МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ВГУ»)

КОНСПЕКТ ЛЕКЦИЙ

по курсу

«Математические основы защиты информации и информационной безопасности»

ЭЛЕКТРОННОЕ УЧЕБНОЕ ПОСОБИЕ

Составители: Б. Н. Воронков,
Ю. А. Крыжановская

ВОРОНЕЖ
2017

Содержание

ŋqdqyeɤ bɐ dəqƎbɤɜe d ɐɔɑbɔɤ Ɉqdqɤqɤè

__Защита информации__ – деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию. Или по-другому – совокупность технических и организационных мер, обеспечивающих информационную безопасность.

__Закрытая информация__ содержит государственную, коммерческую или иную тайну.

__Секретная информация__ содержит государственную тайну.

__Конфиденциальная информация__ – служебная, профессиональная, промышленная, коммерческая или иная информация, правовой режим которой устанавливается ее собственниками на основе законов о коммерческой, профессиональной тайне, государственной службе и других законодательных актов.

__Защищаемая информация__ – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственниками информации.

__Утечка информации__ – неконтролируемое распространение защищаемой информации.

Утечки бывают трех видов:

а) разглашение,

б) несанкционированный доступ к информации,

в) разведка.

__Уничтожение информации__ – утрата информации при невозможности ее восстановления.

__Блокировка информации__ – невозможность ее использования при сохранности.

__Модификация информации__ – изменение ее содержания по сравнению с первоначальной.

Цена информации – полезность информации для участников информационного рынка.

Ценность информации – полезность информации для ее владельца (пользователя).

Угрозы информации:

а) нарушение конфиденциальности – потеря ценности информации при ее раскрытии;

б) нарушение целостности – потеря ценности информации при ее модификации или уничтожении;

в) нарушение доступности – потеря ценности информации при невозможности ее оперативного использования;

Эффективность защиты информации – мера соответствия уровня информационной безопасности требованиям при заданном ресурсе на ее защиту.

Политика безопасности – ***это набор документированных норм, правил и практических приемов, регулирующих управление, защиту и распределение информации ограниченного доступа***.

Телекоммуникационная система – система связи, в которой перенос информации осуществляется сигналами, однозначно отображающими сообщения, при этом сообщение является формой представления информации и задает закон изменения, т.е. модуляции тех или иных информационных признаков сигнала (амплитуды, фазы, частоты).

Алфавит – конечное множество используемых для шифрования знаков.

Z33 – 32 буквенный русский алфавит и пробел.

Z256 – расширенный ASCII (American Standard Code for Information Interchange – Американский стандарт кодирования для обмена информацией).

Z2 – {0;1}.

Текст – набор элементов алфавита имеющий определенный логический смысл. Открытый текст (ОТ) – исходное, шифруемое сообщение.

Ключ – информация, необходимая для беспрепятственного шифрования или расшифрования текстов.

Обычно, ключ – последовательность символов того же алфавита, в котором набрано сообщение.

Пространство ключей – набор всевозможных значений ключа.

Криптография – раздел прикладной математики, в котором изучаются модели, методы, алгоритмы, программные и аппаратные средства преобразования информации в целях сокрытия ее содержания, проверки подлинности, предотвращения, видоизменения или несанкционированного использования.

Задачи криптографии:

1. **Шифрование и расшифрование.**
2. **Аутентификация.**
3. **Хеширование.**
4. **Формирование, хранение и распределение ключей.**

Аутентификация **–** процедура проверки подлинности.

Хеширование **–** преобразование по определённому алгоритму входного массива данных произвольной длины в выходную битовую строку фиксированной длины.

Основная идея шифрования – скрытие содержимого (смысла) передаваемого секретного сообщения.

Расшифрование – нахождение открытого текста на основе известного секретного ключа и шифрованного текста.

Дешифрование – нахождение закрытого ключа или открытого текста на основе шифрованного текста.

Криптограмма – шифрованный текст (ШТ).

Криптосистема – это система, реализованная программно, аппаратно или программно-аппаратно и осуществляющая криптографическое преобразование информации.

Криптоанализ (наука о дешифрации) – это раздел прикладной математики, в котором изучаются модели, методы, алгоритмы, программные и аппаратные средства анализа криптосистемы или ее входных и выходных сигналов с целью извлечения конфиденциальных параметров, включая открытый текст.

Совокупность криптографии и криптоанализа образует новую науку ***криптологию***.

Принцип Керкгоффса – правило разработки криптографических систем, согласно которому в засекреченном виде держится только определённый набор параметров алгоритма, называемый **ключом**, а сам алгоритм шифрования должен быть открытым (Огюст Керкгоффс – великий нидерландский криптограф, лингвист, историк, математик (1835 – 1903)).

Криптостойкость – характеристика шифра, определяющая его стойкость к дешифрации. Часто криптостойкость измеряется количеством операций, необходимых для перебора всех возможных ключей (если длина ключа в битах равна ***n***, то криптостойкость шифра определяется величиной 2^n или интервалом времени, необходимого для дешифрования (MIPS-годы).

MIPS (Million Instructions Per Second) – миллион инструкций в секунду.

Иногда смешивают два понятия: **шифрование** и **кодирование**. Для шифрования надо знать открытый текст, алгоритм шифрования и секретный ключ для симметричных (одноключевых) криптосистем или открытый (публичный) ключ для асимметричных (двухключевых) криптосистем. При кодировании нет ничего секретного, есть только замена

символов открытого текста или слов на заранее определенные символы. Методы кодирования направлены на то, чтобы представить открытый текст в более удобном виде для передачи по телекоммуникационным каналам, для уменьшения длины сообщения (архивация), для повышения помехоустойчивости (обнаружение и исправление ошибок) и т. д. В принципе, кодирование, конечно же, можно рассматривать как шифр замены, для которого «набор» возможных ключей состоит только из одного ключа (например, буква «а» в азбуке Морзе всегда кодируется знаком «. – » и это не является секретом).

Стеганография – наука о методах и средствах скрытия самого факта существования сообщения.

Наибольший общий делитель (НОД) двух натуральных чисел – **наибольшее** натуральное число, делящее одновременно каждое из этих чисел. Запись $(a_i, n) = 1$ означает, что НОД чисел a_i и n равен единице, то есть a_i и n – взаимно простые числа.

Наименьшее общее кратное (НОК) двух и более натуральных чисел – **наименьшее** натуральное число, которое само делится нацело на каждое из этих чисел.

НОК $(a,b)=[a,b]=\frac{a \cdot b}{(a,b)}$.

Основная теорема арифметики

Каждое натуральное число $n > 1$ можно представить в виде $n = p_1 \cdot \ldots \cdot p_k$, где $p_1, \ldots, p_k$ – простые числа, причём такое представление единственно с точностью до порядка следования сомножителей.

Так как некоторые из простых чисел в произведении могут повторяться, то справедливо ***каноническое разложение***