Информационна сигурност чрез Свободни технологии

OpenFest

Информационна сигурност чрез Свободни технологии

Адриан Н. Илиев

OpenFest

Информационна сигурност чрез Свободни технологии

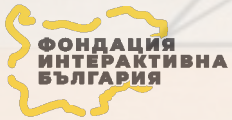
адв. **Адриан Н. Илиев**
www.Advocati.org

www.Advocati.org
право | адвокати | консултация

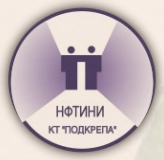
OpenFest

Информационна сигурност чрез Свободни технологии

Адриан Н. Илиев
www.Advocati.org



Фондация „Интерактивна България“
www.InterAct.bg



Национална федерация
Техническа индустрия, Наука, Информатика
www.NFTINI.org

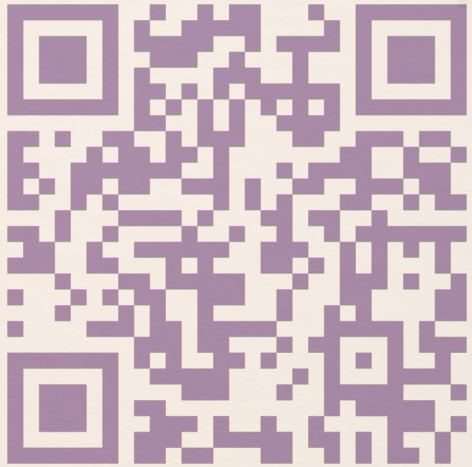
LibTec
Институт за Свободни технологии
www.LibTec.org

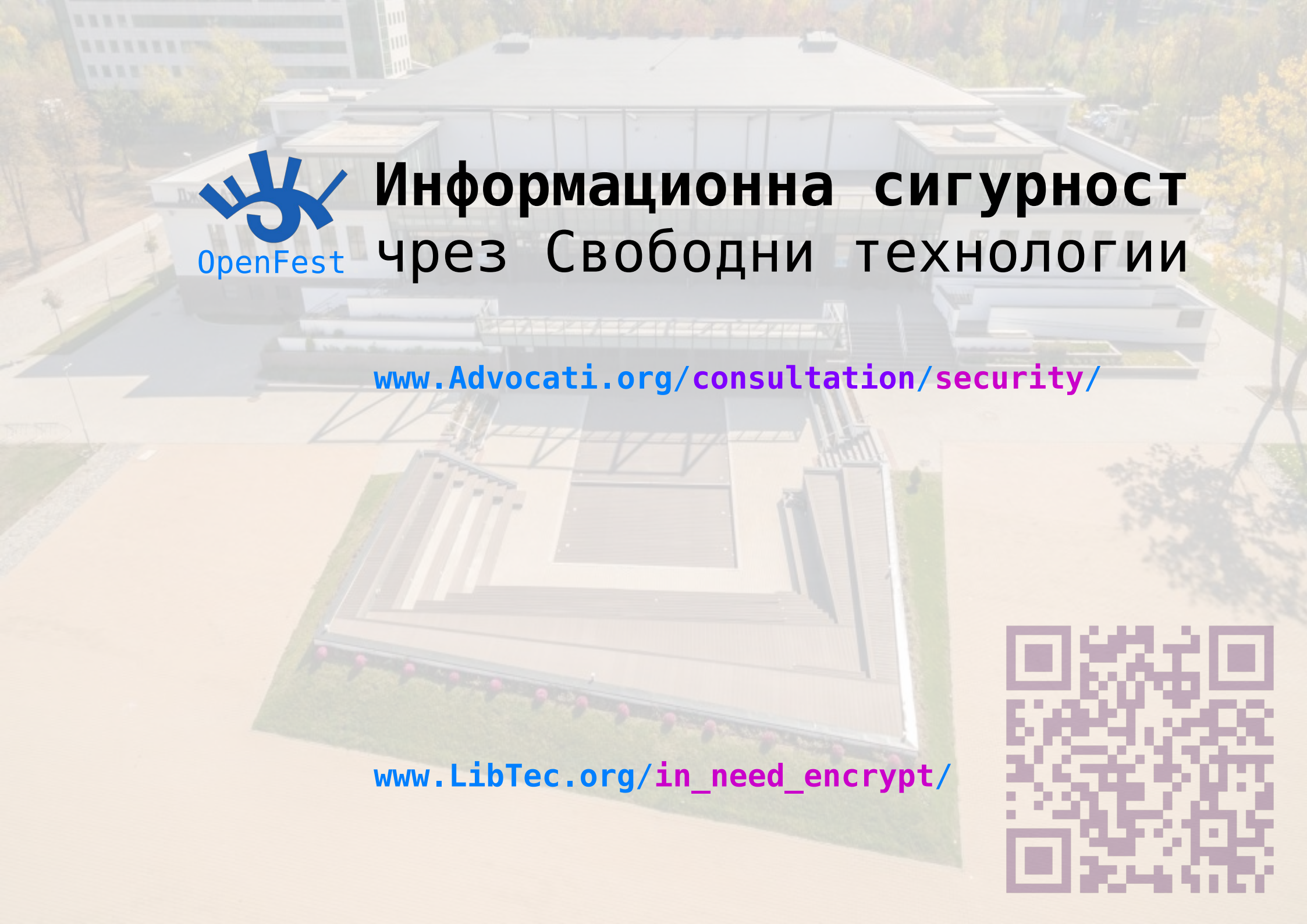
Информационна сигурност чрез Свободни технологии

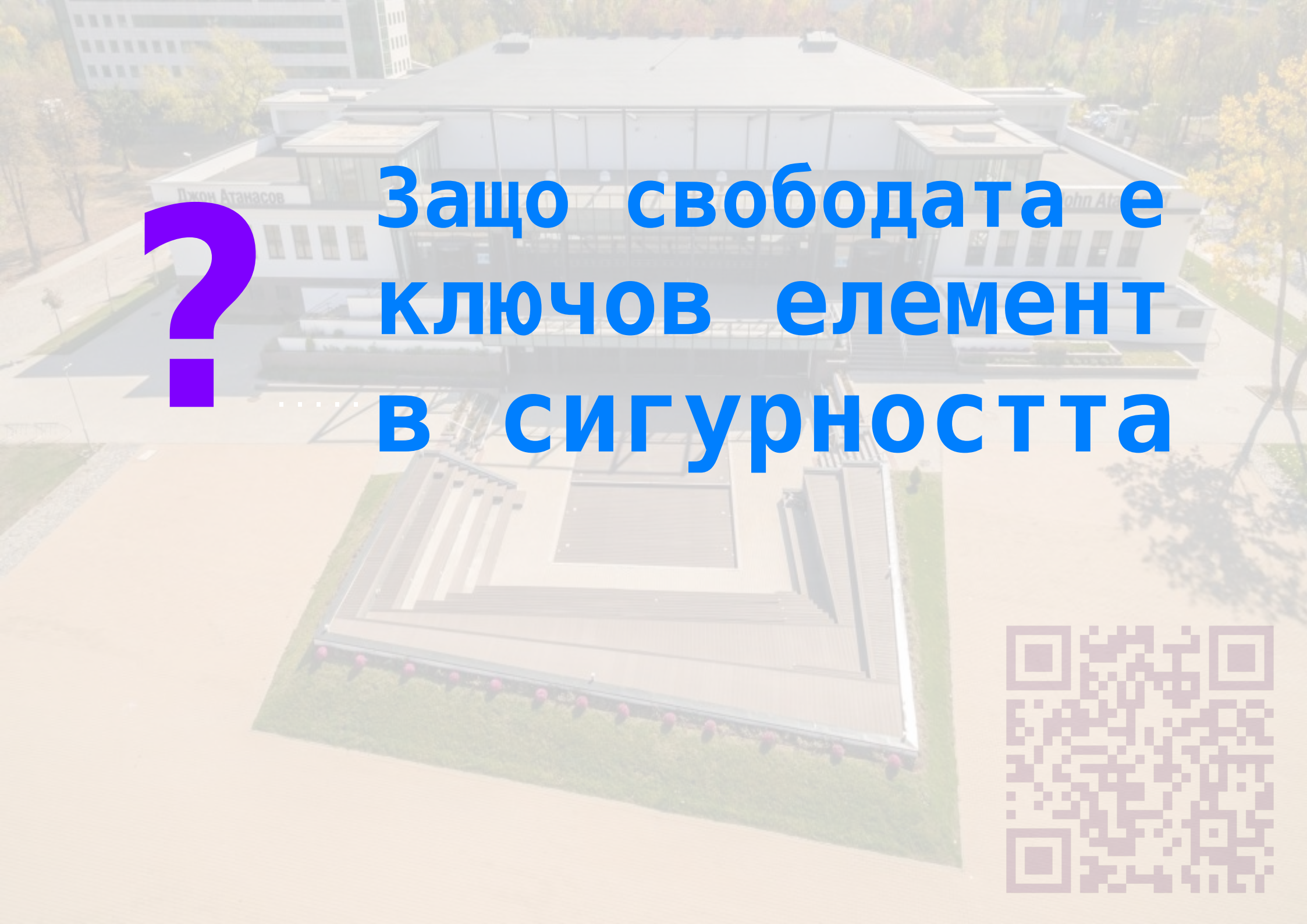
Адриан Н. Илиев
www.Advocati.org

Richard M. Stallman & **Denis 'GNUtoo' Carikli**

LibTec
Институт за Свободни технологии
www.LibTec.org




OpenFest
Информационна сигурност
чрез Свободни технологии
www.Advocati.org/consultation/security/
www.LibTec.org/in_need_encrypt/



? Защо свободата е ключов елемент в сигурността

свобода

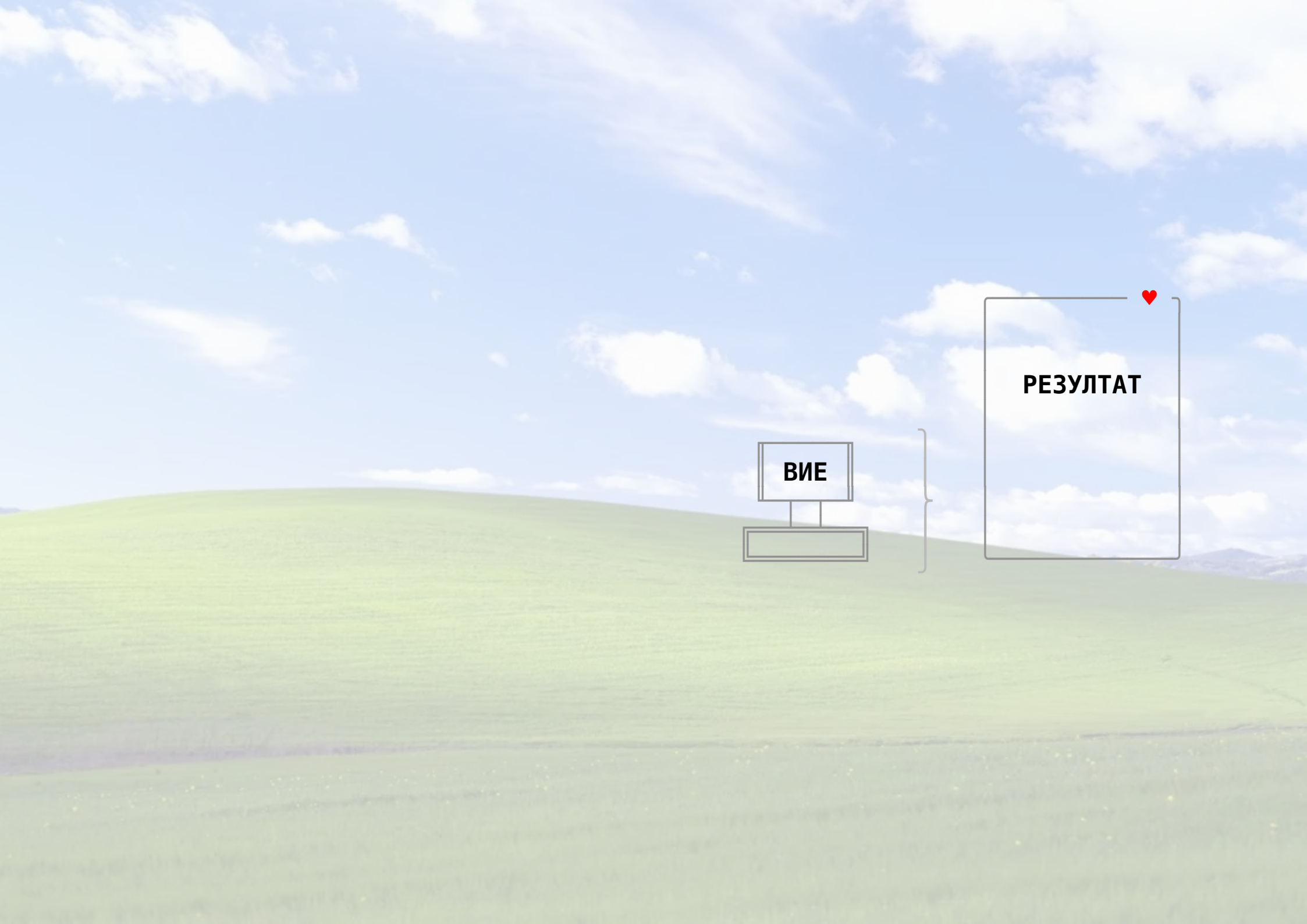
„Свобода (лат. libertas) –
способност човек да действа безпрепятствено,
без ограничения, според своите желания.“

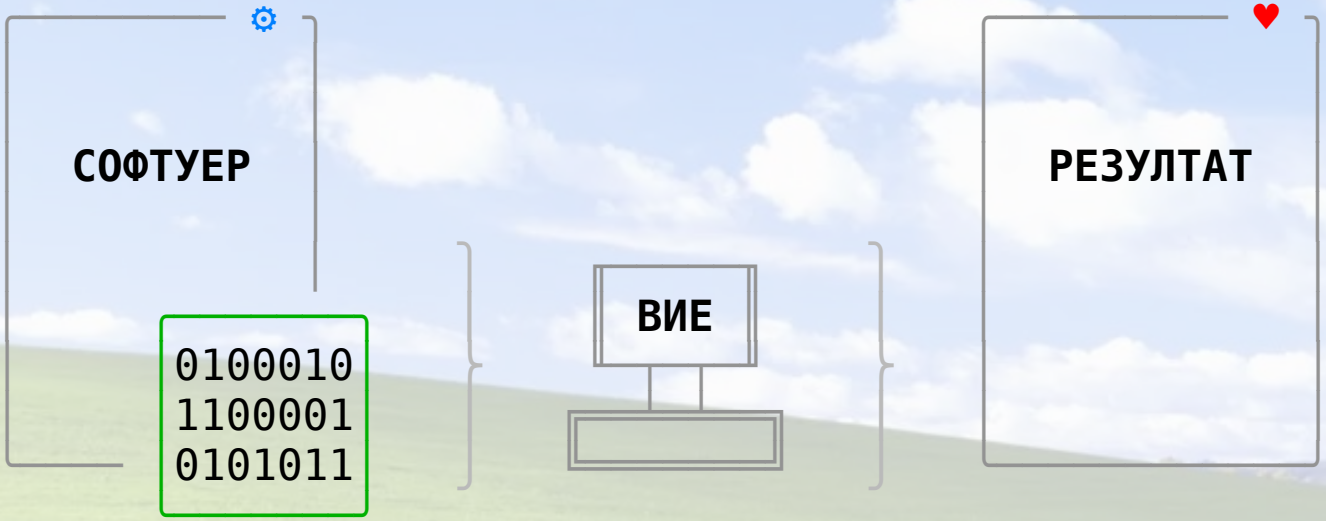
Oxford English Dictionary
Словарь Институт Философии РАН

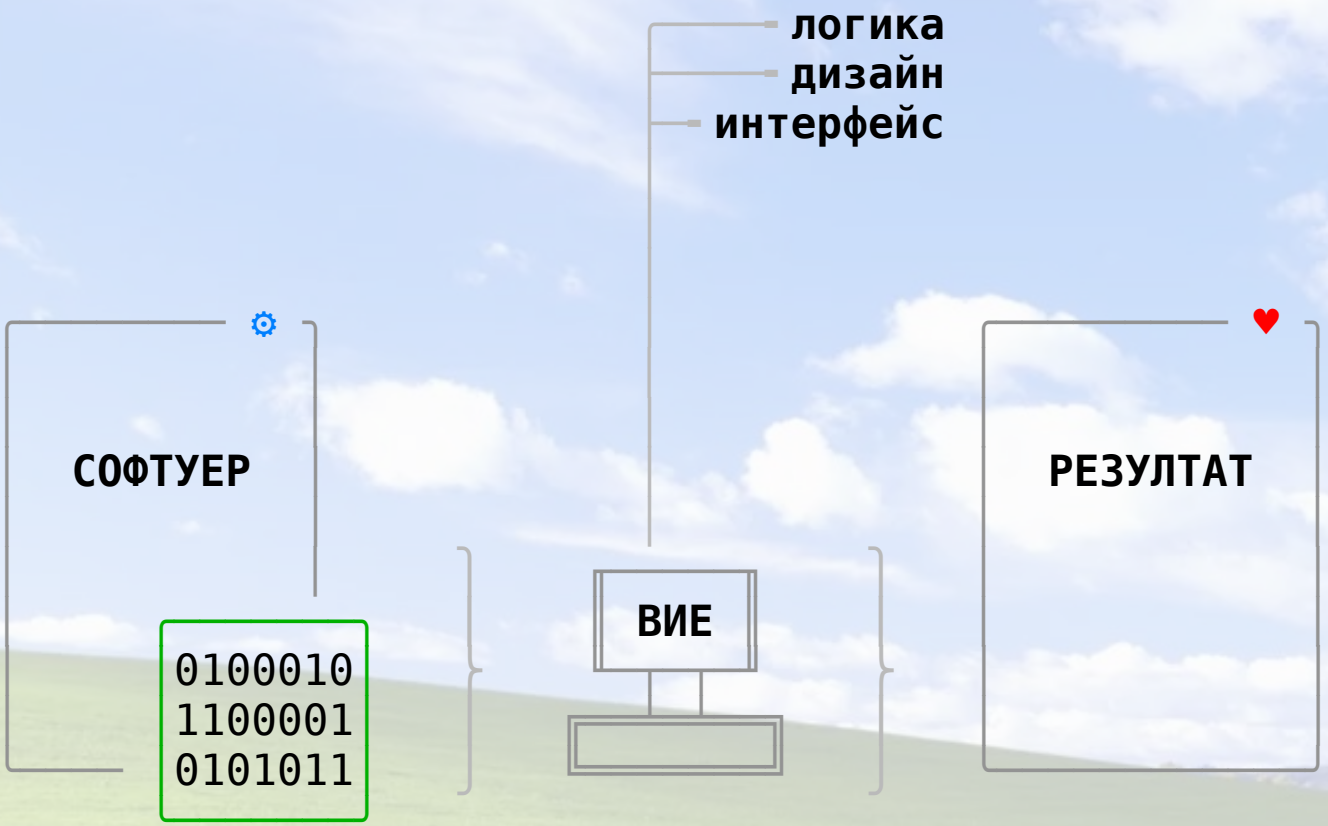
сигурност

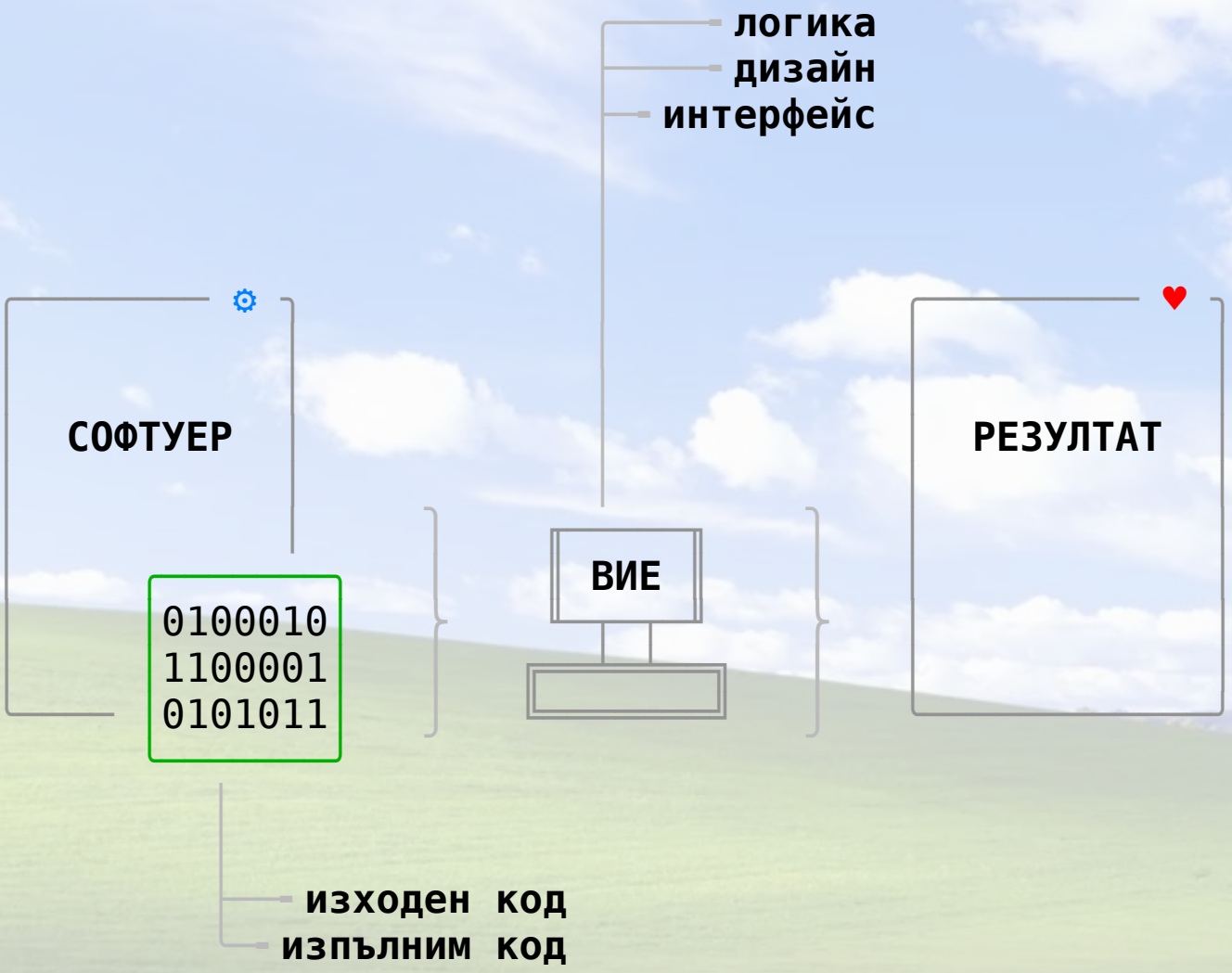
„Сигурност (лат. securitas) –
функционално състояние, осигуряващо
противодействие и неутрализиране
на фактори, които влият
или могат да повлияят деструктивно.“

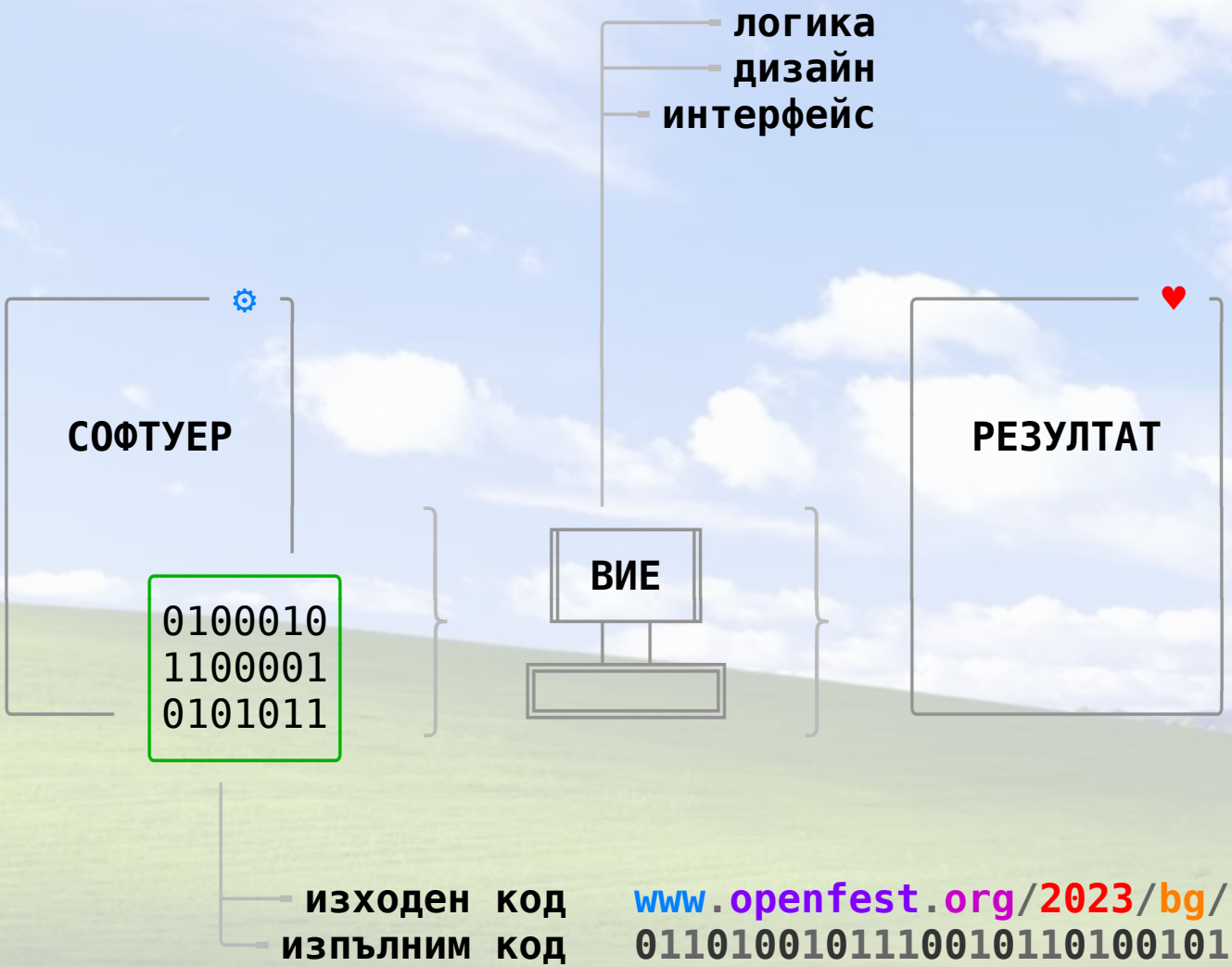

ВИЕ

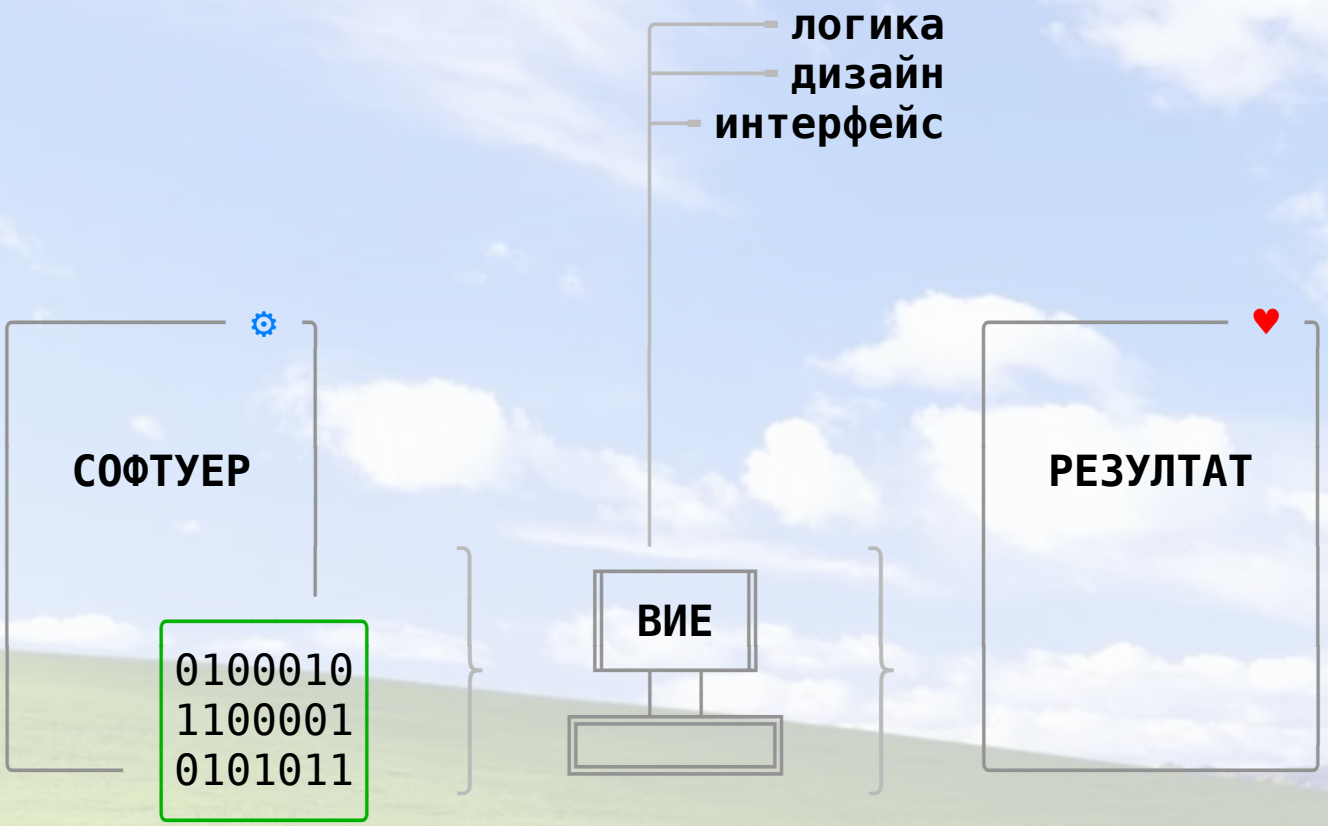

РЕЗУЛТАТ
ВИЕ


СОФТУЕР
0100010
1100001
0101011
ВИЕ
РЕЗУЛТАТ


логика
дизайн
интерфейс
СОФТУЕР
0100010
1100001
0101011
ВИЕ
РЕЗУЛТАТ


логика
дизайн
интерфейс
СОФТУЕР
0100010
1100001
0101011
ВИЕ
РЕЗУЛТАТ
изходен код
изпълним код

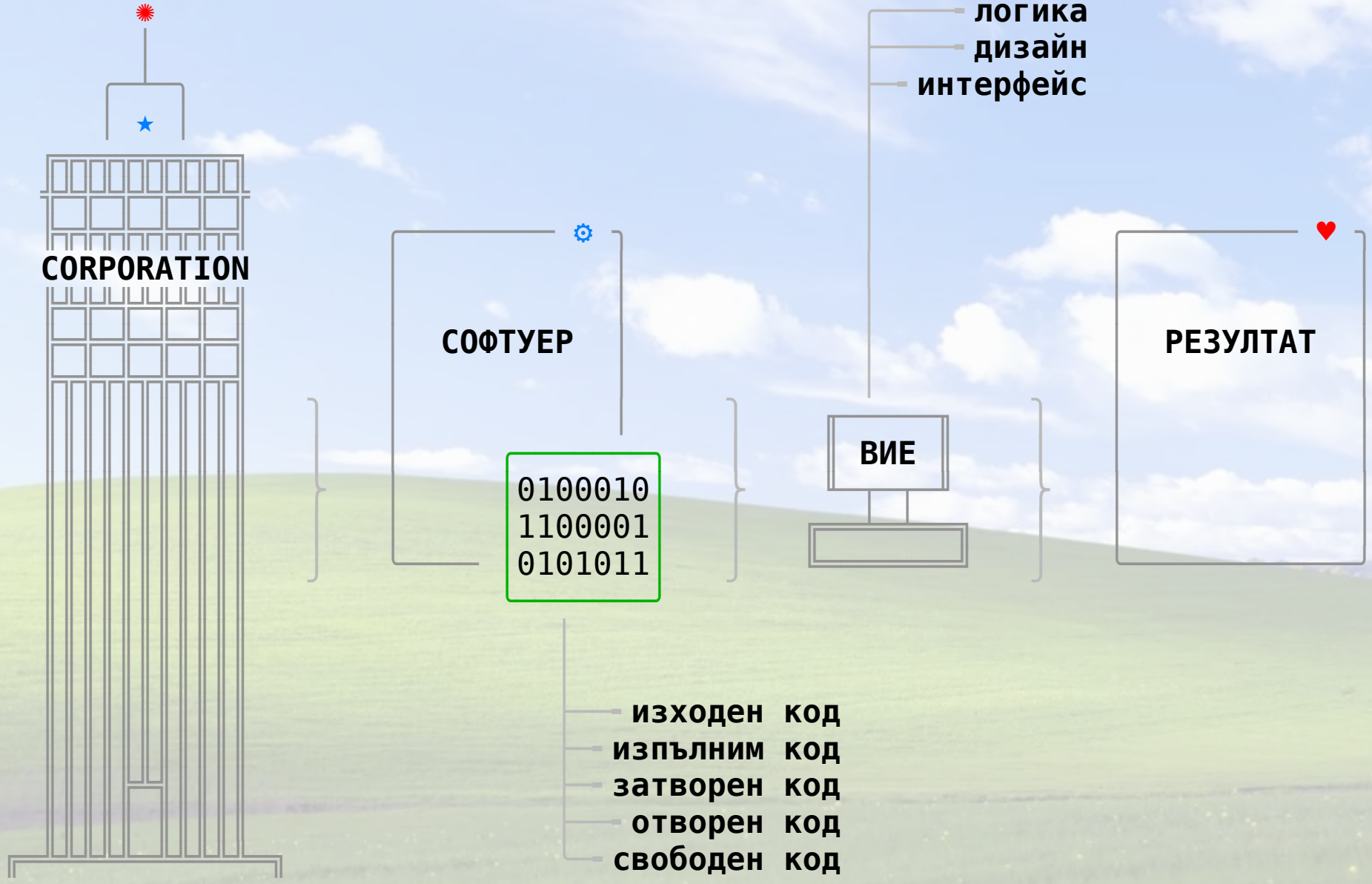

логика
дизайн
интерфейс
СОФТУЕР
0100010
1100001
0101011
ВИЕ
РЕЗУЛТАТ
изходен код
изпълним код
www.openfest.org/2023/bg/
01101001011100101101001 01

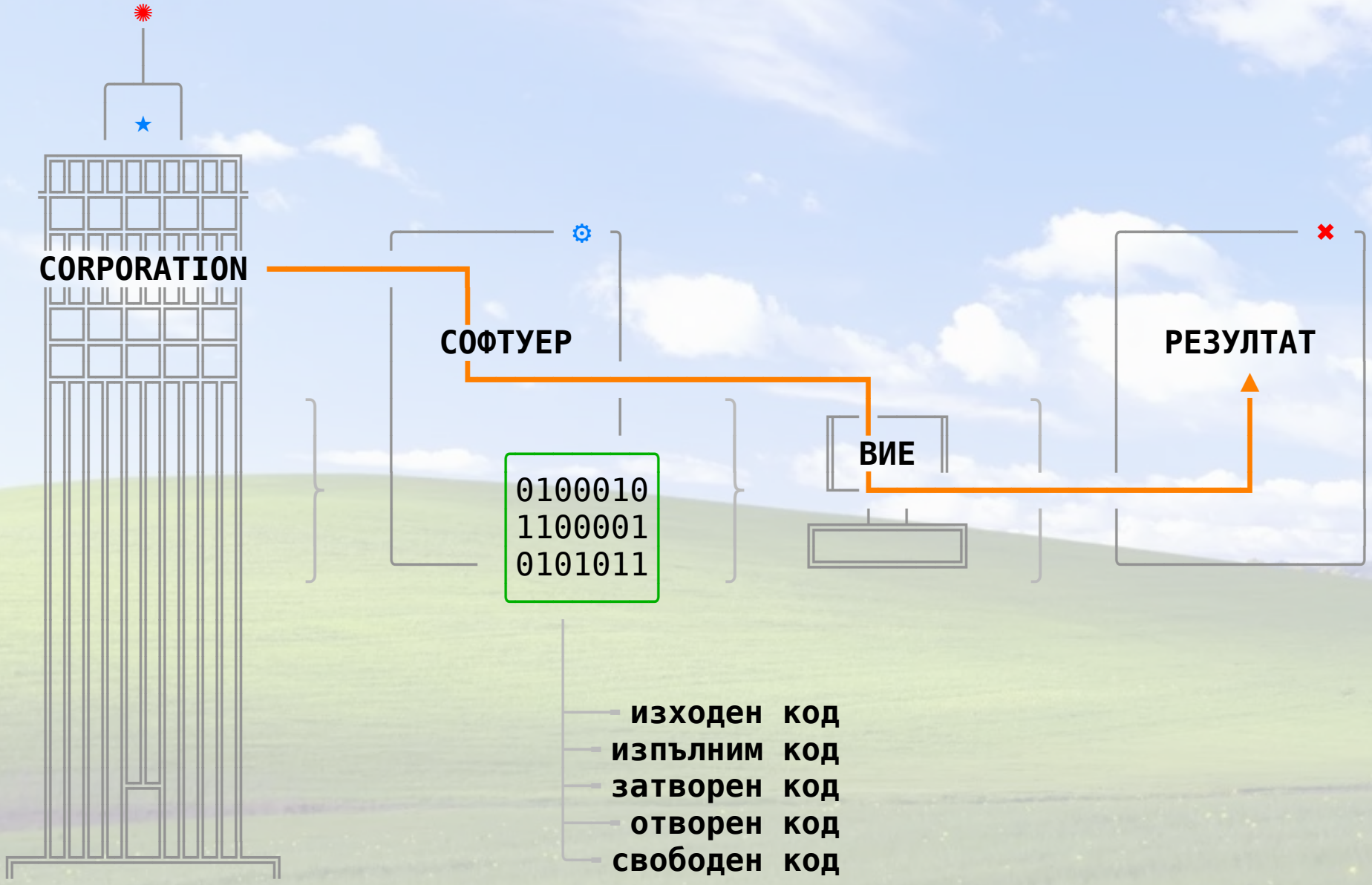


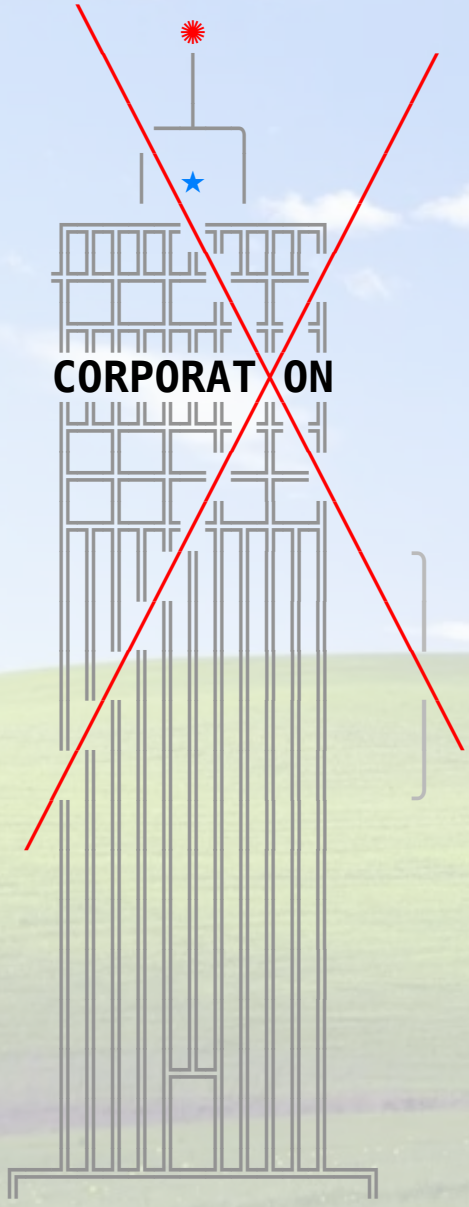
- изходен код
- изпълним код
- затворен код
- отворен код
- свободен код

www.openfest.org/2023/bg/

01101001011100101101001 01


CORPORATION
СОФТУЕР
0100010
1100001
0101011
ВИЕ
РЕЗУЛТАТ
логика
дизайн
интерфейс
изходен код
изпълним код
затворен код
отворен код
свободен код


CORPORATION
СОФТУЕР
0100010
1100001
0101011
ВИЕ
РЕЗУЛТАТ
изходен код
изпълним код
затворен код
отворен код
свободен код



СОФТУЕР

0100010
1100001
0101011

ВИЕ

РЕЗУЛТАТ

- изходен код
- изпълним код
- затворен код
- отворен код
- свободен код

(!) УСИЛЕНО СВОБОДЕН КОД

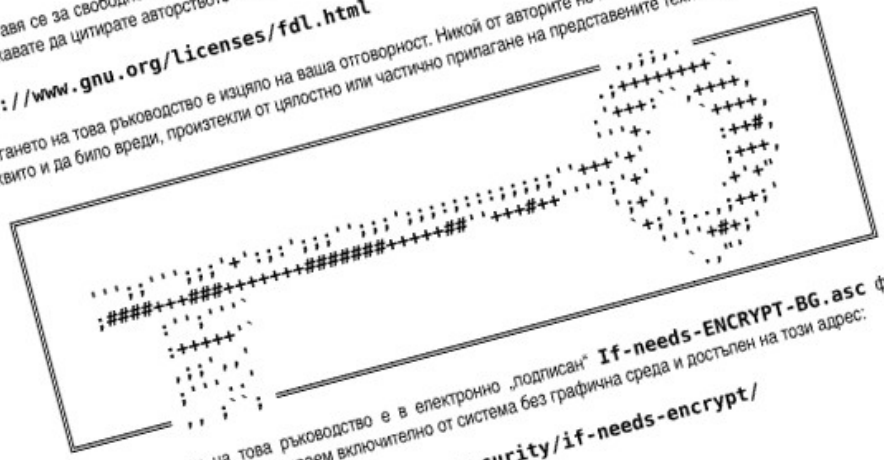
АКО НЕОБХОДИМО
ШИФРУВАЈТЕ

АКО Е НЕОБХОДИМО
ШИФРОВАЙТЕ

Следват напътствия за надеждно шифроване на вашата поверителна информация. Това е важно, ако мислите да обработвате и съхранявате такава информация в електронна среда или да я споделяте по електронен път. Въпреки, че на места напътствията са трудни за прилагане от обикновения компютърен потребител (поне докато се преодолеят известни предразсъдъци и задръжки), изпълнението им е постижимо „в домашни условия", изцяло с достъпни за гражданска употреба средства. Нищо от предложените напътствия не зависи от един единствен производител или доставчик, а правилното функциониране на всеки от компонентите може да се потвърди от поне няколко независими и алтернативни източника. Това е ключов момент в нашата концепция, чието цялостно и точно прилагане ще осигури респектиращи нива на информационна сигурност. Но още тук честно ще отбележим, че „абсолютна сигурност" няма. Помислите отново, преди да въведете поверителна информация в електронна среда и просто не го правете, ако не е наистина необходимо!

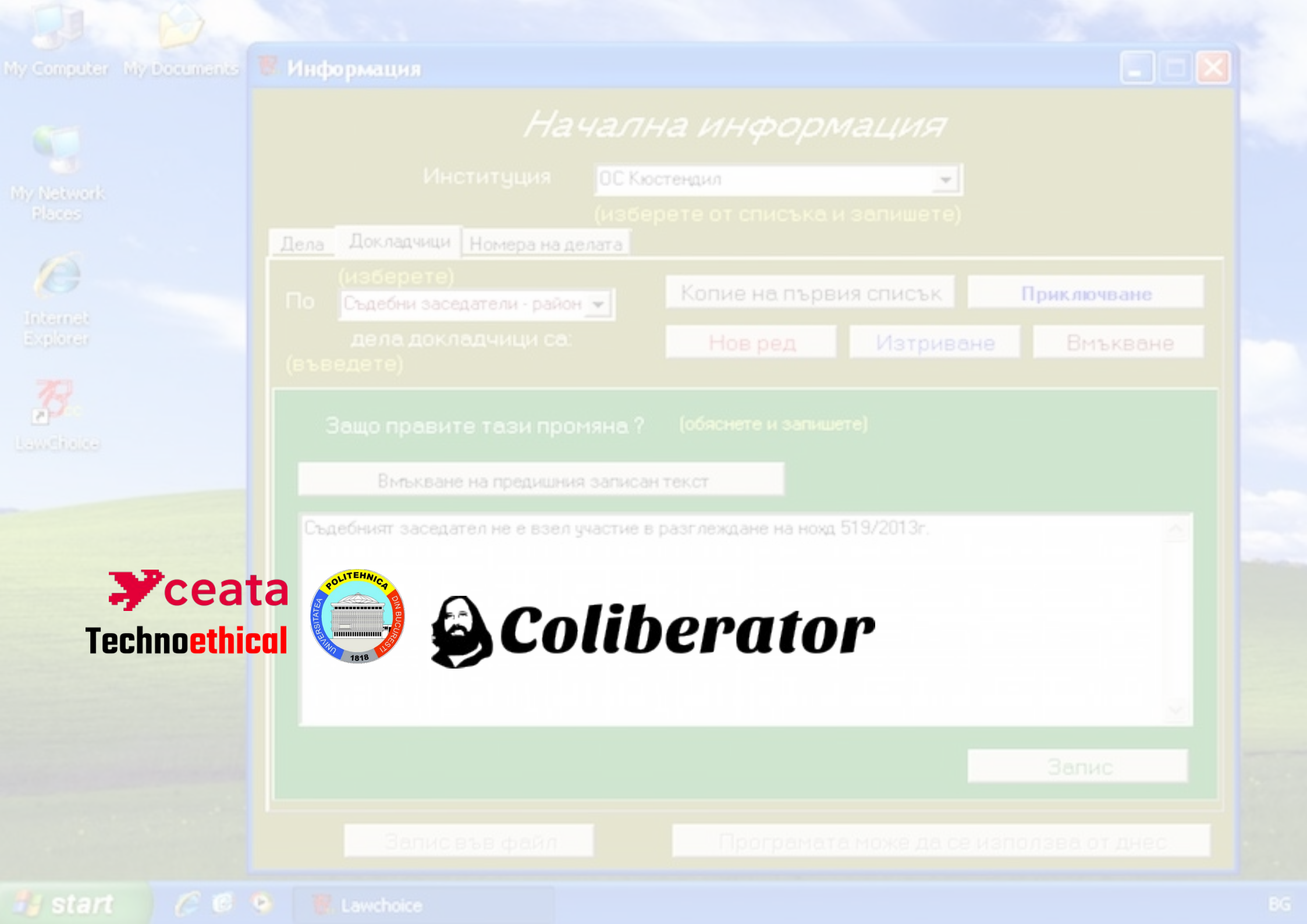
Това ръководство е резултат от работата на **www.Advocati.org** и Института за Свободни технологии **www.LibTec.org** със специални благодарности към **Richard M. Stallman** и **Denis 'GNUtoo' Carikli**

https://www.advocati.org/
https://www.libtec.org/



Официалната версия на това ръководство е в електронно „подписан" **If-needs-ENCRYPT-BG.asc** файл с обикновен текстови формат, ползваем включително от система без графична среда и достъпен на този адрес:

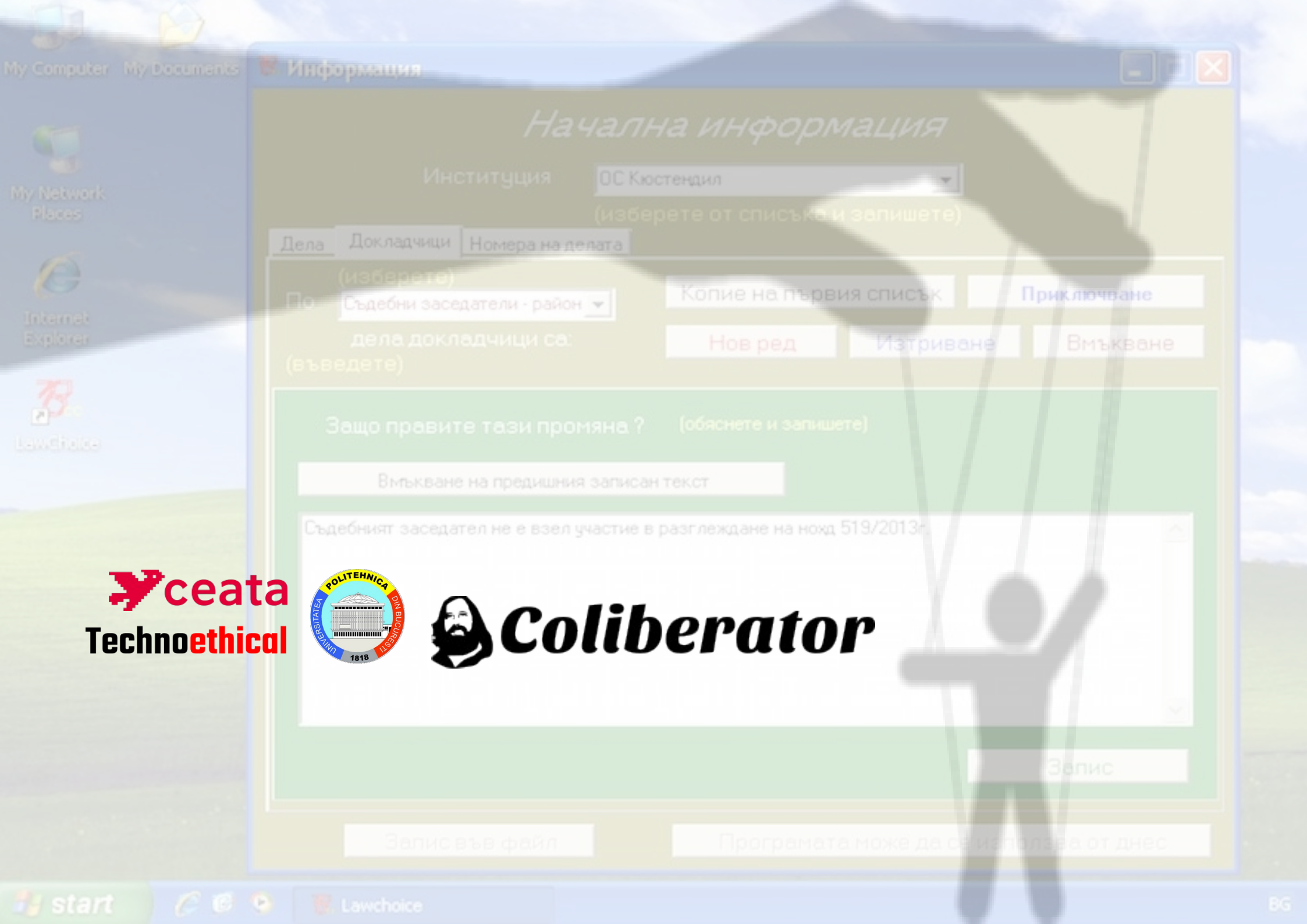
https://advocati.org/consultation/security/if-needs-encrypt/



ceata
Technoethical

POLITEHNICA
UNIVERSITATEA DIN BUCUREȘTI
1818

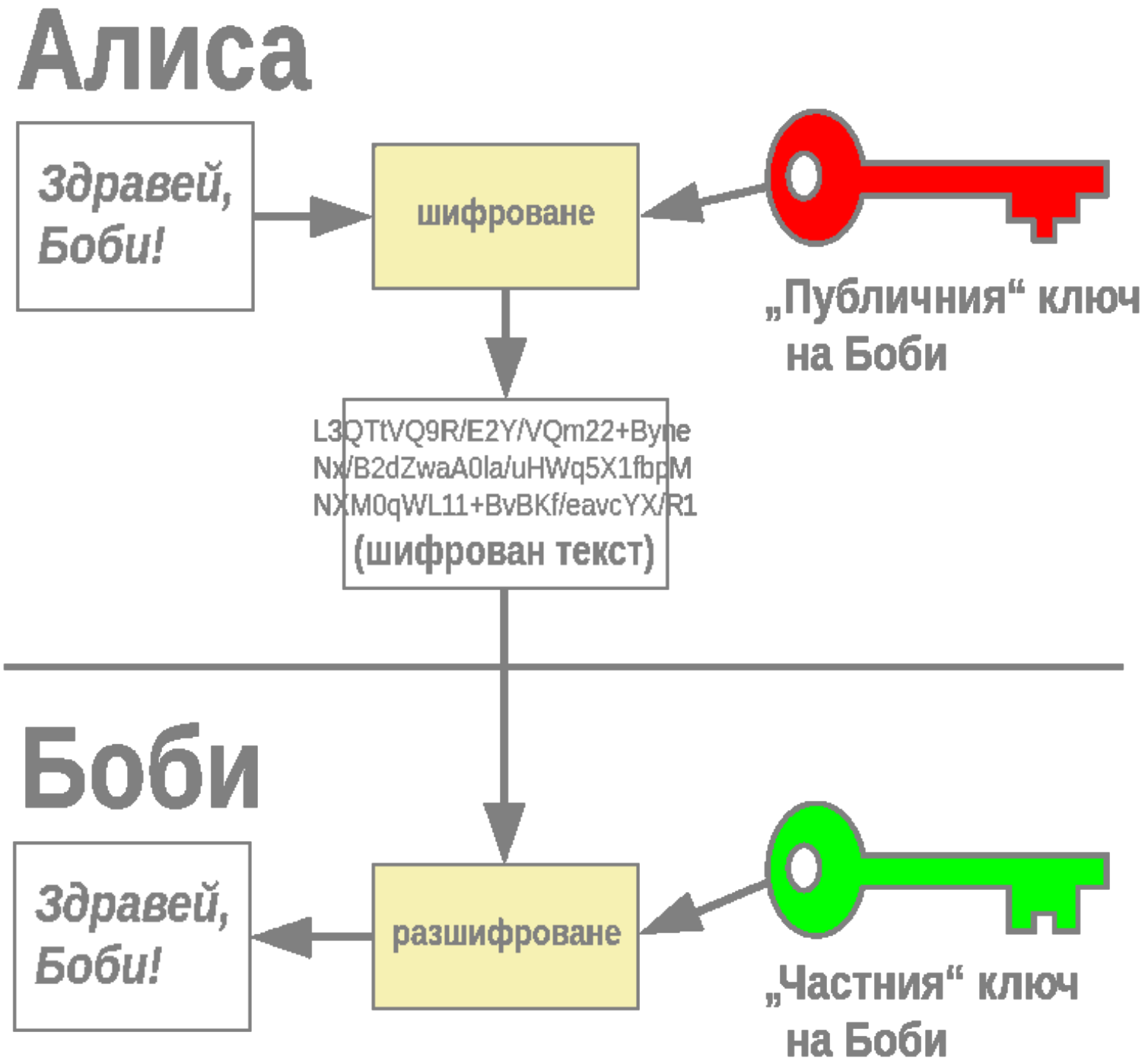
Coliberator



ceata
Technoethical

POLITEHNICA
UNIVERSITATEA DIN BUCUREȘTI
1818

Coliberator

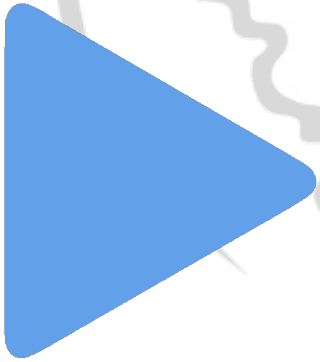

Алиса
Здравей, Боби!
шифроване
„Публичния“ ключ на Боби
L3QTtVQ9R/E2Y/VQm22+Byne
Nx/B2dZwaA0la/uHWq5X1fbpM
NXM0qWL11+BvBKf/eavcYX/R1
(шифрован текст)
Боби
Здравей, Боби!
разшифроване
„Частния“ ключ на Боби

СЪДЪРЖАНИЕ

I. Напълно свободна операционна система
II. Инсталиране на операционната система
III. Защитаване на софтуера от ниско ниво
IV. Цялостно шифроване на вашата система
V. Обезпечаване сигурността на паролите
VI. Защитаване на свързването с internet
VII. Организация на физическата сигурност
VIII. Извършване на надеждно GPG-шифроване
IX. Представяме ви нашия 'публичен' ключ

I. НАПЪЛНО СВОБОДНА ОПЕРАЦИОННА СИСТЕМА

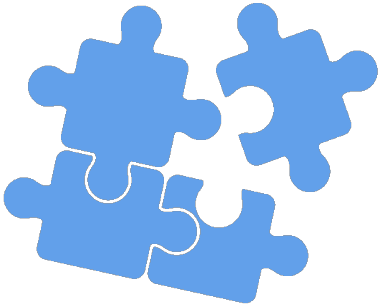
1. Защо Свободният софтуер е от решаващо значение
2. Най-общо за командния ред, терминала и системата



ползваш

проучваш

споделяш



надграждаш

Free as in Freedom

=== Welcome to Parabola GNU/Linux-libre Live - OpenRC/CLI Edition 2018.05 ===

This ISO is capable of installing a complete Parabola system
without a connection to the internet. If you would like to fetch
the latest packages from the internet, run the following command
before beginning the install:

```
# cp /etc/pacman-online.conf /etc/pacman.conf
```

For help establishing an internet connection, enter this command:

```
lynx network.html
```

For an installation wizard, enter either of these commands:

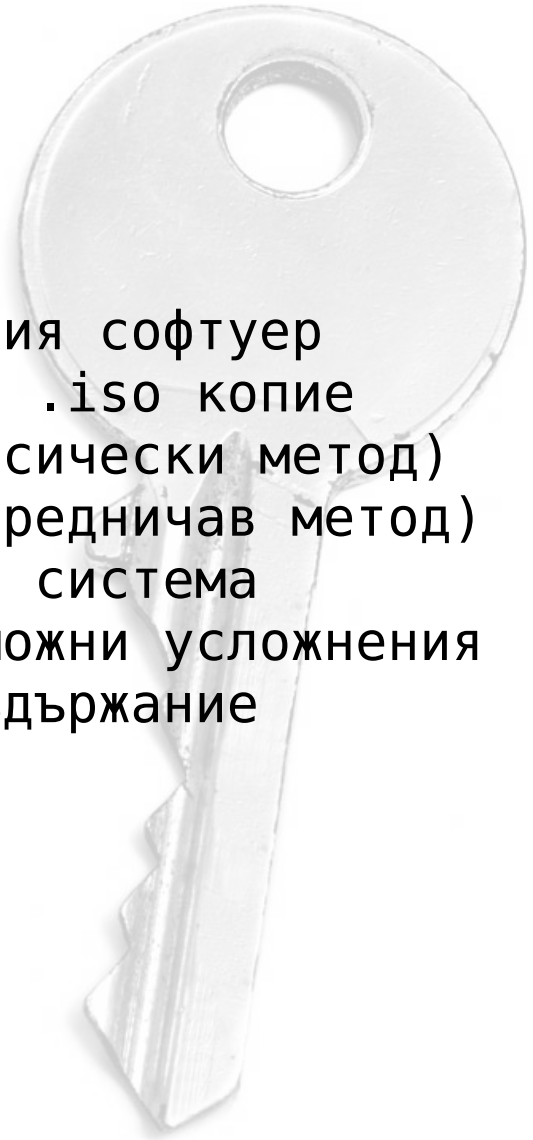
```
./install-openrc-lxde.sh
./install-systemd-mate.sh
```

Press Alt+F1, Alt+F2, ..., Alt+F6 to switch virtual terminals.

==========

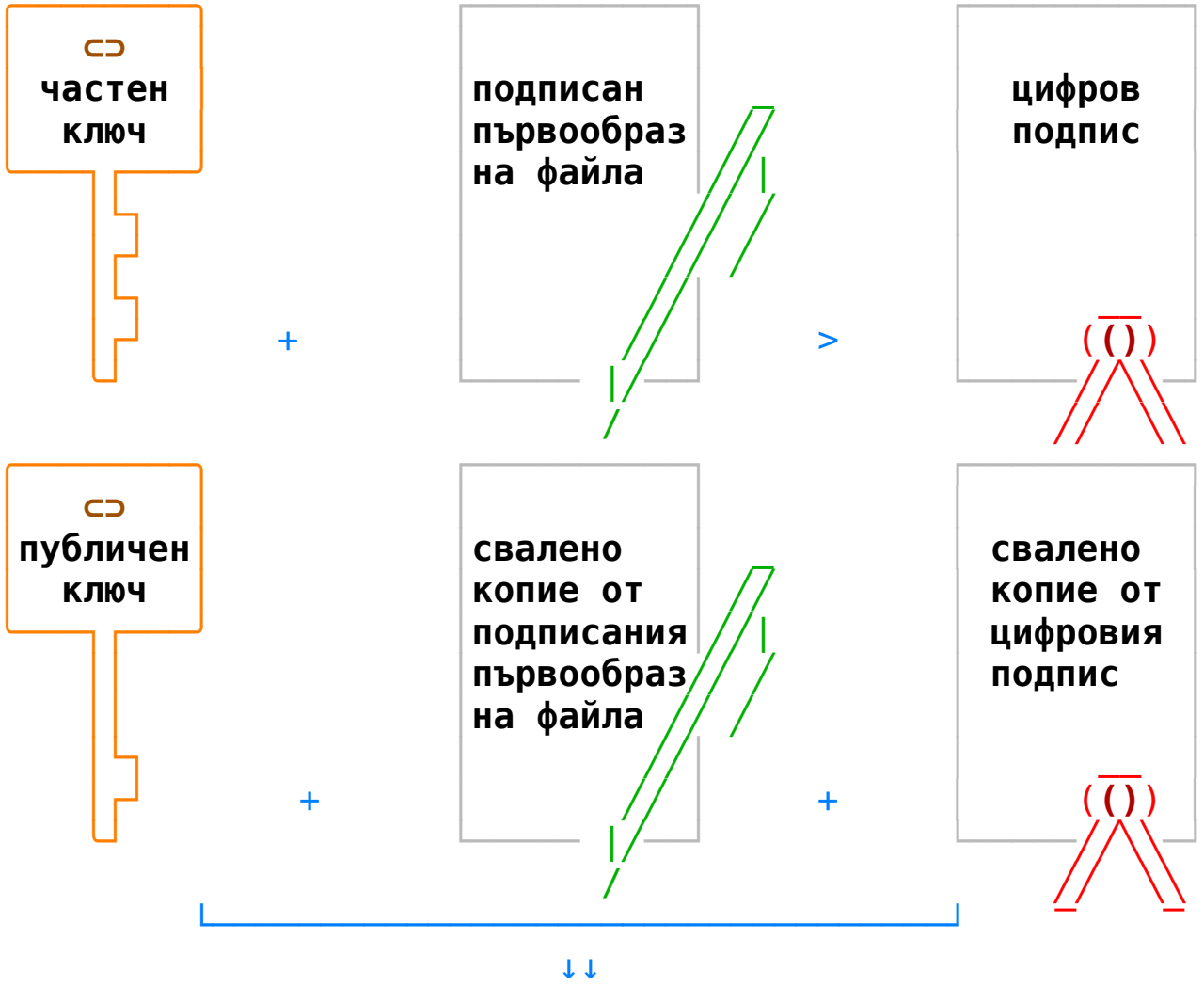
```
[root@parabolaiso ~]#
```

II. ИНСТАЛИРАНЕ НА ОПЕРАЦИОННАТА СИСТЕМА

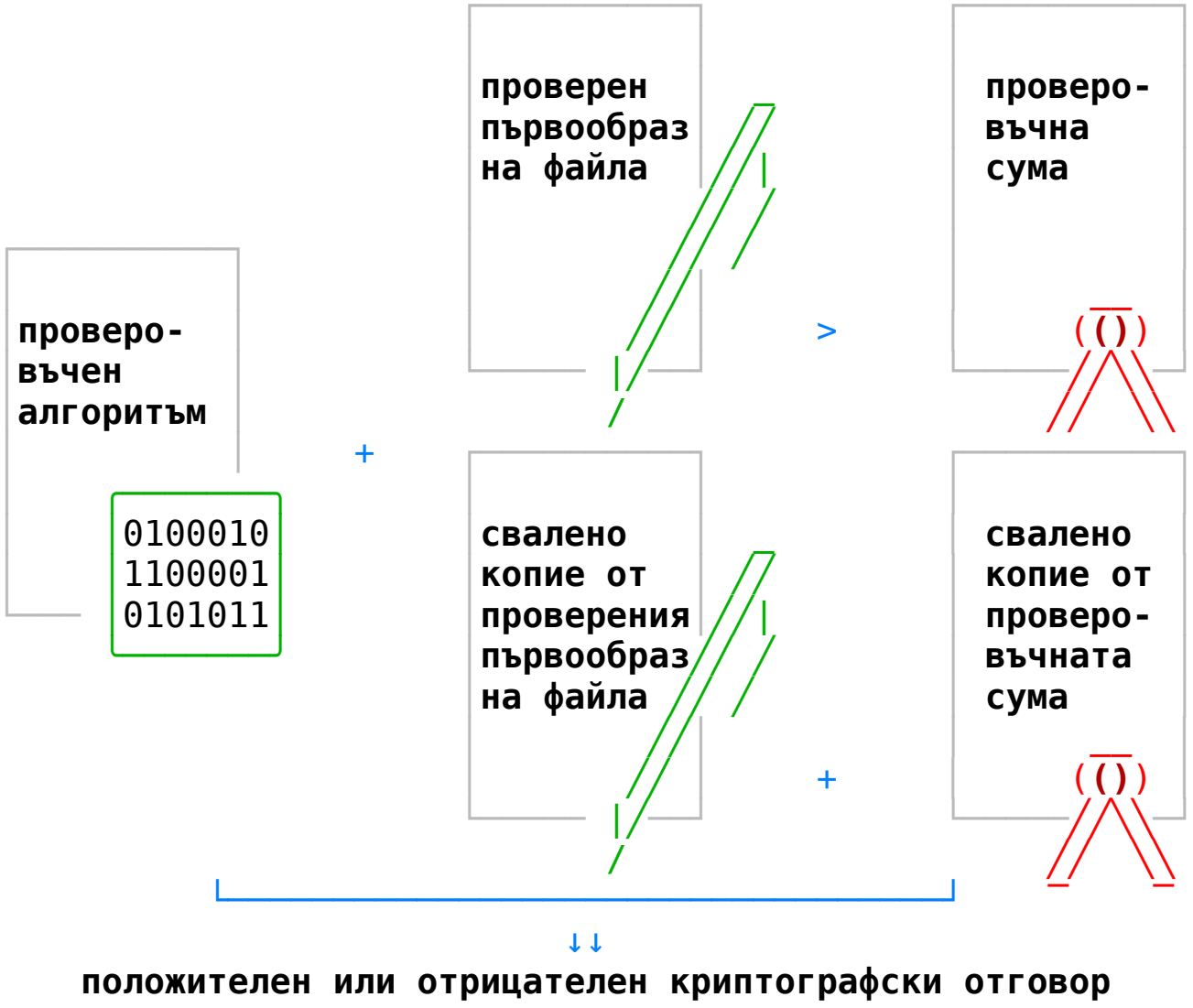


1. Особености на общността при Свободния софтуер
2. Сваляне на автентично инсталационно .iso копие
3. Подготвяне на „жив“ инсталатор (класически метод)
4. Подготвяне на „жив“ инсталатор (напредничав метод)
5. Инсталиране на Свободна операционна система
6. За обновяването на системата и възможни усложнения
7. Създаване на външни хранилища за съдържание

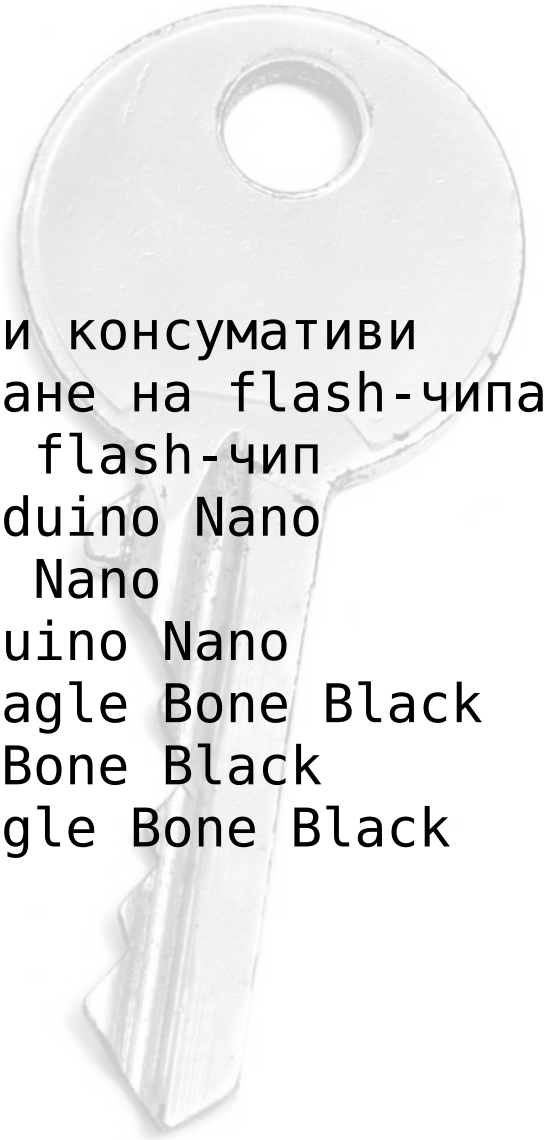
ПРИНЦИПНА СХЕМА НА ЦИФРОВОТО „ПОДПИСВАНЕ“ НА ФАЙЛОВЕ



ПРИНЦИПНА СХЕМА НА ИЗПОЛЗВАНЕТО НА 'ПРОВЕРОВЪЧНИ СУМИ'

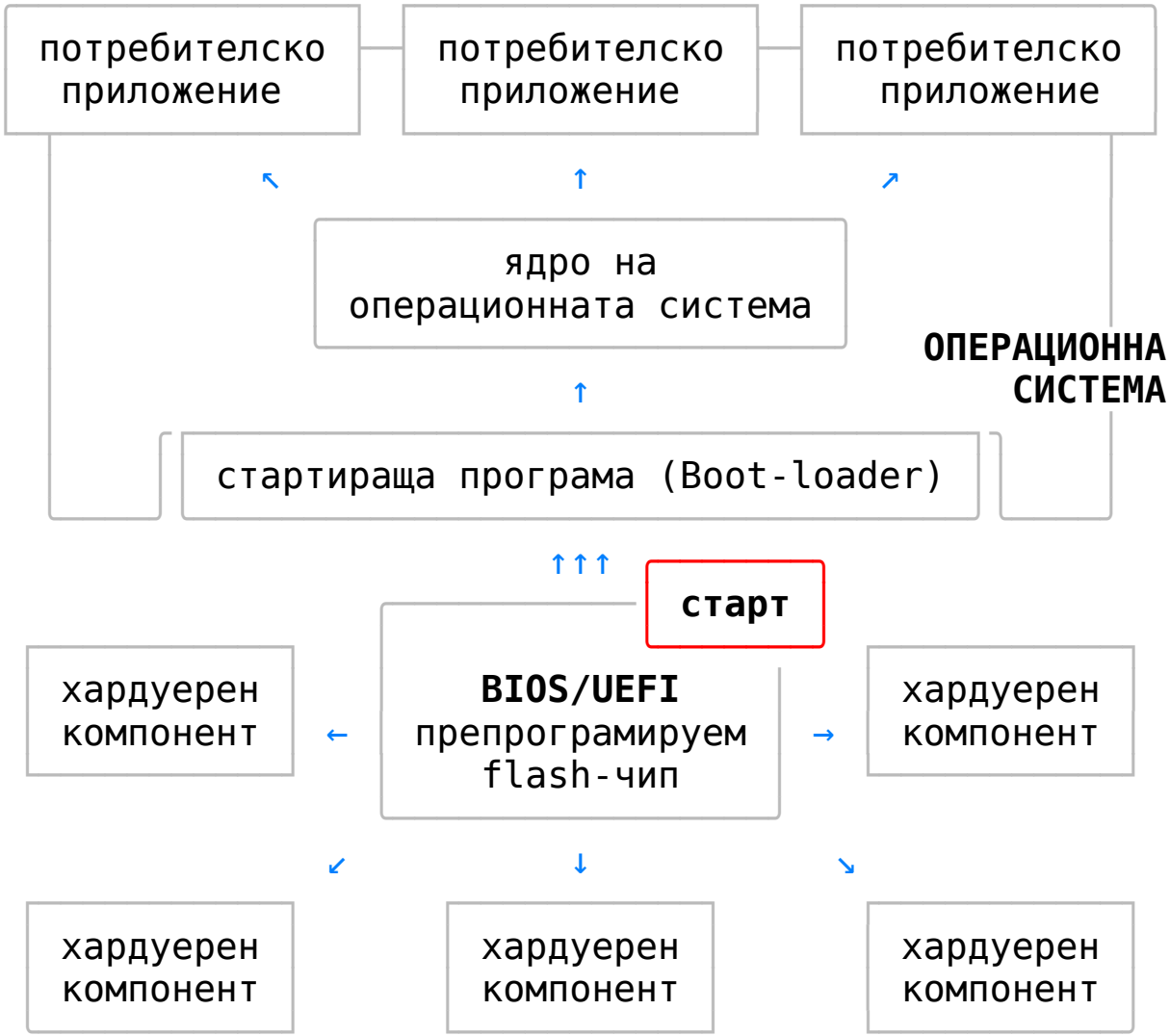


III. ЗАЩИТАВАНЕ НА СОФТУЕРА ОТ НИСКО НИВО

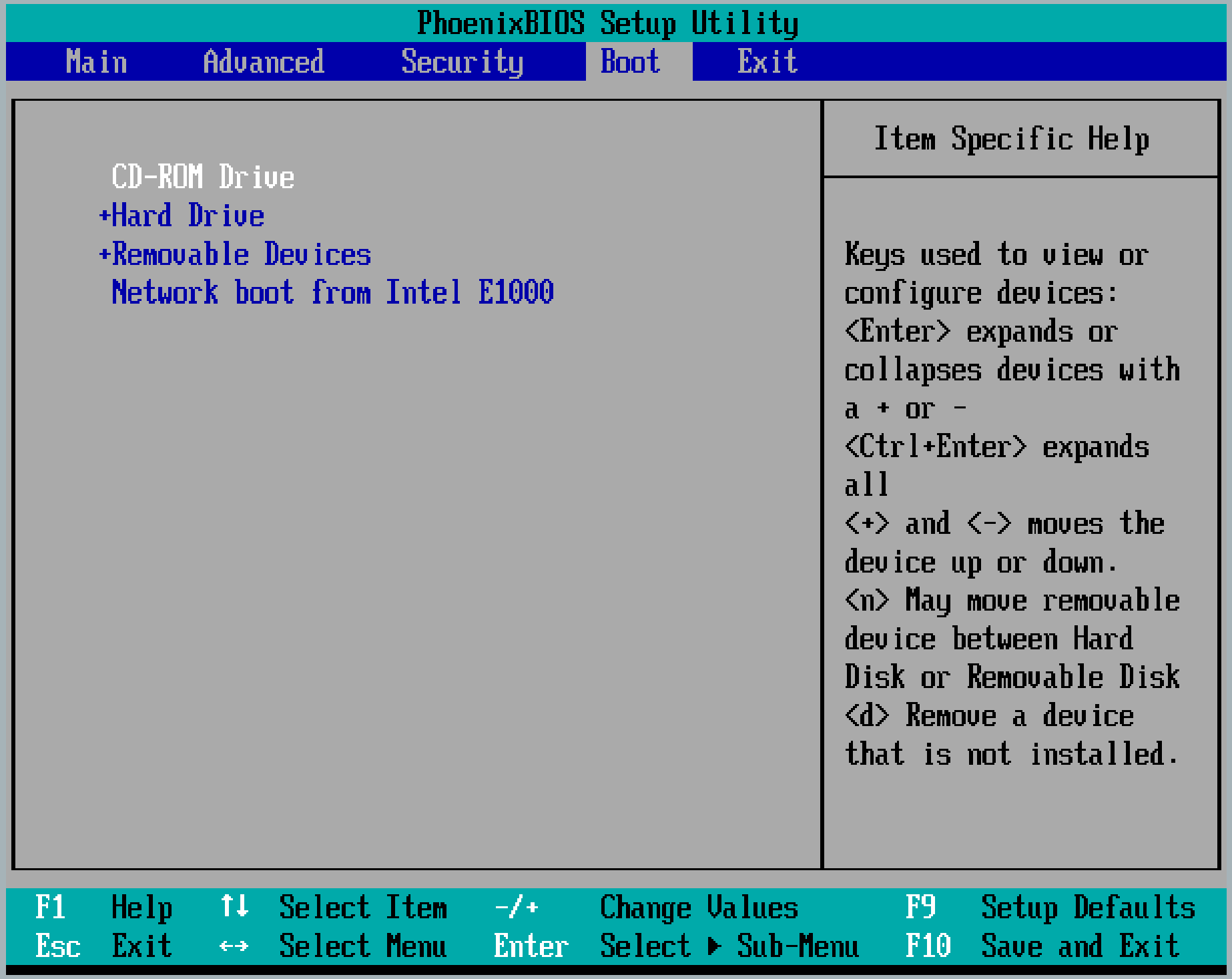


1. Необходими устройства, инструменти и консумативи
2. Разглобяване на компютъра и достъпване на flash-чипа
3. Идентифициране на препрограмируемия flash-чип
4. Архитектура и функционалности на Arduino Nano
5. Инсталиране на устройството Arduino Nano
6. Препрограмиране на flash-чипа с Arduino Nano
7. Архитектура и функционалности на Beagle Bone Black
8. Инсталиране на устройството Beagle Bone Black
9. Препрограмиране на flash-чипа с Beagle Bone Black

ПРИНЦИПНА СТРУКТУРА НА ЕДНО КОМПЮТЪРНО УСТРОЙСТВО



Lenovo Thinkpad x200


PhoenixBIOS Setup Utility
Main
Advanced
Security
Boot
Exit
CD-ROM Drive
+Hard Drive
+Removable Devices
Network boot from Intel E1000
Item Specific Help
Keys used to view or configure devices:
<Enter> expands or collapses devices with a + or -
<Ctrl+Enter> expands all
<+> and <-> moves the device up or down.
<n> May move removable device between Hard Disk or Removable Disk
<d> Remove a device that is not installed.
F1 Help
↑↓ Select Item
-/+ Change Values
F9 Setup Defaults
Esc Exit
↔ Select Menu
Enter Select ▸ Sub-Menu
F10 Save and Exit

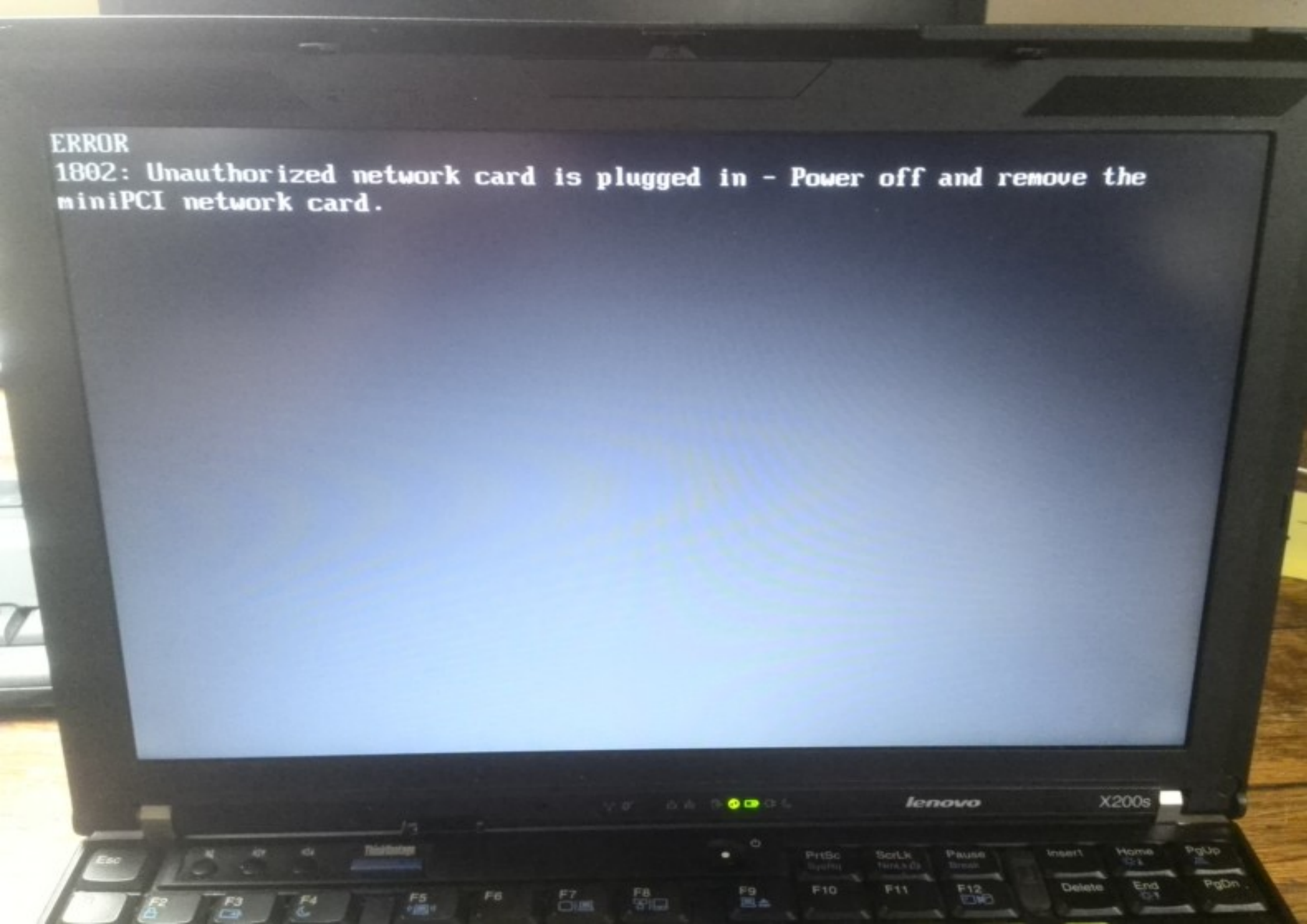
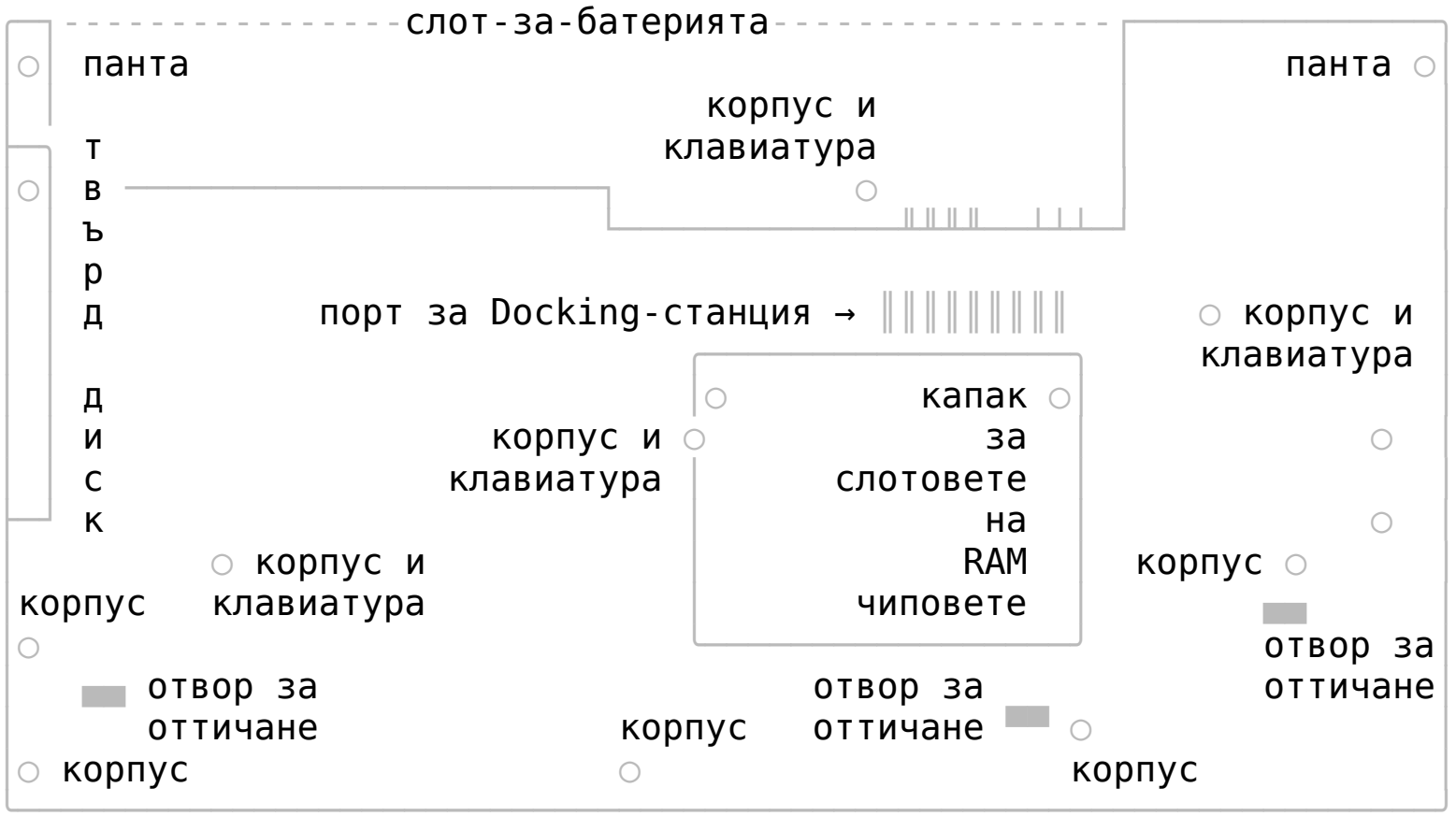
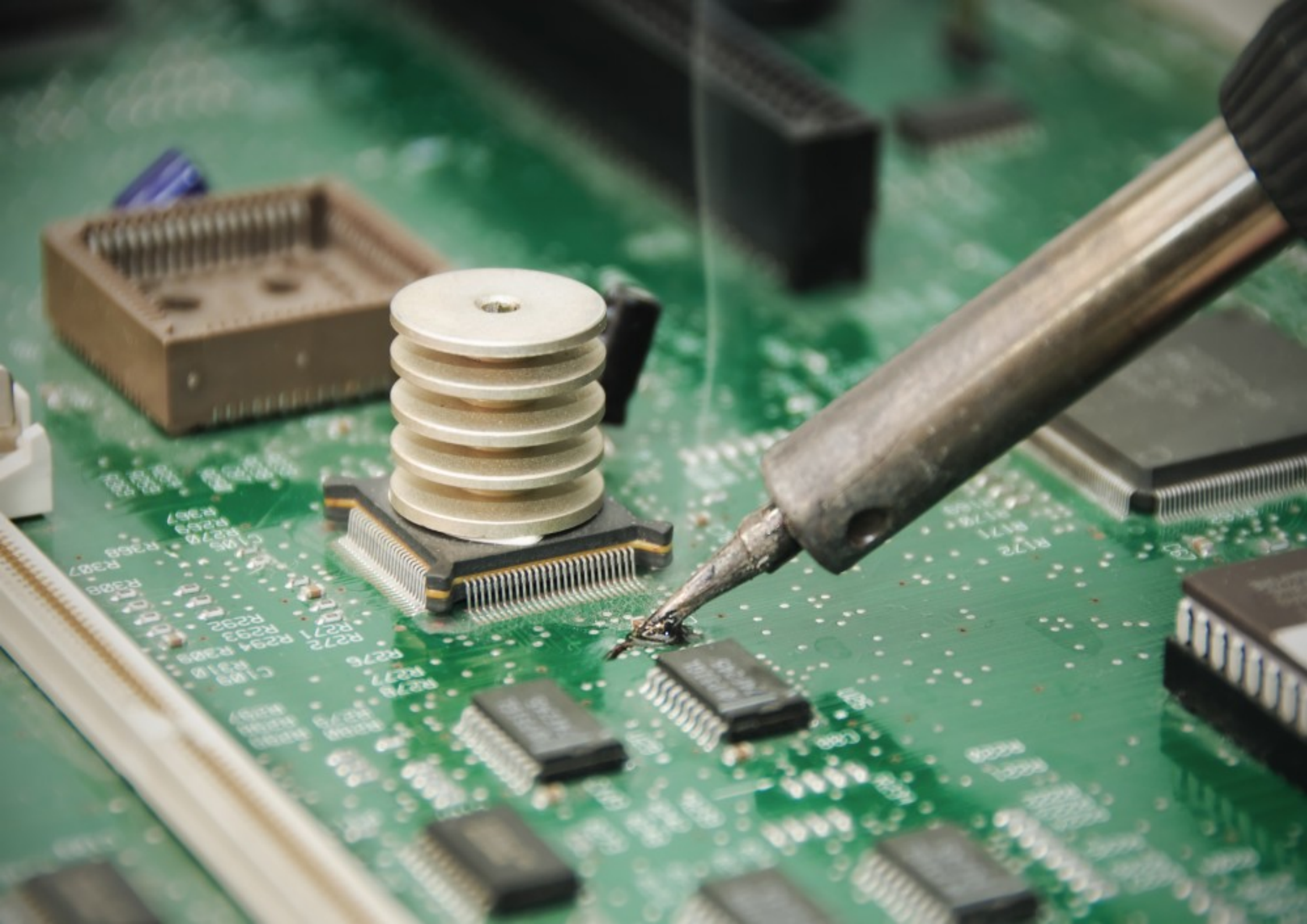
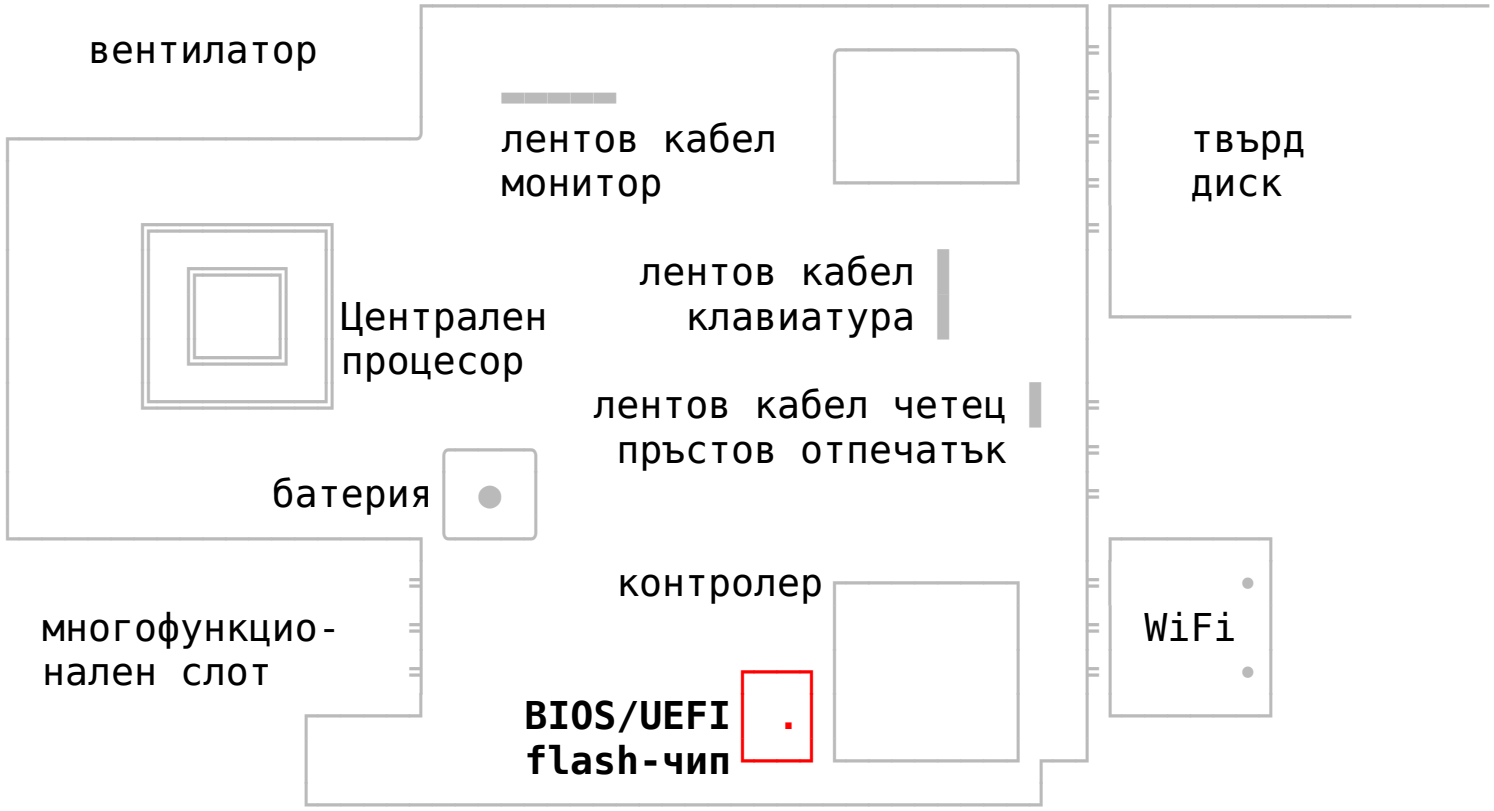

ERROR
1802: Unauthorized network card is plugged in - Power off and remove the miniPCI network card.
lenovo
X200s

СХЕМА С ВИНТОВЕТЕ В КОРПУСА НА ThinkPad x200 и x200S

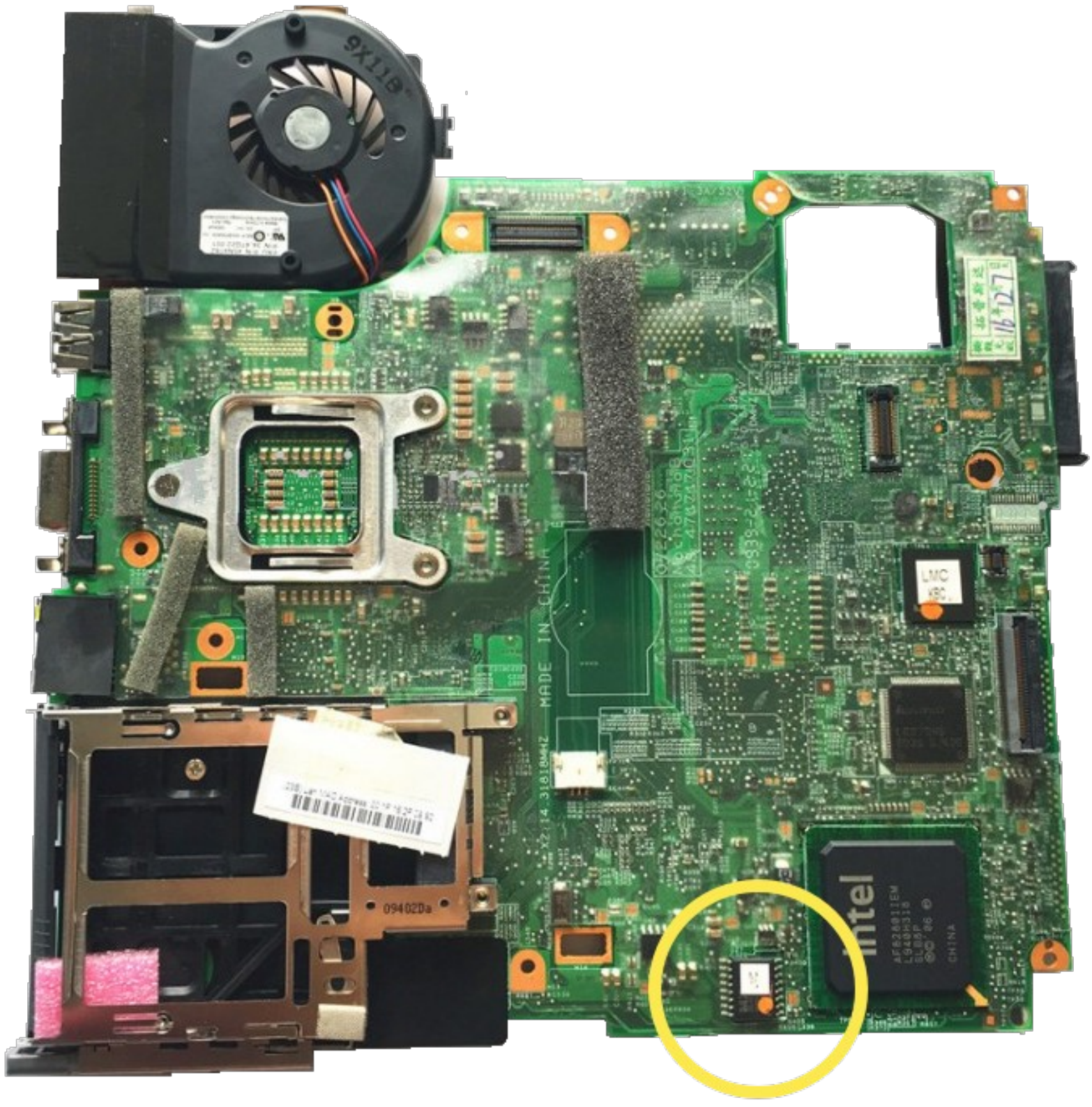




ДЪННА ПЛАТКА С ОСНОВНИ КОМПОНЕНТИ НА ThinkPad x200

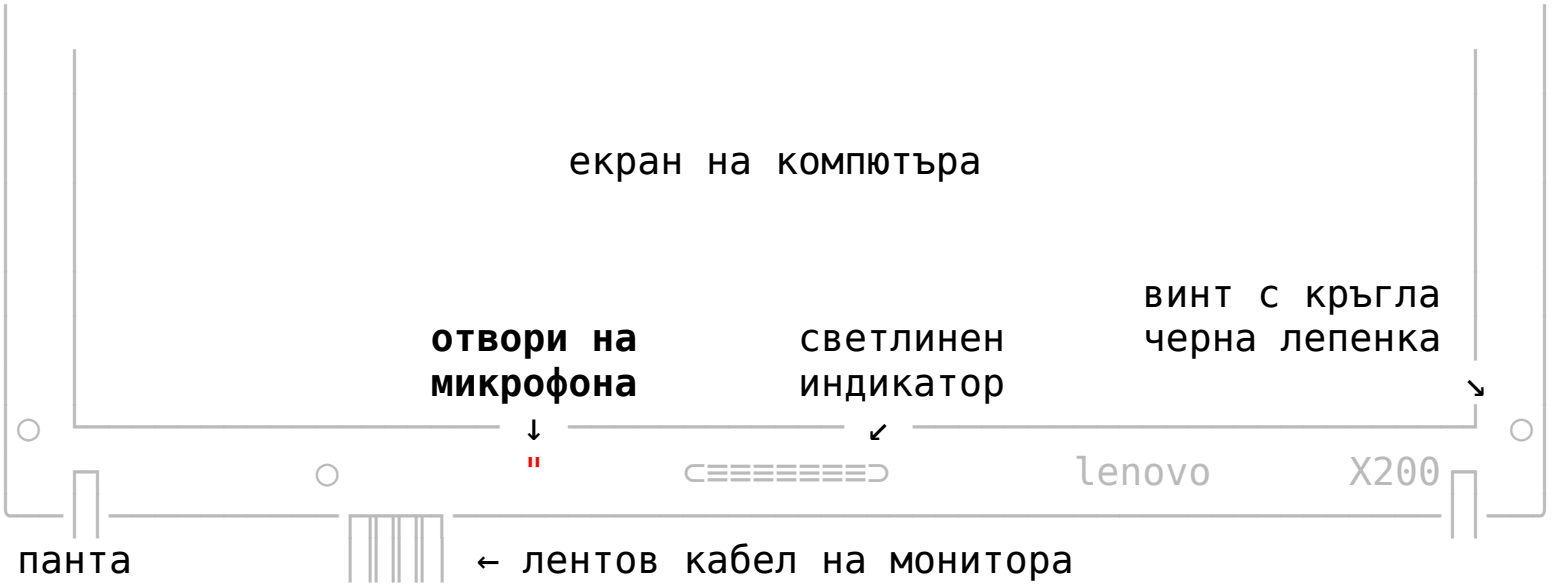


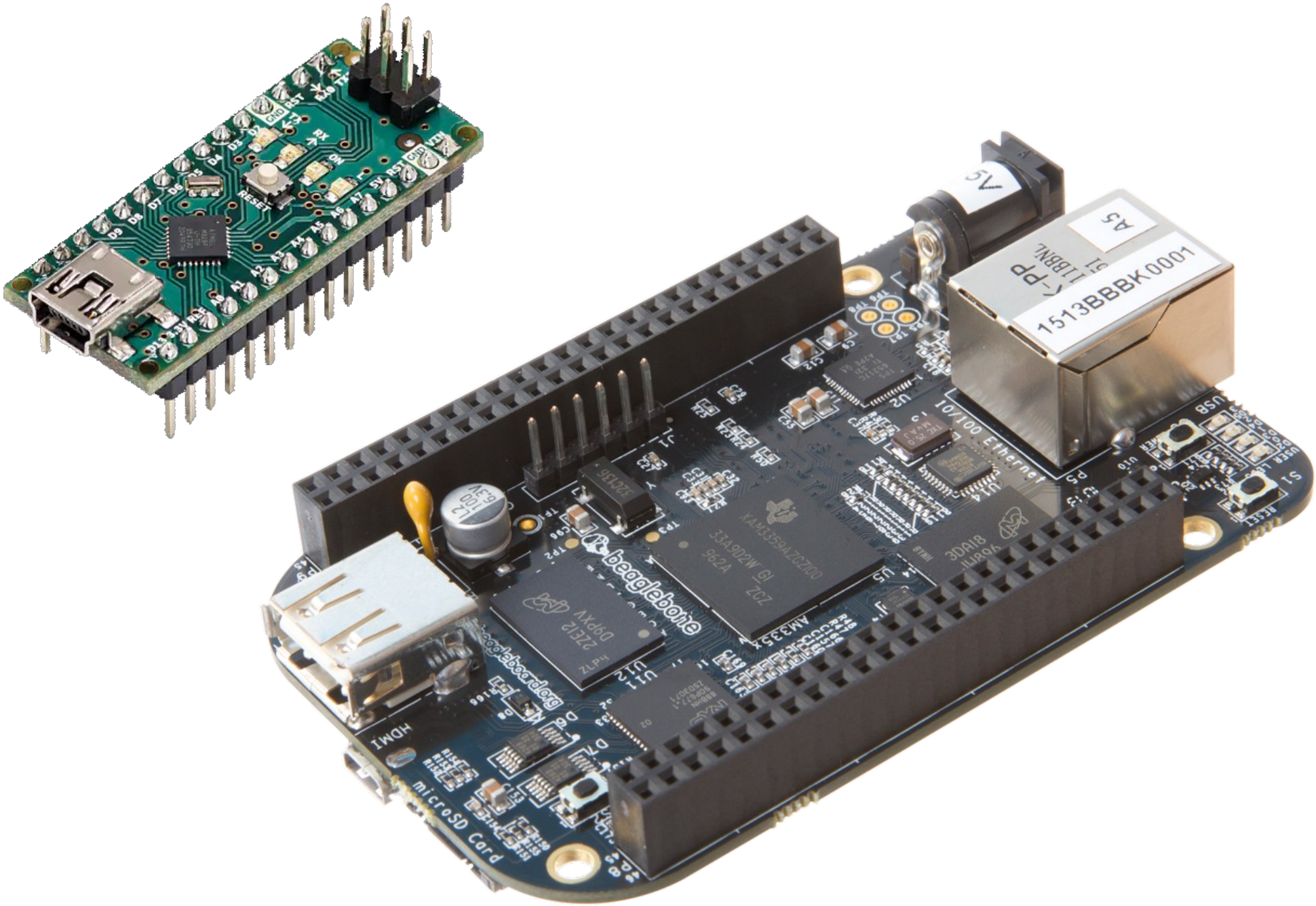

9X11B
MADE IN CHINA
intel
CHINA


9X11B
MADE IN CHINA
intel

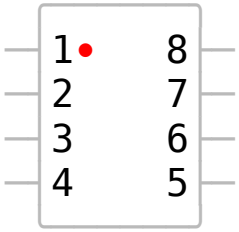

LMC
25L640
3B3427
TAIWAN
intel

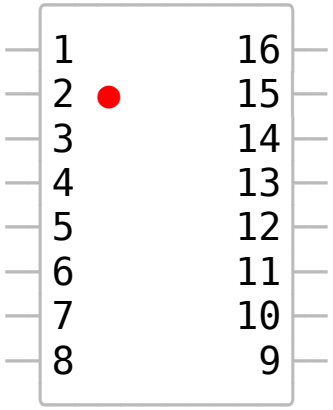
МЯСТО НА МИКРОФОНА В РАМКАТА НА МОНИТОРА ПРИ x200 и x200s



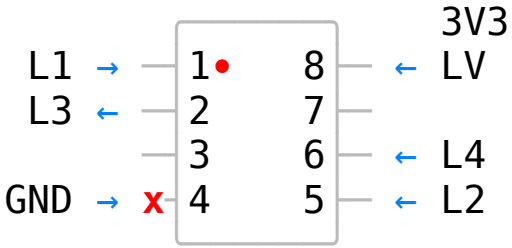

beagleboard.org
beagleboard.org
microSD Card
HDMI
10/100 Ethernet
5V
1513BBBK0001
AM335x

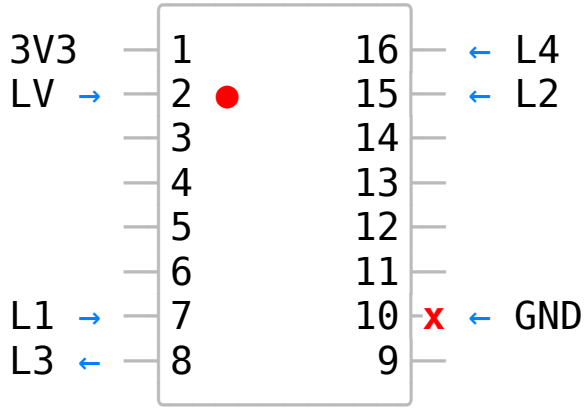
НОМЕРА НА ПИНОВЕТЕ В BIOS/UEFI FLASH-ЧИПА (8 или 16 пина)

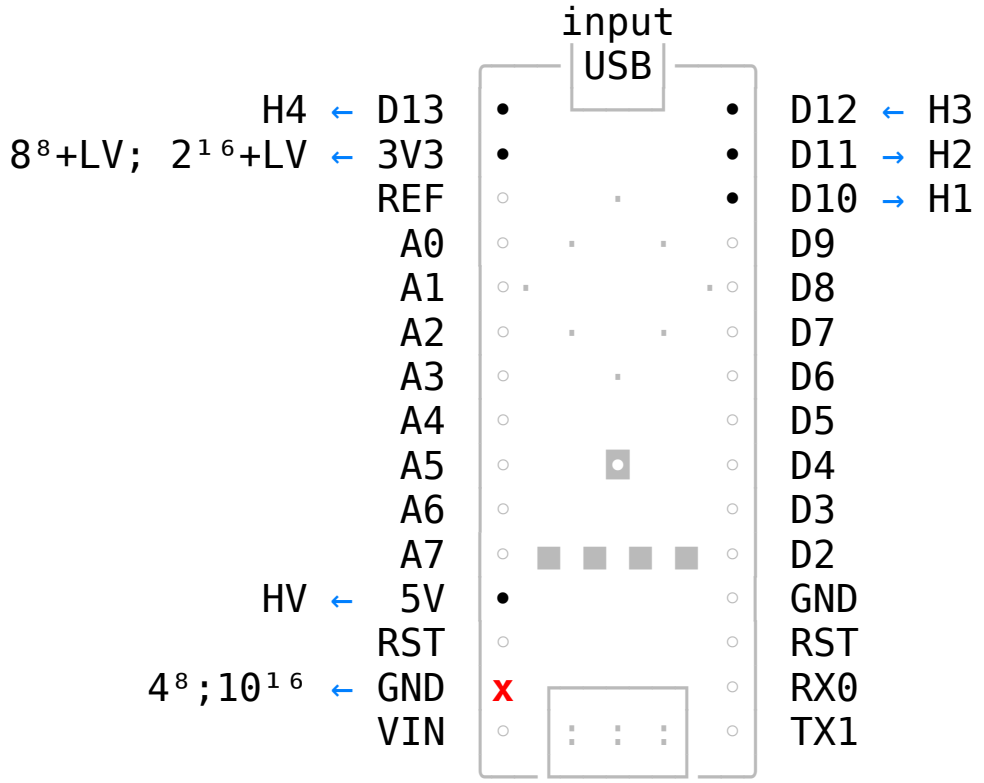


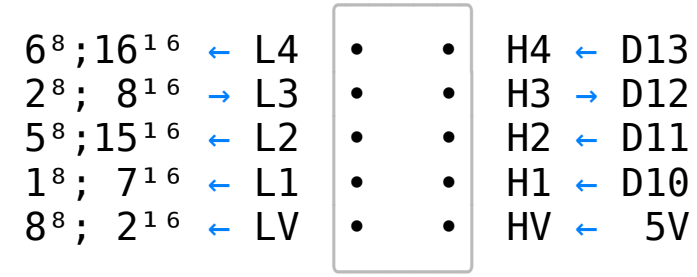


СВЪРЗВАНЕ НА BIOS/UEFI FLASH-ЧИПА С Arduino Nano

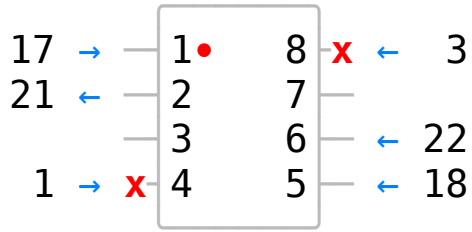


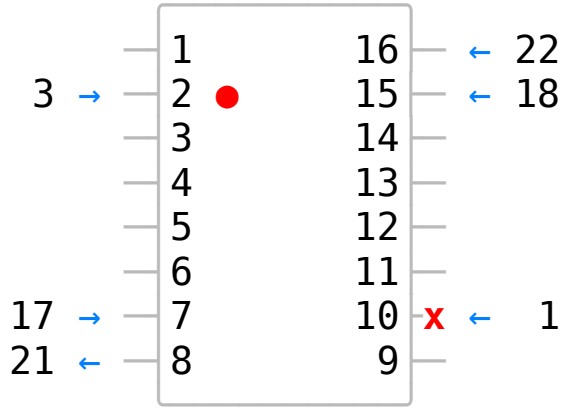


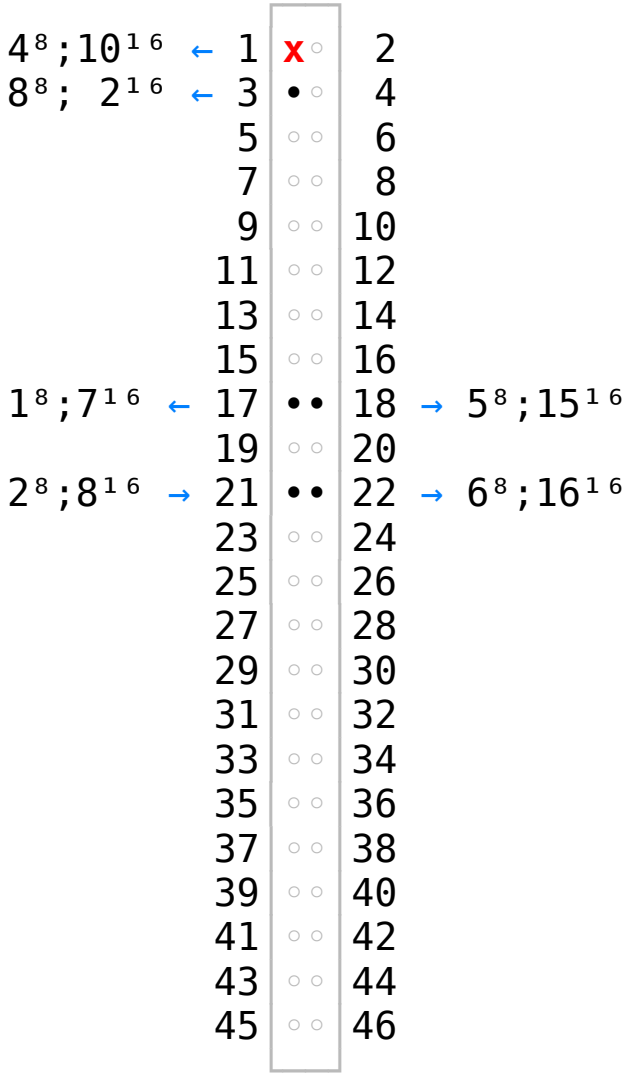


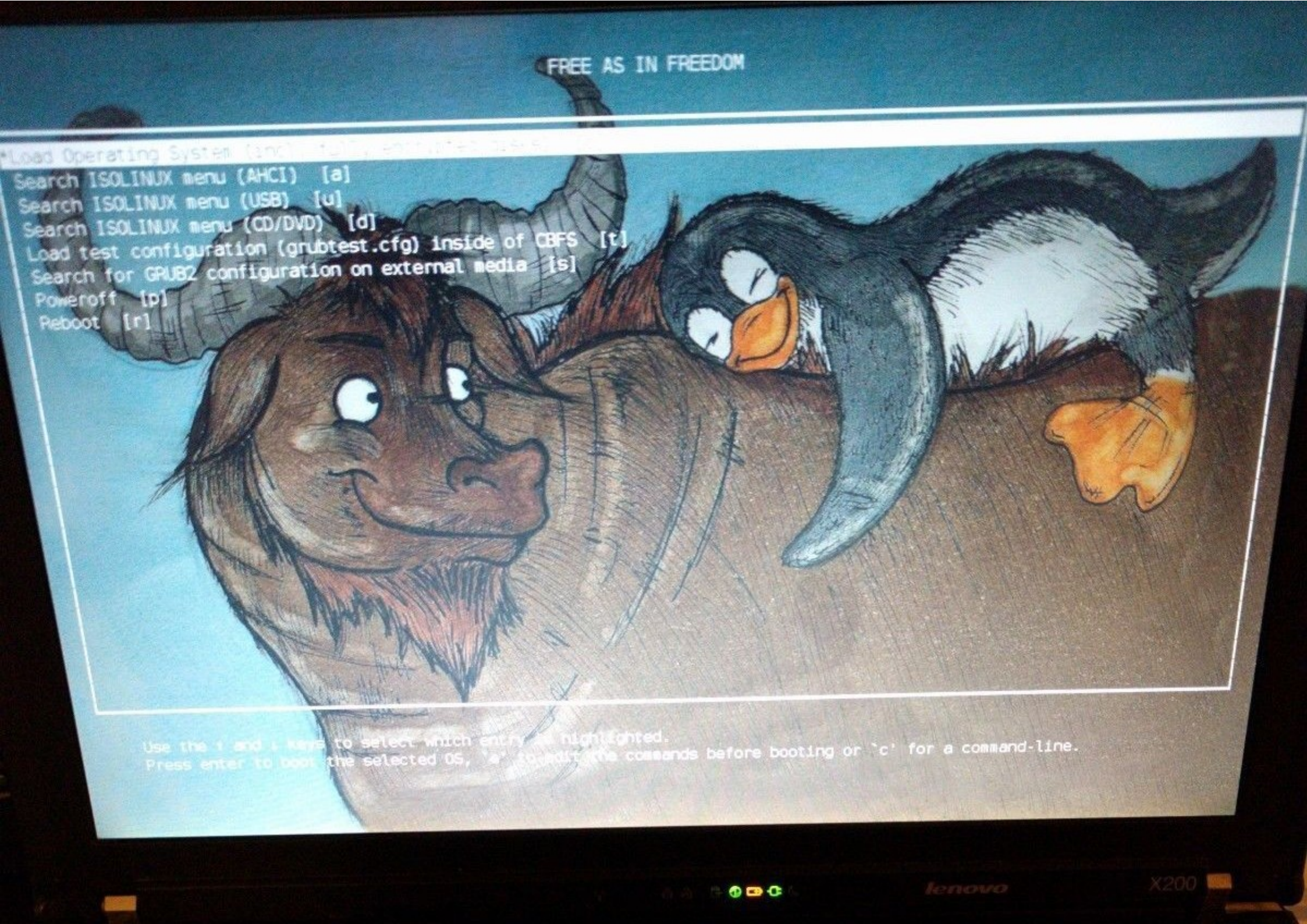


СВЪРЗВАНЕ НА BIOS/UEFI FLASH-ЧИПА С Beagle Bone Black

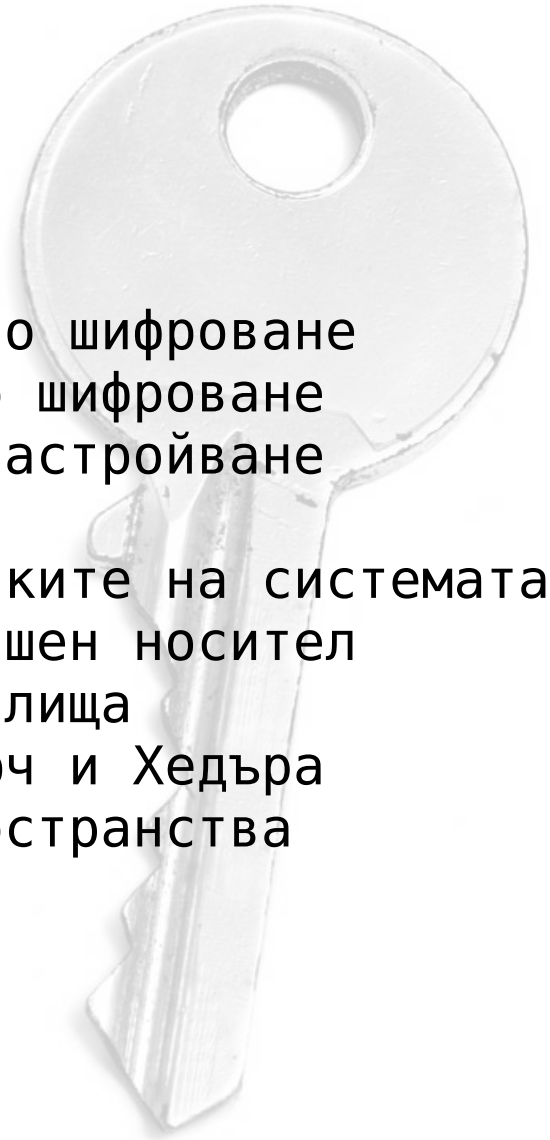






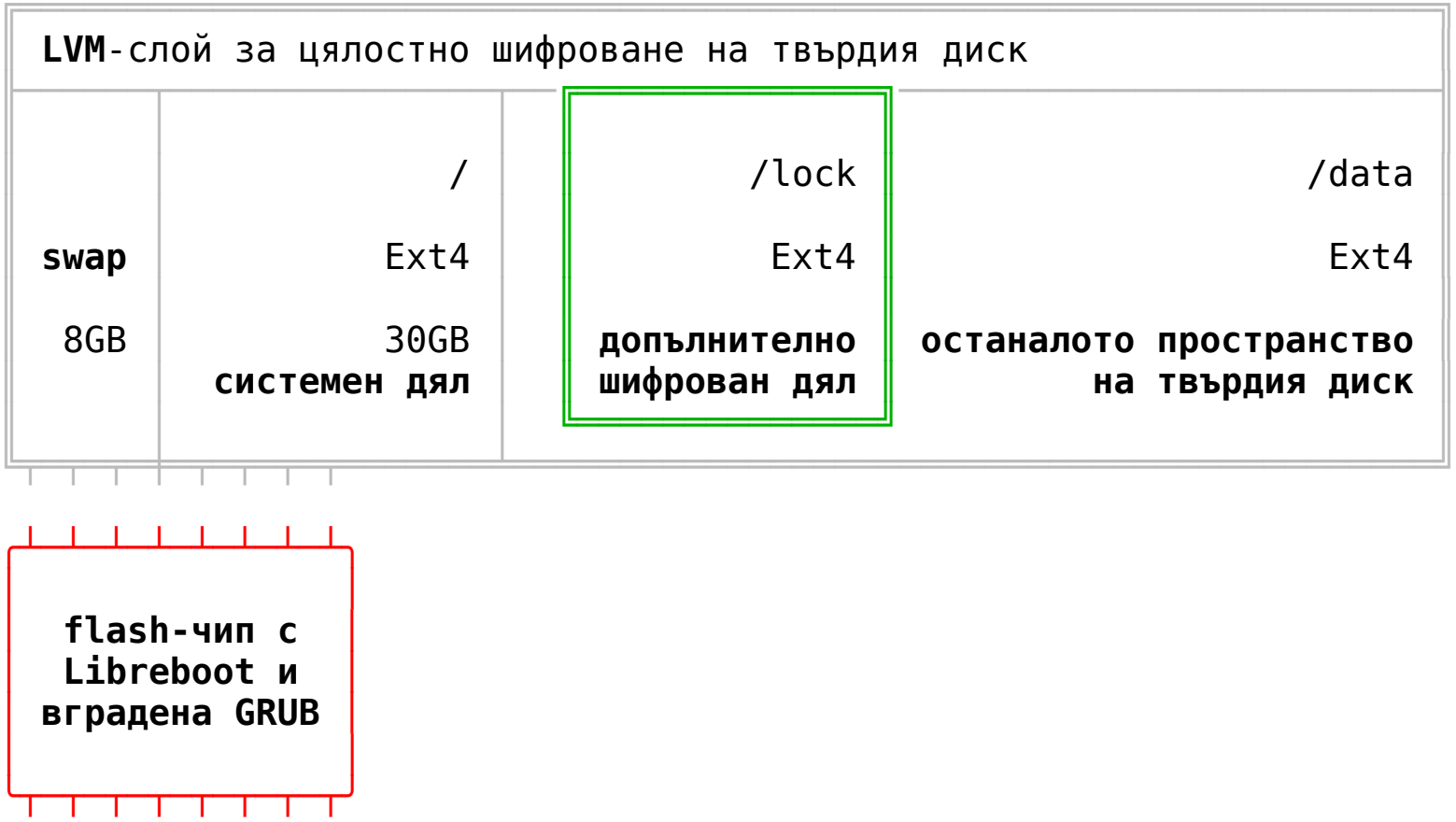

FREE AS IN FREEDOM
Search ISOLINUX menu (AHCI) [a]
Search ISOLINUX menu (USB) [u]
Search ISOLINUX menu (CD/DVD) [d]
Load test configuration (grubtest.cfg) inside of CBFS [t]
Search for GRUB2 configuration on external media [s]
Poweroff [p]
Reboot [r]
Press enter to boot the selected OS, `e' to edit the commands before booting or `c' for a command-line.
lenovo
X200

IV. ЦЯЛОСТНО ШИФРОВАНЕ НА ВАШАТА СИСТЕМА

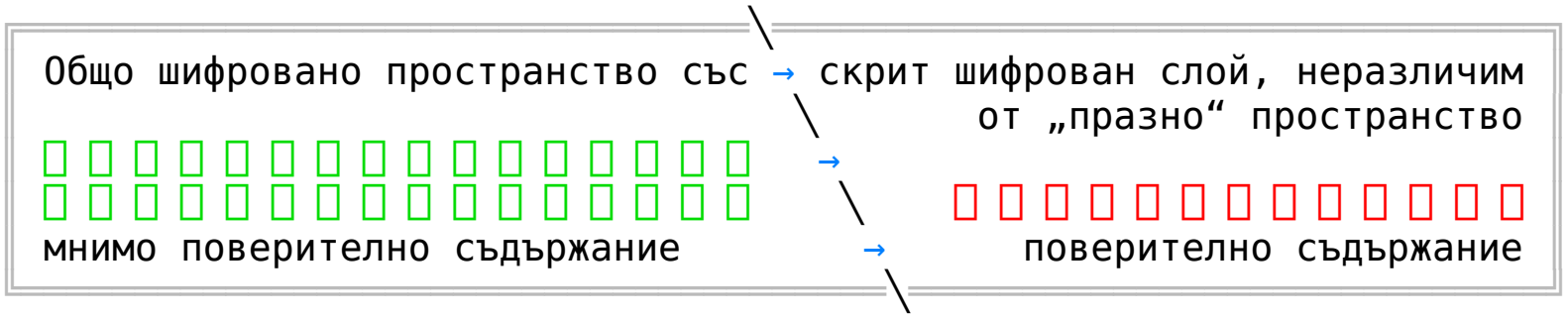


1. Теоретична архитектура на цялостното шифроване
2. Подготовка на системата за цялостно шифроване
3. Цялостно шифроване, инсталиране и настройване
4. Настройване на GRUB и Libreboot
5. Финализиране инсталацията и настройките на системата
6. Цялостно шифроване чрез ключ от външен носител
7. Създаване на шифровани външни хранилища
8. Критичното значение на Основния ключ и Хедъра
9. Обособяване на скрити шифровани пространства

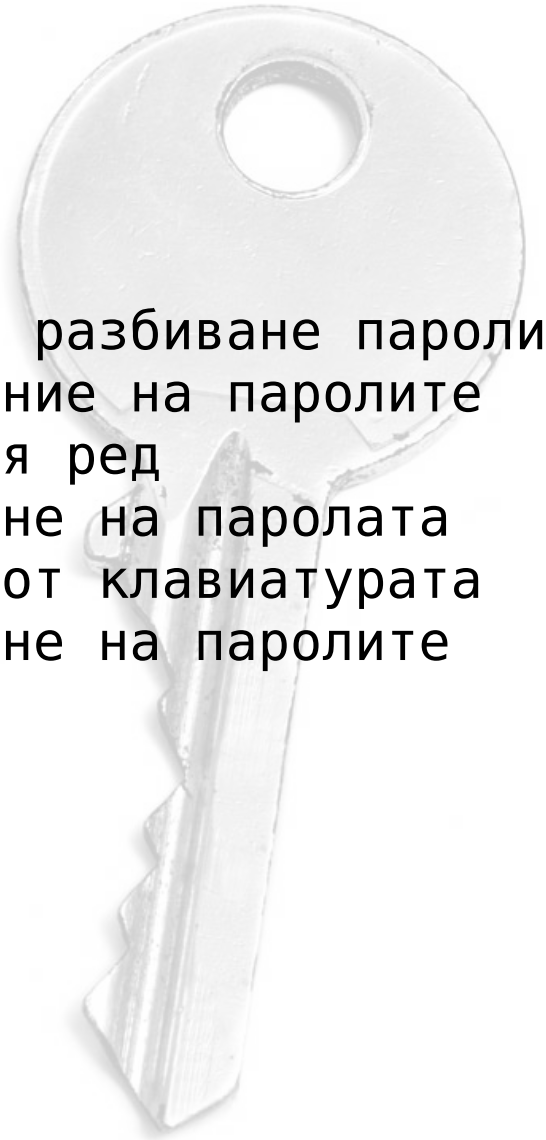
ЦЯЛОСТНО ШИФРОВАН ТВЪРД ДИСК С ИЗНЕСЕНА GRUB ПРОГРАМА



ОБЩО ШИФРОВАНО ПРОСТРАНСТВО СЪС СКРИТ ШИФРОВАН СЛОЙ



V. ОБЕЗПЕЧАВАНЕ СИГУРНОСТТА НА ПАРОЛИТЕ



1. Съставянето на достатъчно трудни за разбиване пароли
2. Особености на поведението по отношение на паролите
3. Променяне на паролите чрез командния ред
4. Критичния момент при самото въвеждане на паролата
5. Проблеми, които могат да възникнат от клавиатурата
6. Неотложни действия при компрометиране на паролите

„СТОЙНОСТТА“ НА ВСЕКИ ОТ СИМВОЛИТЕ В ПАРОЛАТА

Б^Д

само десетте цифри от 0 до 9

10^5 = 100'000

+ малките букви от латиницата

36^5 = 60'466'176

цялата символна таблица ASCII

95^5 = 7'737'809'375

само + още един символ с ASCII

95^6 = 735'091'890'625

символна таблица Extended ASCII

218^12 = 11'520'674'946'182'735'813'538'942'976

ПРИМЕРНИ ВАРИАЦИИ НА ТЕМА „ПАРОЛА“

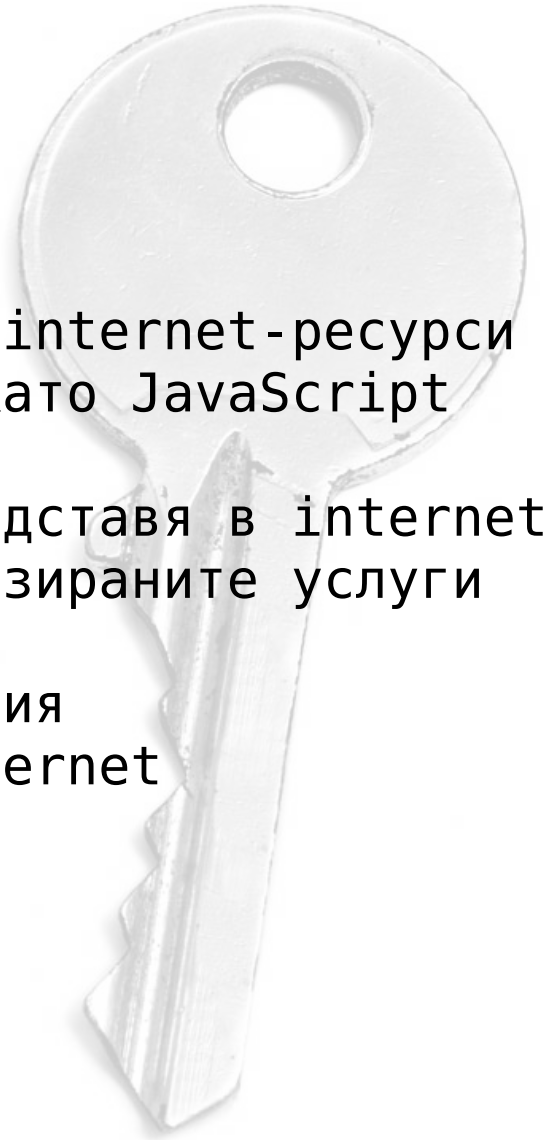
АзОбичамБира
A3O6i4am6ira И.с.1 + И.с.3 + И.2.к
DpF/r'd;?r,d
Åʒ0bи茶µБí®α AsenTodorkaSharoBalkan

АзОбичамБира123aaa
5a5a5aA3O6i4am6ira

A3O6i4am6ira > a#)^I$AM^IRA
DpF/r'd;?r,d > dPf.R"D:/R<D

ЗА КЛАВИАТУРНАТА ПОДРЕДБА

VI. ЗАЩИТАВАНЕ НА СВЪРЗВАНЕТО С INTERNET



1. За фалшивите адреси и подправените internet-ресурси
2. За опасностите на програмни езици като JavaScript
3. За ползването на „защитни стени“
4. За данните, които компютърът се представя в internet
5. За цялостната несигурност на web-базираните услуги
6. За ползването на електронна поща
7. За ползването на моментна комуникация
8. За ползването на анонимизация в internet
9. За ползването на търсещи машини

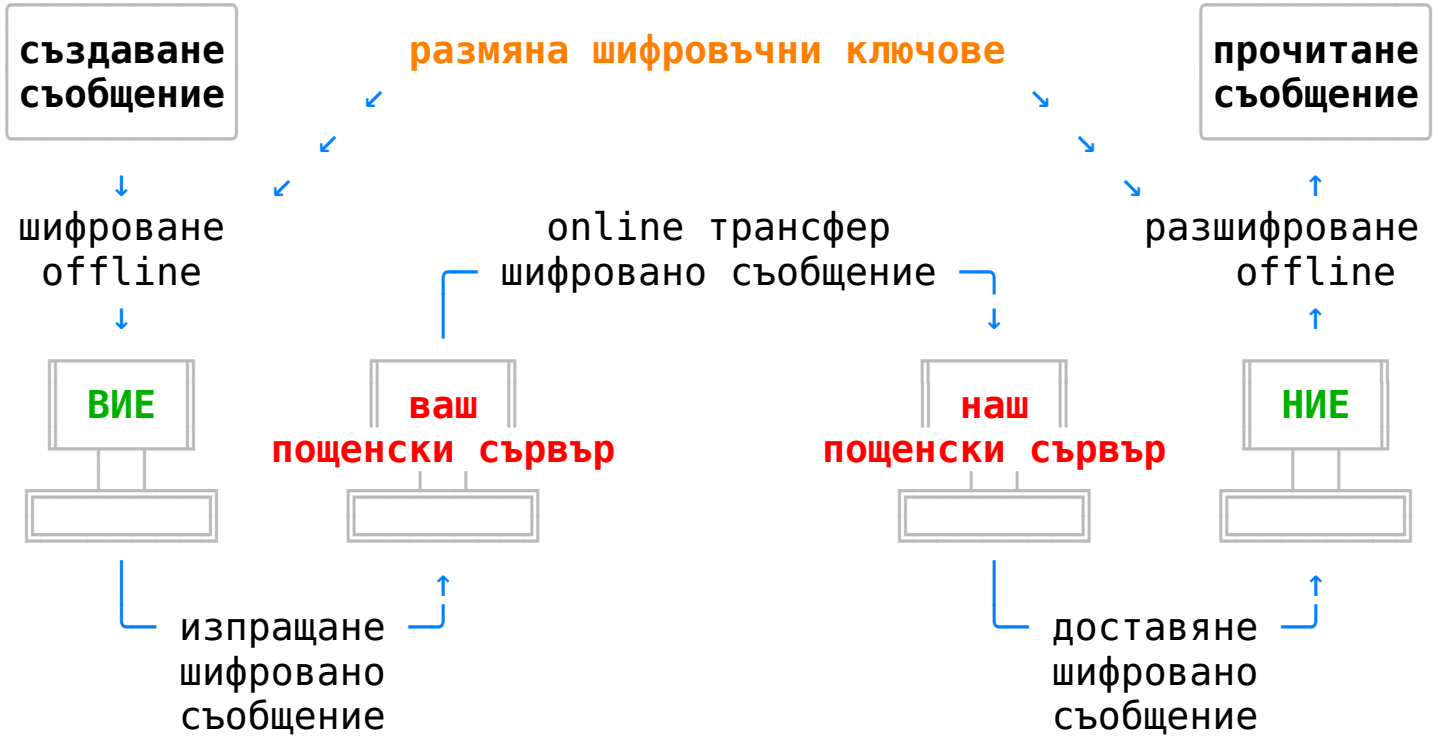
A B C

https://googl1e.com/
google.com.login.fraud.site/settings
fraud.site/settings/google.com

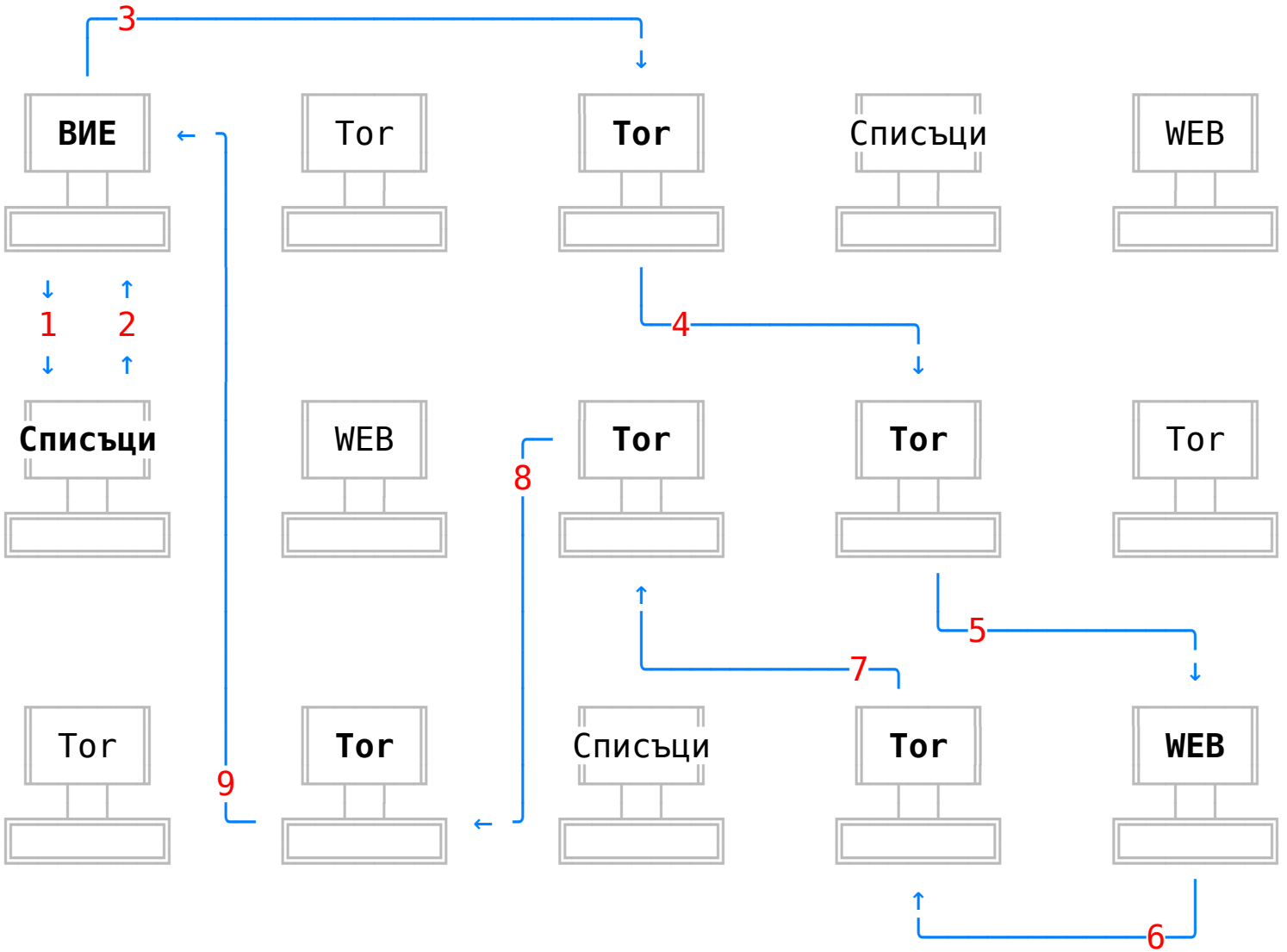
A B C

https://goog1e.com/
google.com.login.fraud.site/settings
fraud.site/settings/google.com

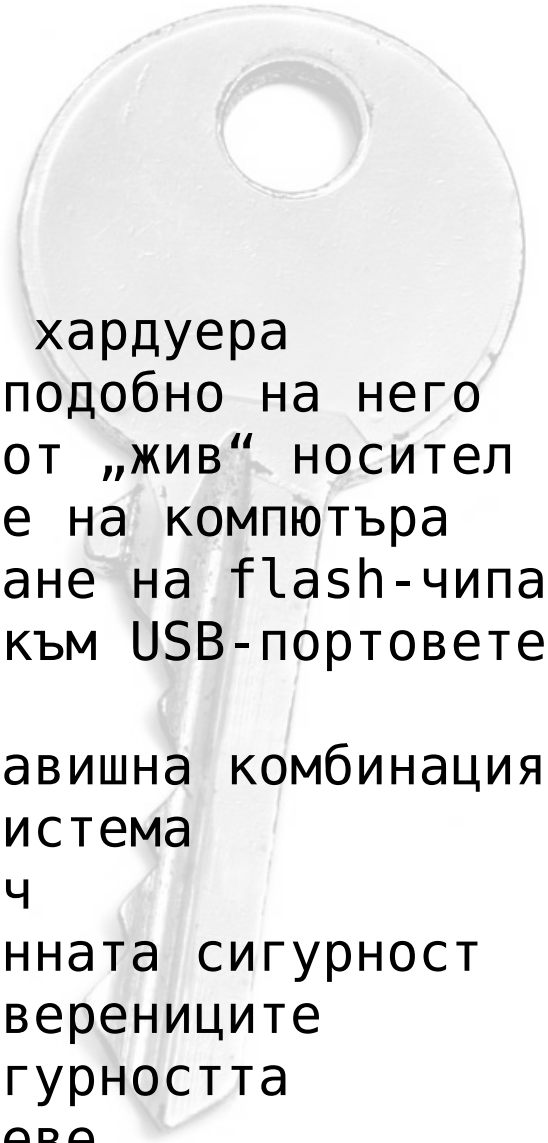
ПРИНЦИПНА СХЕМА ЗА ШИФРОВАНЕ ПРИ ПОЛЗВАНЕТО НА E-MAIL



ПРИНЦИПНА СХЕМА НА НАЧИНА НА ФУНКЦИОНИРАНЕ НА TOR

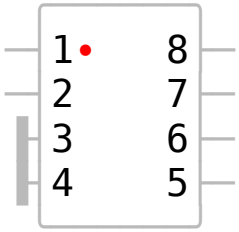


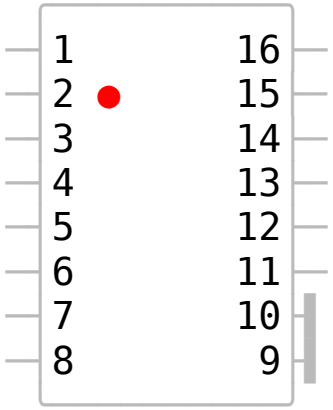
VII. ОРГАНИЗАЦИЯ НА ФИЗИЧЕСКАТА СИГУРНОСТ



1. Неразрешено физическо проникване в хардуера
2. Подменяне на устройството с друго подобно на него
3. Стартиране на операционна система от „жив“ носител
4. Защита срещу неразрешено стартиране на компютъра
5. Защита срещу неразрешено програмиране на flash-чипа
6. Защита срещу неразрешено закачане към USB-портовете
7. Обслужване на компютъра в сервиз
8. Заключване на системата с бърза клавишна комбинация
9. Защитен достъп до компрометирана система
10. Инцидентна загуба на 'частния' ключ
11. Цялостна организация на информационната сигурност
12. За информационната сигурност на доверениците
13. Неотложни действия при пробив в сигурността
14. Информационната сигурност като слоеве

БЛОКИРАНЕ ПРЕПРОГРАМИРАНЕТО НА FLASH-ЧИПА (8 и 16 пина)



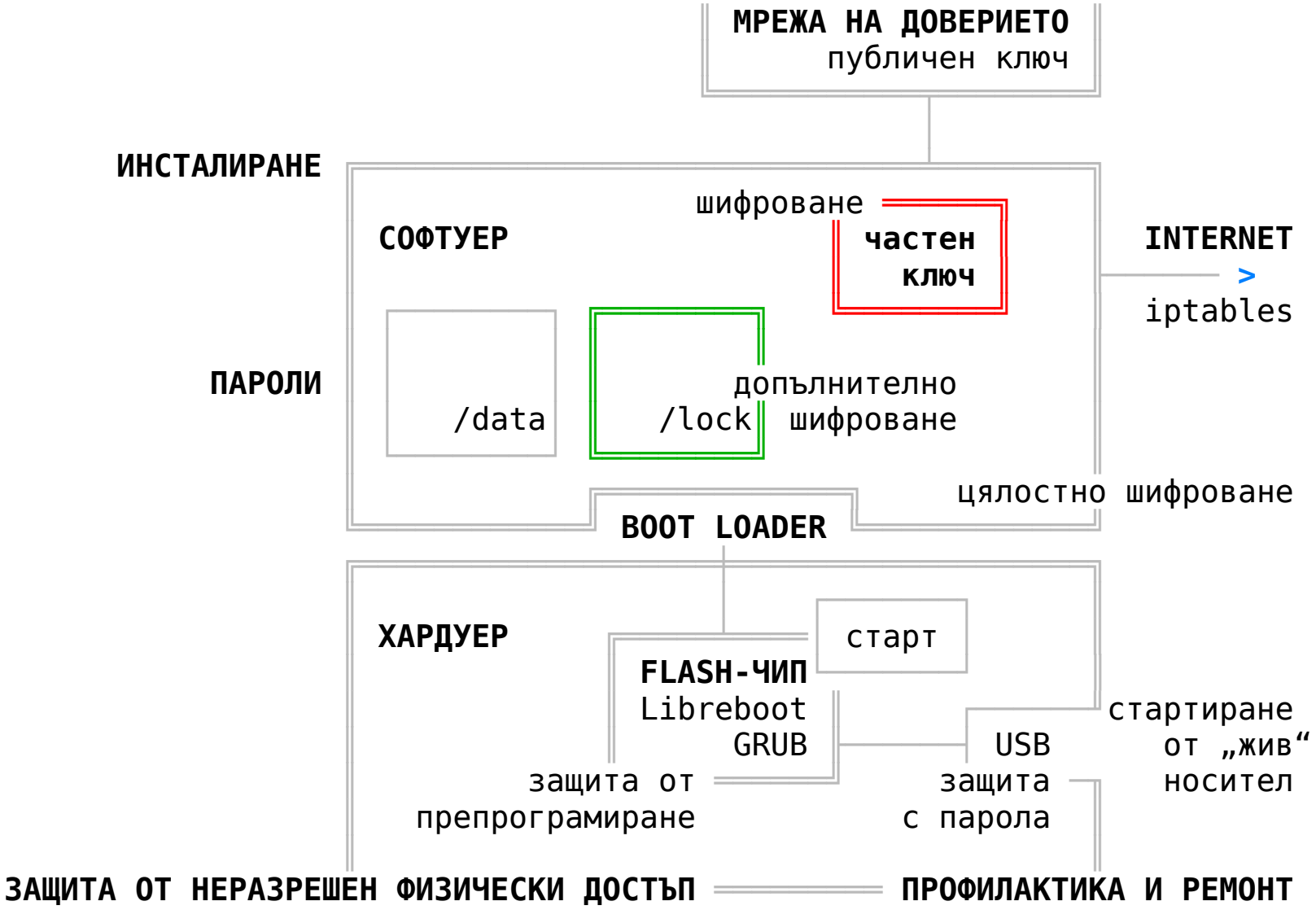


ТЪРСЕНЕ НА ИНЦИДЕНТНО ИЗГУБЕНИЯ 'ЧАСТЕН' КЛЮЧ

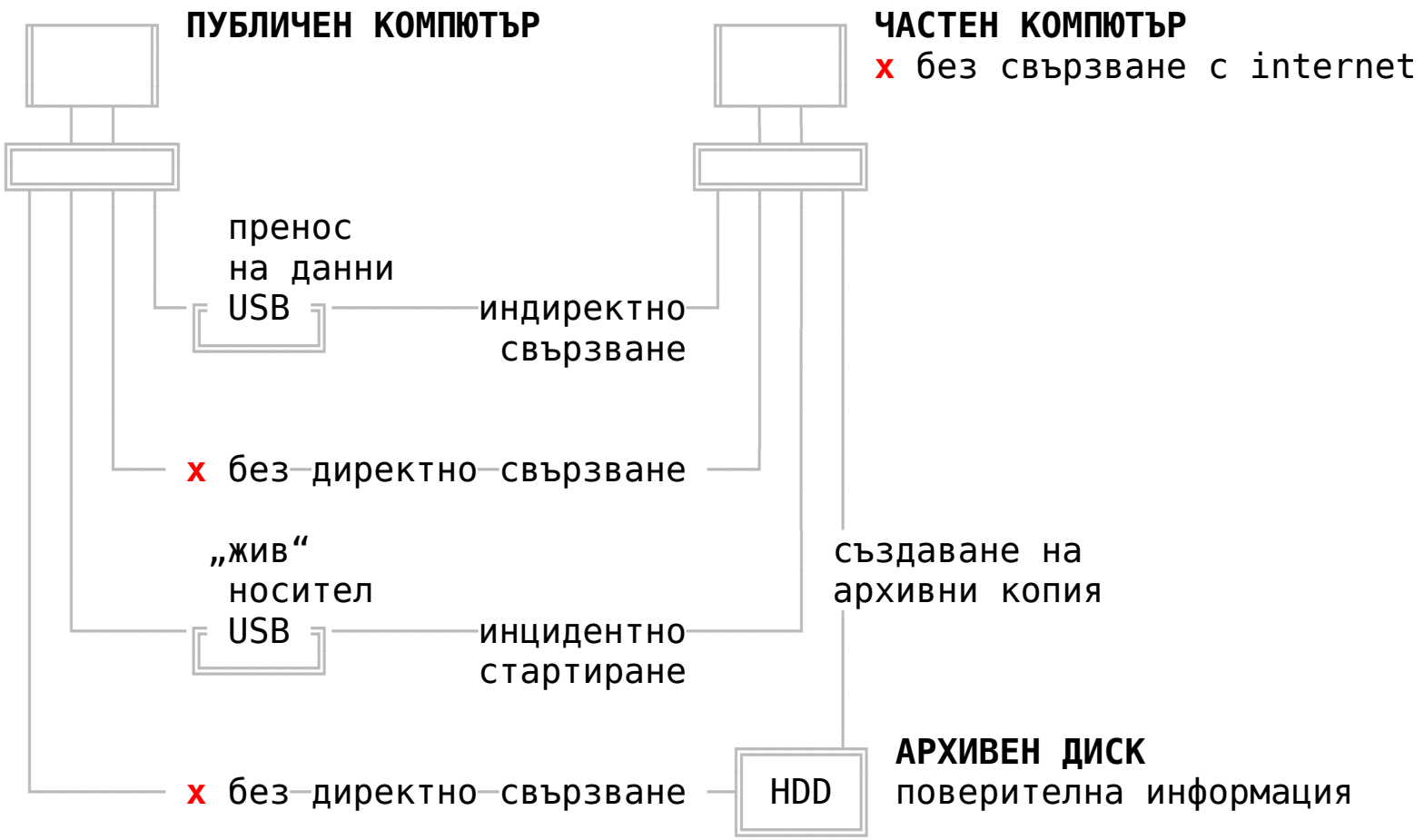
120549778

```
00000000 43 72 65 61 74 65 64 3a  20 32 30 32 33 30 37 32 |Created: 2023072|
00000010 33 54 32 30 33 36 30 33  0a 4b 65 79 3a 20 28 70 |3T203603.Key: (p|
00000020 72 6f 74 65 63 74 65 64  2d 70 72 69 76 61 74 65 |rotected-private|
00000030 2d 6b 65 79 20 28 72 73  61 20 28 6e 20 23 30 30 |-key (rsa (n #00|
00000040 43 46 35 32 43 46 43 31  34 34 42 39 41 31 41 44 |CF52CFC144B9A1AD|
00000050 30 37 36 44 39 38 39 45  38 33 43 41 46 34 33 35 |076D989E83CAF435|
00000060 0a 20 33 32 39 36 37 35  39 41 45 35 35 41 35 42 |. 3296759AE55A5B|
(...)
00000bd0 34 35 44 39 45 43 41 44  44 32 42 37 44 46 43 44 |45D9ECADD2B7DFCD|
00000be0 42 34 32 38 32 33 37 30  43 39 44 37 41 39 32 42 |B4282370C9D7A92B|
00000bf0 32 42 30 32 31 36 33 23  29 28 70 72 6f 74 65 63 |2B02163#)(protec|
00000c00 74 65 64 2d 61 74 0a 20  20 22 32 30 32 33 30 37 |ted-at.  "202307|
00000c10 32 33 54 32 30 33 36 33  31 22 29 29 29 0a       |23T203631"))).|
```

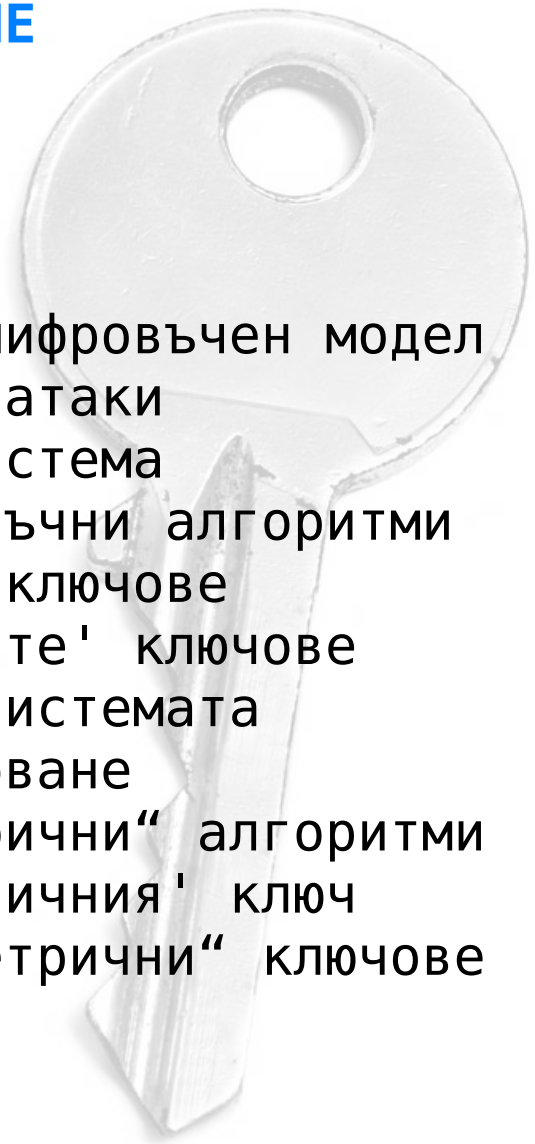
ПРИНЦИПНА СХЕМА НА ИНФОРМАЦИОННАТА СИГУРНОСТ (УСТРОЙСТВО)



ПРИНЦИПНА СХЕМА НА ИНФОРМАЦИОННАТА СИГУРНОСТ (МРЕЖА)



VIII. ИЗВЪРШВАНЕ НА НАДЕЖДНО GPG-ШИФРОВАНЕ



1. Обща характеристика и теоретичен шифровъчен модел
2. Основни криптоаналитични методи и атаки
3. Инсталиране на GnuPG във вашата система
4. Шифроване чрез „симетрични“ шифровъчни алгоритми
5. Създаване на двойка „асиметрични“ ключове
6. Извличане и въвеждане на 'публичните' ключове
7. Извличане на 'частни' ключове от системата
8. „Асиметрично“ шифроване и разшифроване
9. Цифрово „подписване“ чрез „асиметрични“ алгоритми
10. Установяване актуалността на 'публичния' ключ
11. Анулиране на компрометирани „асиметрични“ ключове

ТЕОРЕТИЧЕН МОДЕЛ

Две взаимно прости числа **q** и **p** => **'Публичен' ключ** (**n** ; **e**)

Модул **n** = **q** * **p**

Експонента **e** < **φ** = (**q**-**1**) * (**p**-**1**) ; без общ делител с **φ**

Експонента **d**: **d** * **e** ≡ **1** (mod **φ** (**n**)) => **'Частен' ключ** (**n** ; **d**)

=> (**d** * **e**) / **n**

Шифроване: **c** ≡ **m** ^ **e** (mod **n**) **Разшифроване:** **m** = **c** ^ **d** (mod **n**)

ТЕОРЕТИЧЕН МОДЕЛ

Две взаимно прости числа **q** и **p** => **'Публичен' ключ** (**n** ; **e**)
3 и **11** **33** ; **7**

Модул **n** = **q** * **p**
3 * **11** = **33**

Експонента **e** < **φ** = (**q**-**1**) * (**p**-**1**) ; без общ делител с **φ**
(**3** **1**) * (**11**-**1**) = **20**

↘

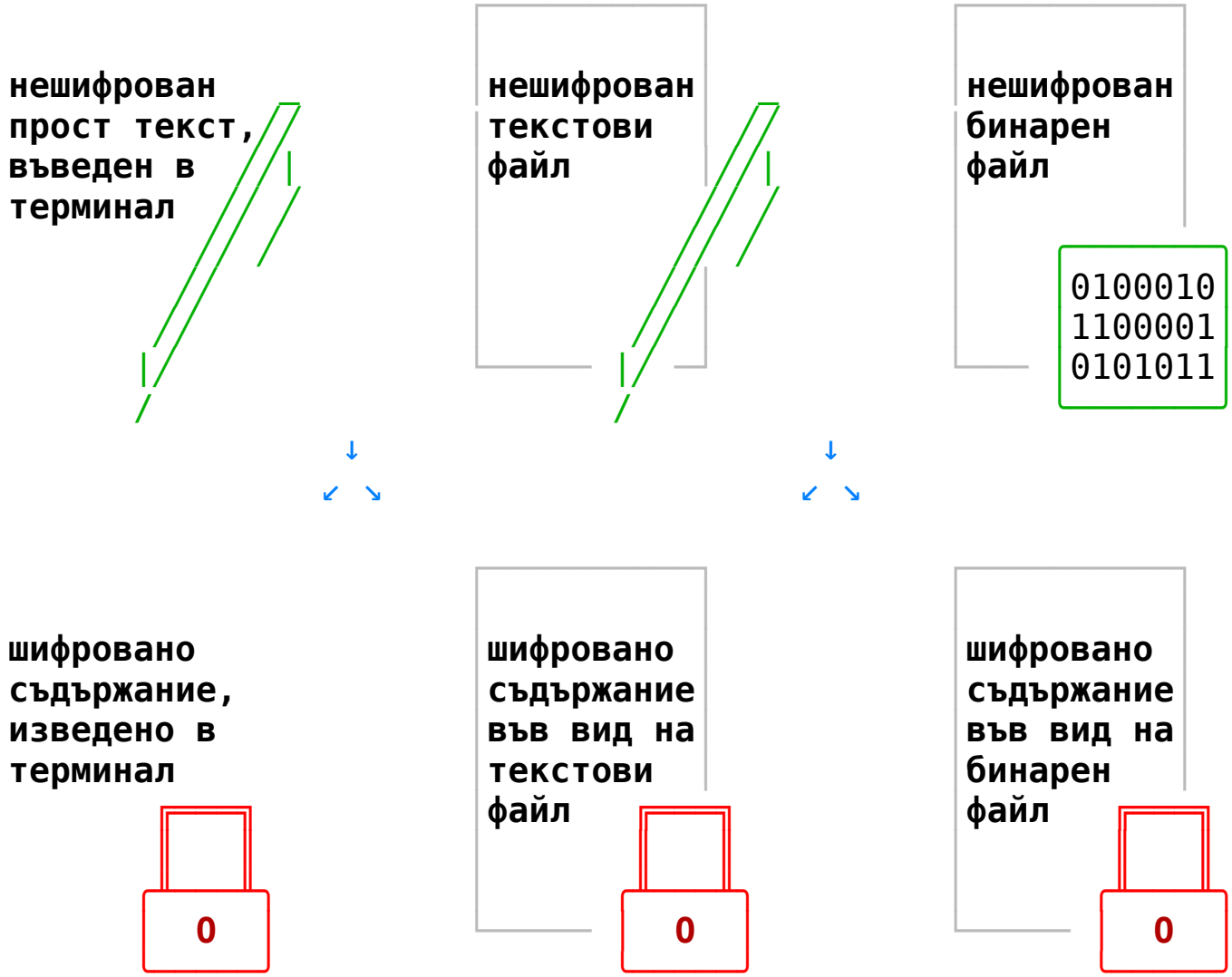
=> **3**, **7**, **9**, **11**, **13**, **15**, **17**, **19**

Експонента **d**: **d** * **e** ≡ **1** (mod **φ** (**n**)) => **'Частен' ключ** (**n** ; **d**)
33 ; **3**

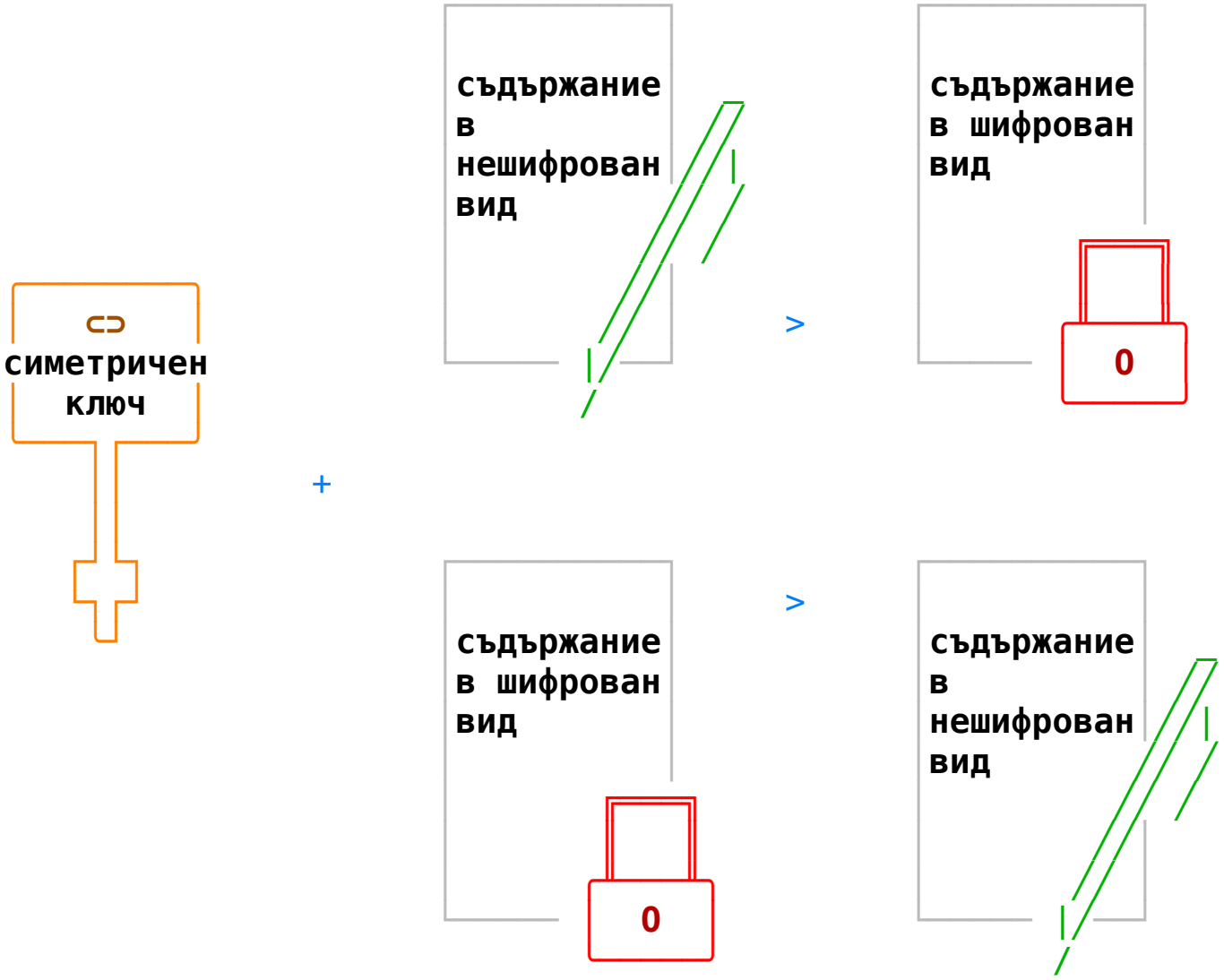
=> (**d** * **e**) / **n**
(**3** * **7**) /**20** = **20** + **1**

Шифроване: **c** ≡ **m** ^ **e** (mod **n**) **Разшифроване:** **m** = **c** ^ **d** (mod **n**)
5 ^ **7** (**mod** **33**) = **14** **14** ^ **3** (mod **33**) = **5**

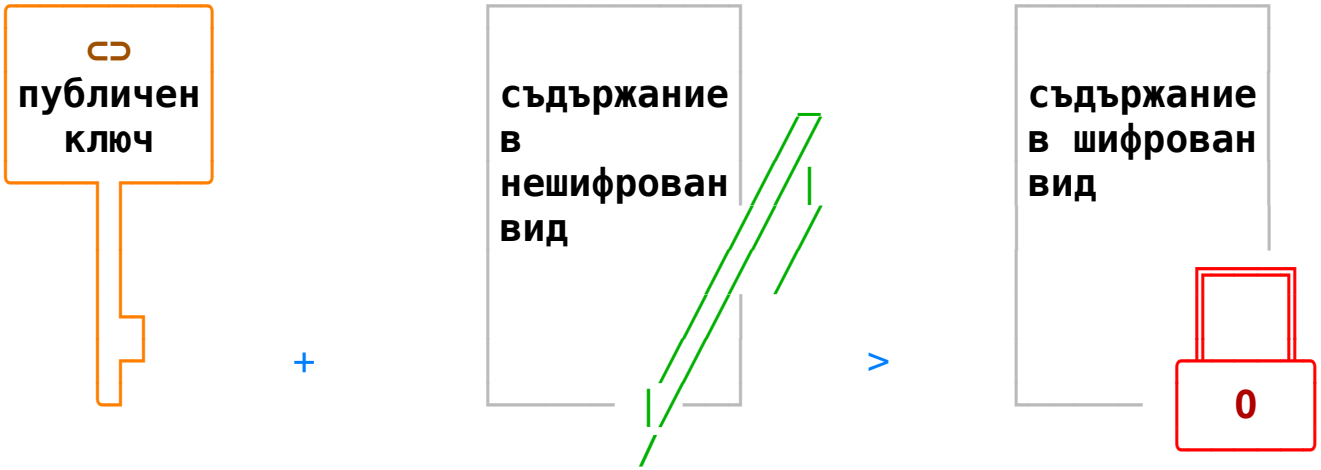
ВИДОВЕ ПОВЕРИТЕЛНО СЪДЪРЖАНИЕ В (НЕ)ШИФРОВАН ВИД



„СИМЕТРИЧНО“ (РАЗ)ШИФРОВАНЕ С 'СИМЕТРИЧЕН' КЛЮЧ (ПАРОЛА)



„АСИМЕТРИЧНО“ (РАЗ)ШИФРОВАНЕ С 'ПУБЛИЧЕН' И 'ЧАСТЕН' КЛЮЧ



IX. ПРЕДСТАВЯМЕ ВИ НАШИЯ 'ПУБЛИЧЕН' КЛЮЧ

Информационна сигурност чрез Свободни технологии

www.Advocati.org/consultation/security/

www.LibTec.org/in_need_encrypt/