# ОСНОВНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

**Защита информации** – это применение различных средств и методов, использование мер и осуществление мероприятий для того, чтобы обеспечить систему надежности передаваемой, хранимой и обрабатываемой информации.

# Защита информации включает в себя

- обеспечение физической целостности информации, исключение искажений или уничтожения элементов информации
- недопущение подмены элементов информации при сохранении ее целостности
- отказ в несанкционированном доступе к информации лицам или процессам, которые не имеют на это соответствующих полномочий
- приобретение уверенности в том, что передаваемые владельцем информационные ресурсы будут применяться только в соответствии с обговоренными сторонами условиями

**Процессы по нарушению надежности информации бывают:**

случайные - непреднамеренные, ошибочные действия людей, технические сбои

злоумышленные (преднамеренные) - умышленных действий людей

# Случайные сбои

- отказы и сбои аппаратуры
- системные и системотехнические ошибки
- программные ошибки
- ошибки человека при работе с компьютером

# Виды несанкционированного доступа к информации

- просмотр;
- копирование и подмена данных;
- ввод ложных программ и сообщений в результате подключения к каналам связи;
- чтение остатков информации на ее носителях;
- прием сигналов электромагнитного излучения и волнового характера;
- использование специальных программ.

**Объект защиты** – это такой компонент системы, в котором находится защищаемая информация (например, компьютер)

**Элемент защиты** - это совокупность данных, которая может содержать необходимые защите сведения (база известных антивирусу вредоносных программ)

**Система защиты информации** – это совокупность организационных (административных) и технологических мер, программно-технических средств, правовых и морально-этических норм, которые применяются для предотвращения угрозы нарушителей с целью сведения до минимума возможного ущерба пользователям и владельцам системы.

**Организационно-административные средства защиты** - это регламентация доступа к информационным и вычислительным ресурсам, а также функциональным процессам систем обработки данных.

# Основные организационно-административные средства

- допуск к обработке и передаче охраняемой информации только проверенных должностных лиц
- хранение носителей информации, которые представляют определенную тайну, а также регистрационных журналов в сейфах, недоступных для посторонних лиц
- учет применения и уничтожения документов (носителей) с охраняемой информацией
- разделение доступа к информационным и вычислительным ресурсам должностных лиц в соответствии с их функциональными обязанностями

**Технические средства защиты** применяются для создания некоторой физически замкнутой среды вокруг объекта и элементов защиты.

- ограничение электромагнитного излучения через экранирование помещений, в которых осуществляется обработка информации
- реализация электропитания оборудования, отрабатывающего ценную информацию, от автономного источника питания или общей электросети через специальные сетевые фильтры

# Программные средства и методы защиты

- разграничение и контроль доступа к ресурсам
- регистрация и изучение протекающих процессов
- предотвращение возможных разрушительных воздействий на ресурсы
- криптографическая защита информации

**Технологические средства защиты информации** - ряд мероприятий, органично встраиваемых в технологические процессы преобразования данных.

- создание архивных копий носителей
- ручное или автоматическое сохранение обрабатываемых файлов во внешней памяти компьютера
- автоматическая регистрация доступа пользователей к различным ресурсам
- выработка специальных инструкций по выполнению всех технологических процедур и др.

**Правовые и морально-этические меры и средства защиты** включают в себя действующие в стране законы, нормативные акты, регламентирующие правила, нормы поведения, соблюдение которых способствует защите информации.

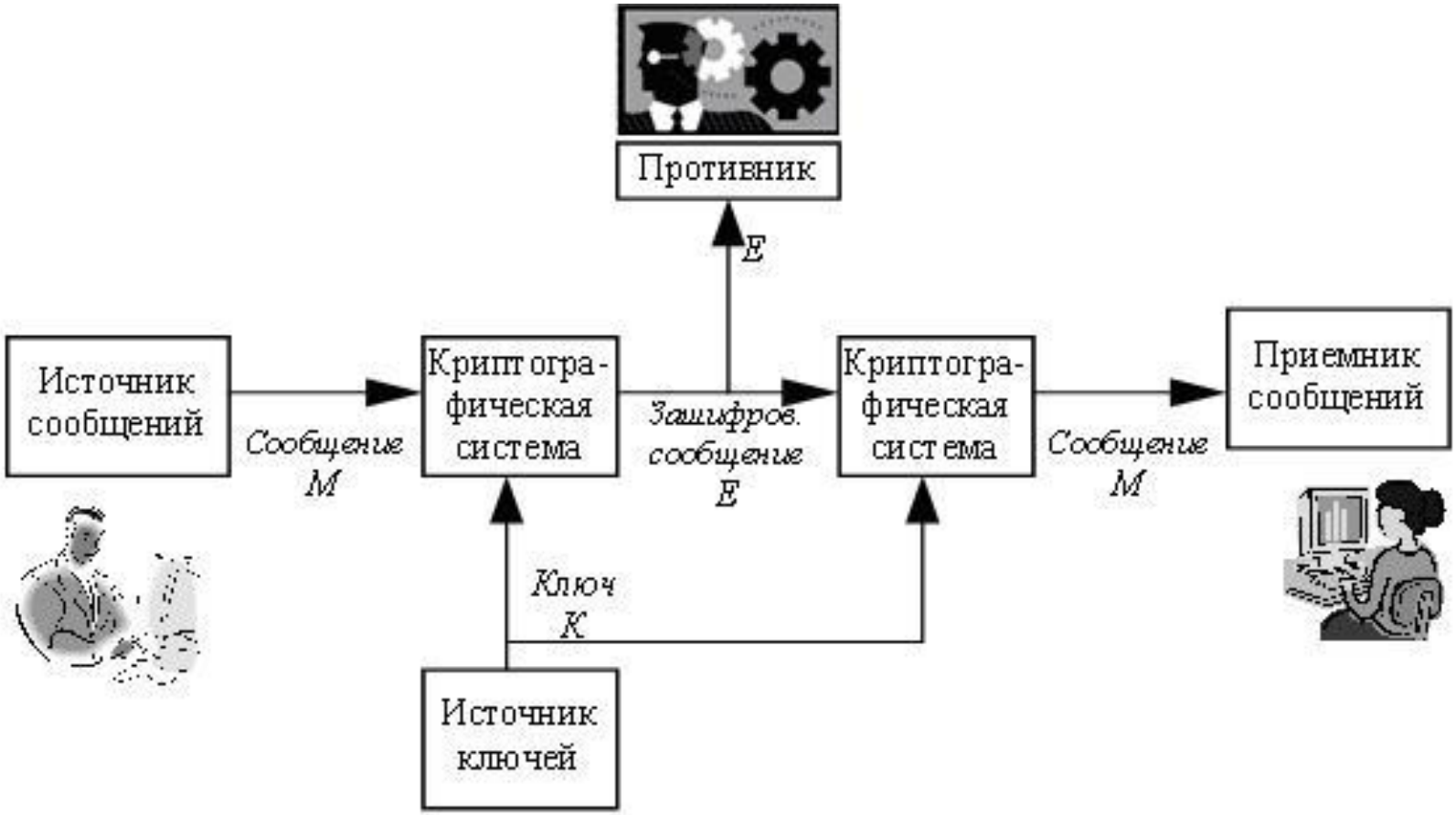
# Криптографический метод защиты информации

**Защита информации методом криптографического преобразования** - это приведении ее к неявному виду через преобразование составных частей информации (букв, цифр, слогов, слов) с применением специальных алгоритмов либо аппаратных средств и кодов ключей.

**Ключ** - изменяемая часть криптографической системы, хранящейся в тайне и определяющей, какое шифрующее преобразование из возможных выполняется в данном случае.

## Требования, предъявляемые к методам криптографического преобразования

- метод должен быть достаточно устойчивым к попыткам раскрытия исходного текста с помощью использования зашифрованного
- обмен ключа не должен быть тяжел для запоминания
- затраты на защитные преобразования следует сделать приемлемыми при заданном уровне сохранности информации
- ошибки в шифровании не должны вызывать явную потерю информации
- размеры зашифрованного текста не должны превышать размеры исходного текста


Противник
E
Источник сообщений
Сообщение M
Криптографическая система
Зашифров. сообщение E
Криптографическая система
Сообщение M
Приемник сообщений
Ключ K
Источник ключей

## Симметричные методы защитных преобразований:

- методы перестановки
- методы замены (подстановки)
- аддитивные методы
- комбинированные методы

Особенности методов перестановки и замены (подстановки): короткий ключ и сложный алгоритм преобразования

Особенность аддитивных методов: простые алгоритмы и длинные ключи

Комбинированные методы являются более надежными и сочетают в себе достоинства используемых компонентов

**Метод перестановки** - разбиение исходного текста на блоки, а затем запись этих блоков и чтение шифрованного текста по разным путям геометрической фигуры.

**Метод замены** - символы исходного текста (блока), записанные в одном алфавите, заменяются символами другого алфавита в соответствии с используемым ключом преобразования.

# Шифр Цезаря

Каждая буква сообщения заменяется на другую, которая в русском алфавите отстоит от исходной на три позиции дальше.

Например, буква **А** заменяется на **Г** , **Б** на **Д** и так далее вплоть до буквы **Ь** , которая заменялась на **Я** , затем **Э** на **А** , **Ю** на **Б** и, наконец, **Я** на **В** .

# ЗАМЕНА
# КГПЗРГ

# Одноалфавитная замена

| Откр. текст | Шифр 1 | Шифр 2 | | Откр. текст | Шифр 1 | Шифр 2 | | Откр. текст | Шифр 1 | Шифр 2 |
|---|---|---|---|---|---|---|---|---|---|---|
| А | В | ^ | | М | Т | № | | Ч | М | ∑ |
| Б | И | @ | | Н | Ц | # | | Ш | У | ∇ |
| В | О | ) | | О | . | - | | Щ | Д | ϒ |
| Г | А | + | | П | Ж | = | | Ъ | Э | ℵ |
| Д | Щ | < | | Р | Г | ( | | Ы | Н | ⊕ |
| Е | П | > | | С | Л | ? | | Ь | Ю | × |
| Ж | К | ∀ | | Т | Х | % | | Э | Ы | ω |
| З | Б | ♦ | | У | С | ⊗ | | Ю | Ш | $ |
| И | Ъ | * | | Ф | Ь | ! | | Я | Е | Δ |
| К | пробел | ♥ | | Х | Ч | № | | пробел | Ф | ∞ |
| Л | Р | ♠ | | Ц | З | ® | | . | Я | ♣ |

| Открытое сообщение | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| В | Ы | Ш | Л | И | Т | Е | | П | О | Д | К | Р | Е | П | Л | Е | Н | И | Е |
| Зашифрованное сообщение с использованием шифра 1 | | | | | | | | | | | | | | | | | | | |
| О | Н | У | Р | Ъ | Х | П | Ф | Ж | . | Щ | | Г | П | Ж | Р | П | Ц | Ъ | П |
| Зашифрованное сообщение с использованием шифра 2 | | | | | | | | | | | | | | | | | | | |
| ) | ⊕ | ∇ | ♠ | * | % | > | ∞ | = | - | < | ♥ | ( | > | = | ♠ | > | # | * | > |

ТНФЖ.ИПЩЪРЪ

# Пропорциональные шифры

| Символ | Варианты замены | Символ | Варианты замены |
|---|---|---|---|
| А | 760 128 350 201 | С | 800 767 105 |
| Б | 101 | Т | 759 135 214 |
| В | 210 106 | У | 544 |
| Г | 351 | Ф | 560 |
| Д | 129 | Х | 768 |
| Е | 761 130 802 352 | Ц | 545 |
| Ж | 102 | Ч | 215 |
| З | 753 | Ш | 103 |
| И | 762 211 131 | Щ | 752 |
| К | 754 764 | Ъ | 561 |
| Л | 132 354 | Ы | 136 |
| М | 755 742 | Ь | 562 |
| Н | 763 756 212 | Э | 750 |
| О | 757 213 765 133 353 | Ю | 570 |
| П | 743 766 | Я | 216 104 |
| Р | 134 532 | Пробел | 751 769 758 801 849 035.. |

101 757 132 562 103 213 762

751 800 761 754 134 130 759

# БОЛЬШОЙ СЕКРЕТ

# Многоалфавитные подстановки (таблицы Вижинера)

| | |
|---|---|
| АБВГДЕ..... | .....ЭЮЯ |
| БВГДЕЖ..... | .....ЮЯА |
| ВГДЕЖЗ..... | .....ЯАБ |
| ГДЕЖЗИ..... | .....АБВ |
| ДЕЖЗИК..... | .....БВГ |
| ЕЖЗИКЛ..... | .....ВГД |
| ..... | ..... |
| ЯАБВГД..... | .....ЬЭЮ |

АБВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ

ВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯАБ

ЕЖЗИКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯАБВГД

НОПРСТУФХЦЧШЩЪЫЬЭЮЯАБВГДЕЖЗИКЛМ

СТУФХЦЧШЩЪЫЬЭЮЯАБВГДЕЖЗИКЛМНОПР

| | |
|---|---|
| ИСХОДНЫЙ ТЕКСТ – МЕТОД ПЕРЕСТАНОВКИ<br>КЛЮЧ – ВЕСНА ВЕСНАВЕСНАВЕ<br>ЗАШИФРОВ.ТЕКСТ – ОЛВЬД СЛАТСФЕЭЬВМО | АБВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЬЫЪЭЮЯ<br>**ВГДЕЖЗИКЛМНО**ПРСТУФХЦЧШЩЬЫЪЭЮЯАБ<br>**ЕЖЗИКЛ**МНОПРСТУФХЦЧШЩЬЫЪЭЮЯАБВГД<br>НОПРСТУФХЦЧШЩЬЫЪЭЮЯАБВГДЕЖЗИКЛМ<br>СТУФХЦЧШЩЬЫЪЭЮЯАБВГДЕЖЗИКЛМНОПР |