РЕДСОФТ

Об использовании средств электронной подписи Windows-приложениями в среде Linux

Коптев Алексей Петрович
заместитель генерального директора ООО «РЕД СОФТ»

РЕДСОФТ

краткая история проблемы импортозамещения в сфере ИТ

1966

- отказ от СМ и БЭСМ
- освоение IBM-360

1991

- развал СССР, открытие рынка
- интервенция Microsoft

2000-2010

- Доктрина информационной безопасности, № Пр-1895
- первые отечественные операционные системы на ядре Linux

2010

- взлет и падение НПП
- попытка перехода на СПО

2014

- #КрымНаш!
- начало санкций

2015

- выработка политики в ответ на санкции
- создание РОПО, № 188-ФЗ

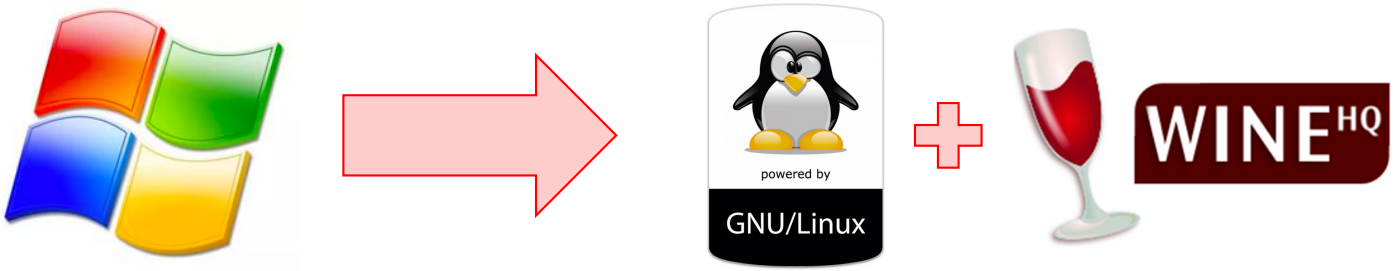
2017

- Стратегия развития информационного общества до 2030 года
- вирусная атака WannaCry

Андрей Петрович Ершов (1931–1988) – один из зачинателей теоретического и системного программирования в СССР, создатель Сибирской школы информатики и неформальный лидер всего советского программистского сообщества (**http://ershov.iis.nsk.su**)

РЕДСОФТ

характеристика текущей ситуации

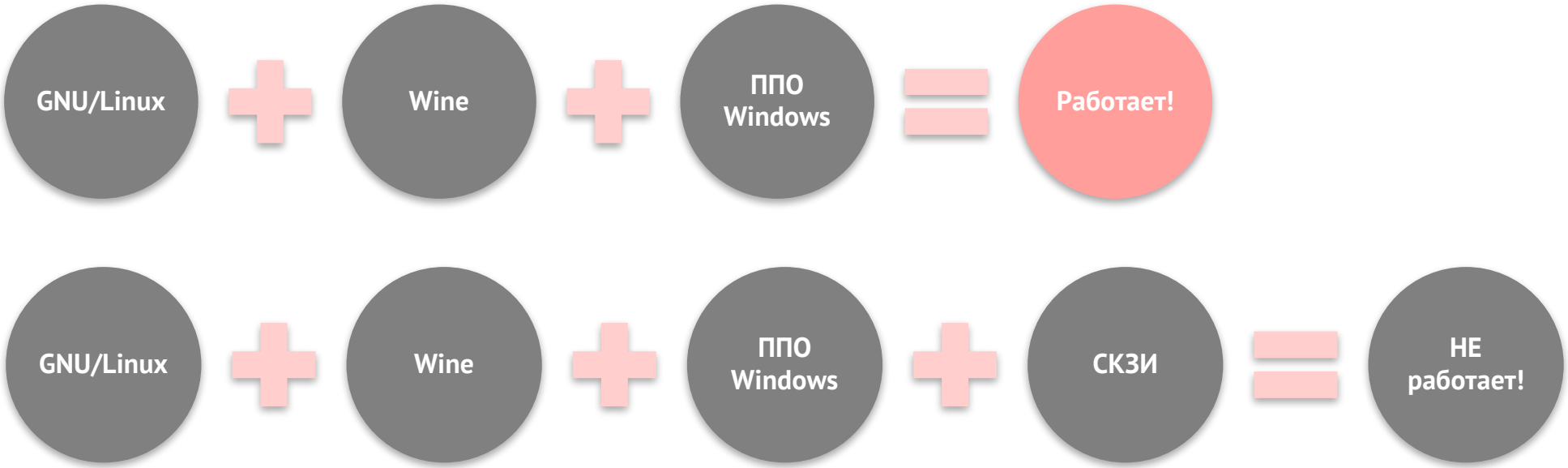


3 – 5 млн. рабочих станций

федеральные организации	региональные организации	иные организации
• Администрация Президента, Аппарат Правительства, Совет Федерации, Государственная дума • Следственный Комитет, Судебные органы, Органы прокуратуры, Счетная палата • Федеральные органы исполнительной власти, Подведомственные организации федеральных органов исполнительной власти	• Органы государственной власти субъектов Российской Федерации • Подведомственные организаций органов государственной власти субъектов Российской Федерации	• Органы местного самоуправления • Государственные корпорации • Иные организации с государственным участием

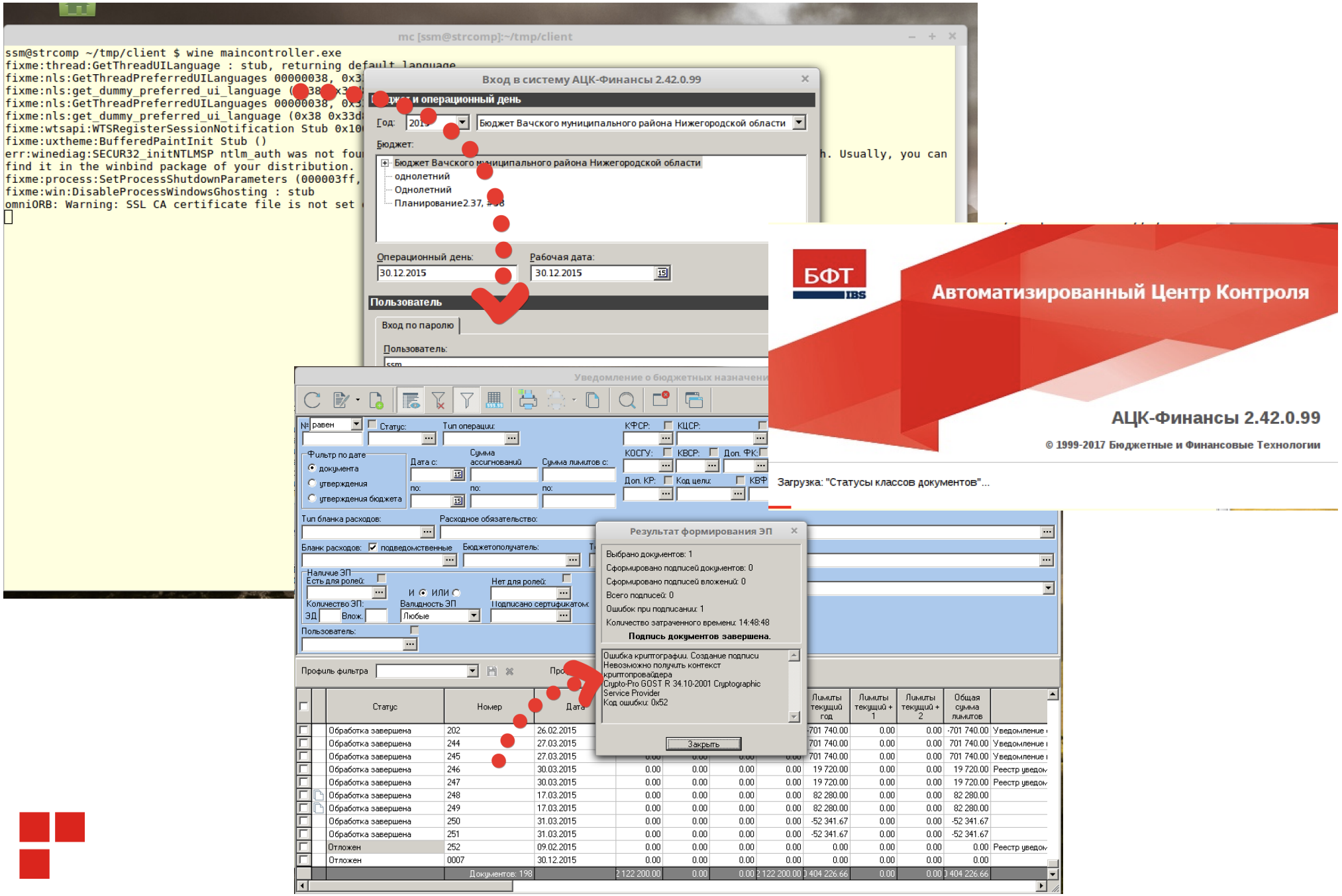
РЕДСОФТ

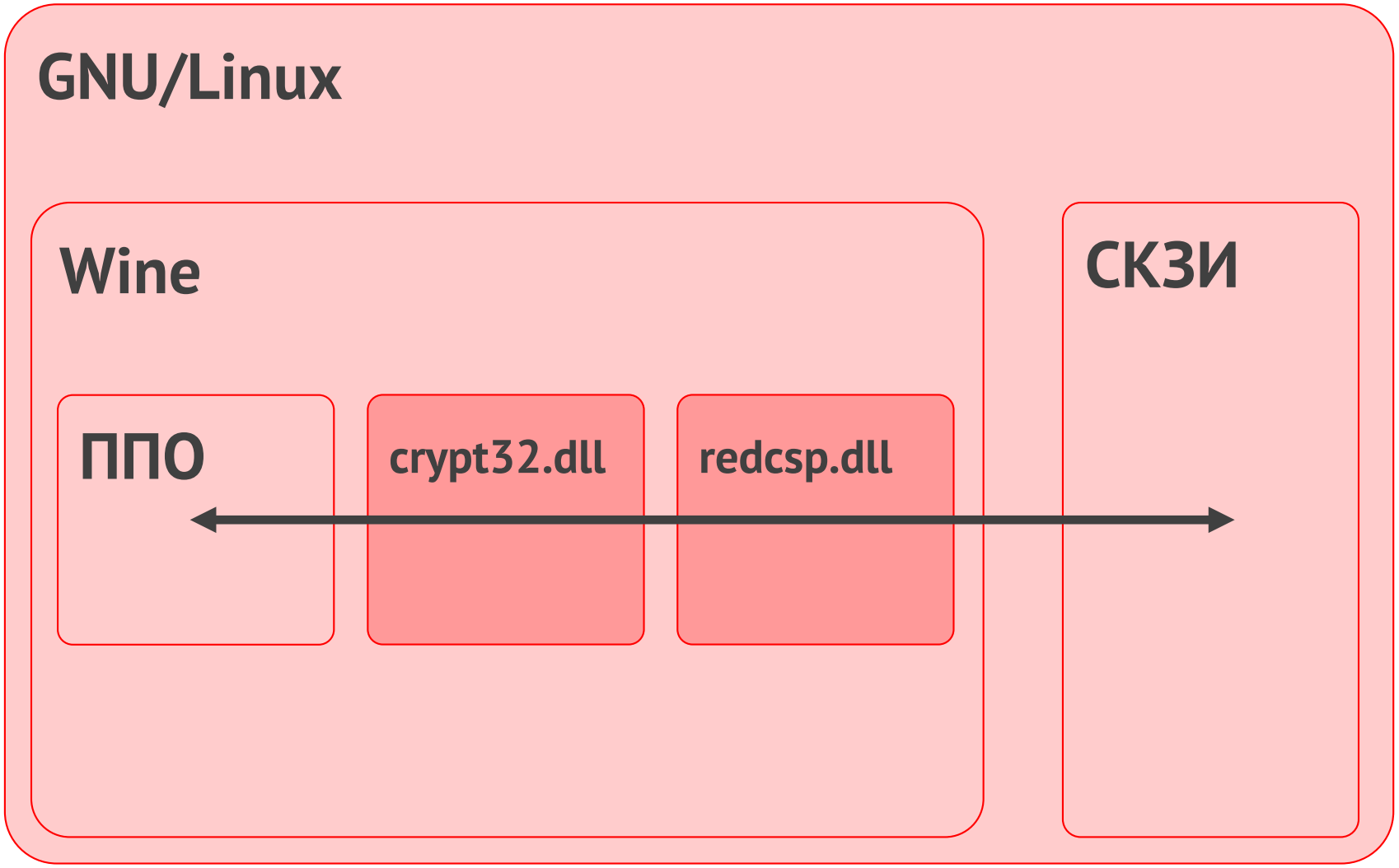
камень преткновения



РЕДСОФТ

конкретный пример, точка зрения пользователя

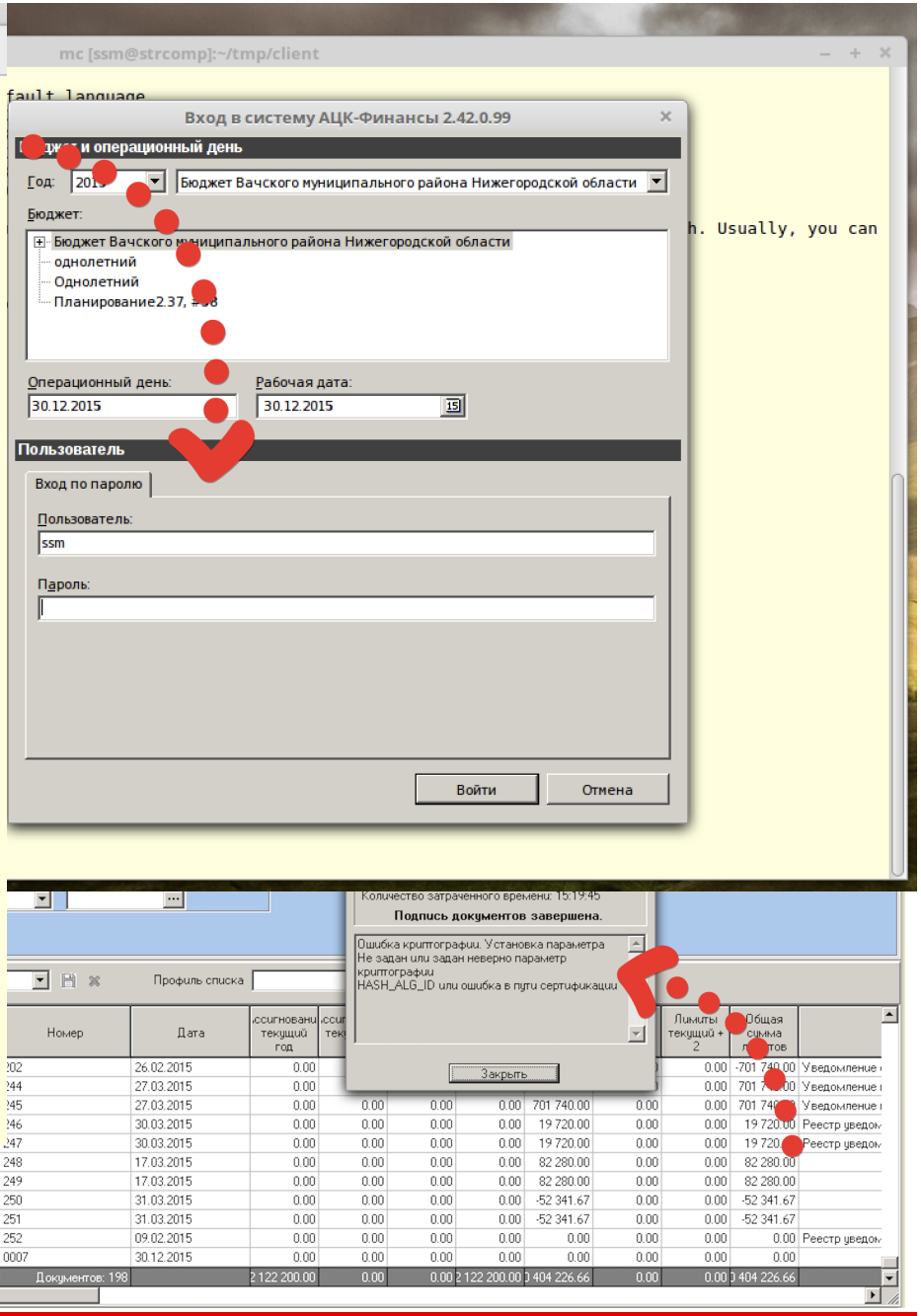



GNU/Linux
Wine
ППО
crypt32.dll
redcsp.dll
СКЗИ

РЕДСОФТ

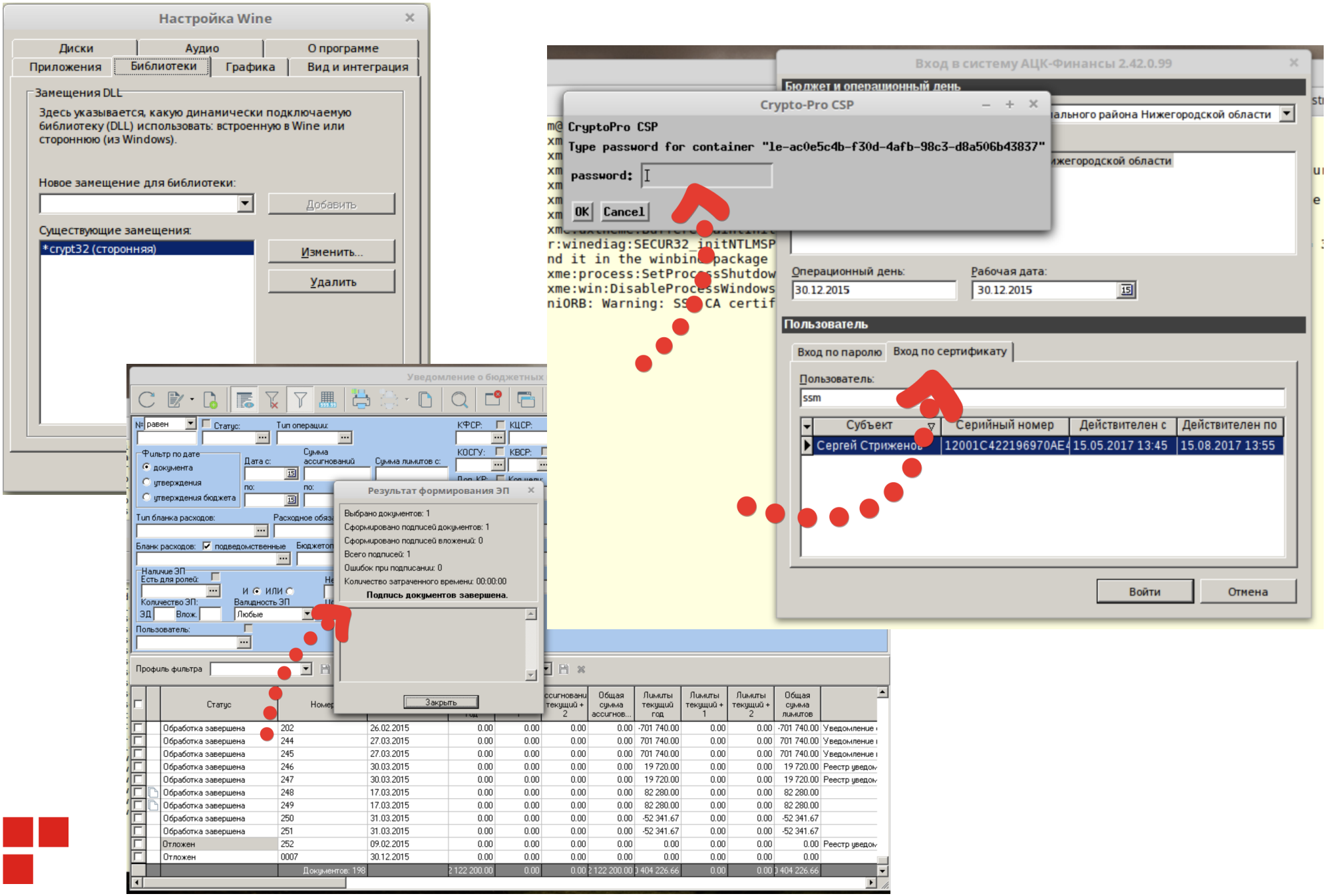
первый подход, реализация адаптера

```
mc [ssm@strcomp]:~/tmp
ssm@strcomp ~/tmp $ wine listProviders.exe
fixme:module:load_library unsupported flag(s) used (flags: 0x00000800)
fixme:module:load_library unsupported flag(s) used (flags: 0x00000800)
fixme:module:load_library unsupported flag(s) used (flags: 0x00000800)
fixme:module:load_library unsupported flag(s) used (flags: 0x00000800)
fixme:module:load_library unsupported flag(s) used (flags: 0x00000800)
fixme:module:load_library unsupported flag(s) used (flags: 0x00000800)
fixme:module:load_library unsupported flag(s) used (flags: 0x00000800)
Listing Available Provider Types.
Provider type    Provider Type Name
_____________    _____________________________________
          1      RSA Full (Signature and Key Exchange)
         12      RSA SChannel
         24      RSA Full and AES
         75      GOST R 34.10-2001 Signature with Diffie-Hellman Key Exchange


Listing Available Providers.
Provider type    Provider Name
_____________    _____________________________________
         75      Crypto-Pro GOST R 34.10-2001 Cryptographic Service Provider
          1      Microsoft Base Cryptographic Provider v1.0
          1      Microsoft Enhanced Cryptographic Provider v1.0
         24      Microsoft Enhanced RSA and AES Cryptographic Provider
         24      Microsoft Enhanced RSA and AES Cryptographic Provider (Prototype)
         12      Microsoft RSA SChannel Cryptographic Provider
          1      Microsoft Strong Cryptographic Provider

The default provider name is "Microsoft Enhanced Cryptographic Provider v1.0"

Enumerating the supported algorithms

     Algid      Bits      Type         Name          Algorithm
                                     Length           Name
     _____________________________________________________
    0000661eh    256     Encrypt       14          GOST 28147-89
    0000801eh    256     Hash          16          GOST R 34.11-94
    00002e23h    512     Signature     18          GOST R 34.10-2001
    0000aa24h    512     Exchange      18          Diffie-Hellman EL
    0000aa25h    512     Exchange      18          Diffie-Hellman EL
    0000801fh    32      Hash          19          HMAC GOST 28147-89

The program completed without error.
```



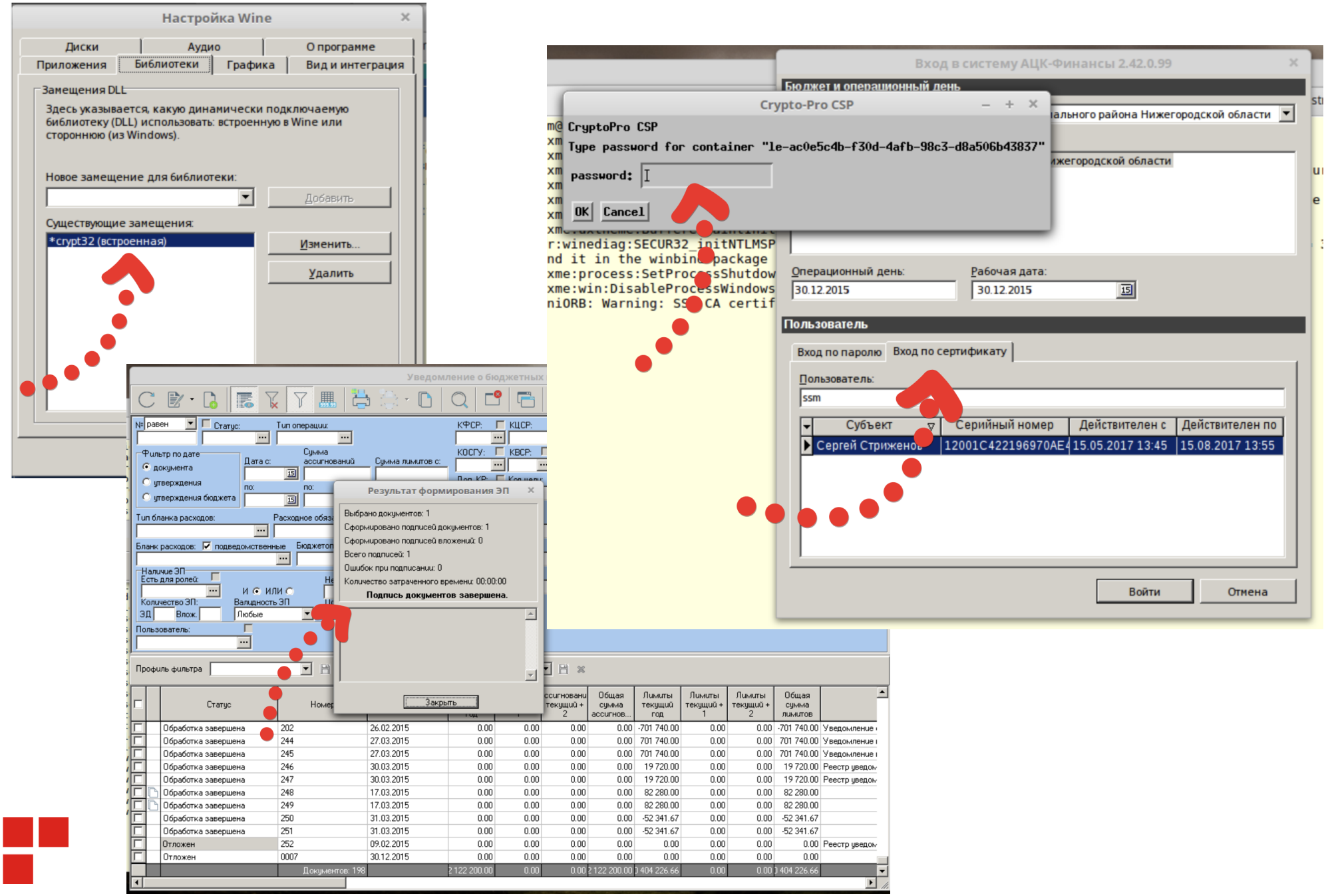
РЕДСОФТ

первый подход, искушение winetricks



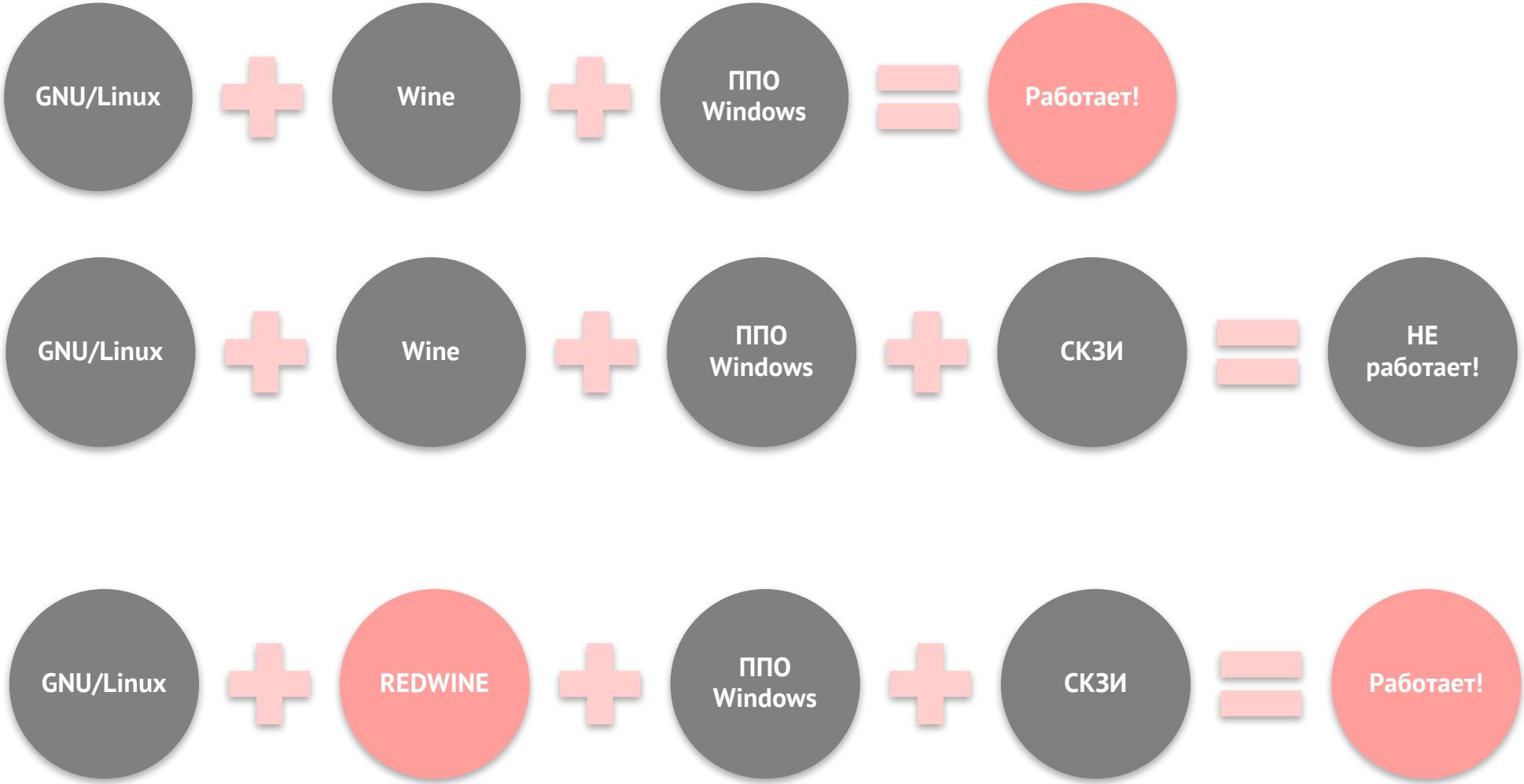
РЕДСОФТ

второй подход



РЕДСОФТ

хрустальная туфелька



РЕДСОФТ

что делаем и какие дальнейшие шаги

- дистрибутив для ОС Гослинукс
- дистрибутив для РедОС
- партнерство с разработчиками других отечественных ОС
- партнерство с разработчиками ППО
- создание дистрибутивов ППО со встроенным REDWINE

РЕДСОФТ

Спасибо за внимание!

Коптев Алексей Петрович
заместитель генерального директора ООО «РЕД СОФТ»

alexey.koptev@red-soft.ru
www.red-soft.ru