Технологии защиты информации

Преподаватели

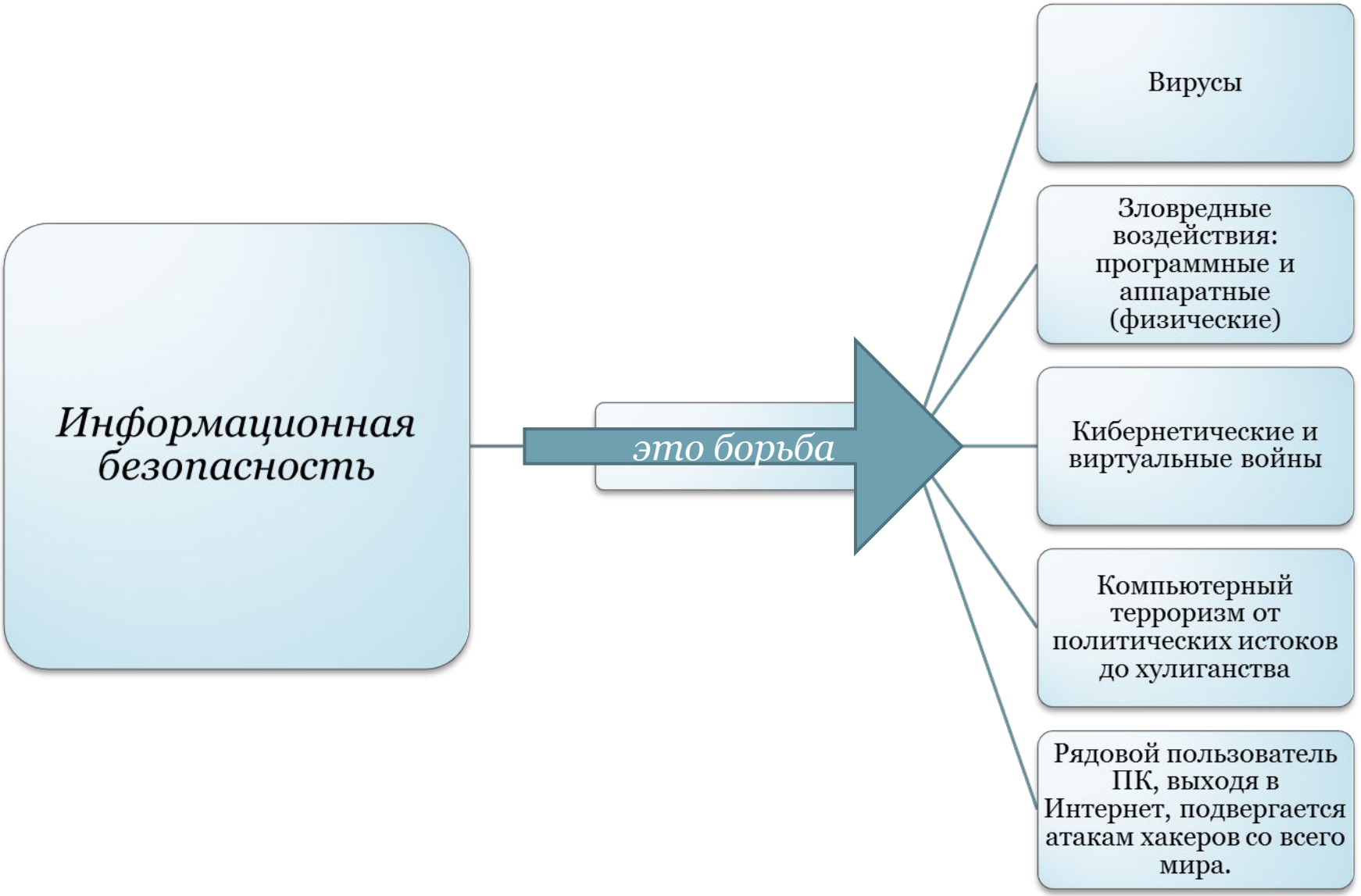
- ст.преп. Сафронов Константин Николаевич
  - 201/12
- асс. Дремач Николай Евгеньевич
  - 215/12

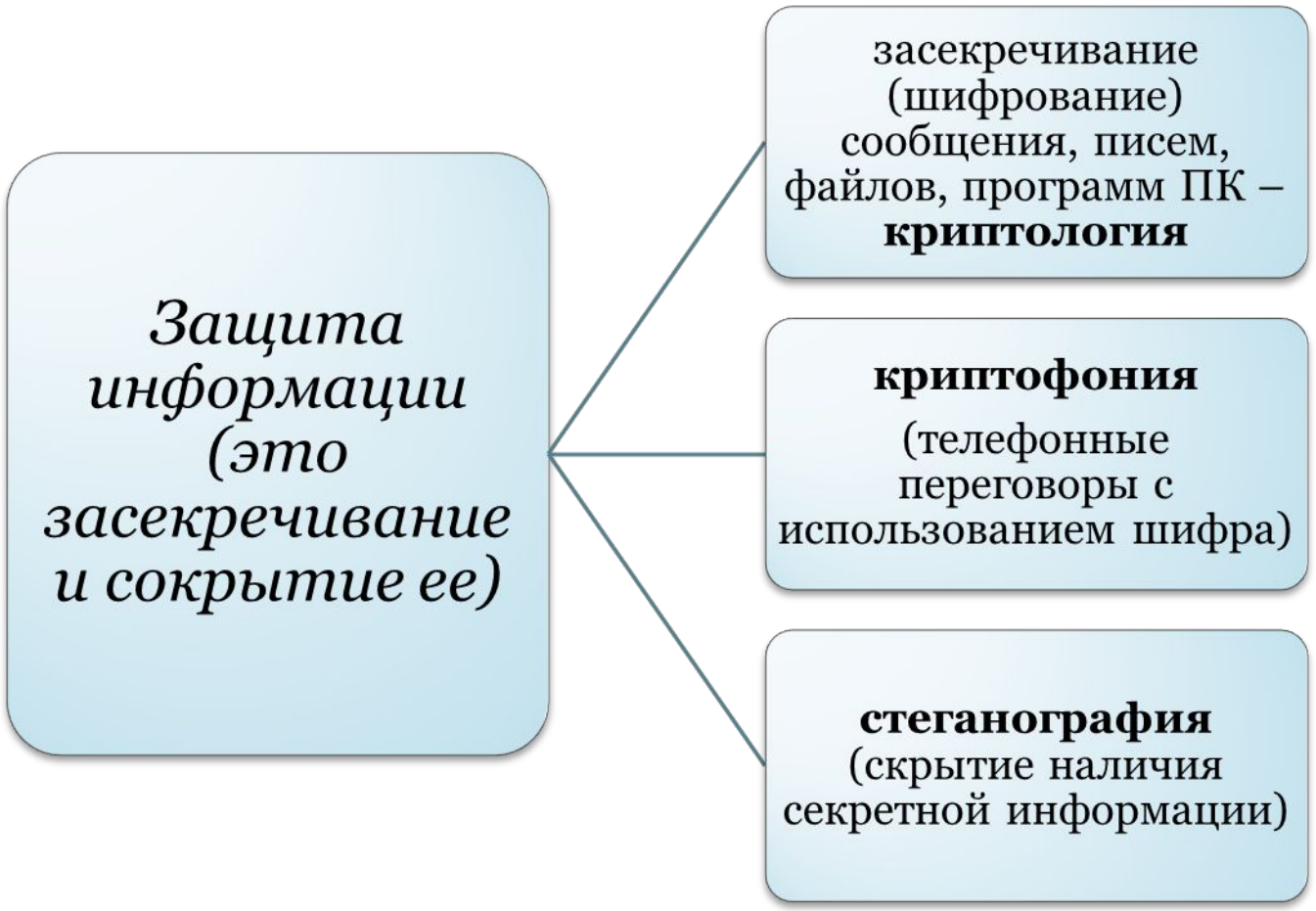
Цели курса

- Изучение основных вопросов криптографии и стеганографии, необходимые для обеспечения компьютерной безопасности информации, защиты информации от несанкционированного доступа и обеспечения конфиденциальности обмена информацией в информационно-вычислительных системах.

Основные темы курса

- Общие вопросы компьютерной безопасности
- Модулярная арифметика
- Генерация ПСП чисел и бит, пригодных для криптографии
- Классическая криптографическая система с одним ключом
- Потоковое шифрование
- Криптосистемы с открытым ключом
- Стеганография


Информационная безопасность
это борьба
Вирусы
Зловредные воздействия: программные и аппаратные (физические)
Кибернетические и виртуальные войны
Компьютерный терроризм от политических истоков до хулиганства
Рядовой пользователь ПК, выходя в Интернет, подвергается атакам хакеров со всего мира.



Между методами информационной безопасности и методами защиты информации особо выделяются методы идентификации и аутентификации.

Угрозы и необходимость сохранности информации

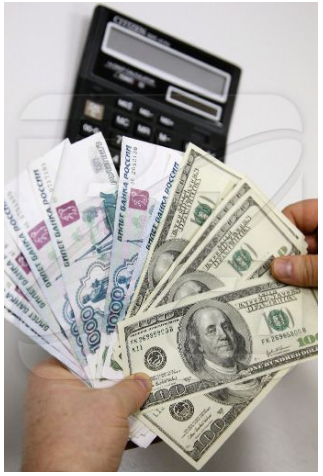
- Необходимость защиты информации осознавалась и предпринималась еще в самом начале широкого внедрения средств вычислительной техники (середина 60-х годов).

Возросла и продолжает увеличиваться зависимость человеческого общества от различных компьютерных систем:

например, на них возлагаются обязанности по:

- сбору налогов
- страхованию
- медицинскому обслуживанию
- электронной оплате сделок и банковским операциям
- управлению транспортом и авиацией и т.п.

Угрозы и необходимость сохранности информации

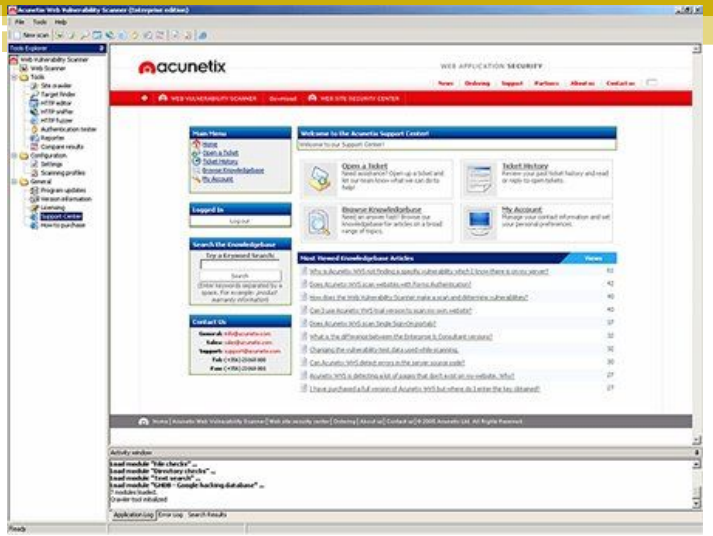


- Изменился сам подход к понятию «информация». Этот термин стал использоваться и для обозначения специального товара, который можно купить, продать, обменять.
- При этом стоимость этого товара часто значительно больше стоимости самой вычислительной системы и устройств (например, системы связи), в рамках которых информация функционирует.

Слабые места ИВС, привлекательные для злоумышленников

- Ввод данных.
  - Часто преступление начинается с целенаправленного искажения вводимых данных или изъятия важных входных документов.
  - Например, можно заставить ИВС оплачивать несостоявшиеся услуги, переводить платежи за закупки, которых не было, формировать ложный курс акций на бирже, указывать несуществующих пользователей системы массового обслуживания и т.п.

Слабые места ИВС, привлекательные для злоумышленников



- Прикладное и системное программное обеспечение (ПО).
  - Чем сложнее программа, тем более уязвима она для умышленного внесения ошибок и искажений.
  - Пример, так называемый «троянский конь». Это такая искаженная программа, которая кроме действий, предусмотренных ее назначением, совершает и несанкционированные операции: считывание или запись чужого секретного файла, изменение защищенного участка ЗУ, выдачу блокирующих сигналов на внешне устройства, передачу ложных сообщений на другие ЭВМ в составе сети.

Слабые места ИВС, привлекательные для злоумышленников

- ПО может быть разработано также и целью его похищения конкурентами, размножением его с целью коммерции.

Слабые места ИВС, привлекательные для злоумышленников

- Процесс связи.
  - Это передача от одной ЭВМ к другой, связь между центральными ЭВМ и терминалами, тракты связи в сети ЭВМ.
  - Этот процесс доступен для постороннего вмешательства и является слабым местом в системе безопасности ИВС. Нарушитель получает возможность доступа к секретной информации и подделывания чужих сообщений для влияния на работу ИВС.

Каналы утечки информации

Наиболее вероятны следующие каналы утечки информации.

- *А) Косвенные каналы,* т.е. без физического доступа злоумышленника к ИВС:

  1. Подслушивающие устройства.

  2. Дистанционное фотографирование экрана дисплея.

  3. Перехват электромагнитных излучений.

Каналы утечки информации

В) *Прямые каналы,* т.е. с доступом к ИВС:

1. Хищение носителей информации.

2. Копирование носителей информации.

3. Хищение производственных отходов.

4. Считывание данных в массивах других пользователей.

5. Чтение остаточной информации в ЗУ системы после выполнения санкционированных запросов.

6. Несанкционированное использование терминалов зарегистрированных пользователей.

7. Маскировка под зарегистрированного пользователя с помощью хищений паролей и других реквизитов разграничения доступа.

8. Маскировка несанкционированных запросов под запросы операционной системы (мистификация).

9. Использование программных ловушек.

10. Получение защищенных данных с помощью серии разрешенных запросов.

11. Использование недостатков языков программирования и ОС.

Каналы утечки информации

С) Каналы с изменением структуры ИВС пли ее компонентов.

1. Незаконное подключение к аппаратуре пли линии связи ИВС.
2. Злоумышленный вывод из строя механизмов защиты.

Методы и средства обеспечения защиты информации

Препятствие

Метод физического преграждения пути злоумышленнику к защищаемой информации (к аппаратуре, носителям информации)

Управление доступом

Метод защиты информации регулированием использования всех ресурсов компьютерной ИС

Идентификация пользователей
Проверка полномочий
Регистрация обращений к ресурсам
Реагирование при попытках несанкционированного доступа

Маскировка

Метод защиты информации путем ее криптографического закрытия (при обработке, хранении, передаче информации)

Регламентация

Метод защиты информации создающий такие условия автоматизированной обработки, хранения и передачи, информации, при которых возможности несанкционированного доступа к ней сводились бы к минимуму

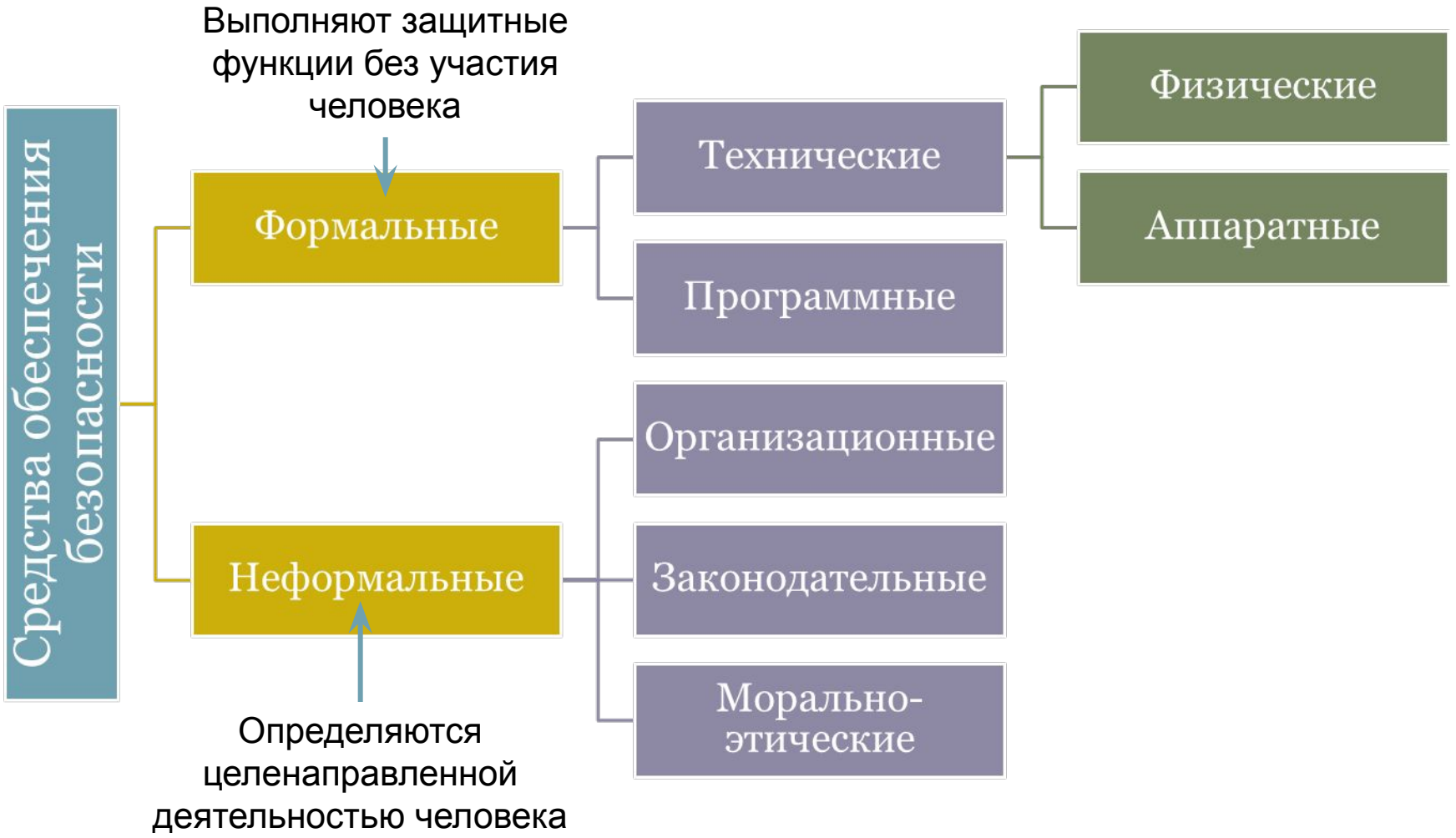
Принуждение

Метод защиты информации при котором пользователи и персонал системы вынуждены соблюдать правила обработки, хранения, передачи информации под угрозой материальной, административной или уголовной ответственности

Побуждение

Метод защиты информации который побуждает пользователей и персонал системы не разрушать установленные порядки за счет соблюдения сложившихся моральных и этических норм

Методы и средства обеспечения защиты информации



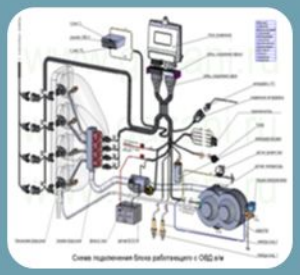
Формальные средства защиты

Технические (электрические, электромеханические, электронные устройства)

- **Физические** (автономные устройства и системы – замки, решетки, охранная сигнализация)
- **Аппаратные** (устройства, встраиваемые в выч. технику.)

Программные - ПО, предназначенное для выполнения функций защиты информации

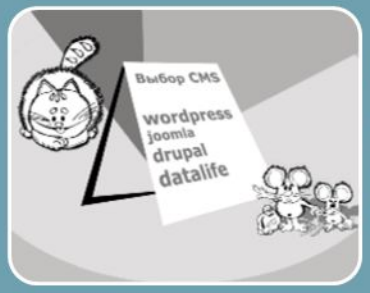
Неформальные средства защиты



Организационные (организационно-технические, организационно-правовые мероприятия, осуществляемые в процессе эксплуатации выч. техники для обеспечения защиты)

Строительство помещений, проектирование сети, монтаж оборудования

Законодательные (определяются законодательными актами страны, регламентирующими правила пользования, обработки, передачи информации ограниченного доступа)



Морально-этические (реализуются в виде норм, сложившихся традиционно). Эти нормы не являются обязательными, но их несоблюдение ведет к потере авторитета человека

Элементы криптологии

CRYPTOS — тайный. LOGOS — слово. Криптология (cryptology) - объединенная дисциплина, охватывающая криптографию и криптоанализ.

Криптография – наука об обеспечении секретности или аутентичности (подлинности) передаваемых сообщений

Криптография — методы засекречивания *исходной (открытой)* информации с использованием *кодов* и/или *шифров* для защитных (секретных) преобразований *формы* информации.

Элементы криптологии

Криптоанализ — методы раскрывания кода или шифра. *Кодируется* информация с целью ее передачи, хранения и обработки. *Шифруется* (перекодируется) — с целью засекречивания.

Все криптопреобразования можно рассматривать как *замену*, в которой исходная информация *(открытый текст)* в понятной форме заменяется некоторой непонятной формой — *шифротекстом (криптограммой)*.

Алгоритмы криптографии

- подстановка (одного знакового ряда вместо другого);
- транспозиция (перестановка порядка следования знаков исходного текста);
- дополнение (алгебраические преобразования знаков (кодов) исходного текста со знаками ключа);
- комбинации вышеприведенных методов.

Классы шифров

- Подстановка или простая (прямая) замена. Каждой букве алфавита ставится в соответствие буква, цифра, символ или какая-либо их комбинация. Эта таблица замены одна для всего текста.
- Многозначная замена (многобуквенная/многоалфавитная система шифрования). В зависимости от порядка следования буквы в сообщении (например: номера ее знакоместа в сообщении) применяются разные алфавиты — таблицы замены.
- Перестановка. Буквы сообщения каким-нибудь способом переставляются между собой.
- Системы шифрования с ключами. Общая схема:

Модулярная арифметика (mod-арифметика)

- Любые целые числа сравниваются по модулю N отображением их на множество модуля N равное

(0,1,2,....N-1) (1)

- Для неотрицательных чисел a > 0 отображение их на множество модуля получается циклическим вычитанием из 'a' величины N до тех пор пока не получится результат r, принадлежащий множеству модуля. Этот результат и есть число 'a' представленное (взятое) по модулю N

$$r = a \bmod N \quad (2)$$