сообщения. Поэтому можно расшифровать каждый столбец простым подсчетом частот.

Классификация методов дешифрования. Модель предполагаемого противника. Правила Керкхоффа.

Фундаментальное правило криптоанализа, впервые сформулированное голландцем А.Керкхоффом еще в XIX веке заключается в том, что стойкость шифра (криптосистемы) должна определяться только секретностью ключа. Иными словами, правило Керкхоффа состоит в том, что весь алгоритм шифрования, кроме значения секретного ключа, известен криптоаналитику противника. Это обусловлено тем, что криптосистема, реализующая семейство криптографических преобразований, обычно рассматривается как открытая система. Такой подход отражает очень важный принцип технологии защиты информации: защищенность системы не должна зависеть от секретности чего-либо такого, что невозможно быстро изменить в случае утечки секретной информации.

Обычно криптосистема представляет собой совокупность аппаратных и программных средств, которую можно изменить только при значительных затратах времени и средств,

тогда как ключ является легко изменяемым объектом. Именно поэтому стойкость криптосистемы определяется только секретностью ключа.

Другое почти общепринятое допущение состоит в том, что криптоаналитик имеет в своем распоряжении шифртексты сообщений.
Существует четыре основных типа криптоаналитических атак 10.2.4 . Конечно, все они формулируются в предположении, что криптоаналитику известны применяемый алгоритм шифрования и шифртексты сообщений.

1. Криптоаналитическая атака при наличии только известногошифртекста.
Криптоаналитик имеет только шифртексты C1, C2, …, Ci нескольких сообщений, причем все они зашифрованы с использованием одного и того же алгоритма шифрования Ek. Работа криптоаналитика заключается в том, чтобы раскрыть исходные тексты M1, M2, …, Mi по возможности большинства сообщений или, еще лучше, вычислить ключ K, использованный для шифрования этих сообщений, с тем, чтобы расшифровать и другие сообщения, зашифрованные этим шифром.
Этот вариант соответствует модели внешнего нарушителя, который имеет физический доступ к линии связи, но не имеет доступ к аппаратуре шифрования и дешифрования.

2. Криптоаналитическая атака при наличии известного открытого текста. Криптоаналитик имеет доступ не только к шифртекстам C1, C2, …, Ci и нескольких сообщений, но также к открытым текстам M1, M2, …, Mi этих сообщений. Его работа заключается в нахождении ключа K, используемого при шифровании этих сообщений, или алгоритма расшифрованияDk любых новых сообщений, зашифрованных тем же ключом.причем все они зашифрованы с использованием одного и того же алгоритма шифрования Ek.

Возможность проведения такой атаки складывается при шифровании стандартных документов, подготавливаемых по стандартным формам, когда определенные болки данных повторяются и известны. Он также применим при использовании режима глобального шифрования, когда вся информация на встроенном магнитном носителе записывается в виде шифртекста, включая главную корневую запись, загрузочный сектор, системные программы и пр. При хищении этого носителя (или компьютера) легко установить, какая часть криптограммы соответствует системной информации и получить большой объем известного исходного текста для выполнения криптоанализа.

3. Криптоаналитическая атака при возможности выбора открытого текста.
Криптоаналитик не только имеет доступ к шифртекстам C1, C2, …, Ci и связанным с ними открытым текстам M1, M2, …, Mi этих сообщений, но и может по желанию выбирать открытые тексты, которые затем получает в зашифрованном виде. Такой криптоанализ получается более мощным по сравнению с криптоанализом с известным открытым текстом, потому что криптоаналитик может выбрать для шифрования такие блоки открытого текста, которые дадут больше информации о ключе. Работа криптоаналитика состоит в поиске ключа K, использованного для шифрования сообщений, или алгоритма рашифрованияDk новых сообщений, зашифрованных тем же ключом.
Этот вариант атаки соответствует модели внутреннего нарушителя. На практике такая ситуация может возникнуть при вовлечении в криптоатаку лиц, которые не знают секретного ключа, но в силу своих служебных полномочий имеют возможность использовать шифрование для передачи своих сообщений.

4. Криптоаналитическая атака с адаптивным выбором открытого текста. Это - особый вариант атаки с выбором открытого текста. Криптоаналитик может не только выбирать открытый текст, который затем шифруется, но и изменять свой выбор в зависимости от результатов предыдущего шифрования. При криптоанализе с простым выбором открытого текста криптоаналитик обычно может выбирать несколько крупных блоков открытого текста для их шифрования; при криптоанализе с адаптивным выбором открытого текста он имеет возможность выбрать сначала более мелкий пробный блок открытого текста, затем выбрать следующий блок в зависимости от результатов первого выбора, и т.д. Эта атака предоставляет криптоаналитику еще больше возможностей, чем предыдущие типы атак.

Кроме перечисленных основных типов криптоаналитических атак, можно отметить, по крайней мере, еще два типа.

5. Криптоаналитическая атака с использованием выбранногошифртекста. Криптоаналитик может выбирать для расшифрования различные шифртексты и имеет доступ к расшифрованным открытым текстам . Например, криптоаналитик получил досту к защищенному от несанкционированного вскрытия блоку, который выполняет автоматическое расшифрование. Работа криптоаналитика заключается в нахождении ключа. Этот тип криптоанализа представляет особый интерес для раскрытия алгоритмов с открытым ключом.

6. Криптоаналитическая атака методом полного перебора всех возможных ключей. Эта атака предполагает использование криптоаналитикомизвестногошифртекста и осуществляется посредством полного перебора всех возможных ключей с проверкой, является ли осмысленным получающийся открытый текст. Такой подход требует привлечения предельных вычислительных ресурсов и иногда называется силовой атакой.

Предположим, что имеется конечное число возможных сообщений $\boldsymbol{M}_1,...,\boldsymbol{M}_n$ с априорными вероятностями $\boldsymbol{P}(\boldsymbol{M}_1),...,\boldsymbol{P}(\boldsymbol{M}_n)$ и что эти сообщения преобразуются в возможные криптограммы $\boldsymbol{E}_1,...,\boldsymbol{E}_m$, так что

$\boldsymbol{E} = \boldsymbol{T}_i\boldsymbol{M}$.

После того как шифровальщик противника перехватил некоторую криптограмму $\boldsymbol{E}$, он может вычислить, по крайней мере в принципе, апостериорные вероятности различных сообщений $\boldsymbol{P}_{\boldsymbol{E}}(\boldsymbol{M})$. Естественно определить *совершенную секретность* с помощью следующего условия: для всех $\boldsymbol{E}$ апостериорные вероятности равны априорным вероятностям независимо от величины этих последних. В этом случае перехват сообщения не дает шифровальщику противника никакой информации. Теперь он не может корректировать никакие свои действия в зависимости от информации, содержащейся в криптограмме, так как все вероятности, относящиеся к содержанию криптограммы, не изменяются. С другой стороны, если это условие равенства вероятностей не выполнено, то имеются такие случаи, в которых для определенного ключа и определенных выборов сообщений апостериорные вероятности противника отличаются от априорных. А это в свою очередь может повлиять на выбор противником своих действий и, таким образом, совершенной секретности не получится. Следовательно, приведенное определение неизбежным образом следует из нашего интуитивного представления о совершенной секретности.

Необходимое и достаточное условие для того, чтобы система была совершенно секретной, можно записать в следующем виде. По теореме Байеса

$$\boldsymbol{P}_{\boldsymbol{E}}(\boldsymbol{M}) = \frac{\boldsymbol{P}(\boldsymbol{M}) \cdot \boldsymbol{P}_{\boldsymbol{M}}(\boldsymbol{E})}{\boldsymbol{P}(\boldsymbol{E})},$$

где

$\boldsymbol{P}(\boldsymbol{M})$ – априорная вероятность сообщения $\boldsymbol{M}$;

$\boldsymbol{P}_{\boldsymbol{M}}(\boldsymbol{E})$ – условная вероятность криптограммы $\boldsymbol{E}$ при условии, что выбрано сообщение $\boldsymbol{M}$, т.е. сумма вероятностей всех тех ключей, которые переводят сообщение $\boldsymbol{M}$ в криптограмму $\boldsymbol{E}$;

$\boldsymbol{P}(\boldsymbol{E})$ – вероятность получения криптограммы $\boldsymbol{E}$;

$\boldsymbol{P}_{\boldsymbol{E}}(\boldsymbol{M})$ – апостериорная вероятность сообщения $\boldsymbol{M}$ при условии, что перехвачена криптограмма $\boldsymbol{E}$.

Для совершенной секретности системы величины $\boldsymbol{P}_{\boldsymbol{E}}(\boldsymbol{M})$ и $\boldsymbol{P}(\boldsymbol{M})$ должны быть равны для всех $\boldsymbol{E}$ и $\boldsymbol{M}$. Следовательно, должно быть выполнено одно из равенств: или $\boldsymbol{P}(\boldsymbol{M}) = 0$ [это решение должно быть отброшено, так как требуется, чтобы равенство осуществлялось при любых значениях $\boldsymbol{P}(\boldsymbol{M})$], или же

$\boldsymbol{P}_{\boldsymbol{M}}(\boldsymbol{E}) = \boldsymbol{P}(\boldsymbol{E})$

для любых $\boldsymbol{M}$ и $\boldsymbol{E}$. Наоборот, если $\boldsymbol{P}_{\boldsymbol{M}}(\boldsymbol{E}) = \boldsymbol{P}(\boldsymbol{E})$, то

$\boldsymbol{P}_{\boldsymbol{E}}(\boldsymbol{M}) = \boldsymbol{P}(\boldsymbol{M})$,

и система совершенно секретна. Таким образом, можно сформулировать следующее:

Теорема 6. *Необходимое и достаточное условие для совершенной секретности состоит в том, что*

$\boldsymbol{P}_{\boldsymbol{M}}(\boldsymbol{E}) = \boldsymbol{P}(\boldsymbol{E})$

для всех M *и* E, *т.е.* $P_M(E)$ *не должно зависеть от* M.

Другими словами, полная вероятность всех ключей, переводящих сообщение M_i в данную криптограмму E, равна полной вероятности всех ключей, переводящих сообщение M_j в ту же самую криптограмму E для всех M_i, M_j и E.

Далее, должно существовать по крайней мере столько же криптограмм E, сколько и сообщений M, так как для фиксированного i отображение T_i дает взаимнооднозначное соответствие между всеми M и некоторыми из E. Для совершенно секретных систем для каждого из этих E и любого $MP_M(E) = P(E) \neq 0$. Следовательно, найдется по крайней мере один ключ, отображающий данное M в любое из E. Но все ключи, отображающие фиксированное M в различные E, должны быть различными, и *поэтому число различных ключей не меньше числа сообщений* M. Как показывает следующий пример, можно получить совершенную секретность, когда число сообщений точно равно числу ключей. Пусть M_iзанумерованы числами от 1 до n, так же как и E_i, и пусть используются n ключей. Тогда

$T_i M_j = E_s$,

где$s = i + j \pmod n$. В этом случае оказывается справедливым равенство $P_E(M) = 1/n = P(E)$ и система является совершенно секретной. Один пример такой системы показан на рис. 5, где

$s = i + j - 1 \pmod 5$.

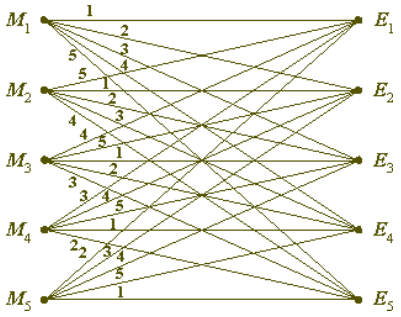

Рис 5. Совершенная система.

Совершенно секретные системы, в которых число криптограмм равно числу сообщений, а также числу ключей, характеризуются следующими двумя свойствами: 1) каждое M связывается с каждым E только одной линией; 2) все ключи равновероятны. Таким образом, матричное представление такой системы является "латинским квадратом".

В "Математической теории связи" показано, что количественно информацию удобно измерять с помощью энтропии. Если имеется некоторая совокупность возможностей с вероятностями $p_1,\ldots,p_n$, то энтропия дается выражением

$$H = -\sum p_i \log p_i.$$

Секретная система включает в себя два статистических выбора: выбор сообщения и выбор ключа. Можно измерять количество информации, создаваемой при выборе сообщения, через $H(M)$

$$H(M) = -\sum P(M) \log P(M),$$

где суммирование выполняется по всем возможным сообщениям. Аналогично, неопределенность, связанная с выбором ключа, дается выражением

$$H(K) = -\sum P(K) \log P(K).$$

В совершенно секретных системах описанного выше типа количество информации в сообщении равно самое большее $\log n$ (эта величина достигается для равновероятных сообщений). Эта информация может быть скрыта полностью лишь тогда, когда неопределенность ключа не меньше $\log n$. Это является первым примером общего принципа, который будет часто встречаться ниже: существует предел, которого нельзя превзойти при заданной неопределенности ключа – количество неопределенности, которое может быть введено в решение, не может быть больше, чем неопределенность ключа.

Положение несколько усложняется, если число сообщений бесконечно. Предположим, например, что сообщения порождаются соответствующим марковским процессом в виде бесконечной последовательности букв. Ясно, что никакой конечный ключ не даст

совершенной секретности. Предположим тогда, что источник ключа порождает ключ аналогичным образом, т.е. как бесконечную последовательность символов.

Предположим далее, что для зашифрования и расшифрования сообщения длины L_M требуется только определенная длина ключа L_K. Пусть логарифм числа букв в алфавите сообщений будет R_M, а такой же логарифм для ключа – R_K. Тогда из рассуждений для конечного случая, очевидно, следует, что для совершенной секретности требуется, чтобы выполнялось неравенство

$$R_M L_M \leqslant R_K L_K.$$

Такой вид совершенной секретности реализован в системе Вернама.

Эти выводы делаются в предположении, что априорные вероятности сообщений неизвестны или произвольны. В этом случае ключ, требуемый для того, чтобы имела место совершенная секретность, зависит от полного числа возможных сообщений.

Можно было бы ожидать, что если в пространстве сообщений имеются фиксированные известные статистические связи, так что имеется определенная скорость создания сообщений R в смысле, принятом в "Математической теории связи", то необходимый объем ключа можно было бы снизить в среднем в R/R_M раз, и это действительно верно. В самом деле, сообщение можно пропустить через преобразователь, который устраняет избыточность и уменьшает среднюю длину сообщения как раз во столько раз. Затем к результату можно применить шифр Вернама. Очевидно, что объем ключа, используемого на букву сообщения, статистически уменьшается на множитель R/R_M, и в этом случае источник ключа и источник сообщений в точности согласован – один бит ключа полностью скрывает один бит информации сообщения. С помощью методов, использованных в "Математической теории связи", легко также показать, что это лучшее, чего можно достигнуть.

Совершенно секретные системы могут применяться и на практике, их можно использовать или в том случае, когда полной секретности придается чрезвычайно большое значение, например, для кодирования документов высших военных инстанций управления, или же в случаях, где число возможных сообщений мало. Так, беря крайний пример, когда имеются в виду только два сообщения – "да" или "нет", – можно, конечно, использовать совершенно секретную систему со следующей таблицей отображений:

M	K	
	A	B
да	0	1
нет	1	0

Недостатком совершенно секретных систем для случая корреспонденции большого объема является, конечно, то, что требуется посылать эквивалентный объем ключа. В следующих разделах будет рассмотрен вопрос о том, чего можно достигнуть при помощи меньших объемов ключа, в частности, с помощью конечного ключа.

Подделка ключа - наиболее слабое место в криптографии с открытым ключом. Злоумышленник может изменить пользовательскую связку ключей или подделать открытый ключ пользователя и посылать его другим для загрузки и использования. Например, предположим, что Хлой хочет отслеживать сообщения, которые Элис посылает Блэйку. Она могла бы использовать атаку, называемую *человек в середине (maninthemiddle)*. Для этого Хлой создает новую пару ключей. Она заменяет копию открытого ключа Блэйка, принадлежащую Элис, новым открытым ключом. Затем она перехватывает сообщения, которые Элис посылает Блэйку. Каждое перехваченное сообщение она расшифровывает, используя новый секретный ключ, зашифровывает настоящим открытым ключом Блэйка и направляет их ему. Все сообщения, направленные Элис Блэйку, теперь могут быть прочитаны Хлой.

Правильное управление ключами является решающим фактором для обеспечения целостности не только Ваших связок ключей, но и связок ключей других пользователей. Основой управления ключами в GnuPG является подписание ключей. Подписание ключей имеет два основных применения: это позволяет Вам обнаруживать вмешательство в Вашу связку ключей, а также позволяет удостоверять, что ключ действительно принадлежит человеку, чьим идентификатором пользователя он помечен. Подписи на ключах также

используются в схеме известной как *сеть доверия (weboftrust)*, которая расширяет допустимые ключи не только подписанными лично Вами, но и подписанными людьми, которым Вы доверяете. Аккуратные пользователи, правильно реализовавшие управление ключами, могут исключить подмену ключей как вид атаки на конфиденциальность связи при помощи GnuPG.

Управление Вашей парой ключей

Пара ключей состоит из открытого и секретного ключей. Открытый ключ состоит из открытой части главного подписывающего ключа, открытых частей подчиненных подписывающих и шифрующих ключей, набора идентификаторов пользователя, ассоциирующих открытый ключ с реальным человеком. Каждая часть содержит данные о себе. Для ключа это его идентификатор, дата создания, срок действия и т.д. Для идентификатора пользователя это имя человека, дополнительный комментарий и адрес email. Структура секретного ключа аналогична, но содержит секретные части ключей и не содержит информацию об идентификаторе пользователя.

Для просмотра пары ключей используется команда --edit-key. Например,

```
chloe%gpg --edit-key chloe@cyb.org
Secret key is available.

pub  1024D/26B6AAE1  created: 1999-06-15 expires: never      trust: -/u
sub  2048g/0CF8CB7A  created: 1999-06-15 expires: never
sub  1792G/08224617  created: 1999-06-15 expires: 2002-06-14
sub   960D/B1F423E7  created: 1999-06-15 expires: 2002-06-14
(1)  Chloe (Jester) <chloe@cyb.org>
(2)  Chloe (Plebian) <chloe@tel.net>
Command>
```

При отображении открытого ключа выводится информация о том, доступен секретный ключ или нет. Затем выводится информация о каждом компоненте открытого ключа. Первая колонка показывает тип ключа. Символы pub указывают открытую часть главного подписывающего ключа, а символы sub открытую часть подчиненных ключей. Вторая колонка показывает длину ключа в битах, тип и идентификатор. Тип D это ключ DSA, g - ключ ElGamal, пригодный только для шифрования, и G - ключ ElGamal, который может использоваться и для подписи и для шифрования. Дата создания и окончания срока действия показана в колонках три и четыре. Идентификаторы пользователя перечислены после ключей.

Дополнительная информация о ключе может быть получена различными командами. Команда **toggle** переключает между открытой и закрытой компонентами пары ключей, если обе из них доступны.

```
Command>toggle

sec  1024D/26B6AAE1  created: 1999-06-15 expires: never
sbb  2048g/0CF8CB7A  created: 1999-06-15 expires: never
sbb  1792G/08224617  created: 1999-06-15 expires: 2002-06-14
sbb   960D/B1F423E7  created: 1999-06-15 expires: 2002-06-14
(1)  Chloe (Jester) <chloe@cyb.org>
(2)  Chloe (Plebian) <chloe@tel.net>
```

Представленная информация подобна выводимой для открытого ключа. Символы sec указывают секретный главный подписывающий ключ, символы sbb указывают секретные подчиненные ключи. Также выводятся идентификаторы пользователя из открытого ключа.

Интерактив 2 часа (фильма + обсуждение)

4. КРИПТОСИСТЕМЫ

Устройство шифров

Блочные шифры оперируют с блоками открытого текста. К ним предъявляются следующие требования:

- достаточная криптостойкость;

- простота процедур зашифрования и расшифрования;
- приемлимая надежность.

Под криптостойкостью понимают время, необходимое для раскрытия шифра при использовании наилучшего метода криптоанализа. Надежность - доля информации, дешифруемая при помощи какого-то криптоаналитического алгоритма. Само преобразование шифра должно использовать следующие принципы (по К. Шеннону):

- ***Рассеивание (diffusion)*** - т.е изменение любого знака открытого текста или ключа влияет на большое число знаков шифротекста, что скрывает статистические свойства открытого текста;
- ***Перемешивание (confusion)*** - использование преобразований, затрудняющих получение статистических зависимостей между шифротектстом и открытым текстом.

Практически все современные блочные шифры являются *композиционными* - т.е состоят из композиции простых преобразований или $\mathbf{F=F_1 \square F_2 o F_3 o F_4 o..o F_n}$, где **F**-преобразование шифра, $\mathbf{F_i}$-простое преобразование, называемое также i-ым*циклом шифрования*. Само по себе преобразование может и не обеспечивать нужных свойств, но их цепочка позволяет получить необходимый результат. Например, стандарт DES состоит из 16 циклов. В иностранной литературе такие шифры часто называют послойными (layered). Если же используется одно и то же преобразование, т.е. $\mathbf{F_i}$ постоянно для $\square$i, то такой композиционный шифр называют *итерационным* шифром. Наибольшую популярность имеют шифры, устроенные по принципу "шифра Фейстеля (Файстеля - Feistel)" (петли Фейстеля, сети Файстеля), т.е в которых:

1. входной блок для каждого преобразования разбивается на две половины: **p=(l,r)**, где **l**-левая, **r**-правая;
2. используется преобразование вида $\mathbf{F_i(l, r)=(r, l \square f_i (r))}$, где $\mathbf{f_i}$ - зависящая от ключа $\mathbf{K_i}$ функция, а $\square$ - операция XOR или некая другая.

. Функция $\mathbf{f_i}$ называется *цикловой функцией*, а ключ $\mathbf{K_i}$, используемый для получения функции $\mathbf{f_i}$ называется *цикловым ключом*. Как можно заметить, с цикловой функцией складывается только левая половина, а правая остается неизменной. Затем обе половины меняются местами. Это преобразование прокручивается несколько раз (несколько циклов) и выходом шифра является получившаяся в конце пара **(l,r)** Графически все выглядит следующим образом:

В качестве функции $\mathbf{f_i}$ выступает некая комбинация перестановок, подстановок, сдвигов, добавлений ключа и прочих преобразований. Так, при использовании подстановок информация проходит через специальные блоки, называемые *S-блоками (S-боксами, S-boxes)*, в которых значение группы битов заменяется на другое значение. По такому принципу (с небольшими отличиями) построены многие алгоритмы: DES, FEAL, серия LOKI и т.д.

В других алгоритмах используются несколько иные принципы. Так, например, алгоритмы, построенные по *SP-принципу* (*SP-сети*) осуществляют преобразование, пропуская блок через последовательность подстановок (*Substitutions*) и перстановок (*Permutations*). Отсюда и название - *SP-сети*, т.е. сети "подстановок-перстановок". Примером такого алгоритма является очень перспективная разработка Rijndael. Возможно применение в алгоритмах и каких-либо новых конструкций, но как правило, они несут в себе оперделенные ошибки (пример - FROG, HPC). Но все перечисленные алгоритмы являются композиционными. Саму идею построения криптографически стойкой системы путем последовательного применения относительно простых криптографических преобразований была высказана Шенноном (идея многократного шифрования).

Размеры блоков в каждом алгоритме свои. DES использует блоки по 64 бита (две половинки по 32 бита), LOKI97 - 128 бит. При размере выходных блоков до 8 бит шифр можно считать поточным.

Получение цикловых ключей.

Ключ имеет фиксированную длину. Однако при прокрутке хотя бы 8 циклов шифрования с размером блока, скажем, 128 бит даже при простом прибавлении посредством XOR потребуется 8*128=1024 бита ключа, поскольку нельзя добавлять в каждом цикле одно и то же значение - это ослабляет шифр. Посему для получения последовательности ключевых бит придумывают специальный алгоритм выработки цикловых ключей (ключевое расписание -

keyschedule). В результате работы этого алгоритма из исходных бит ключа шифрования получается массив бит определенной длины, из которого по определенным правилам составляются цикловые ключи. Каждый шифр имеет свой алгоритм выработки цикловых ключей.

Чтобы использовать алгоритмы блочного шифрования для различных криптографических задач существует несколько режимов их работы. Наиболее часто встречающимися в практике являются следующие режимы:

- электронная кодовая книга - ECB (ElectronicCodeBook);
- сцепление блоков шифротекста - CBC (CipherBlockChaining);
- обратная связь по шифротектсту - CFB (CipherFeedBack);
- обратная связь по выходу - OFB (OutputFeedBack);

Обозначим применение шифра к блоку открытого текста как $\mathbf{E_k(M)=C}$, где **k** - ключ, **M** - блок открытого текста, а **C** - получающийся шифротекст.

Электронная Кодовая Книга (ECB)

Исходный текст разбивается на блоки, равные размеру блока шифра. Затем с каждый блок шифруют независимо от других с использованием одного ключа шифрования. Графически это выглядит так:

Непосредственно этот режим применяется для шифрования небольших объемов информации, размером не более одного блока или для шифрования ключей. Это связано с тем, что одинаковые блоки открытого текста преобразуются в одинаковые блоки шифротекста, что может дать взломщику (криптоаналитику) определенную информацию о содержании сообщения. К тому же, если он предполагает наличие определенных слов в сообщении (например, слово "Здравствуйте" в начале сообщения или "До свидания" в конце), то получается, что он обладает как фрагментом открытого текста, так и соответствующего шифротекста, что может сильно облегчить задачу нахождения ключа. Основным достоинством этого режима является простота реализации.

Сцепление блоков шифротекста (CBC)

Один из наиболее часто применимых режимов шифрования для обработки больших количеств информации. Исходный текст разбивается на блоки, а затем обрабатывается по следующей схеме:

1. Первый блок складывается побитно по модулю 2 (XOR) с неким значением IV - начальным вектором (InitVector), который выбирается независимо перед началом шифрования.
2. Полученное значение шифруется.
3. Полученный в результате блок шифротекста отправляется получателю и одновременно служит начальным вектором IV для следующего блока открытого текста.

Расшифрование осуществляется в обратном порядке. Графически схема выглядит следующим образом:

В виде формулы, преобразование в режиме CBC можно представить как $\mathbf{C_i=E_k(M_i \oplus C_{i-1})}$, где **i** - номер соответствующего блока. Из-за использования такого сцепления блоков шифротекста с открытым текстом пропадают указанные выше недостатки режима ECB, поскольку каждый последующий блок зависит от всех предыдущих. Если во время передачи один из блоков шифротекста исказится (передастся с ошибкой), то получатель сможет корректно расшифровать последующие блоки сообщения. Проблемы возникнут только с этим "бракованным" и следующим блоками. Одним из важных свойств этого режима является "распространение ошибки" - изменение блока открытого текста меняет все последующие блоки шифротекста. Поскольку последний блок шифротекста зависит от всех блоков открытого текста, то его можно использовать для контроля целостности и аутентичности (проверки подлинности) сообщения. Его называют *кодом аутентификации сообщения (MAC - MessageAuthenticationCode)*. Он может защитить как от случайных, так и преднамеренных изменений в сообщениях.

Обратная связь по шифротексту (CFB

Режим может использоваться для получения из поточного шифра из блочного. Размер блока в данном режиме меньше либо равен размеру блока шифра. Схема данного режима:

1. IV представляет собой сдвиговый регистр. Вначале IV заполняется неким значением, которое называется синхропосылкой, не является секретным и передается перед сеансом связи получателю.
2. Значение IV шифруется.
3. Берутся первые k бит зашифрованного значения IV и складываются (XOR) с k битами открытого текста □□получается блок шифротекста из k бит.
4. Значение IV сдвигается на k битов влево, а вместо него становится значение ш.т.
5. Затем опять 2 пункт и т.д до конца.

Расшифрование аналогично.

Особенностью данного режима является распространение ошибки на весь последующий текст. Рекомендованные значения k: 1 =< k =< 8.

Применяется как правило для шифрования потоков информации типа оцифрованной речи, видео.

Обратная связь по выходу (OFB)

Данный режим примечателен тем, что позволяет получать поточный шифр в его классическом виде (см ПОТОЧНЫЕ ШИФРЫ), в отличии от режима CFB, в котором присутствует связь с шифротекстом. Принцип работы схож с принципом работы режима CFB, но сдвиговый регистр IV заполняется не битами шифротекста, а битами, выходящими из под усечения. Вот его схема:

Расшифрование осуществляется аналогично. Т.е. для любого блока длины k операция зашифрования выглядит следующим образом: $\mathbf{C_i=M_i \square G_i}$, где $\mathbf{G_i}$ - результат зашифрования некоторого вектора, являющегося заполнением сдвигового регистра. Главное свойство шифра - единичные ошибки не распространяются, т.к заполнение сдвигового регистра осуществляется не зависимо от шифротекста.
Область применения: потоки видео, аудио или данных, для которых необходимо обеспечить оперативную доставку. Широко используется у военных наряду с поточными шифрами.

Аутентификация сообщений с помощью блочных шифров.

Настал черед еще нескольких определений:

Аутентификация (authentication) - проверка подлинности чего(или кого-)-либо. Может быть аутентификация пользователя, сообщения и т.д. Необходимо отличать ее от следующего понятия:
Идентификация (identification) - некое описательное представление какого-тосубьекта. Так, если кто-то заявляет, что он - Вася Иванов, то он идентифицирует себя как "Вася Иванов". Но проверить, так ли это на самом деле (провести аутентификацию) мы можем только при помощи его паспорта.
Итак, как же можно проверить подлинность сообщения с помощью блочного шифра? Довольно просто.

1. Отправитель А хочет отправить некое сообщение $(a_1,..,a_t)$. Он зашифровывает его на секретном ключе, который знает только он и получатель, в режиме CBC или CFB это сообщение, а затем из получившегося шифротекста берет последний блок b_t изκ бит (при этом κ должно быть достаточно большим).
2. Отправитель А посылает сообщение $(a_1, .. , a_t , b_t)$ получателю в открытом виде или зашифровав его на другом ключе.
3. Получатель В, получив сообщение, $(a_1, .. , a_t , b_t)$, зашифровывает $(a_1,..,a_t)$ в том же режиме, что и А (должна быть договоренность) на том же секретном ключе (который знает только он и А).
4. Сравнивая полученный результат с b_t он удостоверяется, что сообщение отправил А, что оно не было подделано на узле связи (в случае передачи в открытом виде).

В данной схемеb_t является *кодом аутентификации сообщения (MAC)*. Для российского стандарта шифрования процесс получения кода аутентификации называется работой в режиме *имитовставки*.
Некоторые комментарии:

Режим шифрования должен быть обязательно с распространением ошибок (т.е CBC или CFB). Необходимо использовать шифр с достаточной длиной блока, а то может появиться ситуация, когда из-за небольшого числа используемых бит для аутентификации возможно

подменить исходное сообщение и при знании ключа получить тот же самый результат. Также очевидно, что схема опирается на то, что оба абонента имеют один и тот же секретный ключ, который получили заранее.

Поточные шифры

Устройство шифров

Шифрование в поточных шифрах осуществляется на основе сложения некоторой *ключевой последовательности* (*гаммы*) с открытым текстом сообщения. Сложение осуществляется познаково посредством XOR. Уравнение зашифрования выглядит следующим образом:

$c_i = m_i \oplus k_i$ для i=1,2,3..

где c_i - знак шифротекста, m_i - знак открытого текста, k_i - знак ключевой последовательности. Расшифрование выглядит так:

$m_i = c_i \oplus k_i$ для i=1,2,3... В качестве знаков могут выступать как отдельные биты, так и символы (байты). Таким образом, поточные шифры подходят для шифрования непрерывных потоков данных - голоса, видео и т.д. В общем виде схему шифра можно изобразить следующим образом:

Можно сказать, что шифрование осуществляется наложением *гаммы*(шифрование *гаммированием*). А сама гамма является ключом шифрования. Но иметь ключ, равный по размеру шифруемым данным представляется проблематичным. Поэтому поточные шифры и вырабатывают выходную гамму на основе некоторого секретного ключа небольшого размера, а значит основной задачей поточных шифров является выработка некоторой последовательности (*выходной гаммы*) для шифрования. Т.е. выходная гамма является ключевым потоком для сообщения. Поточные шифры классифицируют следующим образом:

- *синхронные*;
- *самосинхронизирующиеся (асинхронные)*.

Синхронные поточные шифры - ключевой поток (выходная гамма) получается независимо от исходного и шифрованного текстов. В данном случае наша иллюстрация меняется в следующую:

Шифр вырабатывает гамму на основе секретного ключа, она складывается с открытым текстом и результат посылается другому абоненту и расшифровывается аналогично. Блок, вырабатывающий гамму называется*генератором гаммы* или *псевдослучайным генератором (гаммы) - PRG(PseudoRandomGenerator)*. Любой блочный шифр в режиме OFB представляет собой синхронный поточный шифр.

Очевидно, что на вырабатываемую последовательность накладываются требования. Ведь если в ней есть большие последовательности нулей, то получается, что в линию при передаче передается текст сообщения с открытом виде. Или если последовательность из единиц - тот же эффект (т.к. ничто не мешает противнику попробовать "протянуть" несколько подряд идущих единиц в качестве гаммы для перехваченного сообщения.Результат - кусок открытого текста у противника). Поэтому наилучшей гаммой является случайная последовательность. Однако нельзя независимо друг от друга сгенерировать 2 одинаковые случайные последовательности.

Генераторы гаммы вырабатывают так называемые *псевдослучайные последовательности*, которые зависят от ключа шифрования, но тем не менее по своим характеристикам сходны со случайными. Задача ставится таким образом, чтобы при наличии определнного количества битов последовательности нельзя было предсказать следующие биты. Помимо этого 1 и 0 на входе должны быть равновероятны (т.е. вероятность появления 1 = вер-ти появления 0 = 0.5). Для достижения этого последовательности исследуются статистическими тестами.

Вообще, генерирование непредсказуемых псевдослучайных последовательностей является одной из важных криптографических задач на сегодняшний день (и проблем). Придумано множество генераторов, статистических тестов. Исследование псевдослучайных последовательностей мы рассмотрим далее.

Синхронные поточные шифры обладают следующими свойствами:

- *требования по синхронизации*. При использовании синхронных поточных шифров получатель и отправитель должны быть *синхронизированы* - т.е. вырабатывать одинаковые

значения ключевого потока для соответствующих знаков передаваемого потока данных. Если синхронизация нарушится (например, вследствие потери знака при передаче), процесс расшифрования не даст корректного результата.

- *отсутствие размножения ошибок*. Изменение знака шифртекста при передаче не вызывает ошбок при расшифровании других знаков шифртекста.
- *свойство активной атаки*. Как следствие первого свойства, любая вставка или удаление символа в шифртекст активным противником приводит к нарушению синхронизации и обнаруживается получателем, расшифровывающим сообщение. Как следствие второго свойства, активный противник может изменять символы шифртекста и эти изменения приведут к соответствующим изменениям в открытом тексте, получаемом при расшифровании. Посему необходимы дополнительные механизмы, позволяющие предотвратить это.

Криптоаналитик противника перехватил обе последовательности $C_1C_2C_3C_4$ и $C_1C'_2C'_3C'_4$. Составив затем уравнения: $K_2 = C'_2 \oplus O'$; $O_2 = C_2 \oplus K_2$; $K_3 = C'_3 \oplus O_2 \oplus O_3 = C_3 \oplus K_3$ и т.д., и подобрав значение одного знака O' он сможет прочитать сообщение после этого знака. Поскольку в результате исследований у него будет фрагмент ключевой последовательности (гаммы), то он может попытаться восстановить всю гамму и получить сообщение целиком (если вэтом есть необходимость, конечно). Отсюда можно сделать вывод, что ***нельзя дважды использовать один и тот же ключ***.

Хотя описание атаки носит гипотетический характер, тем не менее она очень и очень реальна, Ведь в качестве вставленного знака с таким же успехом может выступать и последовательность знаков. В этом случае подбираться будет последний знак вставленной последовательности. Представим себе ситуацию шифрования 2 файлов одним ключом, причем файлы имеют одинаковый заголовок и, скажем, середину (довольно реальная ситуация!!!). Проведя описанную атаку, криптоаналитик получит либо полностью исходные файлы, либо их фрагменты, что может иметь непоправимые последствия.

Даже если 2 абсолютно различных текста шифруются на одном ключе, противник может вычислить сумму знаков шифртекстов $C_i^1 \oplus C_i^2 = O_i^1 \oplus K_i \oplus K_i \oplus O_i^2 = O_i^1 \oplus O_i^2$, где C_i^1- i-ый знак первого шифртекста, C_i^2 - i-ый знак второго, O_i^1 и O_i^2 - знаки открытых текстов соответственно.

Сумма открытых текстов отнюдь не случайна и противник сможет восстановить 2 сообщения.

Самосинхронизирующиеся поточные шифры - каждый знак ключевого потока определяется фиксированным числом предшествующих знаков шифротекста. Схематично это можно изобразить так:

Данному типу шифров соответствуют блочные шифры, работающие в режиме CFB.

Самосинхронизирующиеся поточные шифры обладают следующими свойствами:

- *самосинхронизация*. Самосинхронизация существует при удалении или вставке некоторых знаков шифртекста, поскольку процесс расшифрования зависит от некоторого фиксированного числа предшествующих знаков шифртектста. Это означает, что в случае удаления знака из шифртекста сначала будут ошибки при расшифровании, а затем все станет хорошо и ошибок не будет.
- *ограниченное размножение ошибок*. Предположим, что состояние шифра зависит от *t*предидущих знаков шифртекста. Если во время передачи один знак шифротекста был изменен или удален/вставлен, то при расшифровке будет искажено не более t знаков, после которых пойдет опять нормальный текст.
- *свойство активной атаки*. Из второго свойства следует, что любое изменение знаков шифртекста активным противником приведет к тому, что несколько знаков шифротекста расшифруются неправильно и это сбольшей (по сравнению с синхронными шифрами) веротностью будет замечено со стороны получателя, расшифровывающего сообщение. Однако в случае вставки или удаления знаков шифртекста (по св-ву 1) это намного труднее обнаружить (по сравнению с синхронными шифрами - там получается рассинхронизация). Поэтому необходимы дополнительные механизмы для контроля этой ситуации.

- *рассеивание статистики открытого текста*. Поскольку каждый знак открытого текста влияет на весь последующий шифртекст, статистические свойства открытого текста (ведь он далеко не случаен) не сохраняются в шифртексте.

Для исследования свойств поточных шифров очень часто используется теория конечных автоматов.

Алгоритм DES

Принципы разработки

Самым распространенным и наиболее известным алгоритмом симметричного шифрования является ***DES*** (DataEncryptionStandard). Алгоритм был разработан в 1977 году, в 1980 году был принят NIST (NationalInstituteofStandardsandTechnolody США) в качестве стандарта (FIPS PUB 46).

DES является классической *сетью Фейштеля* с двумя ветвями. Данные шифруются 64-битными блоками, используя 56-битный ключ. Алгоритм преобразует за несколько *раундов* 64-битный вход в 64-битный выход. Длина ключа равна 56 битам. Процесс шифрования состоит из четырех этапов. На первом из них выполняется начальная перестановка (IP) 64-битного исходного текста (забеливание), во время которой биты переупорядочиваются в соответствии со стандартной таблицей. Следующий этап состоит из 16 *раундов* одной и той же функции, которая использует операции сдвига и подстановки. На третьем этапе левая и правая половины выхода последней (16-й) итерации меняются местами. Наконец, на четвертом этапе выполняется перестановка IP^{-1} результата, полученного на третьем этапе. Перестановка IP^{-1} инверсна начальной перестановке.

Рис.4.7 Общая схема DES

Справа на рисунке показан способ, которым используется 56-битный ключ. Первоначально ключ подается на вход функции перестановки. Затем для каждого из 16 *раундовподключ*K_i является комбинацией левого циклического сдвига и перестановки. Функция перестановки одна и та же для каждого *раунда*, но *подключи*K_i для каждого *раунда* получаются разные вследствие повторяющегося сдвига битов ключа.

Шифрование

Начальная перестановка

Начальная перестановка и ее инверсия определяются стандартной таблицей. Если M - это произвольные 64 бита, то X = IP (M) - переставленные 64 бита. Если применить обратную функцию перестановки $Y = IP^{-1} (X) = IP^{-1} (IP(M))$, то получится первоначальная последовательность битов.

Последовательность преобразований отдельного раунда

Теперь рассмотрим последовательность преобразований, используемую в каждом *раунде*.

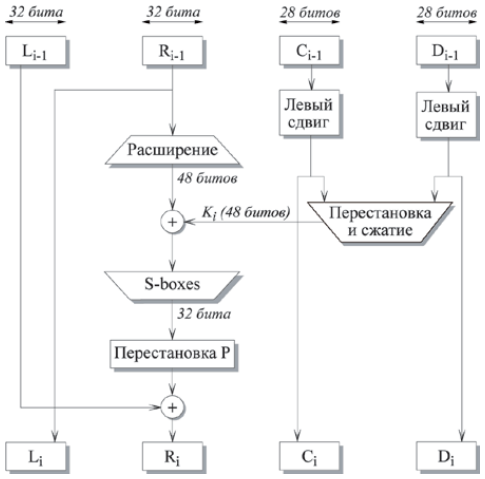

Рис. 4.8 I-ый раунд DES

64-битный входной блок проходит через 16 *раундов*, при этом на каждой итерации получается промежуточное 64-битное значение. Левая и правая части каждого промежуточного значения трактуются как отдельные 32-битные значения, обозначенные L и R. Каждую итерацию можно описать следующим образом:

$L_i = R_{i-1}$

$R_i = L_{i-1} \oplus F(R_{i-1}, K_i)$

Где $\oplus$обозначает операцию XOR.

Таким образом, выход левой половины L_i равен входу правой половины R_{i-1}. Выход правой половины R_i является результатом применения операции XOR к L_{i-1} и функции F, зависящей от R_{i-1} и K_i.

Рассмотрим функцию F более подробно.

R_i, которое подается на вход функции F, имеет длину 32 бита. Вначале R_i расширяется до 48 битов, используя таблицу, которая определяет перестановку плюс расширение на 16 битов. Расширение происходит следующим образом. 32 бита разбиваются на группы по 4 бита и затем расширяются до 6 битов, присоединяя крайние биты из двух соседних групп. Например, если часть входного сообщения

. . . efghijklmnop . . .

то в результате расширения получается сообщение

. . . defghihijklmlmnopq . . .

После этого для полученного 48-битного значения выполняется операция XOR с 48-битным *подключом*K_i. Затем полученное 48-битное значение подается на вход функции подстановки, результатом которой является 32-битное значение.

Подстановка состоит из восьми *S-boxes* , каждый из которых на входе получает 6 бит, а на выходе создает 4 бита. Эти преобразования определяются специальными таблицами. Первый и последний биты входного значения *S-box* определяют номер строки в таблице, средние 4 бита определяют номер столбца. Пересечение строки и столбца определяет 4-битный выход. Например, если входом является 011011, то номер строки равен 01 (строка 1) и номер столбца равен 1101 (столбец 13). Значение в строке 1 и столбце 13 равно 5, т.е. выходом является 0101.

Далее полученное 32-битное значение обрабатывается с помощью перестановки P, целью которой является максимальное переупорядочивание битов, чтобы в следующем *раунде* шифрования с большой вероятностью каждый бит обрабатывался другим *S-box*.

Создание подключей

Ключ для отдельного *раунда*K_i состоит из 48 битов. Ключи K_i получаются по следующему алгоритму. Для 56-битного ключа, используемого на входе алгоритма, вначале выполняется перестановка в соответствии с таблицей PermutedChoice 1 (PC-1). Полученный 56-битный ключ разделяется на две 28-битные части, обозначаемые как C_0 и D_0 соответственно. На каждом *раунде*C_i и D_i независимо циклически сдвигаются влево на 1 или 2 бита, в зависимости от номера *раунда*. Полученные значения являются входом следующего *раунда*.

Они также представляют собой вход в PermutedChoice 2 (PC-2), который создает 48-битное выходное значение, являющееся входом функции $F(R_{i-1}, K_i)$.

Дешифрование

Процесс дешифрования аналогичен процессу шифрования. На входе алгоритма используется зашифрованный текст, но ключи K_i используются в обратной последовательности. K_{16} используется на первом *раунде*, K_1 используется на последнем *раунде*. Пусть выходом i-ого *раунда* шифрования будет $L_i||R_i$. Тогда соответствующий вход (16-i)-ого*раунда* дешифрования будет $R_i||L_i$.

После последнего *раунда* процесса расшифрования две половины выхода меняются местами так, чтобы вход заключительной перестановки IP^{-1} был $R_{16}||L_{16}$. Выходом этой стадии является незашифрованный текст.

Проверим корректность процесса дешифрования. Возьмем зашифрованный текст и ключ и используем их в качестве входа в алгоритм. На первом шаге выполним начальную перестановку IP и получим 64-битное значение $L^d_0||R^d_0$. Известно, что IP и IP^{-1}взаимнообратны. Следовательно

$L^d_0||R^d_0 = IP$ (зашифрованный текст)

Зашифрованный текст $= IP^{-1}(R_{16}||L_{16})$

$L^d_0||R^d_0 = IP(IP^{-1}(R_{16}||L_{16})) = R_{16}||L_{16}$

Таким образом, вход первого *раунда* процесса дешифрования эквивалентен 32-битному выходу 16-ого *раунда* процесса шифрования, у которого левая и правая части записаны в обратном порядке.

Теперь мы должны показать, что выход первого *раунда* процесса дешифрования эквивалентен 32-битному входу 16-ого *раунда* процесса шифрования. Во-первых, рассмотрим процесс шифрования. Мы видим,что

$L_{16} = R_{15}$

$R_{16} = L_{15} \oplus F(R_{15}, K_{16})$

При дешифровании:

$L^d_1 = R^d_0 = L_{16} = R_{15}$

$R^d_1 = L^d_0 \oplus F(R^d_0, K_{16}) =$

$= R_{16} \oplus F(R^d_0, K_{16}) =$

$= (L_{15} \oplus F(R_{15}, K_{16})) \oplus F(R_{15}, K_{16})$

XOR имеет следующие свойства:

$(A \oplus B) \oplus C = A \oplus (B \oplus C)$

$D \oplus D = 0$

$E \oplus 0 = E$

Таким образом, мы имеем $L^d_1 = R_{15}$ и $R^d_1 = L_{15}$. Следовательно, выход первого *раунда* процесса дешифрования есть $L_{15}||R_{15}$, который является перестановкой входа 16-го *раунда* шифрования. Легко показать, что данное соответствие выполняется все 16 *раундов*. Мы можем описать этот процесс в общих терминах. Для i-ого *раунда* шифрующего алгоритма:

$L_i = R_{i-1}$

$R_i = L_{i-1} \oplus F(R_{i-1}, K_i)$

Эти равенства можно записать по-другому:

$R_{i-1} = L_i$

$L_{i-1} = R_i \oplus F(R_{i-1}, K_i) = R_i \oplus F(L_i, K_i)$

Таким образом, мы описали входы i-ого *раунда* как функцию выходов.

Выход последней стадии процесса дешифрования есть $R_0||L_0$. Чтобы входом IP^{-1} стадии было $R_0||L_0$, необходимо поменять местами левую и правую части. Но

$IP^{-1}(R_0||L_0) = IP^{-1}(IP$ (незашифрованный текст)) = незашифрованный текст

Т.е. получаем незашифрованный текст, что и демонстрирует возможность дешифрования *DES*.

Проблемы DES

Так как длина ключа равна 56 битам, существует 2^{56} возможных ключей. На сегодня такая длина ключа недостаточна, поскольку допускает успешное применение лобовых атак.

Альтернативой *DES* можно считать *тройной DES*, IDEA, а также алгоритм Rijndael, принятый в качестве нового стандарта на алгоритмы симметричного шифрования.

Также без ответа пока остается вопрос, возможен ли криптоанализ с использованием существующих характеристик алгоритма *DES*. Основой алгоритма являются восемь таблиц подстановки, или *S-boxes*, которые применяются в каждой итерации. Существует опасность, что эти *S-boxes* конструировались таким образом, что криптоанализ возможен для взломщика, который знает слабые места *S-boxes*. В течение многих лет обсуждалось как стандартное, так и неожиданное поведение *S-boxes*, но все-таки никому не удалось обнаружить их фатально слабые места.

Алгоритм ГОСТ 28147

Алгоритм ГОСТ 28147 является отечественным стандартом для алгоритмов симметричного шифрования. ***ГОСТ 28147*** разработан в 1989 году, является блочным алгоритмом шифрования, длина блока равна 64 битам, длина ключа равна 256 битам, количество *раундов* равно 32. Алгоритм представляет собой классическую сеть Фейштеля.

$L_i = R_{i-1}$

$R_i = L_i \oplus f(R_{i-1}, K_i)$

Функция F проста. Сначала правая половина и i-ый*подключ* складываются по модулю 2^{32}. Затем результат разбивается на восемь 4-битовых значений, каждое из которых подается на вход *S-box*. *ГОСТ 28147* использует восемь различных *S-boxes*, каждый из которых имеет 4-битовый вход и 4-битовый выход. Выходы всех *S-boxes* объединяются в 32-битное слово, которое затем циклически сдвигается на 11 битов влево. Наконец, с помощью XOR результат объединяется с левой половиной, в результате чего получается новая правая половина.

Генерация ключей проста. 256-битный ключ разбивается на восемь 32-битных *подключей*. Алгоритм имеет 32 *раунда*, поэтому каждый *подключ* используется в четырех *раундах*

Считается, что стойкость *алгоритма ГОСТ 28147* во многом определяется структурой *S-boxes*. Долгое время структура *S-boxes* в открытой печати не публиковалась. В настоящее время известны *S-boxes*, которые используются в приложениях Центрального Банка РФ и считаются достаточно сильными. Напомню, что входом и выходом *S-box* являются 4-битные числа, поэтому каждый *S-box* может быть представлен в виде строки чисел от 0 до 15, расположенных в некотором порядке. Тогда порядковый номер числа будет являться входным значением *S-box*, а само число - выходным значением *S-box*.

Основные различия между DES и *ГОСТ 28147* следующие:

- DES использует гораздо более сложную процедуру создания *подключей*, чем *ГОСТ 28147*. В *ГОСТ* эта процедура очень проста.
- В DES применяется 56-битный ключ, а в *ГОСТ 28147* - 256-битный. При выборе сильных*S-boxesГОСТ 28147* считается очень стойким.
- У *S-boxes* DES 6-битовые входы и 4-битовые выходы, а у *S-boxesГОСТ 28147* 4-битовые входы и выходы. В обоих алгоритмах используется по восемь *S-boxes*, но размер *S-boxГОСТ 28147* существенно меньше размера *S-box* DES.
- В DES применяются нерегулярные перестановки P, в *ГОСТ 28147* используется 11-битный циклический сдвиг влево. Перестановка DES увеличивает лавинный эффект. В *ГОСТ 28147* изменение одного входного бита влияет на один *S-box* одного *раунда*, который затем влияет на два *S-boxes* следующего *раунда*, три *S-boxes* следующего и т.д. В *ГОСТ 28147* требуется 8 *раундов* прежде, чем изменение одного входного бита повлияет на каждый бит результата; DES для этого нужно только 5 *раундов*.
- В DES 16 *раундов*, в *ГОСТ 28147* - 32 *раунда*, что делает его более стойким к дифференциальному и линейному криптоанализу.

Алгоритм ГОСТ 28147-89 - Режим гаммирования

Зашифрование данных

Криптосхема, реализующая алгоритм зашифрования данных в режиме гаммирования показана на схеме.
Открытые данные, разбитые на **64**-разрядные блоки $\mathbf{To^{(1)}}$, $\mathbf{To^{(2)}}$,..., $\mathbf{To^{(M-1)}}$, $\mathbf{To^{(M)}}$, зашифровываются в режиме гаммирования путем поразрядного суммирования по модулю **2** в сумматоре $\mathbf{CM_5}$ с гаммой шифра **Гш**, которая вырабатывается блоками по

64 бита:

$Гш = (Гш^{(1)}, Гш^{(2)},...,Гш^{(M-1)}, Гш^{(M)})$

где **M** - определяется объемом шифруемых данных.
В **КЗУ** вводятся **256** бит ключа. **В**накопителе**N_1, N_2** вводится **64**-разрядная двоичная последовательность (синхропосылка) **$S=(S_1, S_2,..., S_{64})$,** являющаяся исходным заполнением этих накопителей для последующей выработки **M** блоков гаммы шифра.

Исходное заполнение накопителей **N_1** и **N_2** (синхропосылка S**)** зашифровывается в режиме простой замены. Результат зашифрования**$A(S) = (Y_0, Z_0)$** переписывается в **32**-разрядные накопители **N_3** и **N_4.**
Заполнение накопителя **N_4**суммируется по модулю **$(2^{32}-1)$** в сумматоре **$СМ_4$** с **32**-разрядной константой **C_1** из накопителя **N_6**, результат записывается в **N_4**. Заполнение накопителя **N_3** суммируется по модулю **2^{32}**в сумматоре **$СМ_3$** с **32**-разрядной константой **C_2** из накопителя **N_5**, результат записывается в **N_3.**
Заполнение **N_3** переписывается в **N_1**, а заполнение N_4 переписывается в **N_2**, при этом заполнение **N_3, N_4** сохраняется.
Заполнение **N_1** и **N_2**зашифровывается в режиме простой замены. Полученное в результате зашифрования заполнение **N_1, N_2** образует первый **64**-разрядный блок гаммы шифра **$Гш^{(1)}$**), который суммируется поразрядно по модулю **2** в сумматоре **$СМ_5$** с первым **64**-разрядным блоком открытых данных.
В результате суммирования получается **64**-разрядный блок зашифрованных данных. Аналогичным образом зашифровываются остальные блоки открытых данных.
В канал связи или память ЭВМ передаются синхропосылка**S** и блоки зашифрованных данных.

Расшифрование данных

При расшифрованиикриптосхема имеет тот же вид, что и при зашифровании открытых данных в режиме гаммирования. В **КЗУ** вводятся **256** бит ключа, с помощью которого осуществлялось зашифрование данных. В накопители **N_1** и **N_2** вводится синхропосылка S. Процесс выработки M блоков гаммы шифра осуществляется совершенно аналогично описанному выше. Блоки зашифрованных данных суммируются поразрядно по модулю **2** в сумматоре **$СМ_5$** с блоками гаммы шифра, в результате получаются блоки открытых данных.

4.3. Лабораторные работы

№ п/п	*Номер раздела дисциплины*	*Наименование лабораторной работы*	*Объем (час.)*	*Вид занятия в интерактивной, активной, инновационной формах, (час.)*
1	**3.**	Программирование арифметических алгоритмов	1	-
2	**3.**	Программирование алгебраических алгоритмов	2	Работа в малых группах (1 часа)
3	**2.**	Защита от закладок при разработке программ	5	Работа в малых группах (1 часа)
4	**4.**	Программирование алгоритмов криптосистем с открытым ключом	5	Работа в малых группах (1 часа)
5	**2.**	Профилактика заражения вирусами компьютерных систем	4	Работа в малых группах (1 часа)
		ИТОГО	**17**	**4**

4.4. Практические занятия

№ п/п	*Номер раздела дисциплины*	*Наименование практической работы*	*Объем (час.)*	*Вид занятия в интерактивной, активной, инновационной формах, (час.)*
1	**4.**	Криптографические методы защиты	2	Работа в малых группах (1 часа)
2	**4.**	Шифрование методом IDEA	2	Работа в малых группах (1 часа)
3	**4.**	Шифрование методом RC6	2	Работа в малых группах (1 часа)
4	**4.**	Шифрование методом Джиффорда	3	Работа в малых группах (1 часа)
5	**4.**	Шифрование методом аналитических преобразований	4	-
6	**4.**	Сокрытие информации методом стеганографии	4	-
		ИТОГО	**17**	**4**

4.5. Контрольные мероприятия: курсовой проект (курсовая работа), контрольная работа, РГР, реферат

учебным планом не предусмотрено

5. МАТРИЦА СООТНЕСЕНИЯ РАЗДЕЛОВ УЧЕБНОЙ ДИСЦИПЛИНЫ КФОРМИРУЕМЫМ В НИХ КОМПЕТЕНЦИЯМ И ОЦЕНКЕ РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Компетенции / *№, наименование разделов дисциплины*	*Кол-во часов*	*Компетенции* *ПК* *9*	*Σ комп.*	$t_{ср}$, *час*	*Вид учебных занятий*	*Оценка результатов*
1	2	3	4	5	6	7
1. Информационная безопасность.	13	+	1	13	Лк, СРС	ЭКЗАМЕН
2. Защита информации при помощи криптографии.	23	+	1	23	Лк, ЛР, СРС	ЭКЗАМЕН
3. Классификация шифров.	17	+	1	17	Лк, ЛР, СРС	ЭКЗАМЕН
4.Криптосистемы	37	+	1	37	Лк, ЛР,ПЗ, СРС	ЭКЗАМЕН
всего часов	**90**	**90**	**1**	**90**		

6. ПЕРЕЧЕНЬ УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

1. Степанов, Е. А. Информационная безопасность и защита информации : учебное пособие / Е. А. Степанов, И. К. Корнеев. - Москва : Инфра-М, 2001. - 304 с. (страницы 134-170)
2. Информационные технологии : учебник / Под ред. В. В. Трофимова. - Москва :Юрайт, 2011. - 624 с. (страницы 200-350)

7. ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

№	*Наименование издания*	***Вид занятия*** (*Лк, ЛР, ПЗ, КП, КР, кр*)	***Количество экземпляров в библиотеке*, шт.**	***Обеспеченность*, (экз./чел.)**
1	**2**	**3**	**4**	**5**
Основная литература				
1.	Правовое обеспечение информационной безопасности : учебное пособие для вузов / Под ред. С. Я. Казанцева. - 2-е изд., испр. и доп. - Москва : Академия, 2007. - 240 с.	ЛК	15	1
2.	Иванов, М. Ю. Информационные технологии: методы криптографии : учебное пособие / М. Ю. Иванов. - Братск :БрГУ, 2010. - 100 с. - Б. ц.	ЛК, ЛР, ПЗ	31	1
3	Нестеров, С.А. Основы информационной безопасности : учебное пособие / С.А. Нестеров ; Министерство образования и науки Российской Федерации, Санкт-Петербургский государственный политехнический университет. - СПб. : Издательство Политехнического университета, 2014. - 322 с. : схем., табл., ил. - ISBN 978-5-7422-4331-1 ; То же [Электронный ресурс]. - URL: //biblioclub.ru/index.php?page=book&id=363040	ЛК	ЭР	1
4	Новожилов, О. П. Информатика : учебное пособие / О. П. Новожилов. - 2-е изд., испр. и доп. - М. : Юрайт, 2012. - 564 с.	ЛК, ЛР, ПЗ	16	1
Дополнительная литература				
5	Девянин, П. Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками : учебное пособие / П. Н. Девянин. - М. : Горячая линия- Телеком, 2012. - 320 с.	ЛК, ЛР, ПЗ	5	0,3
6	Малюк, А. А. Введение в защиту информации в автоматизированных системах : учебное пособие / А. А. Малюк. - 4-е изд., стереотип. - М. : Горячая линия- Телеком, 2011. - 146 с.	ЛК, ЛР, ПЗ	5	0,3

8.ПЕРЕЧЕНЬ РЕСУРСОВ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ «ИНТЕРНЕТ» НЕОБХОДИМЫХ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.Электронный каталог библиотеки БрГУ
http://irbis.brstu.ru/CGI/irbis64r_15/cgiirbis_64.exe?LNG=&C21COM=F&I21DBN=BOOK&P21DBN=BOOK&S21CNR=&Z21ID=.
2. Электронная библиотека БрГУ
http://ecat.brstu.ru/catalog .
3. Электронно-библиотечная система «Университетская библиотека online»
http://biblioclub.ru .
4. Электронно-библиотечная система «Издательство «Лань»
http://e.lanbook.com .
5. Информационная система "Единое окно доступа к образовательным ресурсам"
http://window.edu.ru .
6. Научная электронная библиотека eLIBRARY.RU http://elibrary.ru .
7. Университетская информационная система РОССИЯ (УИС РОССИЯ)
https://uisrussia.msu.ru/ .
8. Национальная электронная библиотека НЭБ
http://xn--90ax2c.xn--p1ai/how-to-search /.

9. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

9.1. Методические указания для обучающихся по выполнению лабораторных работ/практических работ

Лабораторная работа№1

Программирование арифметических алгоритмов

Цель работы:

Исследование и разработка основных методов симметричных криптосистем.

Задание:

1. Изучить основы криптографии
2. Познакомиться с некоторыми арифметическими алгоритмами криптографии.

Порядок выполнения:

1. Изучить теоретические основы.
2. Изучить шифр перестановки.
3. Изучить шифр одиночной перестановки.

Форма отчетности:

Отчет сдается в печатном виде. В отчете должны присутствовать:

1. Цель работы
2. Задание
3. Поэтапное выполнение всех заданий варианта
4. Заключение.

Задания для самостоятельной работы:

Изучить теоретические данные по теме лабораторной работы.

Рекомендации по выполнению заданий и подготовке к лабораторной работе

Ознакомиться с теоретическим материалом, представленным в третьем разделе данной дисциплины.

Основная литература

1. Иванов, М. Ю. Информационные технологии: методы криптографии : учебное пособие / М. Ю. Иванов. - Братск :БрГУ, 2010. - 100 с. - Б. ц.
2. Новожилов, О. П. Информатика : учебное пособие / О. П. Новожилов. - 2-е изд., испр. и доп. - М. : Юрайт, 2012. - 564 с.

Дополнительная литература

1. Девянин, П. Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками : учебное пособие / П. Н. Девянин. - М. : Горячая линия-Телеком, 2012. - 320 с.
2. Малюк, А. А. Введение в защиту информации в автоматизированных системах : учебное пособие / А. А. Малюк. - 4-е изд., стереотип. - М. : Горячая линия- Телеком, 2011. - 146 с.

Контрольные вопросы для самопроверки

1. В чем заключается главная задача криптографии?
2. В чем особенность шифра перестановки?
3. В чем особенность шифра одиночной перестановки?
4. В чем особенность шифра двойной перестановки?
5. В чем особенность шифрования при помощи магического квадрата?

Лабораторная работа №2

Программирование алгебраических алгоритмов

Цель работы:

Исследование и разработка классических методов симметричных криптосистем

Задание:

1. Изучить принцип работы симметричных криптосистем.
2. Познакомиться с некоторыми алгебраическими способами криптографии..

Порядок выполнения:

1. Изучить теоретические основы
2. Изучить шифр простой замены. Система шифрования Цезаря.
3. Изучить шифр сложной замены. Шифр Гронсфельда.
4. Изучить шифрмногоалфавитной замены.
5. Изучить способ Гаммирование

Форма отчетности:

Отчет сдается в печатном виде. В отчете должны присутствовать:

1. Цель работы
2. Задание
3. Поэтапное выполнение всех заданий варианта
4. Заключение.

Задания для самостоятельной работы:

Изучить теоретические данные по теме лабораторной работы.

Рекомендации по выполнению заданий и подготовке к лабораторной работе

Ознакомиться с теоретическим материалом, представленным в третьем разделе данной дисциплины.

Основная литература

1. Иванов, М. Ю. Информационные технологии: методы криптографии : учебное пособие / М. Ю. Иванов. - Братск :БрГУ, 2010. - 100 с. - Б. ц.
2. Новожилов, О. П. Информатика : учебное пособие / О. П. Новожилов. - 2-е изд., испр. и доп. - М. : Юрайт, 2012. - 564 с.

Дополнительная литература

1. Девянин, П. Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками : учебное пособие / П. Н. Девянин. - М. : Горячая линия-Телеком, 2012. - 320 с.
2. Малюк, А. А. Введение в защиту информации в автоматизированных системах : учебное пособие / А. А. Малюк. - 4-е изд., стереотип. - М. : Горячая линия- Телеком, 2011. - 146 с.

Контрольные вопросы для самопроверки

1. Шифр Гронсфельда.
2. Шифры двойной перестановки. Шифрование с помощью магического квадрата.
3. Шифр многоалфавитной замены и алгоритм его реализации.

Лабораторная работа №3

Защита от закладок при разработке программ

Цель работы:

Исследование и анализ служебных программ Windows для повышения эффективности работы компьютера.

Задание:

1. Установите проверку подлинности доступа к ресурсам компьютера из локальной сети. Запретите доступ к ресурсам вашего компьютера из Интернета.
2. Разрешить удаленный доступ к ресурсам вашего компьютера.
3. Использование удаленного доступа к сетевым ресурсам.
4. Защита и восстановление данных на компьютере.

Порядок выполнения:

1. Установите проверку подлинности доступа к ресурсам компьютера из локальной сети. Запретите доступ к ресурсам вашего компьютера из Интернета.
2. Разрешить удаленный доступ к ресурсам вашего компьютера.
3. Использование удаленного доступа к сетевым ресурсам.
4. Защита и восстановление данных на компьютере.

Форма отчетности:

Отчет сдается в печатном виде. В отчете должны присутствовать:

1. Цель работы
2. Задание
3. Поэтапное выполнение всех заданий варианта
4. Заключение.

Задания для самостоятельной работы:

Изучить теоретические данные по теме лабораторной работы.

Рекомендации по выполнению заданий и подготовке к лабораторной работе

Ознакомиться с теоретическим материалом, представленным в третьем разделе данной дисциплины.

Основная литература

1. Иванов, М. Ю. Информационные технологии: методы криптографии : учебное пособие / М. Ю. Иванов. - Братск :БрГУ, 2010. - 100 с. - Б. ц.
2. Новожилов, О. П. Информатика : учебное пособие / О. П. Новожилов. - 2-е изд., испр. и доп. - М. : Юрайт, 2012. - 564 с.

Дополнительная литература

1. Девянин, П. Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками : учебное пособие / П. Н. Девянин. - М. : Горячая линия-Телеком, 2012. - 320 с.
2. Малюк, А. А. Введение в защиту информации в автоматизированных системах : учебное пособие / А. А. Малюк. - 4-е изд., стереотип. - М. : Горячая линия- Телеком, 2011. - 146 с.

Контрольные вопросы для самопроверки

1. Почему при эксплуатации компьютерной системы важно знать ее параметры?
2. Какие стандартные средства Windows XP обеспечивают пользователю возможность определения параметров компьютерной системы?
3. Почему обеспечение бесперебойной работы дисковой системы компьютера является одной из основных мер обеспечения информационной безопасности?
4. Опишите причины нарушений в работе магнитных дисков.
5. Почему необходима процедура очистки диска?
6. Что такое фрагментация файла? Почему она возникает и как влияет на скорость операций чтения информации с диска?
7. В каких случаях рекомендуется выполнить дефрагментацию диска?
8. С какой целью выполняется архивация данных компьютера?
9. Что такое дискета аварийного восстановления? Какой программой она создается?

Лабораторная работа №4

Программирование алгоритмов криптосистем с открытым ключом

Цель работы:

Исследование и анализ основных методов асимметричных криптосистем

Задание:

1. Изучить шифрования Эль Гамаля.
2. Изучить шифрование данных RSA.

Порядок выполнения:

1. Зашифровать простое сообщение способом Эль Гамаля.
2. Зашифровать текст при помощи шифрования данных RSA.

Форма отчетности:

Отчет сдается в печатном виде. В отчете должны присутствовать:

1. Цель работы
2. Задание
3. Поэтапное выполнение всех заданий варианта
4. Заключение.

Задания для самостоятельной работы:

Изучить теоретические данные по теме лабораторной работы.

Рекомендации по выполнению заданий и подготовке к лабораторной работе

Ознакомиться с теоретическим материалом, представленным в третьем разделе данной дисциплины.

Основная литература

1. Иванов, М. Ю. Информационные технологии: методы криптографии : учебное пособие / М. Ю. Иванов. - Братск :БрГУ, 2010. - 100 с. - Б. ц.
2. Новожилов, О. П. Информатика : учебное пособие / О. П. Новожилов. - 2-е изд., испр. и доп. - М. : Юрайт, 2012. - 564 с.

Дополнительная литература

1. Девянин, П. Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками : учебное пособие / П. Н. Девянин. - М. : Горячая линия-Телеком, 2012. - 320 с.
2. Малюк, А. А. Введение в защиту информации в автоматизированных системах : учебное пособие / А. А. Малюк. - 4-е изд., стереотип. - М. : Горячая линия- Телеком, 2011. - 146 с.

Контрольные вопросы для самопроверки

1. Алгоритм шифрации двойным квадратом. Шифр Enigma.
2. Алгоритм шифрования DES.
3. Алгоритм шифрования ГОСТ 28147-89.
4. Алгоритм шифрования RSA.
5. Алгоритм шифрования Эль Гамаля.
6. Задачи и алгоритмы электронной подписи.
7. Задачи распределения ключей.

Лабораторная работа №5

Профилактика заражения вирусами компьютерных систем

Цель работы:

Анализ и исследование антивирусных программ.

Задание:

1. Познакомиться с работой антивирусных программ.

Порядок выполнения:

1. Изучить теоретические основы.
2. Ознакомится с энциклопедией компьютерных вирусов на сайте лаборатории Касперского.
3. Проверить на присутствие вирусов всех критических областей компьютера.

4. Поиск вирусов на вашем компьютере с тщательной проверкой всех подключенных дисков, памяти, файлов.
5. Проверка на присутствие вирусов объектов, загрузка которых осуществляется при старте операционной системы.
6. Поиск на компьютере руткитов, обеспечивающих сокрытие вредоносных программ в операционной системе.
7. Изучить дополнительные возможности программы NortonAntiVirus по защите данных.

Форма отчетности:

Отчет сдается в печатном виде. В отчете должны присутствовать:

1. Цель работы
2. Задание
3. Поэтапное выполнение всех заданий варианта
4. Заключение.

Задания для самостоятельной работы:

Изучить теоретические данные по теме лабораторной работы.

Рекомендации по выполнению заданий и подготовке к лабораторной работе

Ознакомиться с теоретическим материалом, представленным в третьем разделе данной дисциплины.

Основная литература

1. Иванов, М. Ю. Информационные технологии: методы криптографии : учебное пособие / М. Ю. Иванов. - Братск :БрГУ, 2010. - 100 с. - Б. ц.
2. Новожилов, О. П. Информатика : учебное пособие / О. П. Новожилов. - 2-е изд., испр. и доп. - М. : Юрайт, 2012. - 564 с.

Дополнительная литература

1. Девянин, П. Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками : учебное пособие / П. Н. Девянин. - М. : Горячая линия-Телеком, 2012. - 320 с.
2. Малюк, А. А. Введение в защиту информации в автоматизированных системах : учебное пособие / А. А. Малюк. - 4-е изд., стереотип. - М. : Горячая линия- Телеком, 2011. - 146 с.

Контрольные вопросы для самопроверки

1. Что такое компьютерный вирус? Какими свойствами обладают компьютерные вирусы?
2. По каким признакам классифицируют компьютерные вирусы? Перечислите типы вирусов.
3. Какие вирусы называются резидентными и в чем особенность таких вирусов?
4. Каковы отличия вирусов-репликаторов, стелс - вирусов, мутантов и «троянских» программ?
5. Опишите схему функционирования загрузочного вируса.
6. Опишите схему функционирования файлового вируса.
7. Опишите схему функционирования загрузочно-файловых вирусов.
8. Что такое полиморфный вирус? Почему этот тип вирусов считается наиболее опасным?

Практическое занятие №1

Криптографические методы защиты

Цель работы:

Познакомиться с криптографическими методами защиты.

Задание:

1. Изучить классификацию криптографических методов защиты.
2. Изучить основные определения.

Порядок выполнения:

Изучить теоретические данные.Изучить классификацию криптографических методов защиты.Изучить основные определения.

Форма отчетности:

Отчет не предусмотрен.

Задания для самостоятельной работы:

Изучение новейших методов криптографической защиты информации.

Рекомендации по выполнению заданий и подготовке к лабораторной работе

Ознакомиться с теоретическим материалом, представленным в третьем разделе данной дисциплины.

Основная литература

1. Иванов, М. Ю. Информационные технологии: методы криптографии : учебное пособие / М. Ю. Иванов. - Братск :БрГУ, 2010. - 100 с. - Б. ц.
2. Новожилов, О. П. Информатика : учебное пособие / О. П. Новожилов. - 2-е изд., испр. и доп. - М. : Юрайт, 2012. - 564 с.

Дополнительная литература

1. Девянин, П. Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками : учебное пособие / П. Н. Девянин. - М. : Горячая линия-Телеком, 2012. - 320 с.
2. Малюк, А. А. Введение в защиту информации в автоматизированных системах : учебное пособие / А. А. Малюк. - 4-е изд., стереотип. - М. : Горячая линия- Телеком, 2011. - 146 с.

Контрольные вопросы для самопроверки

1. Что такое шифрование?
2. Чем отличается открытый ключ от закрытого?
3. Дать определение стеганографии.

Практическое занятие №2

Шифрование методом IDEA

Цель работы:

Приобрести навыки работы с методом шифрования IDEA.

Задание:

1. Изучить методом шифрования IDEA.

Порядок выполнения:

Изучить теоретические данные. Изучить описание алгоритма. Познакомиться с блок-схемой метода.

Форма отчетности:

Отчет не предусмотрен.

Задания для самостоятельной работы:

Найти современные области применения данного способа шифрования.

Рекомендации по выполнению заданий и подготовке к лабораторной работе

Ознакомиться с теоретическим материалом, представленным в третьем разделе данной дисциплины.

Основная литература

1. Иванов, М. Ю. Информационные технологии: методы криптографии : учебное пособие / М. Ю. Иванов. - Братск :БрГУ, 2010. - 100 с. - Б. ц.
2. Новожилов, О. П. Информатика : учебное пособие / О. П. Новожилов. - 2-е изд., испр. и доп. - М. : Юрайт, 2012. - 564 с.

Дополнительная литература

1. Девянин, П. Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками : учебное пособие / П. Н. Девянин. - М. : Горячая линия-Телеком, 2012. - 320 с.
2. Малюк, А. А. Введение в защиту информации в автоматизированных системах :

учебное пособие / А. А. Малюк. - 4-е изд., стереотип. - М. : Горячая линия- Телеком, 2011. - 146 с.

Контрольные вопросы для самопроверки

1. Что является входной информацией для шифра IDEA?
2. Сколько нужно циклов шифрования для достаточной степени сокрытия информации?
3. На сколько блоков делиться входная информация?

Практическое занятие №3

Шифрование методом RC6

Цель работы:

Приобрести навыки работы с методом шифрования RC6..

Задание:

1. Познакомиться с шифрованием методом RC6.

Порядок выполнения:

Изучить теоретические данные. Изучить описание алгоритма. Познакомиться с блок-схемой метода. Изучить процедуры: шифрования, дешифрования и генерации ключа.

Форма отчетности:

Отчет не предусмотрен.

Задания для самостоятельной работы:

Найти современные области применения данного способа шифрования.

Рекомендации по выполнению заданий и подготовке к лабораторной работе

Ознакомиться с теоретическим материалом, представленным в третьем разделе данной дисциплины.

Основная литература

1. Иванов, М. Ю. Информационные технологии: методы криптографии : учебное пособие / М. Ю. Иванов. - Братск :БрГУ, 2010. - 100 с. - Б. ц.
2. Новожилов, О. П. Информатика : учебное пособие / О. П. Новожилов. - 2-е изд., испр. и доп. - М. : Юрайт, 2012. - 564 с.

Дополнительная литература

1. Девянин, П. Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками : учебное пособие / П. Н. Девянин. - М. : Горячая линия-Телеком, 2012. - 320 с.
2. Малюк, А. А. Введение в защиту информации в автоматизированных системах : учебное пособие / А. А. Малюк. - 4-е изд., стереотип. - М. : Горячая линия- Телеком, 2011. - 146 с.

Контрольные вопросы для самопроверки

1. Что является входной информацией для шифра RC6?
2. Сколько нужно циклов шифрования для достаточной степени сокрытия информации?
3. На сколько блоков делиться входная информация?

Практическое занятие №4

Шифрование методом Джиффорда.

Приобрести навыки работы с методом шифрования Джиффорда

Задание:

1. Познакомиться с шифрованием методом Джиффорда.

Порядок выполнения:

Изучить теоретические данные. Изучить описание алгоритма. Познакомиться с блок-схемой метода.

Форма отчетности:

Отчет не предусмотрен.

Задания для самостоятельной работы:

Найти современные области применения данного способа шифрования.

Рекомендации по выполнению заданий и подготовке к лабораторной работе

Ознакомиться с теоретическим материалом, представленным в третьем разделе данной дисциплины.

Основная литература

1. Иванов, М. Ю. Информационные технологии: методы криптографии : учебное пособие / М. Ю. Иванов. - Братск :БрГУ, 2010. - 100 с. - Б. ц.
2. Новожилов, О. П. Информатика : учебное пособие / О. П. Новожилов. - 2-е изд., испр. и доп. - М. : Юрайт, 2012. - 564 с.

Дополнительная литература

1. Девянин, П. Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками : учебное пособие / П. Н. Девянин. - М. : Горячая линия-Телеком, 2012. - 320 с.
2. Малюк, А. А. Введение в защиту информации в автоматизированных системах : учебное пособие / А. А. Малюк. - 4-е изд., стереотип. - М. : Горячая линия- Телеком, 2011. - 146 с.

Контрольные вопросы для самопроверки

1. Принцип действия метода шифрования Джиффорда?
2. Для каких целей использовался данный метода шифрования?
3. В каком году он был взломан?.

Практическое занятие №5

Шифрование методом аналитических преобразований.

Цель работы:

Познакомиться с методами аналитически преобразования для сокрытия информации..

Задание:

1. Познакомиться с методами аналитических преобразований.

Порядок выполнения:

Изучить теоретические данные. Изучить описание алгоритмов.

Форма отчетности:

Отчет не предусмотрен.

Задания для самостоятельной работы:

Найти современные области применения данного способа шифрования.

Рекомендации по выполнению заданий и подготовке к лабораторной работе

Ознакомиться с теоретическим материалом, представленным в третьем разделе данной дисциплины.

Основная литература

1. Иванов, М. Ю. Информационные технологии: методы криптографии : учебное пособие / М. Ю. Иванов. - Братск :БрГУ, 2010. - 100 с. - Б. ц.
2. Новожилов, О. П. Информатика : учебное пособие / О. П. Новожилов. - 2-е изд., испр. и доп. - М. : Юрайт, 2012. - 564 с.

Дополнительная литература

1. Девянин, П. Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками : учебное пособие / П. Н. Девянин. - М. : Горячая линия-Телеком, 2012. - 320 с.
2. Малюк, А. А. Введение в защиту информации в автоматизированных системах : учебное пособие / А. А. Малюк. - 4-е изд., стереотип. - М. : Горячая линия- Телеком, 2011. - 146 с.

Контрольные вопросы для самопроверки

1. Дать определение аналитическим преобразованиям.
2. В каких случаях могут быть использованы аналитические преобразования?
3. К какой информации этот вид шифрования может быть применим?

Практическое занятие №6

Сокрытие информации методом стеганографии

Цель работы:

Познакомиться с методами стеганографии.

Задание:

1. Познакомиться с методами аналитических преобразований.

Порядок выполнения:

Изучить теоретические данные. Изучить описание современных методов стеганографии.

Форма отчетности:

Отчет не предусмотрен.

Задания для самостоятельной работы:

Найти современные области применения данного способа шифрования.

Рекомендации по выполнению заданий и подготовке к лабораторной работе

Ознакомиться с теоретическим материалом, представленным в третьем разделе данной дисциплины.

Основная литература

1. Иванов, М. Ю. Информационные технологии: методы криптографии : учебное пособие / М. Ю. Иванов. - Братск :БрГУ, 2010. - 100 с. - Б. ц.
2. Новожилов, О. П. Информатика : учебное пособие / О. П. Новожилов. - 2-е изд., испр. и доп. - М. : Юрайт, 2012. - 564 с.

Дополнительная литература

1. Девянин, П. Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками : учебное пособие / П. Н. Девянин. - М. : Горячая линия-Телеком, 2012. - 320 с.
2. Малюк, А. А. Введение в защиту информации в автоматизированных системах : учебное пособие / А. А. Малюк. - 4-е изд., стереотип. - М. : Горячая линия- Телеком, 2011. - 146 с.

Контрольные вопросы для самопроверки

1. В чем главный принцип стенографии?
2. В каких «контейнерах» может быть спрятано зашифрованное сообщение?
3. Привести примеры стеганографии древних времён.

10. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ИСПОЛЬЗУЕМЫХ ПРИ ОСУЩЕСТВЛЕНИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

-Microsoft Imagine Premium
-ОС Windows 7 Professional
-Microsoft Office 2007 Russian Academic OPEN No Level
-Антивирусное программное обеспечение KasperskySecurity

При реализации дисциплины применяются инновационные технологии обучения, активные и интерактивные формы проведения занятий, указанные в разделах 4.3, 4.4.

11.ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

Вид занятия	***Наименование аудитории***	***Перечень основного оборудования***	***№ ЛР или ПЗ***
1	**2**	**3**	**4**
Лк	Лекционная аудитория	AMD Athlon 64 (5GHz/250Gb/2Gb/DD-RW), 2 ядра	Лк 1-8
ЛР	Дисплейный класс	AMD Athlon 64 (5GHz/250Gb/2Gb/DD-RW), 2 ядра	ЛР 1-5
ПЗ	Дисплейный класс	AMD Athlon 64 (5GHz/250Gb/2Gb/DD-RW), 2 ядра	ПЗ 1-6
СР	Читальный зал № 3	Оборудование 15-CPU 5000/RAM 2Gb/HDD (Монитор TFT 19 LG 1953S-SF);принтер HP LaserJet P3005	

Приложение 1

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯПО ДИСЦИПЛИНЕ

1. Описание фонда оценочных средств (паспорт)

№ компетенции	Элемент компетенции	Раздел	Тема	ФОС
ПК-9	умение проводить расчеты по проекту сетей, сооружений и средств инфокоммуникаций в соответствии с техническим заданием с использованием как стандартных методов, приемов и средств автоматизации проектирования, так и самостоятельно создаваемых оригинальных	**1.**. Информационная безопасность	1.1. Введение в информационную безопасность	Экзаменационный билет
			1.2. Модель сетевой безопасности .Классификация сетевых атак	Экзаменационный билет
		2. Защита информации при помощи криптографии	2.1. Защита передаваемых и хранимых секретных данных от разглашения и искажения	Экзаменационный билет
			2.2. Задача подтверждения авторства сообщения	Экзаменационный билет
		3.Классификация шифров	3.1. Перестановочные шифры	Экзаменационный билет
			3.2. Классификация методов дешифрования. Модель предполагаемого противника. Правила Керкхоффа	Экзаменационный билет
		4.Криптосистемы	4.1. Устройство шифров	Экзаменационный билет
			4.2. Поточные шифры	Экзаменационный билет
			4.3. Алгоритм DES	Экзаменационный билет
			4.4. Алгоритм ГОСТ 28147	Экзаменационный билет

2. Экзаменационные вопросы

№ п/п	Компетенции		ЭКЗАМЕНАЦИОННЫЕ ВОПРОСЫ	№ и наименование раздела (
	Код	Определение		
1	2	3	4	5
1	ПК-9	умение проводить расчеты по проекту сетей, сооружений и средств инфокоммуника-ций в соответствии с	1. Введение в информационную безопасность 2. Модель сетевой безопасности 3. .Классификация сетевых атак	**1.**. Информационная безопасность
			1. Защита передаваемых и хранимых секретных данных от разглашения и искажения 2. Задача подтверждения авторства сообщения	**2.**Защита информации при помощи криптографии

		техническим заданием с использованием как стандартных методов, приемов и средств автоматизации проектирования, так и самостоятельно создаваемых оригинальных	1. Перестановочные шифры 2. Классификация методов дешифрования. 3. Модель предполагаемого противника. 4.Правила Керкхоффа	**3.**Классификация шифров
			1. Устройство шифров 2. Поточные шифры 3. Алгоритм DES 4. Алгоритм ГОСТ 28147	**4.**Криптосистемы

3. Описание показателей и критериев оценивания компетенций

Показатели	Оценка	Критерии
Знать (ПК-9): – основы цифровой вычислительной техники, структуры и функционирование локальных вычислительных сетей и глобальной сети Интернет, основные закономерности передачи информации в инфокоммуникационных системах, основные виды сигналов, используемых в телекоммуникационных системах, особенности передачи различных сигналов по каналам и тракам телекоммуникационных систем;; Уметь (ПК-9): – формулировать основные технические требования к телекоммуникационным сетям и систем, оценивать основные проблемы, связанные с эксплуатацией и внедрением новой телекоммуникационной техники; **Владеть** (ПК-9): – начальными навыками разработки и отладки с использованием соответствующих отладочных средств программного обеспечения сигнальных процессов и микроконтроллеров.	**отлично**	Студент должен во время ответа показать знания: технологии программной защиты в интернете, основные критерии защищённости, основные способы шифрования информации, основных терминов используемые в научно-технической литературе по программной защиты в интернете. Студент должен иметь навыки владения: использования универсальных программных продуктов на ПК, понимания материала и способности высказывания мыслей на научно-техническом языке. Студент во время ответа должен продемонстрировать умения: использования навыков анализа основных способов шифрования.
	хорошо	Ответ содержит неточности. Дополнительные вопросы требуется, но студент с ними справляется отлично.

	удовлетворительно	Ответил только на один вопрос, либо слабо ответил на оба вопроса. На дополнительные вопросы отвечает неуверенно.
	неудовлетворительно	На оба вопроса студент отвечает неубедительно. На дополнительные вопросы преподавателя также не может ответить.

4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и опыта деятельности

Дисциплина Инфокоммуникационные системы в интернете направлена на ознакомление со способами информационной защиты в интернете, и их практическим применением в современных системах телекоммуникаций; на получение теоретических знаний и практических навыков различных работы с различными способами шифрования и организации систем информационной безопасности для их дальнейшего использования в практической деятельности.

Изучение дисциплины информатика предусматривает:

- лекции,
- лабораторные работы,
- практические занятия,
- самостоятельную работу студента,
- экзамен.

В ходе освоения раздела 1 «Информационная безопасность» студенты должны изучить: введение в информационную безопасность, модель сетевой безопасности , классификация сетевых атак.

В ходе освоения раздела 2 «Защита информации при помощи криптографии» студенты должны изучить: защита передаваемых и хранимых секретных данных от разглашения и искажения, задача подтверждения авторства сообщения.

В ходе освоения раздела 3 «Классификация шифров» студенты должны изучить: перестановочные шифры, классификация методов дешифрования, модель предполагаемого противника, правила Керкхоффа.

В ходе освоения раздела 4 «Криптосистемы» студенты должны изучить: устройство шифров, поточные шифры, алгоритм DES, алгоритм ГОСТ 28147.

В процессе проведения лабораторных работ происходит закрепление знаний, формирование умений и навыков реализации представления об различных способах шифрования информации.

В процессе проведения практических работ происходит закрепление знаний, формирование умений и навыков использования продвинутых методов шифрования и сокрытия информации

При подготовке к экзамену рекомендуется особое внимание уделить следующим вопросам :устройство шифров, общая схема цифровой подписи.

Работа с литературой является важнейшим элементом в получении знаний по дисциплине. Прежде всего, необходимо воспользоваться списком рекомендуемой по данной дисциплине литературой. Дополнительные сведения по изучаемым темам можно найти в периодической печати и Интернете.

Приложение 2

АННОТАЦИЯ
рабочей программы дисциплины
Инфокоммуникационные системы в интернете

1. Цель и задачи дисциплины

Целью изучения дисциплины является формирование у обучающихся профессиональных компетенций в области построения и функционирования сетей передачи данных, базовых технологий организации локальных и территориальных компьютерных сетей,

Задачей изучения дисциплины является формирование знаний, умений и навыков, позволяющих проводить самостоятельный анализ сетевых технологий глобальных сетей,

2. Структура дисциплины

2.1 Распределение трудоемкости по отдельным видам учебных занятий, включая самостоятельную работу: Лк – 17 часов, ЛР – 17 часов, ПЗ – 17 часов, СРС – 39 часов.
Общая трудоемкость дисциплины составляет 144 часа, 4 зачетных единиц

2.2 Основные разделы дисциплины:

1. Информационная безопасность.
2. Защита информации при помощи криптографии.
3. Классификация шифров.
4. Криптосистемы.

3. Планируемые результаты обучения (перечень компетенций)

Процесс изучения дисциплины направлен на формирование следующей компетенции:

ПК-9 - умение проводить расчеты по проекту сетей, сооружений и средств инфокоммуникаций в соответствии с техническим заданием с использованием как стандартных методов, приемов и средств автоматизации проектирования, так и самостоятельно создаваемых оригинальных.

4.Вид промежуточной аттестации: экзамен

Приложение 3

Протокол о дополнениях и изменениях в рабочей программе
на 20___-20___ учебный год

1. В рабочую программу по дисциплине вносятся следующие дополнения:
_____
_____

2. В рабочую программу по дисциплине вносятся следующие изменения:

_____
_____
_____

Протокол заседания кафедры №____ от «___» _____ 20 __ __ г.,
(разработчик)

Заведующий кафедрой _____ _____
(подпись) *(Ф.И.О.)*

Программа составлена в соответствии с федеральным государственным образовательным стандартом высшего образования по направлению подготовки 11.03.02 Инфокоммуникационные технологии и системы связи
от «06» марта 2015 г. № 174

для набора 2018 года: и учебным планом ФГБОУ ВО «БрГУ» для очной формы обучения от «12» марта.2018 г. № 130 .

Программу составил:

Григорьева Т.А. к.т.н, доцент кафедры УТС _____

Рабочая программа рассмотрена и утверждена на заседании кафедрыУТС

от «28» __декабря___ 2018 г., протокол № 6

Заведующий кафедрой _____ _____ И.В. Игнатьев

СОГЛАСОВАНО:

Заведующий выпускающей кафедрой _____ И.В. Игнатьев

Директор библиотеки _____ Т.Ф. Сотник

Рабочая программа одобрена методической комиссией факультета ЭиА

от «28» __декабря_____ 2018 г., протокол № 5

Председатель методической комиссии факультета _____ А.Д. Ульянов

СОГЛАСОВАНО:

Начальник
учебно-методического управления _____ Г.П. Нежевец

Регистрационный №_____