Задания СРС:

**Цель: у**глубление теоретических знаний и развитие практических навыков по обеспечению кибербезопасности, формирование компетенций в области защиты информации, освоение принципов функционирования систем защиты, а также анализ современных киберугроз и методов противодействия им.

**Лекция №7: Совершенно секретные системы**

### ****Цель:****

Изучить концепцию совершенно секретных (идеально защищённых) систем и понять критерии, которым должна соответствовать такая система для обеспечения абсолютной криптографической безопасности.

### ****Задание:****

#### ****1. Теоретическая часть:****

Изучить следующие вопросы:

* Определение совершенно секретной системы (по К. Шеннону)
* Принципы идеальной криптографической защиты
* Условия совершенной секретности:
  + Равновероятность ключей
  + Независимость зашифрованного текста от открытого
* Пример: Шифр Вернама (одноразовый блокнот)
* Проблемы и ограничения идеальных систем (практическая неприменимость, сложность генерации и хранения ключей)
* Отличие от просто стойких шифров

#### ****2. Практическая часть:****

* Составить таблицу сравнения:
  + Шифр Вернама vs. Симметричные шифры (AES, DES)
* Рассчитать пример использования шифра Вернама (на коротком сообщении)
* Ответить письменно: возможна ли реализация абсолютно секретной системы в современном мире?

#### ****3. Подготовить:****

* Доклад (1 страница) с кратким изложением теории и выводами
* Презентацию (5–8 слайдов) с примерами и схемами
* Таблицу сравнения и пример шифрования — приложить отдельно

**Цель лекции:** познакомиться с основными положениями теории информации, используемыми в криптографии и с принципами построения совершенно секретных систем.

Основные положения теории информации, используемые в криптографии, были сформулированы в середине ХХ века. Большой вклад в эти исследования внес американский ученый К. Шеннон. Для исследования принципов передачи информации по коммуникационным каналам Шеннон предложил вероятностный подход к оценке количества передаваемой информации. Кроме того, он показал, что в принципе возможны так называемые **совершенно секретные криптографические системы**, которые не могут быть "взломаны". Рассмотрим основные идеи теории Шеннона.

### Основные подходы к измерению информации

Вопросы получения, обработки, передачи и защиты информации тесно связаны с проблемой ее количественного измерения. Выделяют несколько различных подходов к решению подобной проблемы, одним из которых является так называемый *статистический* (или *алфавитный*) подход. Его суть заключается в том, что количественная оценка объема передаваемой информации осуществляется на основе анализа статистических характеристик источника информации. В этом способе учитывается способ представления информации с помощью какого-либо языка.

Очевидно, что информационная ценность некоторого сообщения связана с разнообразием вариантов генерируемых сообщений, или, другими словами, с разнообразием состояний источника информации. Ввиду этого можно считать, что объем информации, передаваемый отдельным сообщением, пропорционален общему числу N различных сообщений (или числу состояний источника информации). На практике, однако, в качестве меры информационной емкости принимается не само число N, а логарифм по основанию 2 от него:

Описание: I= \log_2 N

Данная формула позволяет получить результат в битах. Подобная *мера* получила название формально-логической логарифмической меры информации, или *меры информации по Хартли*.

Для однобуквенных сообщений N равно числу букв в алфавите информационного устройства. В частности, при числе букв равном двум *количество информации*

I = log 22 = 1 биту

Описание: I= \log_2 2 = 1 \text{ биту}

Например, рассмотрим источник, который генерирует сообщения, состоящие из одиночных букв русского языка, в алфавите которого 33 буквы. Определим, сколько информации несет отдельное сообщение, состоящее из одной буквы:

Описание: I_1= \log_2 33 \approx 5 \text{ бит}

При таком подходе для определения количества информации в некотором сообщении надо количество символов в нем умножить на *количество информации*, содержащееся в одном символе, то есть на его информационный *вес*. Подсчитаем, какое *количество информации* несет сообщение, состоящее из четырех букв русского алфавита:

Описание: I_4= 4 \log_2 33 \approx 20 \text{ бит}

Таким образом, при алфавитном подходе объем информации в сообщении оценивается не по смыслу сообщения, а по статистическим характеристикам (количеству символов).

*Мера* Хартли не всегда является верной характеристикой сообщения, так как подразумевает равную *вероятность* любого из возможных сообщений. Так как ценность информации заключается в устранении имеющейся неопределенности, сообщения, имеющие высокую *вероятность*, менее ценны. Их можно в какой-то степени предвидеть заранее. И наоборот, маловероятные сообщения представляют большую ценность. Поэтому иногда используют другой способ количественной оценки информации, учитывающий вероятности генерации конкретных сообщений, – *меру информации по Шеннону*. Этот метод измерения информации называют также *содержательным подходом*.

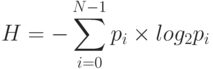
Согласно этому методу состояние источника информации до получения сообщения потребителем характеризуется некоторой неопределенностью. При этом получение информации снимает эту неопределенность (полностью или частично):

I = H нач - Н кон

Описание: I= H_{нач} - Н_{кон}

где H нач– неопределенность, характеризующая источник сообщений до получения сообщения, а Н кон– неопределенность после получения сообщения.

Неопределенность состояния источника информации оценивается по формуле



где p i – *вероятность* *i-го* состояния источника. Знак "минус" перед суммой введен потому, что величины вероятностей являются правильными дробями и имеют отрицательные логарифмы, а оценку неопределенности нужно получить со знаком "плюс".

Рассмотрим пример. При вынимании шаров из урны, где находится один черный и один белый шар, неопределенность составляет

Описание: H = - \frac {1}{2}log_2 \frac {1}{2}- \frac {1}{2}log_2 \frac {1}{2} = - log_2 \frac {1}{2} = -(-1) = 1

Неопределенность оказалась равной одному биту.

Рассмотрим другой пример. В урне находятся семь черных шаров и один белый. На этот раз неопределенность составит

Описание: H = - \frac {7}{8}log_2 \frac {7}{8}- \frac {1}{8}log_2 \frac {1}{8} = \frac {7}{8}( log_2 8-log_27) + \frac {1}{8}(log_2 8)=\frac{7(3-log_27)+3}{8} \approx \frac {7(3-2,8)+3)}{8} \approx 0,55бит

*Мера* неопределенности уменьшилась почти вдвое по сравнению с первым примером.

Неопределенность достигает максимального значения при равенстве вероятностей каждого из состояний друг другу и уменьшается с увеличением разброса этих вероятностей. Также следует заметить, что при равенстве вероятностей между собой Описание: p_i=p_j, \forall i,j=\overline{0 \dots N-1}, *мера* информации по Шеннону совпадает с мерой информации по Хартли.

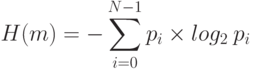
Во многих случаях алфавитный подход к измерению информации оказывается предпочтительнее. Именно *мера* информации по Хартли используется, если мы говорим, что некоторый *файл* содержит 1,5 мегабайта информации или что на одной странице некоторой книги умещается 17 *килобайт* информации.

Основной единицей количества информации является *бит*. Однако для практического применения это слишком мелкая *единица*. Более удобной единицей является *байт* (*byte*), равный восьми битам. Прибавляя к слову "*байт*" децимальные приставки "кило", "мега" и так далее, можно получать более крупные единицы измерения. Нужно только помнить об условности таких обозначений, так как их связывает *множитель*, равный не 1000, а 1024 =2 10.

### Энтропия и неопределенность

Таким образом, мы выяснили, что измерение количества информации в сообщении можно проводить на основе учета изменения неопределенности. К. Шеннон ввел понятие **энтропии** как меры неопределенности. *Энтропия* H(m) определяет *количество информации* в сообщении m и является мерой его неопределенности.

Пусть источник сообщений может создавать n разных сообщений m 1, m 2, ... m nс вероятностями p 1, p 2,... , p n. В этом случае *энтропия* сообщения будет определяться формулой



Так как в данной формуле используется двоичный логарифм, то *энтропия* измеряется в битах, что общепринято в криптографии, теории информации и в компьютерных науках.

"Физический" смысл энтропии состоит в том, что *энтропия* — это количественная *мера* неопределенности. В качестве примера рассмотрим три источника сообщений, каждый из которых может генерировать только по два разных сообщения m1 и m2. Пусть известно, что для первого источника *вероятность* появления первого сообщения р(m1)=0, а *вероятность* второго сообщения р(m1)=1. Для второго источника вероятности сообщений равны, то есть р(m1)=0,5 и р(m2)=0,5. Для третьего источника вероятности сообщений следующие: р(m1)=0,9 и р(m1)=0,1. Определим энтропию каждого из источников сообщений. Для первого источника:

H1 = -0 \* log2 0 – 1 \* log2 1 = 0 – 0 = 0

*Энтропия* или неопределенность первого источника равна нулю. И действительно, если заранее известно, что из двух сообщений всегда генерируется только одно, то никакой неопределенности нет.

Определим энтропию второго источника:

Описание: H_2=-\frac {1}{2} log_2 \frac {1}{2} - \frac {1}{2} log_2 \frac {1}{2} =-log_2 \frac {1}{2}=-(-1)=1

Неопределенность оказалась равной одному биту. Найдем теперь энтропию третьего источника:

Описание: H_3=-0,9log_2\:0,9-0,1log_2\:0,1 \approx -0,9 \times (-0,152)-0,1 \times (-3,322) \approx 0,47

Неопределенность у третьего источника меньше, чем у второго, так как из двух возможных сообщений, генерируемых третьим источником, одно более вероятно, чем другое.

Понятие энтропии играет важную роль во многих задачах теории передачи и хранения информации. В частности, *энтропия* может использоваться для определения максимальной степени сжатия данных. Точнее, если источник сообщений порождает текст достаточно большой длины n с определенной предельной энтропией h на *бит* сообщения, то этот текст теоретически может быть сжат до величины n\*h *бит*. Например, если h = 1/2, то текст может сжиматься вдвое и т.д. *Значение* n\*h является пределом и на практике достигается редко.

С точки зрения криптографии, *энтропия* определяет количество символов, которые необходимо раскрыть, чтобы узнать содержание сообщения. Так, если некоторый 8-битовый *блок данных* хранит одно из двух возможных сообщений (например, ответы "Да" или "Нет" ), то достаточно правильно узнать один *бит*, чтобы определить *значение* исходного сообщения. Сколько бы *бит* мы не отводили для шифрования слов "Да" и "Нет", *энтропия* или неопределенность всегда будет меньше или равна 1.

### Норма языка и избыточность сообщений

Для каждого языка можно ввести величину, называемую **нормой языка** r и определяемую по формуле

r = H(m)/N,

где H(m) – это *энтропия* сообщения, а N – *длина* сообщения в символах используемого языка. Норму языка можно рассматривать как *количество информации*, приходящееся на один символ сообщения. *Норма* языка будет различной для разных языков, а также для сообщений с разной длиной и содержанием. Так, например, различные исследователи оценивают норму английского языка в диапазоне от 1,0 до 1,5 *бит* на символ. Будем считать, что *норма* русского языка примерно равна 1,5 *бит* на символ.

**Абсолютной нормой языка** R называют максимальное количество *бит* информации, которое может быть передано одним символом рассматриваемого языка, при условии, что все последовательности символов равновероятны. Абсолютная *норма* языка, *алфавит* которого состоит из L символов, может быть вычислена как

R = log2 L

Для русского языка, *алфавит* которого состоит из 33 букв, абсолютная *норма* языка

Описание: R_{РУС} = \log_2 33 \approx 5 \text{ бит}

Таким образом, видно, что абсолютная *норма* русского языка значительно больше, чем реальная. В этом нет ничего удивительного, так как все естественные языки обладают значительной избыточностью. Это связано с несколькими факторами. Во-первых, некоторые буквы алфавита встречаются в сообщениях чаще других. Некоторая *статистика* по символам русского алфавита приведена в лекции 2, где рассматривается процесс криптоанализа сообщения на основе статистических данных языка. Второй причиной избыточности является то, что некоторые *сочетания* букв в словах недопустимы. Например, в русском языке нет слов, в которых стояли бы подряд буквы "ц" и "й" или "я" и "ь". Кроме того, естественные языки устроены таким образом, что иногда, зная фрагмент слова или фразы, мы может восстановить недостающую часть. Например, в приветствии

Зд.авствуй, до.огой д.уг!

мы легко сможет восстановить недостающие буквы "р".

**Избыточность языка** D оценивают как

D =R – r.

*Избыточность* русского языка получается равной 3,5 бит на символ. Это означает, что в среднем каждая буква русского языка содержит 3,5 бита неиспользуемой информации. Примерно такую же *избыточность* имеют и другие естественные языки, например, английский.

Минимальной избыточностью сообщений D = 0 обладал бы язык, в котором все символы равновероятны и могут встречаться в сообщениях независимо друг от друга в любом порядке.

### Понятие совершенно секретной системы

*Криптографическая система* называется **совершенно секретной**, если *анализ* зашифрованного текста не может дать никакой информации об открытом тексте, кроме, возможно, его длины.

Если *криптографическая система* не является совершенно секретной, то *знание* шифротекста сообщения предоставляет некоторую информацию относительно соответствующего открытого текста. Для большинства простых систем шифрования, например, методов однократной замены или перестановки, по мере увеличения длины перехваченного зашифрованного сообщения можно делать некоторые выводы о ключе шифрования или об открытом тексте. Это связано с большой избыточностью естественных языков. Так, например, если перехвачено сообщение, зашифрованное методом перестановки, то противник может узнать, какие символы и в каком количестве встречались в исходном сообщении, а после этого может попробовать провести какой-либо более сложный *анализ* с целью определения правила перестановки. Если нам известно зашифрованное методом моноалфавитной замены сообщение ДКДК, мы, конечно, без дополнительной информации не сможем однозначно определить, что содержалось в исходном тексте. Однако, получив в свое распоряжение ДКДК, мы сможем сделать *вывод*, что

1. в исходном сообщении использовалось всего две буквы алфавита
2. первая и третья, а также вторая и четвертые буквы открытого текста были одинаковы.

Можно также предположить, что либо Д, либо К заменяют гласную букву. Может быть, исходное сообщение представляло собой *слово* МАМА, а может быть ПАПА, а может быть что-нибудь еще. Однозначно дешифровать его нельзя, однако некоторую информацию по шифротексту мы смогли определить. Таким образом, можно сделать *вывод*, что методы перестановки или замены не являются совершенно секретными криптографическими шифрами.

На практике возможна следующая реализация совершенно секретной системы, называемая **одноразовая лента** (или **одноразовый блокнот**, или **шифр Вернама** по имени американского инженера, предложившего эту систему в первой половине ХХ века). Будем предполагать, что процессу шифрования подвергаются двоичные данные. На передающей и приемной сторонах подготавливаются две одинаковые ленты, например, магнитные. Они содержат *ключ* шифрования. На передающей стороне лента помещается в устройство шифрования, а на принимающей стороне – в идентичное устройство, используемое для расшифрования. Когда отправитель хочет передать сообщение, он складывает по модулю два один *бит* исходного сообщения и один *бит* с магнитной ленты. После этого лента перемещается в следующее положение и можно шифровать второй *бит* сообщения, используя второй *бит* ключа. Таким образом шифруется все сообщение. На принимающей стороне лента с ключом используется аналогично.

Например, пусть исходное сообщение m содержит следующие двоичные цифры:

m = 1100101110...

Предположим, в качестве ключевой используется последовательность:

k = 1001100111...

Выполним *шифрование* по методу одноразовой ленты, сложив цифры в каждом столбике по модулю 2:

исходный текст m = 1100101110...

биты ключевой послед-ти k = 1001100111...

-------------------

зашифрованный текст с = 0101001001...

Этот процесс напоминает наложение гаммы на *поток* входных данных. *Шифр* с одноразовой лентой действительно является гаммированием, однако, в отличие от всех рассмотренных до этого криптосистем в нем предполагается *бесконечная гамма*.

В одноразовой ленте все буквы встречаются с одинаковой частотой. Поэтому, сколько бы знаков гаммы нам ни было известно, мы не сможем предсказать, какой будет следующая буква. Из этого следует, что все последовательности знаков гаммы равновероятны. Это означает, что сообщение, зашифрованное с помощью шифра Вернама, может быть "дешифровано" в любой *открытый текст* подходящей длины, поскольку предполагаемая последовательность знаков гаммы не имеет никаких свойств, позволяющих отличить её от любой другой.

В шифре Вернама, конечно, совсем необязательно использовать в качестве носителя ключевых данных именно ленту. Главное, чтобы у отправителя и получателя был секретный *ключ* размера не меньшего, чем *длина* исходного сообщения. Проблемы могут возникнуть при шифровании большого объема данных, так как запасы ключевых цифр должны быть заблаговременно доставлены получателю информации и храниться у него.

Совершенно секретные системы могут быть реализованы на практике. Почему же они не используются во всех случаях? Это объясняется несколькими причинами. Во-первых, как и любые системы шифрования с закрытым ключом в них существует проблема распределения ключей. Во-вторых, в совершенной секретной системе *ключ* шифрования должен иметь по крайней мере такую же длину, как и *открытый текст*. Кроме того, для шифрования каждого сообщения должен применяться свой новый *ключ*. Все эти факторы делают реализацию совершенно секретной системы очень дорогой и не слишком удобной. Такие системы имеет смысл использовать лишь для самых важных линий связи, например, правительственных.

### Расстояние единственности

Если *криптографическая система* не является совершенно секретной, то зашифрованное сообщение может дать криптоаналитику некоторую информацию об исходном сообщении. Специалист, может быть, и не сможет сразу однозначно дешифровать шифротекст, однако он будет иметь возможность делать некоторые предположения о ключе или открытом тексте. После получения каждого следующего зашифрованного тем же ключом сообщения криптоаналитик будет расширять свои знания относительно ключа шифрования и в конце концов сможет дешифровать сообщения.

Возникает вопрос, а какой должна быть *длина* зашифрованного сообщения, чтобы можно было однозначно дешифровать его. В примере, рассмотренном в лекции 2 проводилась попытка дешифрования сообщения из 11 символов, *закрытого методом* простой замены. На основе анализа статистических закономерностей русского языка удалось подобрать несколько подходящих вариантов открытых текстов, однако для выбора из них одного "правильного" не хватило информации. По-видимому, существует некоторая *длина* перехваченного сообщения, после которой сообщение может быть дешифровано с вероятностью, близкой к единице.

Шеннон ввел понятие **расстояния единственности** шифра (или **расстояния уникальности** ) U, которое показывает, сколько букв зашифрованного сообщения необходимо перехватить для однозначного восстановления ключа.

Для вычисления расстояния единственности необходимо знать энтропию ключа Н(К). Для симметричных шифров *энтропия* ключа примерно равна логарифму числа ключей NK по основанию 2:

Н(К) = log2 NK

Например, для шифра простой замены, применяемого к русскому языку, число возможных ключей определяется количеством всех возможных таблиц замен и равно Описание: N_K = 33! \approx 8,68*10^{36} поэтому *энтропия* ключа будет равна

Описание: Н(К) = log_2  8,68 * 10^{36} \approx 122,7

Если нам известна *энтропия* ключа Н(К) для некоторого шифра, то *расстояние* единственности U для него вычисляется по формуле

U = H(K) / D,

где D – *избыточность* шифруемого сообщения.

Рассчитаем *расстояние* единственности для шифра простой замены, применяемого к сообщению на русском языке:

Описание: U = H(K) / D = 122,7 / 3,5 \approx 35,1

То есть если *длина* перехваченного зашифрованного сообщения превышает 35 символов, то его, скорее всего, можно будет однозначно дешифровать. А при длине зашифрованного текста меньше 35 символов возможно неоднозначное вскрытие.

*Расстояние* единственности показывает нам не то, какой размер должен иметь перехваченный шифротекст, чтобы его было *легко* дешифровать, а то, насколько большим он должен быть, чтобы было возможно в принципе его *однозначное* *дешифрование*.

Для того чтобы затруднить противнику *определение* ключа и *дешифрование* наших секретных сообщений, необходимо увеличивать (а желательно доводить до бесконечности) *расстояние* единственности в применяемых шифрах. Проанализировав формулу для вычисления расстояния единственности, определим, что это можно сделать двумя способами.

Если *энтропия* ключа равна бесконечности, то *расстояние* единственности шифра будет тоже равно бесконечности. *Энтропия* ключа тем больше, чем длиннее *ключ*. В случае использования системы одноразовой ленты *ключ* теоретически бесконечен и все его символы равновероятны, поэтому *энтропия* ключа такого шифра будет бесконечно большой. Следовательно, *расстояние* единственности шифра Вернама равно бесконечности.

Как уже отмечалось выше, использовать *шифр* с бесконечно большим ключом практически нецелесообразно. Однако на практике можно менять иногда *ключ* шифрования, тем самым затрудняя жизнь противнику. Специалисты рекомендуют использовать системы, в которых *ключ* меняется задолго до достижения расстояния единственности шифра. Этого можно достичь, например, используя *сеансовые ключи* шифрования, то есть применять для шифрования каждого сообщения новый *ключ*.

Второй способ увеличения расстояния единственности состоит в уменьшении избыточности исходного текста. Если *избыточность* сообщения равна нулю, то *ключ* никогда не будет определен, а зашифрованное сообщение вскрыто, так как *расстояние* единственности будет равно бесконечности. К сожалению, на практике такая ситуация невозможна, так как любое осмысленное сообщение будет иметь некоторую отличную от нуля *избыточность*.

Однако возможно уменьшение избыточности в сообщениях за счет сжатия данных. Дело в том, что при сжатии данных *энтропия* "сжатого" текста сохраняется, а *длина* уменьшается. Следовательно, *энтропия* на букву в сжатом тексте больше, чем в исходном, а *избыточность* – меньше. Значит, после сжимающего кодирования *расстояние* единственности шифра увеличивается.

### Ключевые термины

**Абсолютная норма языка** – максимальное количество *бит* информации, которое может быть передано одним символом некоторого языка, при условии, что все последовательности символов в языке равновероятны.

**Избыточность языка** – статистическая величина, обозначающая *избыточность* информации, содержащейся в тексте на определённом языке.

**Норма языка** – величина, характеризующая *количество информации*, приходящееся на один символ сообщения.

**Одноразовая лента (или одноразовый блокнот, или шифр Вернама)** – один из возможных вариантов реализации совершенно секретной системы. Может быть реализован как гаммирование с бесконечной гаммой.

**Расстояние единственности шифра (или расстояния уникальности)** – величина, показывающая, сколько букв зашифрованного сообщения необходимо перехватить для однозначного восстановления ключа.

**Совершенно секретная система** – *криптографическая система*, для которой *анализ* зашифрованного текста не дает никакой информации об открытом тексте, кроме, возможно, его длины.

**Энтропия сообщения** – характеристика, введенная Шенноном. Определяет *количество информации*, приходящейся на одно элементарное сообщение источника, вырабатывающего статистически независимые сообщения. Является мерой неопределённости или непредсказуемости информации.

### Краткие итоги

Основные положения теории информации, используемые в криптографии, были сформулированы в середине ХХ века. Большой вклад в эти исследования внес американский ученый К. Шеннон. Для исследования принципов передачи информации по коммуникационным каналам Шеннон предложил вероятностный подход к оценке количества передаваемой информации. Кроме того, он показал, что в принципе возможны так называемые совершенно секретные криптографические системы, которые не могут быть "взломаны".

*Криптографическая система* называется совершенно секретной, если *анализ* зашифрованного текста не может дать никакой информации об открытом тексте, кроме, возможно, его длины. Одним из возможных вариантов реализации совершенно секретной системы является *шифр* Вернама (или одноразовый блокнот, или одноразовая лента). *Шифрование* по этому методу выполняется как *сложение* по модулю два открытого текста с бесконечным ключом (называемым одноразовым блокнотом или шифроблокнотом). При этом *ключ* должен обладать тремя важными свойствами: быть истинно случайным; совпадать по размеру с заданным открытым текстом; применяться только один раз. Данный метод, к сожалению, не слишком удобен на практике. Во-первых, как и любые системы шифрования с закрытым ключом в них существует проблема распределения ключей. Во-вторых, в совершенной секретной системе *ключ* шифрования должен иметь по крайней мере такую же длину, как и *открытый текст*. Кроме того, для шифрования каждого сообщения должен применяться свой новый *ключ*. Все эти факторы делают реализацию совершенно секретной системы очень дорогой и не слишком удобной. Такие системы имеет смысл использовать лишь для самых важных линий связи, например, правительственных.

Если *криптографическая система* не является совершенно секретной, то *знание* шифротекста сообщения предоставляет некоторую информацию относительно соответствующего открытого текста. Большинство используемых на практике криптографических систем не является совершенно секретными.

Для увеличения безопасности реальных криптографических систем специалисты рекомендуют:

1. использовать *сеансовые ключи* шифрования, то есть применять для шифрования каждого сообщения новый ключ;
2. уменьшать избыточность шифруемых массивов данных, например, выполнять сжатие сообщений перед криптографическим шифрованием.

#### Вопросы для самопроверки

1. Как определяется энтропия источника сообщений?
2. Что характеризует энтропия источника сообщений?
3. Что определяет норма языка?
4. Как вычисляется абсолютная норма языка?
5. Что характеризует избыточность языка?
6. Почему в сообщениях, составленных на естественных языках, всегда имеется избыточность?
7. Дайте определение совершенно секретной криптографической системы.
8. Приведите примеры шифров, которые не являются совершенно секретными системами.
9. Почему шифр одноразовой ленты (шифр Вернама) является совершенно секретной системой?
10. Почему совершенно секретные системы не используются повсеместно на практике для защиты информации?
11. Как определяется энтропия ключа шифра?
12. Каким образом вычисляется расстояние единственности для шифра?