

*Тақырыбы: «Ақпаратты сақтау және қорғау әдістері»*

*Орындаған: Аймбетова Г.А*

*Топ: 101 МІ*

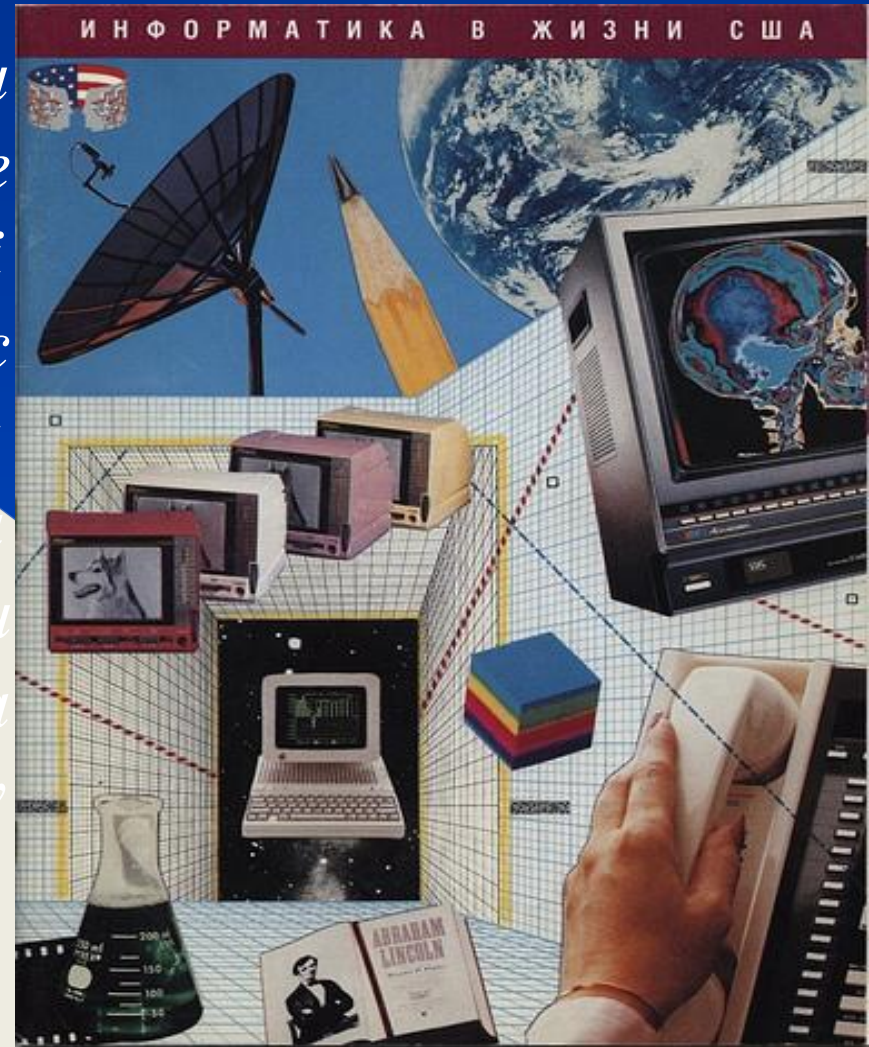
*Тексерген: Адалбек А.А*

# *Жоспар*

- ✓ *Кіріспе*
- ✓ *Ақпаратты қорғау*
- ✓ *Ақпаратты қорғаудың мақсаты*
- ✓ *Ақпаратты қорғау әдістері*
- ✓ *Ақпаратқа төнетін қауіпті әрекеттер*
- ✓ *RSA асимметриялық шифрлеу стандарты*
- ✓ *RealSecure™ жүйесі*
- ✓ *ЭЦҚ*
- ✓ *Компьютерлік вирустар*

# Кіріспе

- Хабарлар тасымалданатын байланыс арналары көбінесе қорғалмаған болып келеді және осы арнаға қатынас құру құқығы бар кез- келген адам хабарларды қолға түсіре алады. Сондықтан тораптарда ақпаратқа біраз шабуылдар жасау мүмкіндігі бар.



## *Ақпаратты қорғау*

- ◎ *Ақпаратты қорғау – ақпараттың сыртқа кетуінің, оны ұрлаудың, жоғалтудың, рұқсатсыз көшірмесін жасаудың алдын алу үшін жүргізілген шаралар кешені.*
- ◎ *Ақпаратты қорғаудың мақсаты*
  1. *Қауіп төндіретін негізгі көздерін анықтау*
  2. *Қорғаныс әдістеріне мінездеме беру*
  3. *Тиімді қорғаныс шараларын қолдану*

# Ақпаратты сақтау әдістері

- **Артықшылығы:** сенімділігі және әр түрлі факторлардан тәуелсіз, модификациялауға жоғарғы төзімділік.
- **Кемшілігі:** көлемі мен массасы үлкен және қымбат.

Техникалық

- **Артықшылығы:** қарапайым, сенімді, модификациялауға және дамуға бейімділік
- **Кемшілігі:** функционалдық желінің шектілігі және компьютер типіне тәуелділік

Бағдарламалық

- **Артықшылығы:** шексіз модификациялауға бейім, олар көптеген мәселелерді шешуге мүмкіндік береді.
- **Кемшілігі:** субъективті факторларға жоғарғы тәуелділік

Аралас

- Техникалық және бағдарламалық тәсілдердің аралық түрі.

Ұйымдастырылған

- Компьютердің жұмысының сенімділігін, бағалы ақпараттың сақталуын, оған өзгеріс енгізуден, құпия сақталуын қамтамасыз етеді.

Криптографиялық

*Ақпаратқа төнетін қауіпті  
әрекеттер*

*Кездейсоқ*

*Әдейілеп жасаған*

*Ақпаратты қорғау  
әдістері:*

```
graph LR; A[Ақпаратты қорғау әдістері] --- B[Архивтеу]; A --- C[Шифрлен жазу]; A --- D[Цифрлық қолтаңба];
```

*Архивтеу*

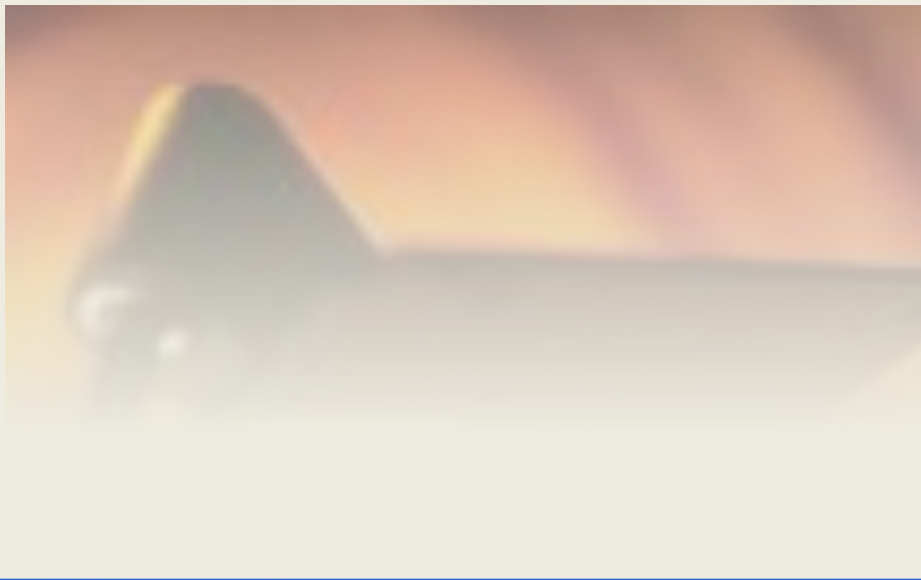
*Шифрлен жазу*

*Цифрлық қолтаңба*

## *RSA асимметриялық шифрлеу стандарты.*

- ◎ *Асимметриялық шифрлеудің ең таралған алгоритмі RSA алгоритмі болып табылады. Ол үш зерттеуші-математик Рональдом Ривестпен (R.Rivest), Ади Шамирмен (A.Shamir) және Леонард Адльманмен (L.Adleman) 1977-78 жылдары ұсынылған болатын. Осы алгоритмнің әзірлеушілеріне құпиямен бір тараптық жұмыс істеу идеясын тиімді асыру мүмкін болды.*



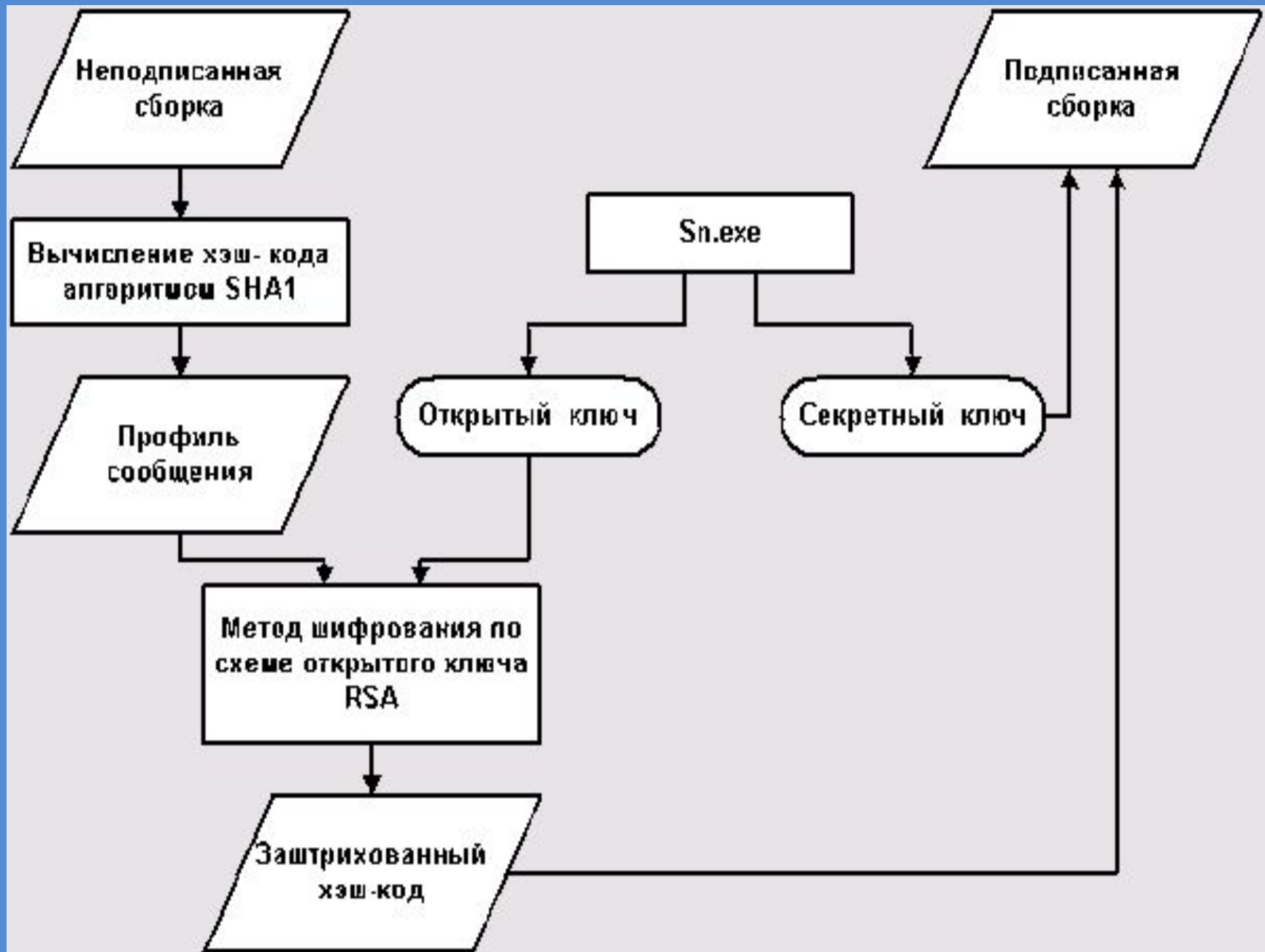


Ашық  
кілт

- *Шифрлеу кілті.*

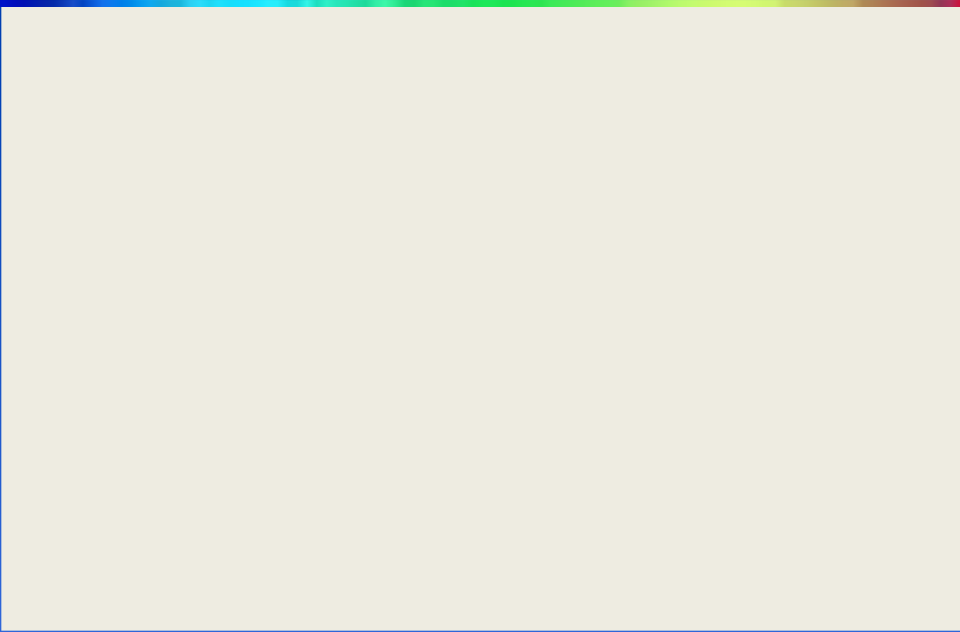
Жабық  
кілт

- *Шифрлеудің мағынасын ашу кілтін хабарламаны алушыға құпияда ұстау.*



**RealSecure™ жүйесі  
дұшпандық  
қызметтерді табуға  
және сіздің  
корпоративтік  
желіңіздің торабына  
шабуылдарды тануға  
мүмкіндік береді.**

**Электрондық  
цифрлық қолтаңба  
(ЭЦҚ) – бұл  
электрондық  
құжаттың деректемесі,  
жасанды көшірмеден  
электрондық  
құжатты қорғау үшін  
арналған.**



# Компьютерлік вирустар

*Компьютерлік вирустар – бұл компьютердің қалыпты жұмыс істеуіне кедергі жасайтын, мәліметтерді қайталап жазатын немесе жоятын бағдарламалар. Бұл бағдарламалар өз бетімен көбейеді де, амалдық жүйе мен желідегі нысандарға зиян келтіруі мүмкін. Компьютерлік вирустардың айрықша сипаттарына олардың өз бетімен іске қосылып, компьютердің дұрыс жұмыс істеуіне кедергі жасауға қабілеттілігі жатады. Ол компьютерге пайдаланушының рұқсатынсыз, "зақымдалған" дискета немесе "зақымдалған" файлмен бірге түсуі мүмкін. Ішінде вирусы бар программа "зақымдалған" деп аталады.*



**Вирустар**



**Компьютердің вируспен  
зақымданғанын қалай  
анықтауға болады?**



**Вирусты қалай  
жоюға болады?**



**Вирусқа қарсы  
бағдарлама**

**ТОҚТА ВИРУС!!!**



**STOP VIRUS!!!**

*Вирустармен күресу үшін антивирустар деп аталатын арнайы бағдарламалар бар. Вирусқа қарсы бағдарлама (антивирус) — компьютерлік вирустарды жұқтырған бағдарламаларды табуға және емдеуге, сондай-ақ файлдың вирус жұқтыруының алдын алуға арналған бағдарлама.*

*Бүгінгі таңда вирусқа қарсы бағдарламалардың алуан түрлері бар: Dr.Web, Касперский Антивируссы, Eset NOD32, McAfee, AVG, Panda Software, Norton Antivirus және т.б.*



## Қолданылған әдебиеттер

- ◎ Информатика: Учебник / под ред. Проф. Н.В. Макаровой. - М.: Базовый курс. Теория. 2004 г.
- ◎ Мельников В. Защита информации в компьютерных системах. М.: Финансы и статистика, Электронинформ, 1997
- ◎ [www.5ballov.ru](http://www.5ballov.ru).
- ◎ Информатика О.Камардинов (Алматы 2008)