Белорусско-Российский университет
Кафедра «Программное обеспечение информационных технологий»

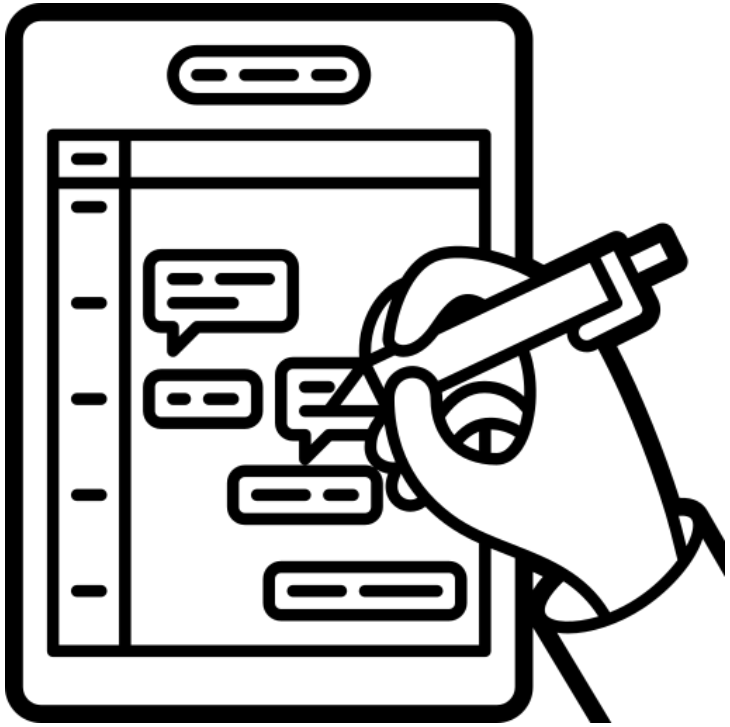
Защита информации

Криптография

Применение криптографических средств защиты информации

КУТУЗОВ Виктор Владимирович

Республика Беларусь, Могилев, 2024



Основные определения

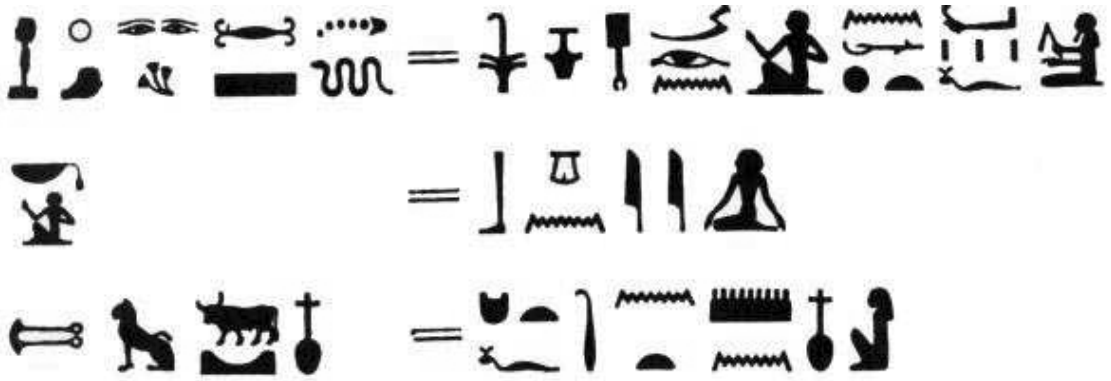
Основные определения

- **Криптография** — наука о методах обеспечения конфиденциальности (невозможности прочтения информации посторонним) и аутентичности (целостности и подлинности авторства, а также невозможности отказа от авторства) информации.

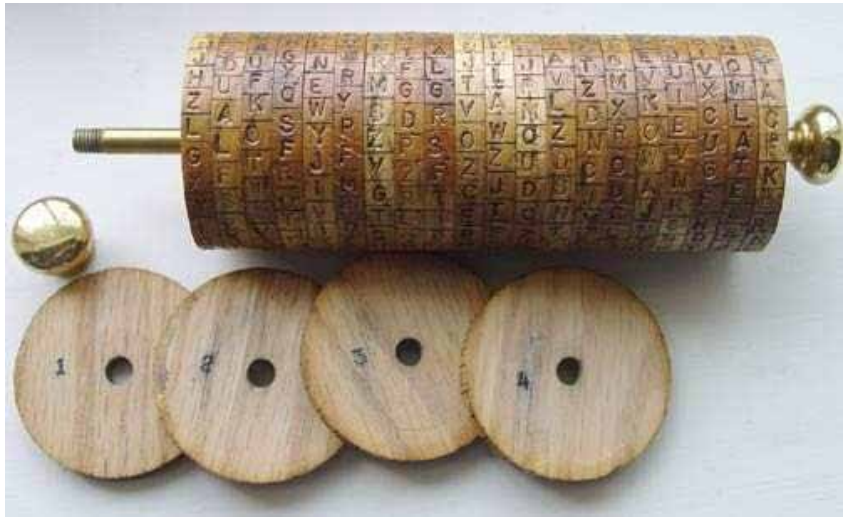
- Изначально **криптография изучала методы шифрования информации** — обратимого преобразования открытого (исходного) текста на основе секретного алгоритма и/или ключа в шифрованный текст (шифротекст).
- **Традиционная криптография** образует раздел симметричных криптосистем, в которых зашифрование и расшифрование проводится с использованием одного и того же секретного ключа. Помимо этого раздела **современная криптография** включает в себя асимметричные криптосистемы, системы электронной цифровой подписи (ЭЦП), хэш-функции, управление ключами, получение скрытой информации, квантовую криптографию.

Криптография

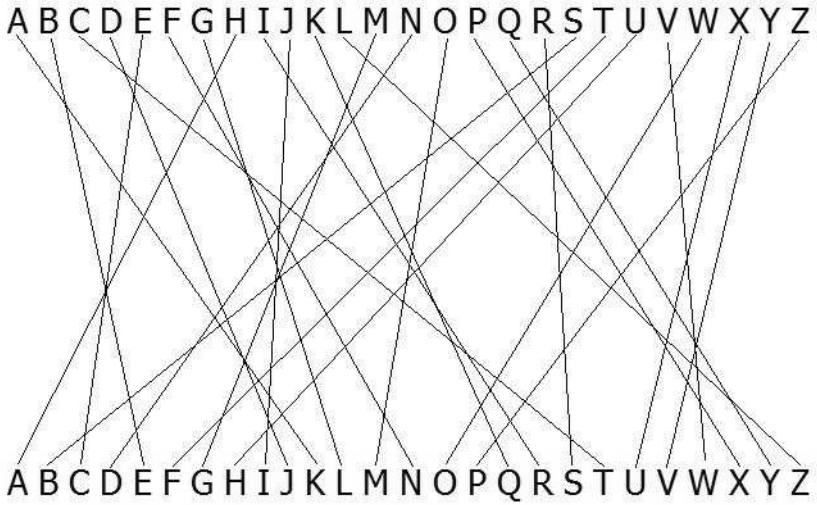
Древняя Греция - Пример скиталы



Древний Египет - Символы из гробницы Хнумхотепа II и их расшифровка

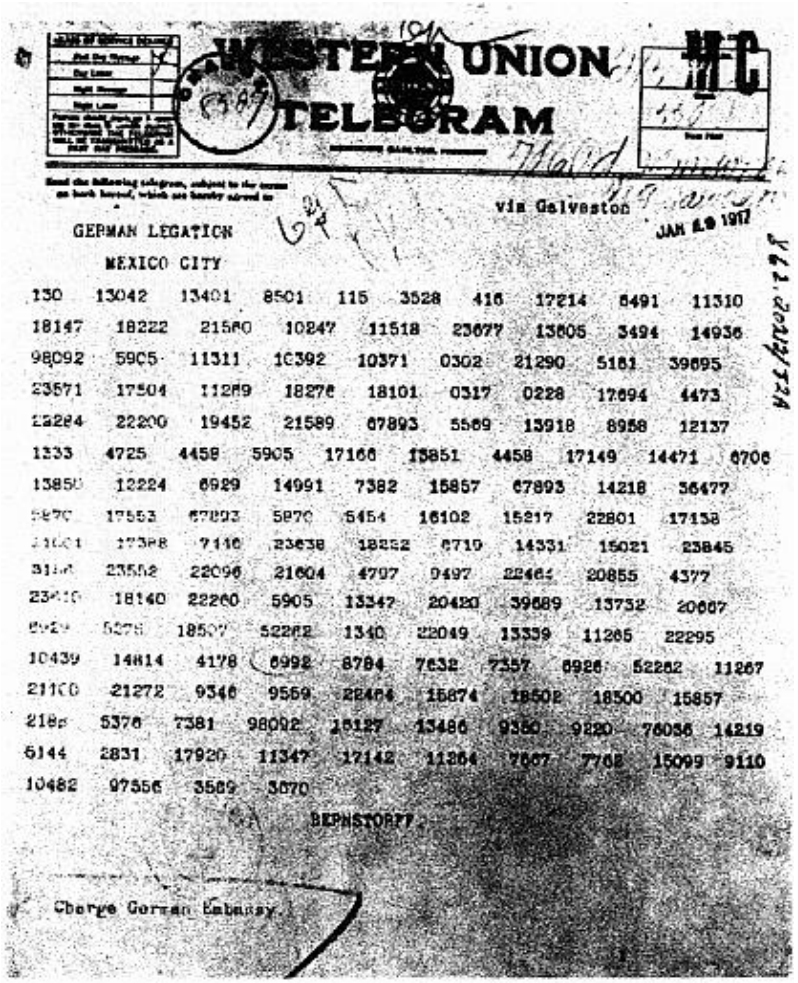


Дисковый шифр Джефферсона



Древний Рим- Пример шифра подстановки

Криптография



Фотокопия телеграммы Циммермана

Германия: «Энигма»

HAGELIN M-209 CIPHER MACHINE (GVG / PD)

Криптографическая машина M-209

Основные определения

- **Шифр** — это совокупность условных знаков (условная азбука из цифр или букв) для секретной переписки дипломатических представителей со своими правительствами, а также в вооруженных силах для передачи текста секретных документов по техническим средствам связи.
- **Открытый (исходный) текст** — данные (текстовые или иного вида), передаваемые без использования криптографии.
- **Шифротекст, шифрованный (закрытый) текст** — данные, полученные после применения криптосистемы (обычно с некоторым указанным ключом).

Основные определения

- **Код** — это совокупность алгоритмов криптографических преобразований (шифрования), отображающих множество возможных открытых данных на множество возможных зашифрованных данных, и обратных им преобразований. Важным параметром любого шифра является ключ.
- **Ключ** — это параметр криптографического алгоритма, обеспечивающий выбор одного преобразования из совокупности преобразований, возможных для этого алгоритма. В современной криптографии предполагается, что вся секретность криптографического алгоритма сосредоточена в ключе, но не деталях самого алгоритма (принцип Керкгоффса).

Основные определения

- **Шифры могут использовать один ключ для шифрования и дешифрования или два различных ключа.**
- По этому признаку различают симметричный и асимметричный шифры.
- **Симметричный шифр** — это шифр, который использует один ключ для шифрования и дешифрования.
- Симметричное шифрование — это способ шифрования данных, при котором один и тот же ключ используется и для кодирования, и для восстановления информации. До 1970-х годов, когда появились первые асимметричные шифры, оно было единственным криптографическим методом.

Основные определения

- **Асимметричный шифр** — это шифр, который для шифрования и дешифрования использует два различных ключа. К асимметричным шифрам относятся следующие известные шифры: RSA, Эль-Гамаля (Elgamal), Elliptic curve cryptography (ECC) — криптосистема на основе эллиптических кривых.

Основные определения

- **Шифры могут быть сконструированы так, чтобы либо шифровать сразу весь текст, либо шифровать его по мере поступления.**
- Таким образом, существуют блочный и поточный шифры.
- **Блочный шифр** шифрует сразу целый блок текста, выдавая шифротекст после получения всей информации.
- В блочных шифрах результат зашифрования очередного блока зависит только от него самого и не зависит от других блоков шифруемого массива данных.
- **К блочным шифрам относятся следующие известные шифры:** ГОСТ 28147-89, Advanced Encryption Standard (AES), также известный как Rijndael, DES, DESX, Triple DES, CAST-Ш, CAST-256, Blowfish, Twofish, IDEA, MARS, RC2, RC5, RC6, Serpent, Safer+, TEA, 3-WAY, WAKE, FROG, Skipjack.

Основные определения

- **Поточный (потоковый) шифр** шифрует информацию и выдает шифротекст по мере ее поступления. За счет этого поточный шифр имеет возможность обрабатывать текст неограниченного размера, используя фиксированный объем памяти.
- **Поточный шифр** — это симметричный шифр, в котором каждый символ открытого текста преобразуется в символ шифрованного текста в зависимости не только от используемого ключа, но и от его расположения в потоке открытого.
- **К поточным шифрам относятся следующие известные шифры: RC4, A5.**

Основные определения

- **Аддитивный шифр** — шифр гаммирования, в котором для наложения гаммы на открытый текст используется бинарная операция аддитивного типа. Обычно это суммирование в каком-либо конечном поле (например, в поле GF(2).

- **Шифрование** — процесс нормального применения криптографического преобразования открытого текста на основе алгоритма и ключа, в результате которого возникает шифрованный текст.

- **Расшифровывание** — процесс нормального применения криптографического преобразования шифрованного текста в открытый.

Классификация криптографических алгоритмов

Классификация криптографических алгоритмов

- В **симметричных криптографических алгоритмах** зашифрование и расшифрование производятся с помощью одного и того же ключа. И соответственно этот ключ необходимо хранить в секрете (отсюда другое название **симметричных криптоалгоритмов — криптоалгоритмы с секретным ключом**).

Классификация криптографических алгоритмов

- В **несимметричных криптографических алгоритмах** существуют два разных ключа — один используется для зашифровывания, который еще называют **открытым**, другой — для расшифровывания, который называют **закрытым**.
- Главное отличие асимметричных криптоалгоритмов заключается в том, что даже тот, кто с помощью открытого ключа зашифровал сообщение, не сможет его самостоятельно расшифровать без знания закрытого ключа. Поэтому эти криптоалгоритмы называются **несимметричными (асимметричными), или алгоритмами с открытым ключом**.

Классификация криптографических алгоритмов

- **Гибридными** принято называть криптоалгоритмы, сочетающие оба типа, в них, как правило, текст сообщения шифруется с использованием симметричного криптоалгоритма, а секретный ключ использованного симметричного криптоалгоритма шифруется с использованием асимметричного криптоалгоритма.

Классификация криптографических алгоритмов

- **По типу обработки входящей информационной последовательности** криптоалгоритмы делятся на
  - **поточные**, в которых преобразуется все сообщение сразу,
  - и **блочные**, в которых сообщение обрабатывается в виде блоков определенной длины.
  - **Комбинированные** криптоалгоритмы сочетают в себе элементы поточного и блочного шифрования.

Классификация криптографических алгоритмов

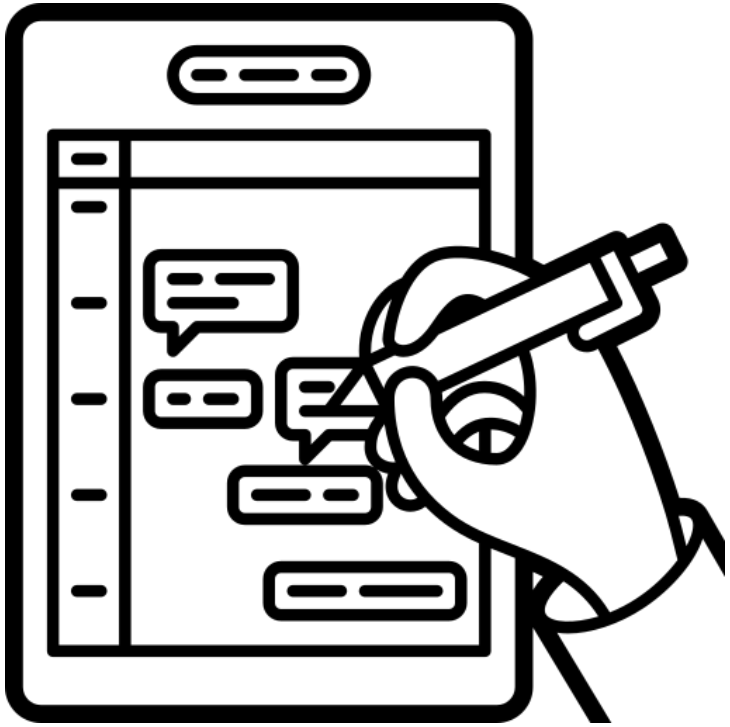
- **По типу шифрующего преобразования** криптосистемы делятся на:
  - — шифры замены;
  - — шифры перестановок;
  - — шифры гаммирования;
  - — шифры, основанные на аналитических преобразованиях шифруемых данных;

Классификация криптографических алгоритмов

- **Шифрование заменой (подстановкой)** заключается в том, что символы шифруемого текста заменяются символами того же или другого алфавита в соответствии с заранее обусловленной схемой замены.
- По сути дела, шифры перестановки и замены являются кирпичиками, из которых строятся различные более стойкие шифры.
- **Шифрование перестановкой** заключается в том, что символы шифруемого текста переставляются по определенному правилу в пределах некоторого блока этого текста. При достаточной длине блока, в пределах которого осуществляется перестановка, и сложном неповторяющемся порядке перестановки можно достигнуть приемлемой для простых практических приложений стойкости шифра.

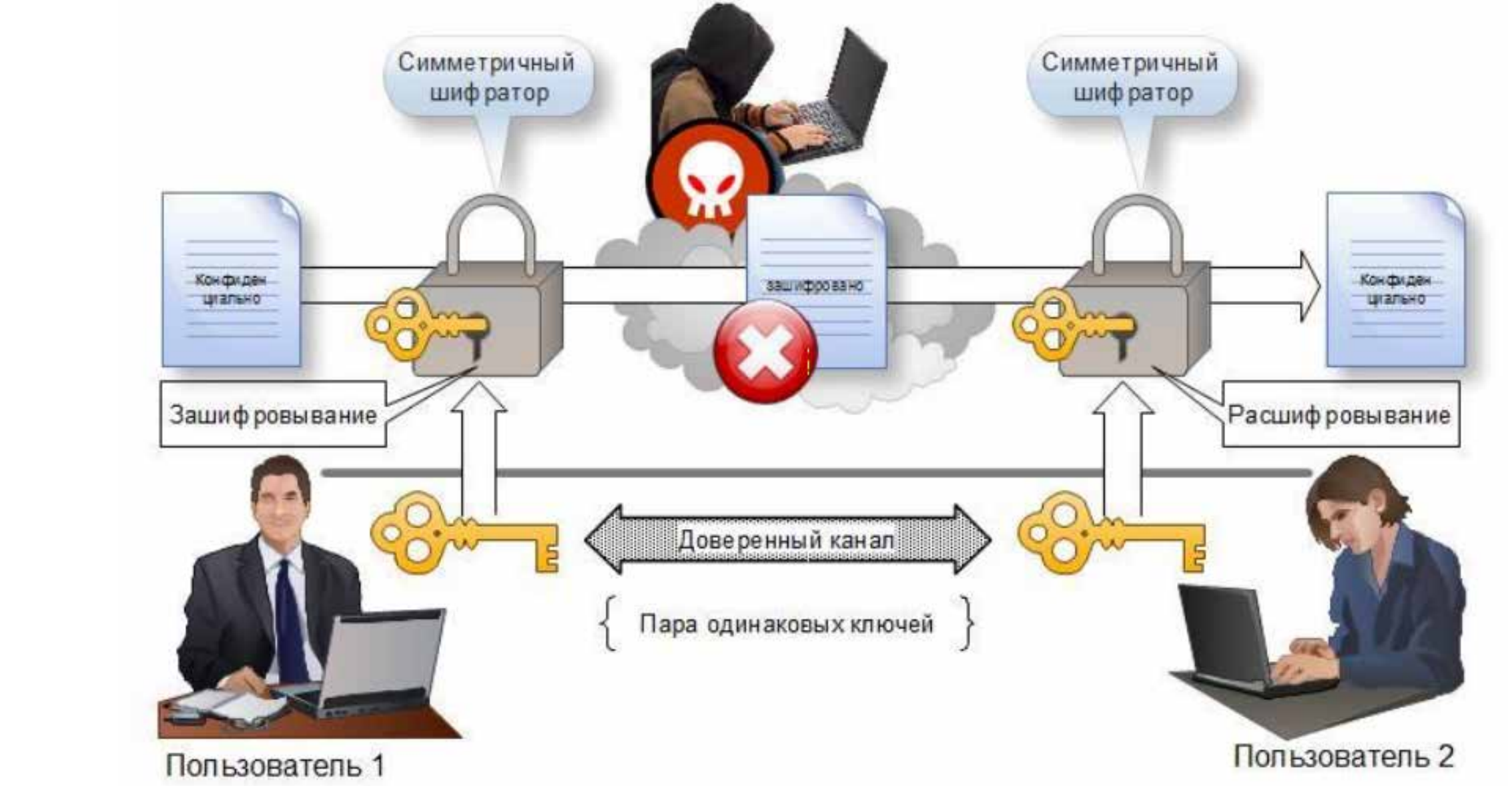
Классификация криптографических алгоритмов

- **Шифрование гаммированием** заключается в том, что символы шифруемого текста складываются с символами некоторой случайной последовательности, именуемой гаммой шифра. Стойкость шифрования определяется в основном длиной (периодом) неповторяющейся части гаммы шифра. Поскольку с помощью ЭВМ можно генерировать практически бесконечную гамму шифра, то данный способ является одним из основных для шифрования информации в автоматизированных системах.
- **Шифрование аналитическим преобразованием** заключается в том, что шифруемый текст преобразуется по некоторому аналитическому правилу (формуле).



Криптография с симметричными ключами

Схема шифрования с симметричными ключами



Криптография с симметричными ключами

- Шифры подстановки
  - Шифр Цезаря
  - Шифр Виженера
  - Шифр Вернама (одноразовые блокноты)
- Шифры перестановки
- Поточные шифры
- Алгоритм XOR
- Блочные шифры
  - DES (Data Encryption Standard)
  - ГОСТ 28147
  - AES / Rijndael

Виды симметричных шифров

https://ru.wikipedia.org/wiki/**Симметричные_криптосистемы**

блочные шифры

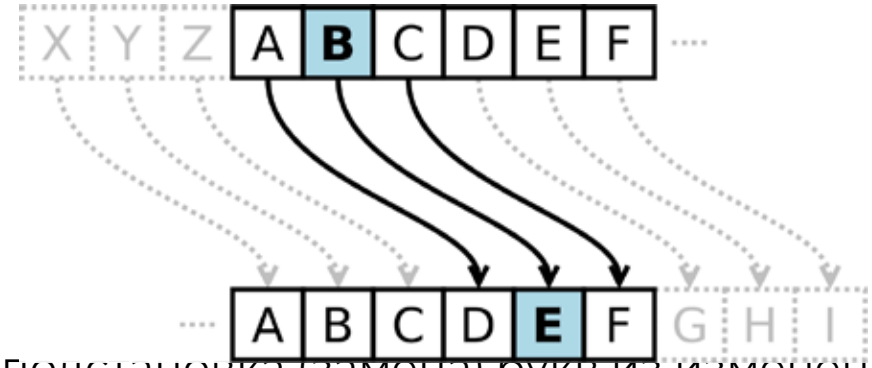
- AES (англ. *Advanced Encryption Standard*) — американский стандарт шифрования
- ГОСТ 28147-89 — советский и российский стандарт шифрования, также является стандартом СНГ
- DES (англ. *Data Encryption Standard*) — стандарт шифрования данных в США
- 3DES (Triple-DES, тройной DES)
- RC2 (Шифр Ривеста (Rivest Cipher или Ron's Cipher))
- RC5
- Blowfish
- Twofish
- NUSH
- IDEA (International Data Encryption Algorithm, международный алгоритм шифрования данных)
- CAST (по инициалам разработчиков Carlisle Adams и Stafford Tavares)
- CRAB
- 3-WAY
- Khufu и Khafre
- Kuznechik

потоковые шифры

- RC4 (алгоритм шифрования с ключом переменной длины)
- SEAL (Software Efficient Algorithm, программно-эффективный алгоритм)
- WAKE (World Auto Key Encryption algorithm, алгоритм шифрования на автоматическом ключе)

Шифр Цезаря

http://ru.wikipedia.org/wiki/Шифр_Цезаря



- Используется подстановка (замена) букв из измененного алфавита. В классическом варианте алфавит получают с помощью сдвига букв на три позиции.
- С точки зрения современной парадигмы, можно выделить:
  1. алгоритм (замена букв из полученного с помощью сдвига алфавита)
  2. ключ - k (величина сдвига)

- **Пример: зашифрованный текст с различными ключами.**
  - k=0 зашифрованный текст с различными ключами
  - k=1 ибщйхспгбооьк уёлту т сбимйшоьнй лмяшбнй
  - k=2 йвъкцтрдвппэл фжмуф у твйнкщпэок мнащвок
  - k=3 кгылчусегррюм хзнфх ф угколърюпл нобъгпл
  - k=4 лдьмшфтёдссян циохц х фдлпмысярм опвыдрм
  - k=5 меэнщхужеттао чйпцч ц хемрньтасн пргьесн
  - k=6 нёюооъцфзёуубп шкрчш ч цёнсоэубто рсдэёто

Шифр Виженера

http://ru.wikipedia.org/wiki/Шифр_Виженера

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Шифр Вернама (одноразовые блокноты)

http://ru.wikipedia.org/wiki/Одноразовый_блокнот

- Каждая страница блокнота является ключом и используется один раз.
- Ключ должен обладать тремя свойствами:
  - быть истинно случайным
  - совпадать по размеру с заданным исходным текстом
  - применяться только один раз
- Пример ключа:

```
ZDXWWW EJKAWO FECIFE WSNZIP PXPKIY URMZHI JZTLBC YLGDYJ
HTSVTV RRYYEG EXNCGA GGQVRF FHZCIB EWLGGR BZXQDQ DGGIAK
YHJYEQ TDLCQT HZBSIZ IRZDYS RBYJFZ AIRCWI UCVXTW YKPQMK
CKHVEX VXYVCS WOGAAZ OUVVON GCNEVR LMBLYB SBDCDC PCGVJX
QXAUIP PXZQIJ JIUWYH COVWMJ UZOJHL DWHPER UBSRUJ HGAAPR
CRWVHI FRNTQW AJVWRT ACAKRD OZKIIB VIQGBK IJCWHF GTTSSE
EXFIPJ KICASQ IOUQTP ZSGXGH YTYCTI BAZSTN JKMFXI RERYWE
```

Шифры перестановки

- **исходный текст:** простой шифр перестановки

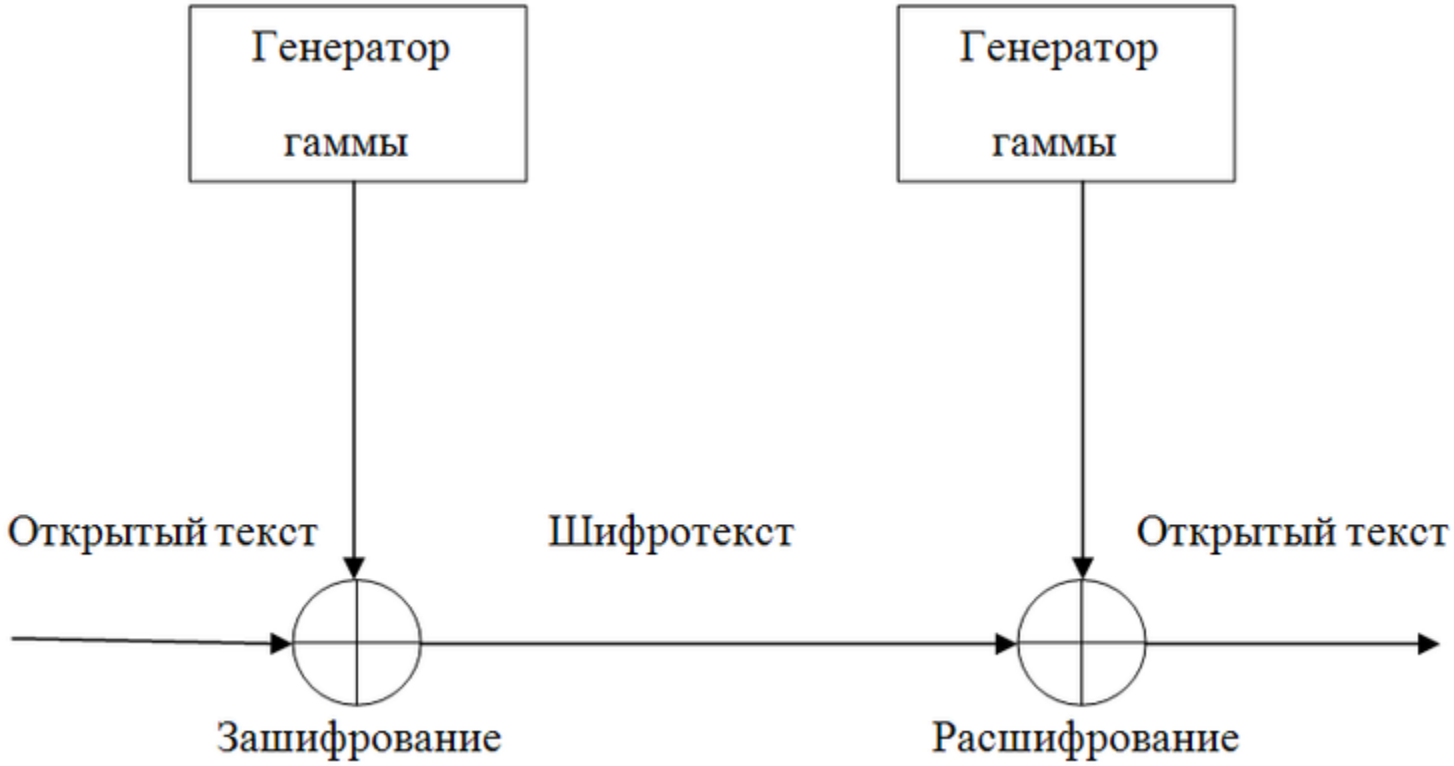
п	т	и	е	т	в
р	о	ф	р	а	к
о	й	р	е	н	и
с	ш	п	с	о	

- **шифрованный текст:** птиетв рофрак ойрени сшпсо
- Алгоритм: запись по столбцам, считывается по строкам.
- Секретный ключ - размер таблицы.

Поточные шифры

http://ru.wikipedia.org/wiki/Поточный_шифр

- Генератор гаммы выдает ключевой поток бит (гамму), который, например, складывается (XOR-ИСКЛЮЧАЮЩЕЕ ИЛИ) с потоком открытого текста.



Алгоритм XOR

https://ru.abcdef.wiki/wiki/XOR_cipher

- Работает с двоичным кодом.
- **правило:**
- 0+0=0
- 0+1=1
- 1+0=1
- 1+1=0
- **исходный текст: Wiki**
- Wiki переведем в двоичный код - 01010111 01101001 01101011 01101001
- Секретный ключ: 11110011 11110011 11110011 11110011
- **Шифрование:**
- 01010111 01101001 01101011 01101001 - открытый текст
- 11110011 11110011 11110011 11110011 - секретный ключ
- 10100100 10011010 10011000 10011010 - шифрованный текст
- **Расшифрование:**
- 10100100 10011010 10011000 10011010 - шифрованный текст
- 11110011 11110011 11110011 11110011 - секретный ключ
- 01010111 01101001 01101011 01101001 - открытый текст

Блочные шифры

http://ru.wikipedia.org/wiki/Блочный_шифр

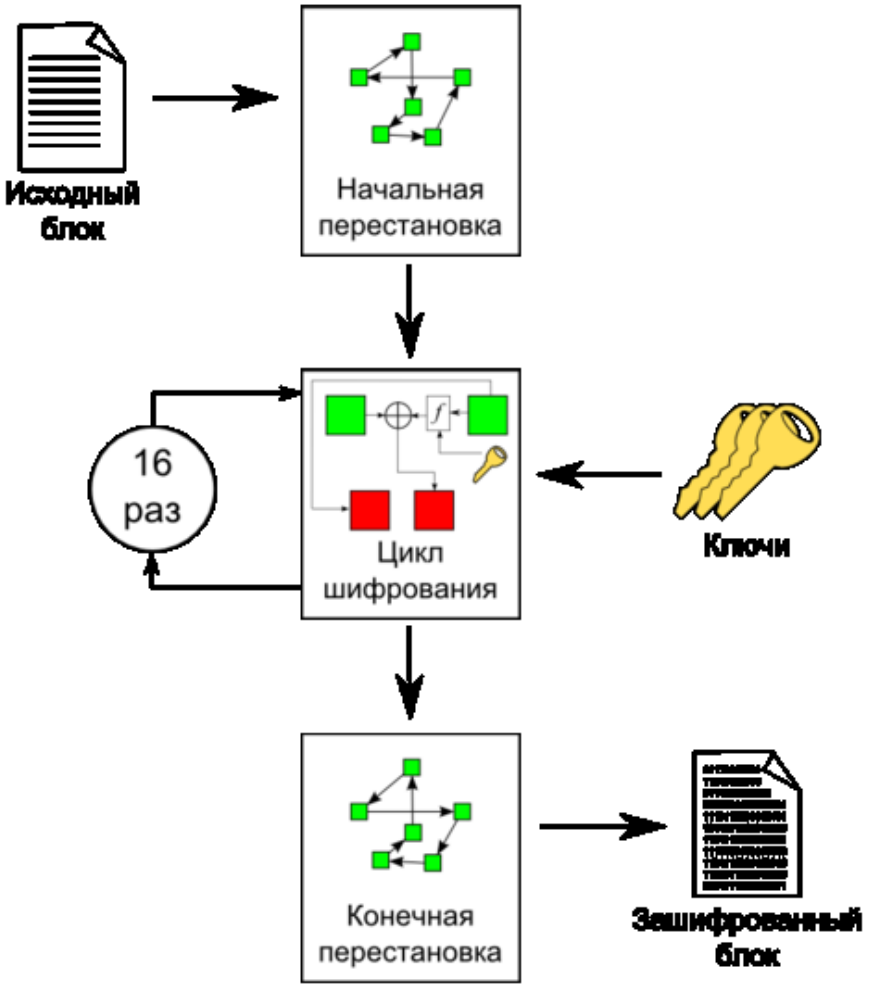
- Данные шифруются блоками.

- Блочные шифры
  - DES (Data Encryption Standard)
  - ГОСТ 28147-89
  - AES / Rijndael

DES (Data Encryption Standard)

http://ru.wikipedia.org/wiki/DES

- Данные шифруются блоками с размером 64 бит
- **DES** (англ. Data Encryption Standard) — алгоритм для симметричного шифрования, разработанный фирмой IBM и утверждённый правительством США в 1977 году как официальный стандарт (FIPS 46-3).
- Размер блока для DES равен 64 битам. В основе алгоритма лежит сеть Фейстеля с 16 циклами (раундами) и ключом, имеющим длину 56 бит. Алгоритм использует комбинацию нелинейных (S-блоки) и линейных (перестановки E, IP, IP-1) преобразований.



Шифрование по ГОСТ 28147

https://ru.wikipedia.org/wiki/**ГОСТ_28147**-89

- **ГОСТ 28147-89** «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования» — **устаревший** государственный стандарт союза ССР (а позже межгосударственный стандарт СНГ), описывающий алгоритм симметричного блочного шифрования и режимы его работы.
- Является примером DES-подобных криптосистем, созданных по классической итерационной схеме Фейстеля.

AES / Rijndael

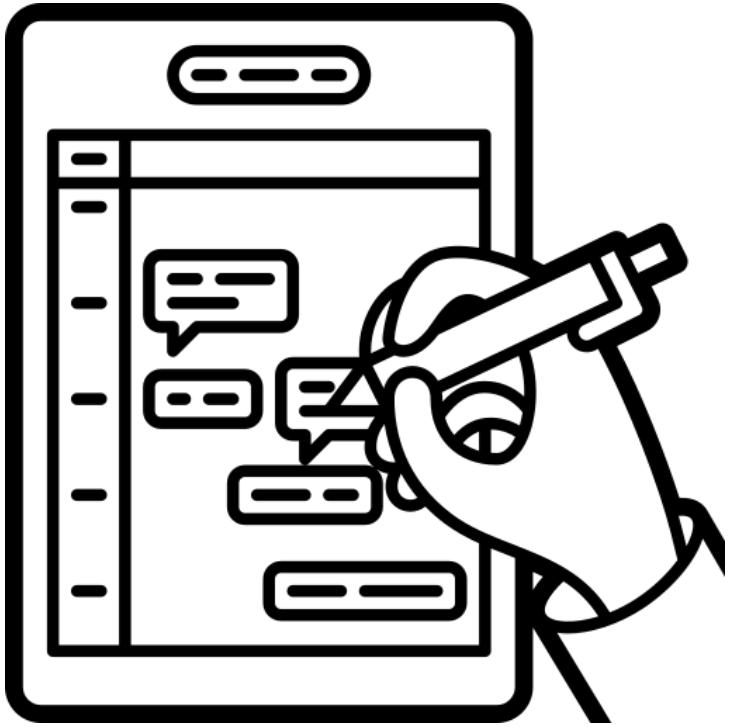
https://ru.wikipedia.org/wiki/Advanced_Encryption_Standard

- **AES**, принятый NIST в 2001 году после 5-летнего общественного конкурса, **заменил собой шифр DES** как федеральный стандарт США. Шифр разработан двумя бельгийскими криптографами Дайменом Йоаном и Рэйменом Винсентом.
- Размер блока составляет 128 бит и размер ключа 128, 192 и 256 бит, несмотря на то, что размер блока может быть определён любым числом бит, кратным 32, с минимальным значением 128 бит.
- Максимальный размер блока равен 256 бит, при этом размер ключа не имеет теоретического предела.
- Поддержка данного шифра введена компанией Intel в семейство процессоров x86.

Сравнение с асимметричными криптосистемами

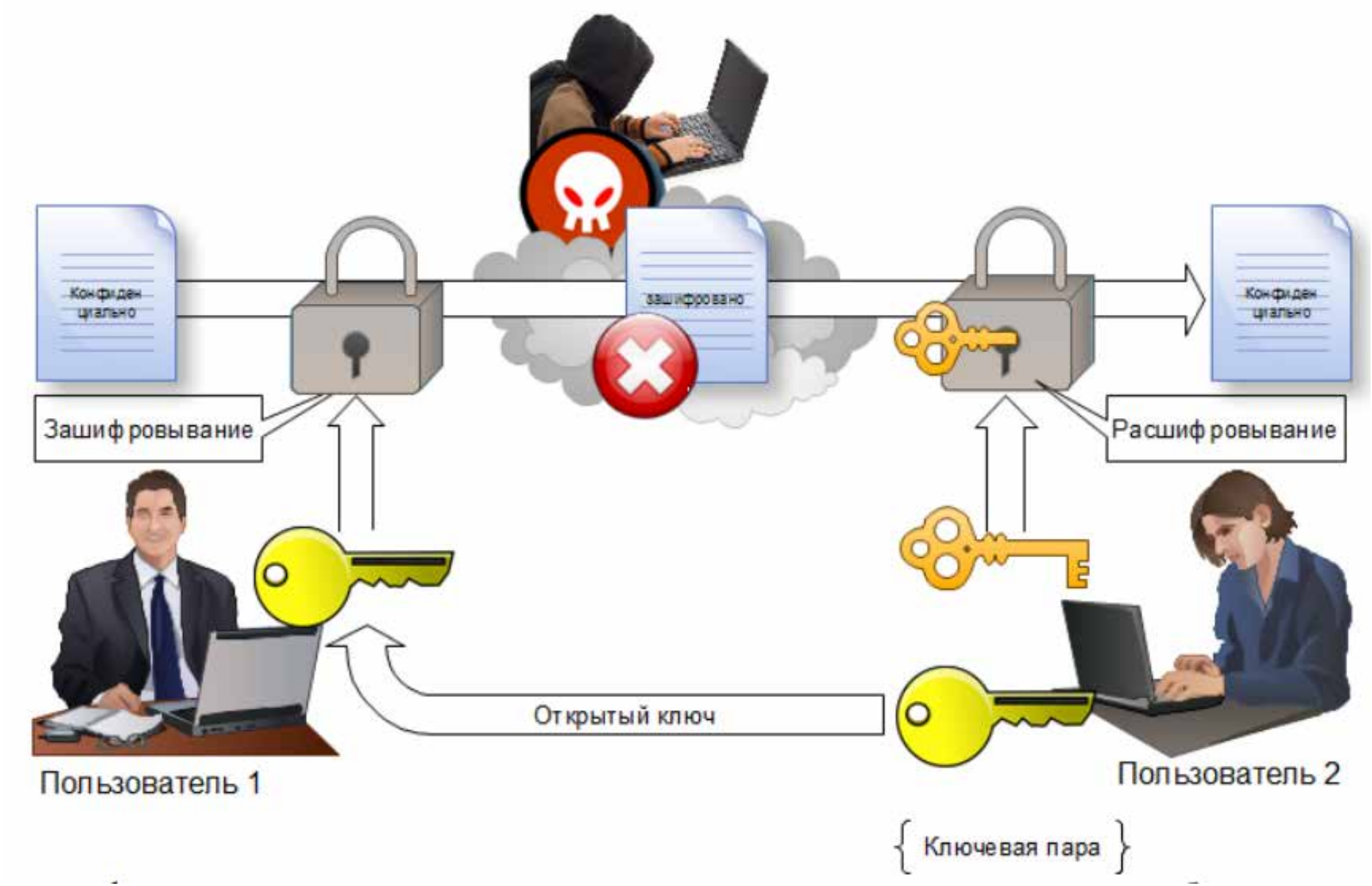
- **Достоинства**
  - скорость
  - простота реализации (за счёт более простых операций)
  - меньшая требуемая длина ключа для сопоставимой стойкости
  - изученность (за счёт большего возраста)
- **Недостатки**
  - сложность управления ключами в большой сети
  - сложность обмена ключами. Для применения необходимо решить проблему надёжной передачи ключей каждому абоненту, так как нужен секретный канал для передачи каждого ключа обеим сторонам

- Для компенсации недостатков симметричного шифрования в настоящее время широко применяется комбинированная (гибридная) криптографическая схема, где с помощью асимметричного шифрования передаётся сеансовый ключ, используемый сторонами для обмена данными с помощью симметричного шифрования.
- Важным недостатком симметричных шифров является **невозможность** их использования в механизмах формирования электронной цифровой подписи и сертификатов, так как ключ известен каждой стороне.



Криптография с асимметричными ключами

Схема шифрования с асимметричными ключами



Криптография с асимметричными ключами

https://ru.wikipedia.org/wiki/**Криптосистема_с_открытым_ключом**

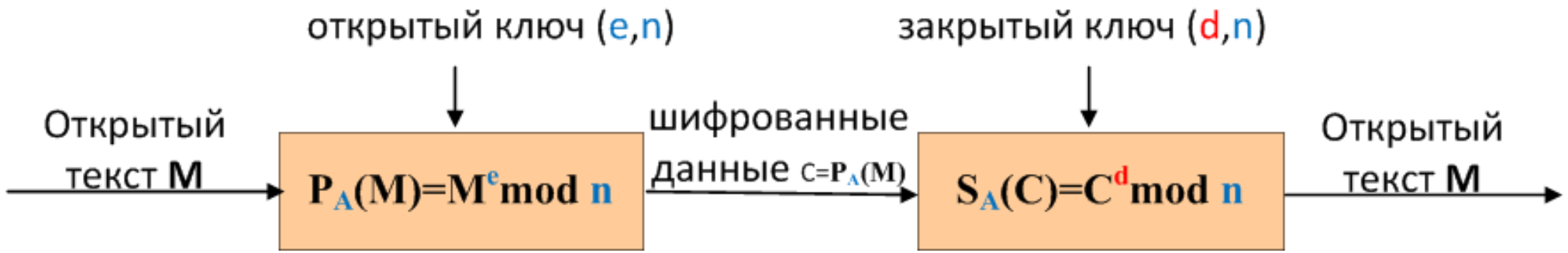
- **Виды асимметричных шифров**
  - RSA (Rivest-Shamir-Adleman)
  - DSA (Digital Signature Algorithm)
  - Elgamal (Шифросистема Эль-Гамаля)
  - Diffie-Hellman (Обмен ключами Диффи — Хелмана) - Алгоритм Диффи — Хеллмана
  - ECDSA (Elliptic Curve Digital Signature Algorithm) — алгоритм с открытым ключом для создания цифровой подписи.
  - ГОСТ Р 34.10-2012
  - Rabin
  - Luc
  - McEliece
  - Криптосистема Уильямса

Алгоритм RSA

http://ru.wikipedia.org/wiki/RSA

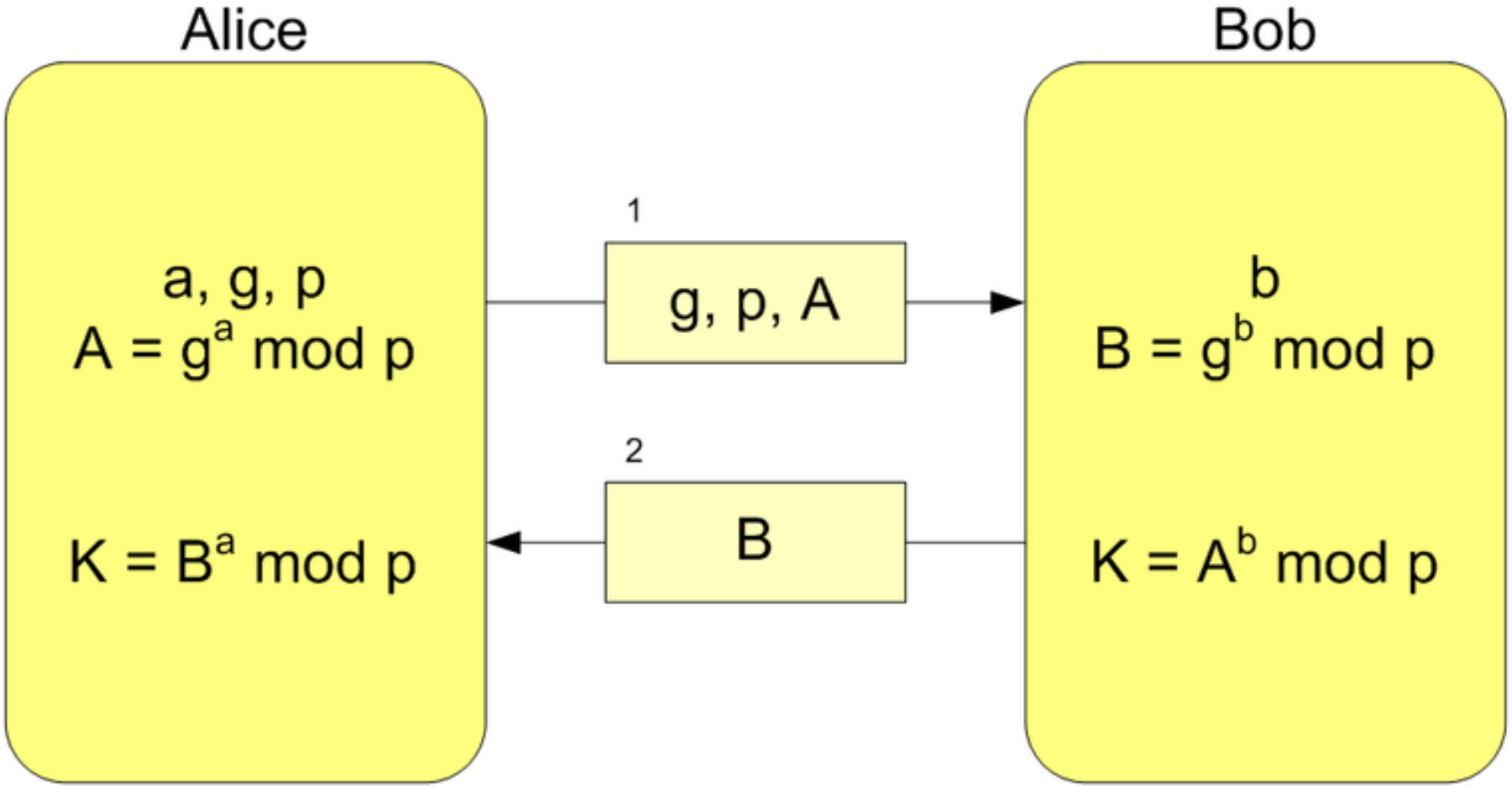
- Алгоритм генерации пары ассиметричных ключей RSA:

1. генерируются два различных случайных простых числа p и q заданного размера (например, 1024 бита каждое).
2. вычисляется их произведение $n=pq$, которое называется модулем.
3. вычисляется значение функции Эйлера от числа n: $\varphi(n)=(p-1)(q-1)$
4. p и q уничтожаются.
5. выбирается целое число (открытая экспонента) $e(1<e<\varphi(n))$, взаимно простое со значением функции $\varphi(n)$.
6. вычисляется число (закрытая экспонента) d,
7. число $\varphi(n)$ - уничтожается.
8. пара e, n публикуется в качестве открытого ключа RSA
9. пара d, n играет роль секретного ключа RSA



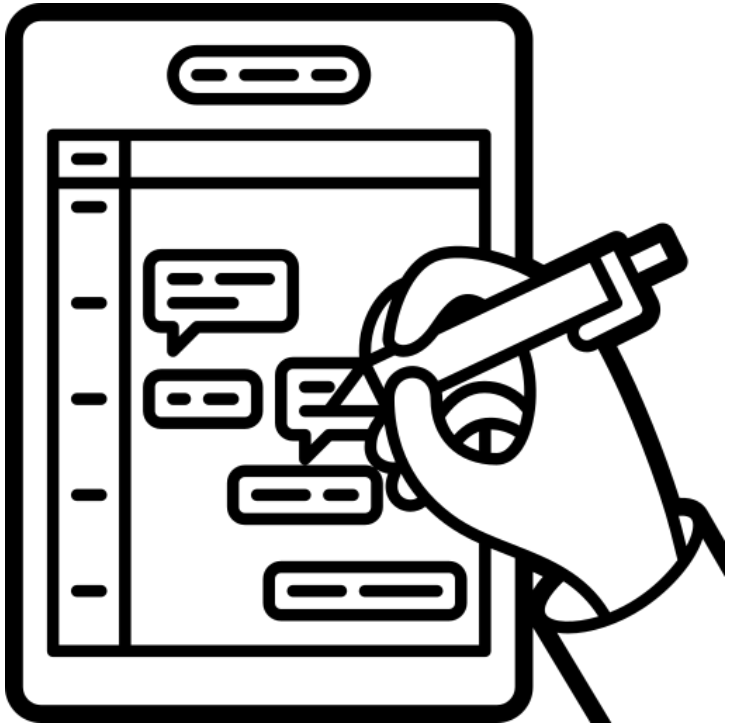
Алгоритм Диффи — Хеллмана

http://ru.wikipedia.org/wiki/Алгоритм_Диффи-Хеллмана



$$K = A^b \bmod p = (g^a \bmod p)^b \bmod p = g^{ab} \bmod p = (g^b \bmod p)^a \bmod p = B^a \bmod p$$

Получение симметричного ключа на алгоритме Диффи — Хеллмана

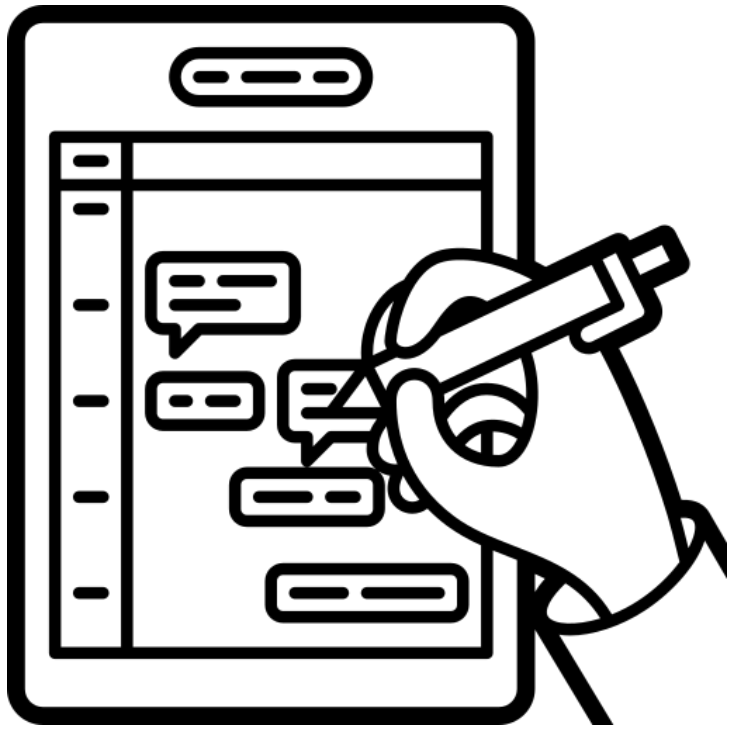


Средства криптографической защиты информации (СКЗИ)

Средства криптографической защиты информации (СКЗИ)

- **Средства криптографической защиты информации (СКЗИ)** – средства шифрования, средства имитозащиты, средства электронной подписи, средства кодирования, средства изготовления ключевых документов, ключевые документы, аппаратные шифровальные (криптографические) средства, программно-аппаратные шифровальные (криптографические) средства.

- **Средства криптографической защиты информации** – программные, программно-аппаратные средства защиты информации, реализующие один или несколько криптографических алгоритмов (шифрование, выработка и проверка электронной цифровой подписи, хэширование, имитозащита) и криптографические протоколы, а также функции управления криптографическими ключами, механизмы идентификации и аутентификации.



Средства криптографической защиты информации (СКЗИ)

с симметричными и асимметричными ключами

Область применения симметричного шифрования

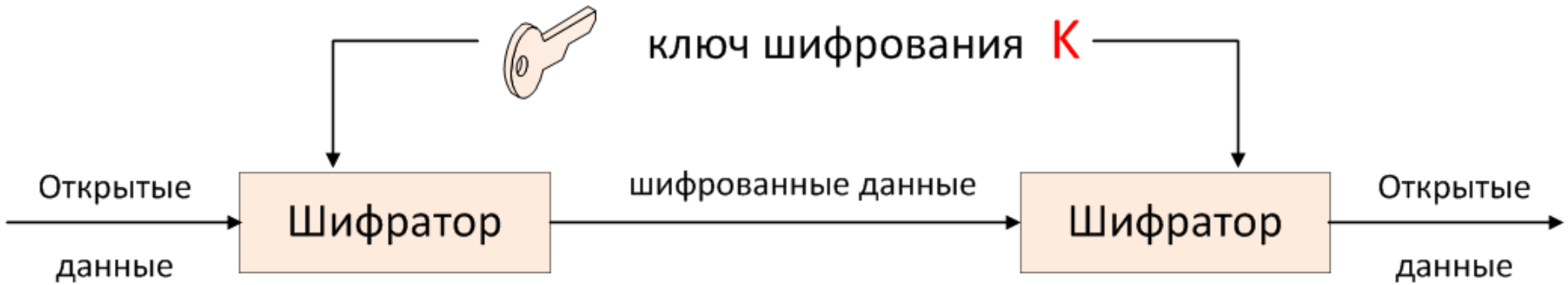
- **Симметричное шифрование используется для обмена данными во многих современных сервисах**, часто в сочетании с асимметричным шифрованием.
- **Например**, мессенджеры защищают с помощью таких шифров переписку (при этом ключ для симметричного шифрования обычно доставляется в асимметрично зашифрованном виде), а сервисы для видеосвязи — потоки аудио и видео.
- В защищенном транспортном протоколе TLS симметричное шифрование используется для обеспечения конфиденциальности передаваемых данных.

- **Симметричные алгоритмы не могут применяться для формирования цифровых подписей и сертификатов**, потому что секретный ключ при использовании этого метода должен быть известен всем, кто работает с шифром, что противоречит самой идее электронной подписи (возможности проверки ее подлинности без обращения к владельцу).

Симметричное распределение ключей

http://ru.wikipedia.org/wiki/Симметричные_криптосистемы

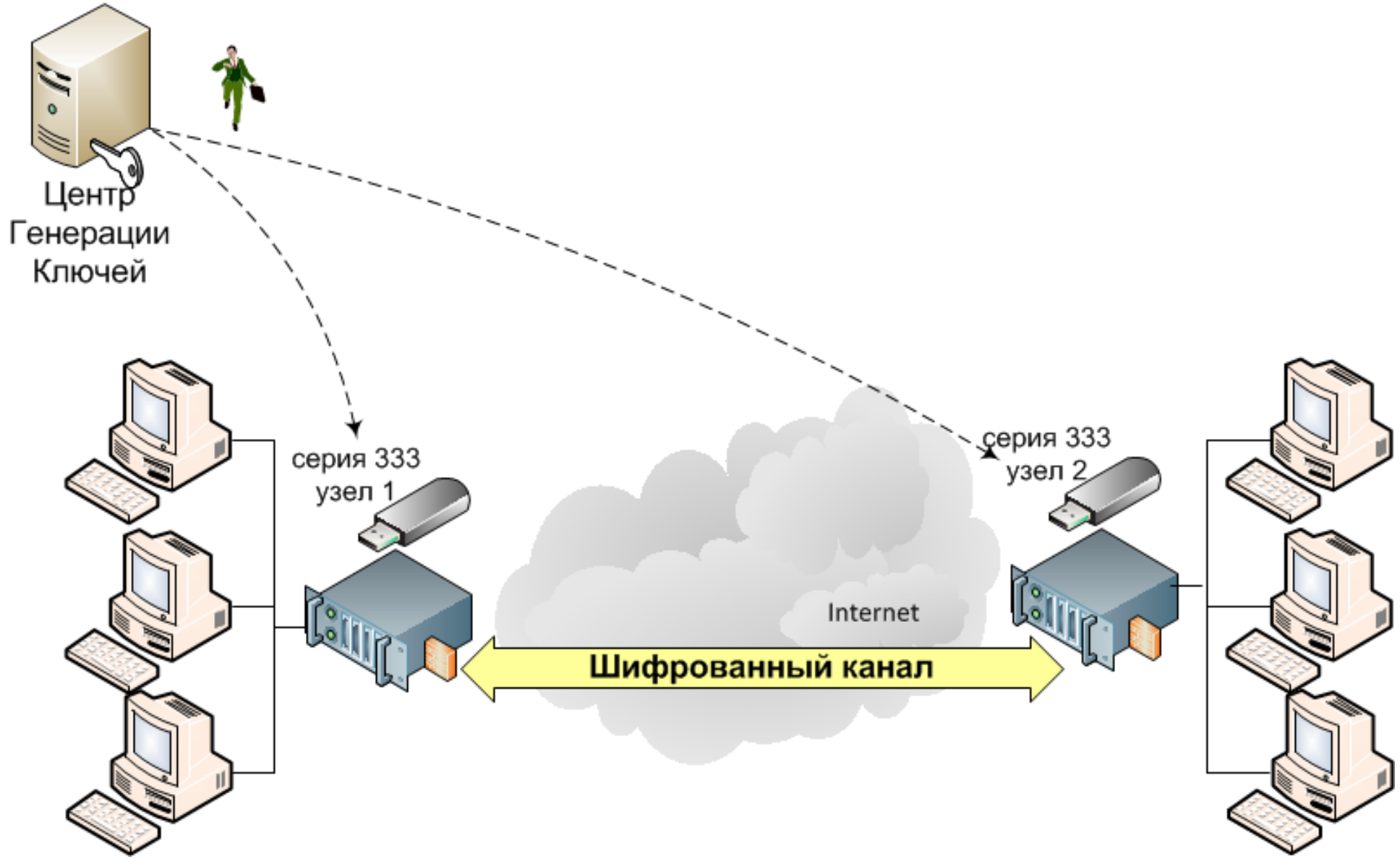
- **Достоинства**
  - высокая скорость шифрования
  - простота реализации
  - меньшая требуемая длина ключа для сопоставимой стойкости
  - изученность (давно используется)
- **Недостатки**
  - сложность управления ключами в большой сети. Для сети в 100 абонентов требуется 4950 ключей, для 1000 — 499500 и т. д.
  - сложность обмена ключами (защита каналов передачи).
- При симметричном шифровании используются одинаковые ключи (симметричные).



Симметричное шифрование

- K - ключ шифрования. Секретный элемент схемы. Должен быть известен паре непосредственно взаимодействующих шифраторов.

Применение симметричного шифрования



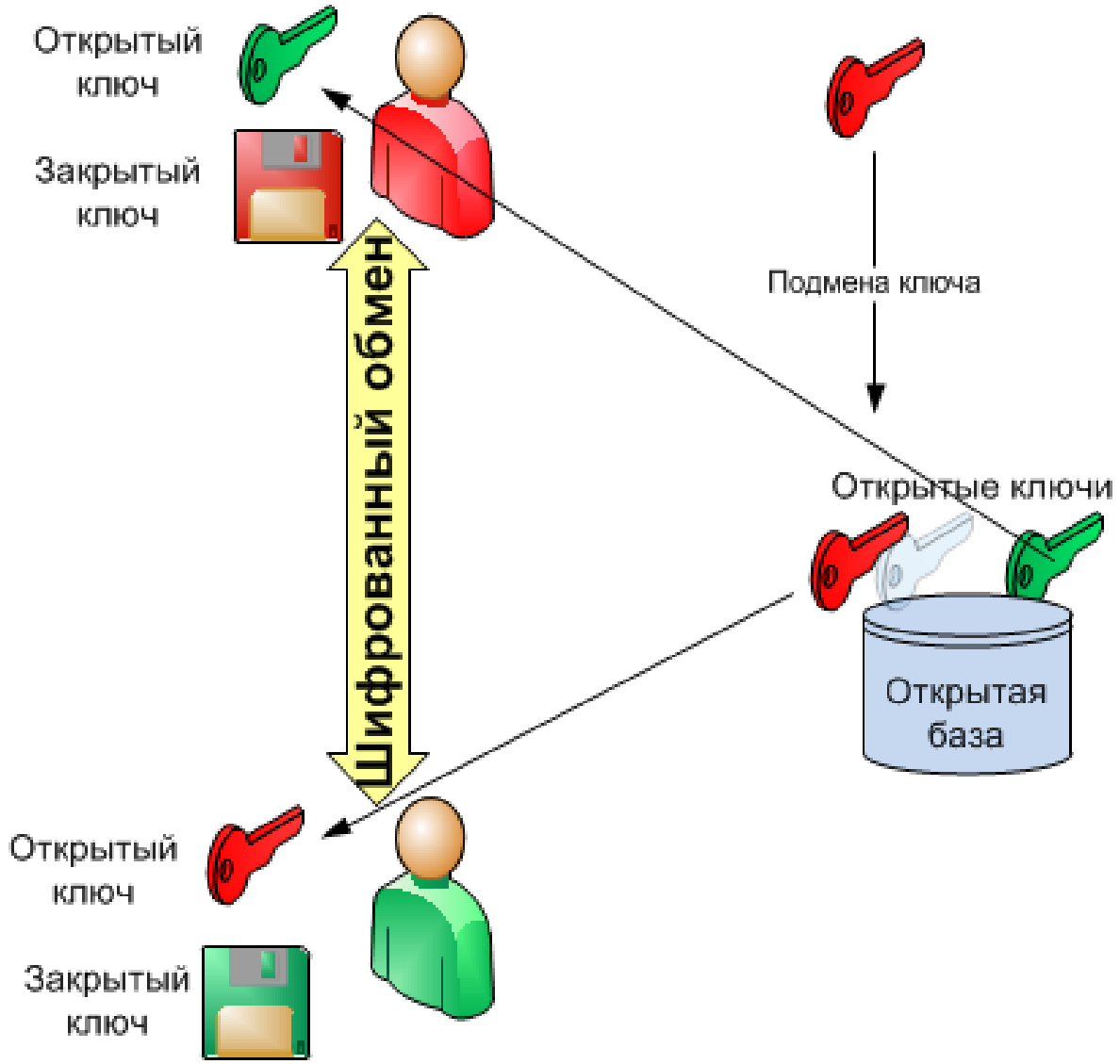
СКЗИ с асимметричными ключами

http://ru.wikipedia.org/wiki/**Криптосистема_с_открытым_ключом**

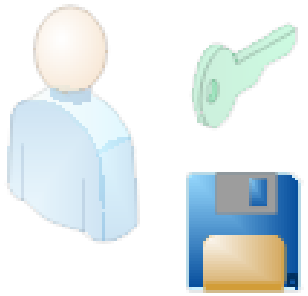
- **Криптографическая система с открытым ключом** (разновидность асимметричного шифрования, асимметричного шифра) — система шифрования и/или электронной подписи (ЭП), при которой открытый ключ передаётся по открытому (то есть незащищённому, доступному для наблюдения) каналу и используется для проверки ЭП и для шифрования сообщения. Для генерации ЭП и для расшифровки сообщения используется закрытый ключ. Криптографические системы с открытым ключом в настоящее время широко применяются в различных сетевых протоколах, в частности, в протоколах TLS и его предшественнике SSL (лежащих в основе HTTPS), в SSH. Также используется в PGP, S/MIME.
- **Преимущества**
  - не нужно передавать секретный ключ.
  - у секретного ключа только один пользователь.
  - число ключей значительно меньше и их количество легче увеличивать при увеличении крипто сети.
- **Недостатки**
  - более длинные ключи, чем симметричные.
  - процесс шифрования-расшифрования на два-три порядка медленнее.

Использование открытых и закрытых ключей

Подмена открытого ключа



Т.к. открытые ключи в базе или при передачи не защищены их можно подменить.
Для защиты открытых ключей используют один из методов контроля целостности данных - ЭЦП. **Вводится третья сторона** Удостоверяющий Центр (**Центр Сертификации**) (CA - Certificate Authority).



Центр сертификации

https://ru.wikipedia.org/wiki/**Центр_сертификации**
https://ru.abcdef.wiki/wiki/Certificate_authority

- **В криптографии центр сертификации или удостоверяющий центр** (англ. Certification authority, CA) — сторона (отдел, организация), чья честность неоспорима, а открытый ключ широко известен.
- **Задача центра сертификации** — подтверждать подлинность ключей шифрования с помощью сертификатов электронной подписи.
- Технически центр сертификации реализован как компонент глобальной службы каталогов и отвечает за управление криптографическими ключами пользователей.
- Открытые ключи и другая информация о пользователях хранится удостоверяющими центрами в виде **цифровых сертификатов**.
- **Формат этих сертификатов определяется стандартом X.509 или EMV** .
- Одним из наиболее частых случаев использования центров сертификации является подписание сертификатов, используемых в HTTPS , протоколе безопасного просмотра во всемирной паутине. Другое распространенное использование - это выдача удостоверений личности национальными правительствами для использования в документах с электронной подписью.

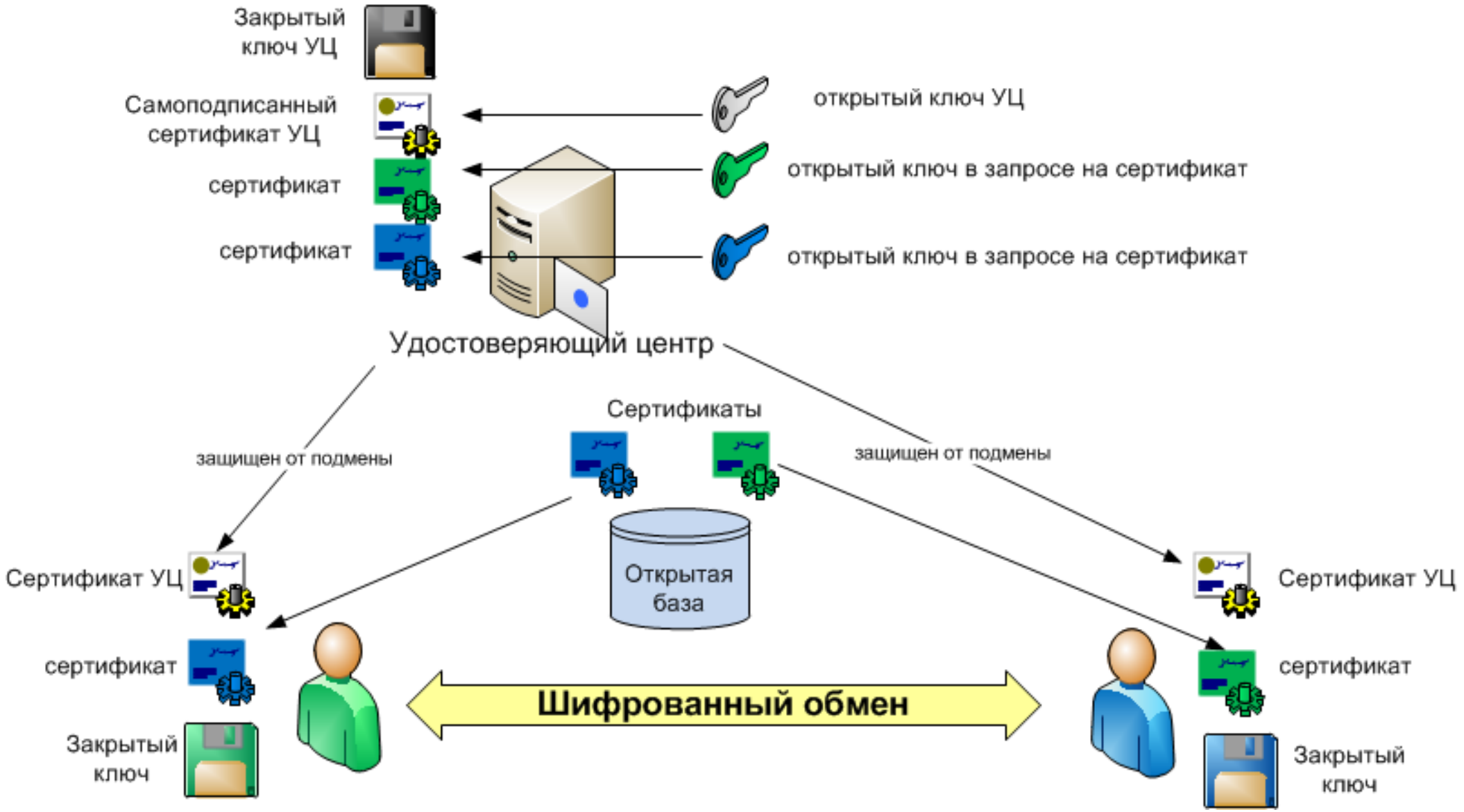
Содержимое сертификата открытого ключа

http://ru.wikipedia.org/wiki/X.509

- **X.509 — стандарт ITU-T для инфраструктуры открытого ключа** (Public key infrastructure, PKI) и инфраструктуры управления привилегиями (Privilege Management Infrastructure).
- **X.509 определяет стандартные форматы данных и процедуры распределения открытых ключей с помощью соответствующих сертификатов с цифровыми подписями**
- Эти сертификаты предоставляются удостоверяющими центрами (Certificate Authority). Кроме того, X.509 определяет формат списка аннулированных сертификатов, формат сертификатов атрибутов и алгоритм проверки подписи путём построения пути сертификации.
- X.509 предполагает наличие иерархической системы удостоверяющих центров для выдачи сертификатов.

Общий стандарт для интернета, использующий формат X.509

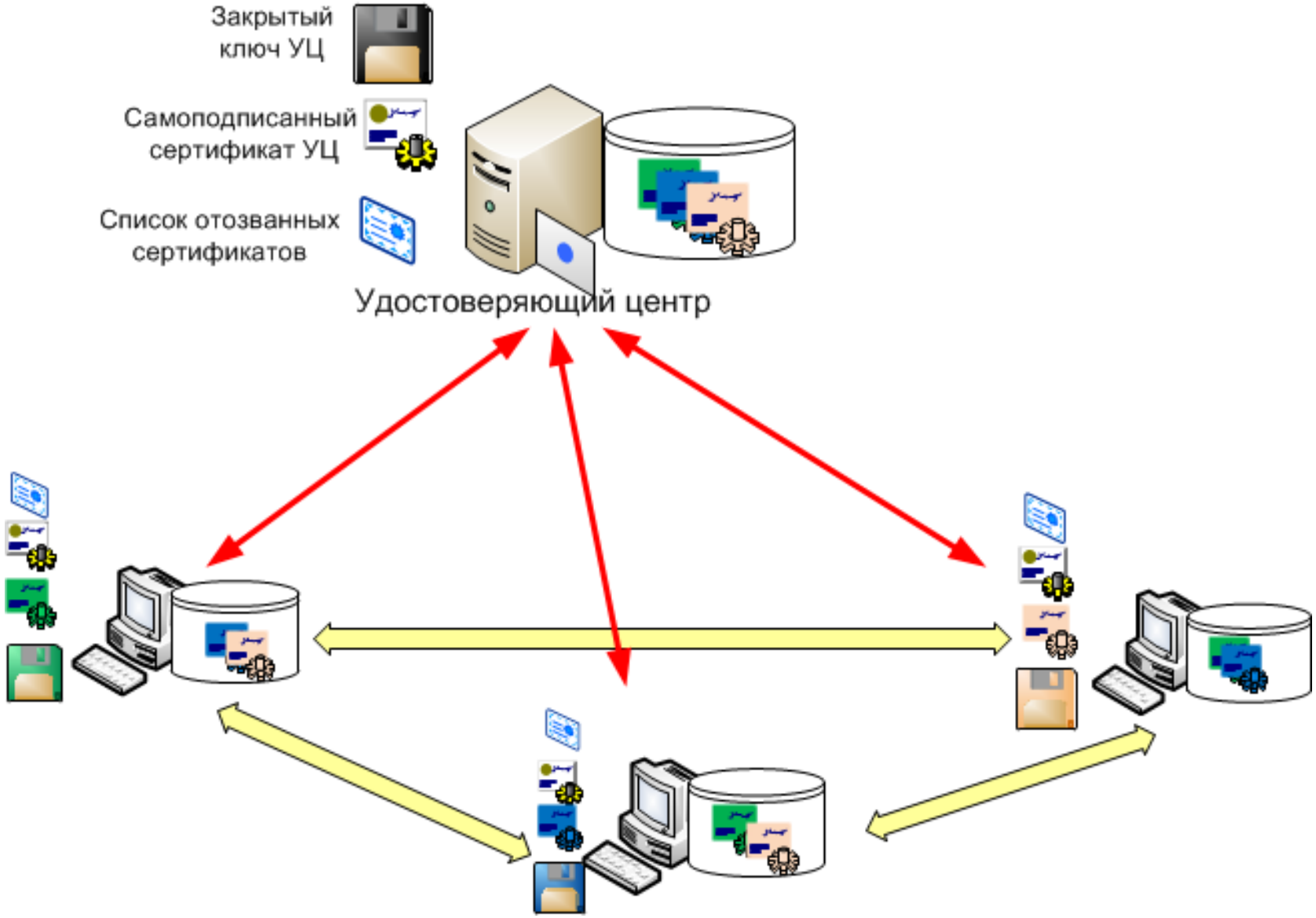
Использование сертификатов



Использование сертификатов

- Алгоритм взаимодействия:
  - УЦ генерит закрытый и открытый ключ
  - УЦ создает самоподписанный сертификат (свой открытый ключ, свои данные подписывает своим закрытым ключом)
  - пользователь генерит закрытый и открытый ключ
  - создает запрос на сертификат содержащий открытый ключ и сопроводительную информацию о владельце (ФИО, должность и т.д.)
  - посылает запрос в УЦ
  - УЦ создает сертификат из запроса и подписывает его ЭЦП
  - УЦ выкладывает сертификат пользователя в открытом доступе
  - пользователь получает (защищенным от подмены способом) самоподписанный сертификат УЦ
  - пользователь берет сертификаты других пользователей из открытой базы
  - начинается защищенный обмен между пользователями

Защищенный обмен между тремя пользователями

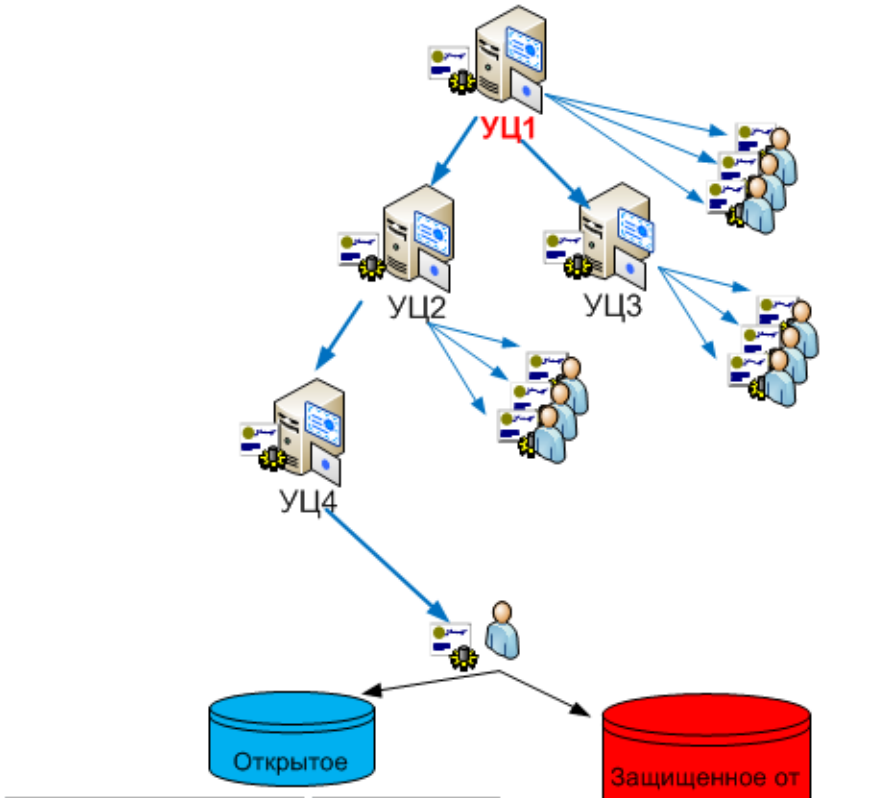


Пример цепочки доверия

Иерархическая структура – это наиболее часто встречающаяся архитектура инфраструктуры открытых ключей (ИОК).
Во главе всей структуры стоит один Корневой УЦ, которому все доверяют и ему подчиняются нижестоящие УЦ.

Пример иерархической структуры:
1. корневой УЦ страны
2. региональные УЦ
3. городские УЦ

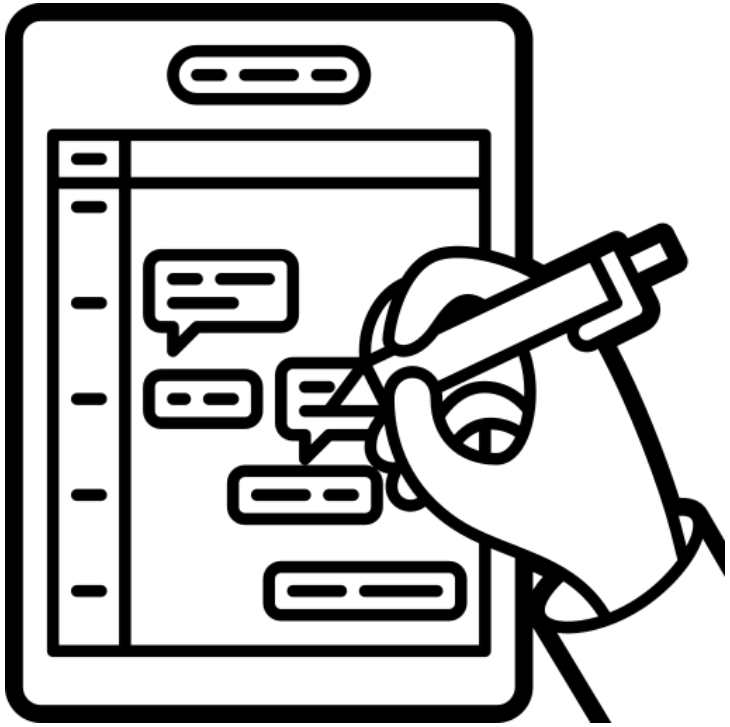
Для проверки сертификатов используется OCSP (Online Certificate Status Protocol) - протокол установления статуса сертификатов в online, используется вместо списков COC (CRL).



Сертификаты
УЦ1
Пользователь 1_A
Пользователь 1_B
Пользователь 1_C
УЦ2
Пользователь 2_A
Пользователь 2_B
Пользователь 2_C
УЦ3
Пользователь 3_A
Пользователь 3_B
Пользователь 3_C
УЦ4

COC
COC УЦ 1
COC УЦ 2
COC УЦ 3
COC УЦ 4

Доверенные УЦ
УЦ1



Электронная подпись

(ЦП – цифровая подпись)
(ЭЦП – электронная цифровая подпись)

Электронная подпись

https://ru.wikipedia.org/wiki/**Электронная_подпись**

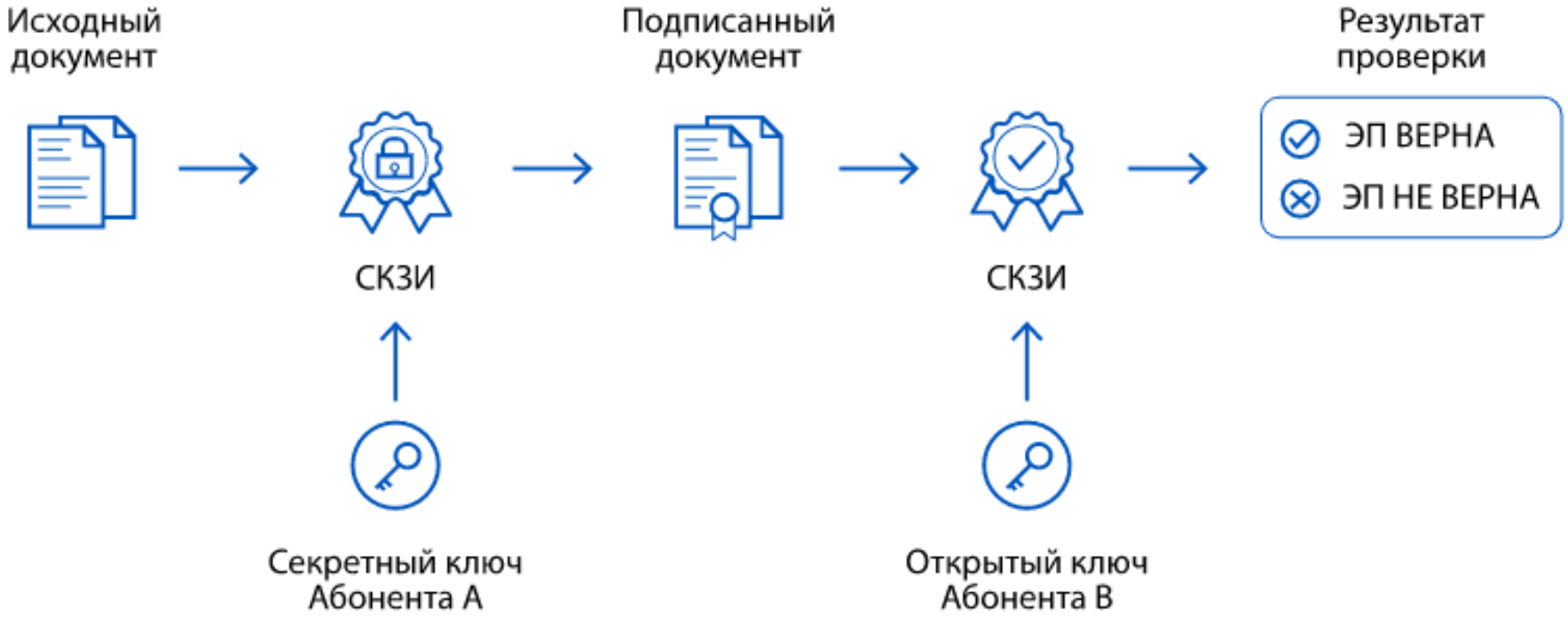
- **Электронная подпись (ЭП),** Электронная цифровая подпись (ЭЦП), Цифровая подпись (ЦП) позволяет подтвердить авторство электронного документа (будь то реальное лицо или, например, аккаунт в криптовалютной системе). Подпись связана как с автором, так и с самим документом с помощью криптографических методов, и не может быть подделана с помощью обычного копирования.
- **ЭЦП** — это реквизит электронного документа, полученный в результате криптографического преобразования информации с использованием закрытого ключа подписи и позволяющий проверить отсутствие искажения информации в электронном документе с момента формирования подписи (целостность), принадлежность подписи владельцу сертификата ключа подписи (авторство), а в случае успешной проверки подтвердить факт подписания электронного документа (неотказуемость).

Средство криптографической защиты информации

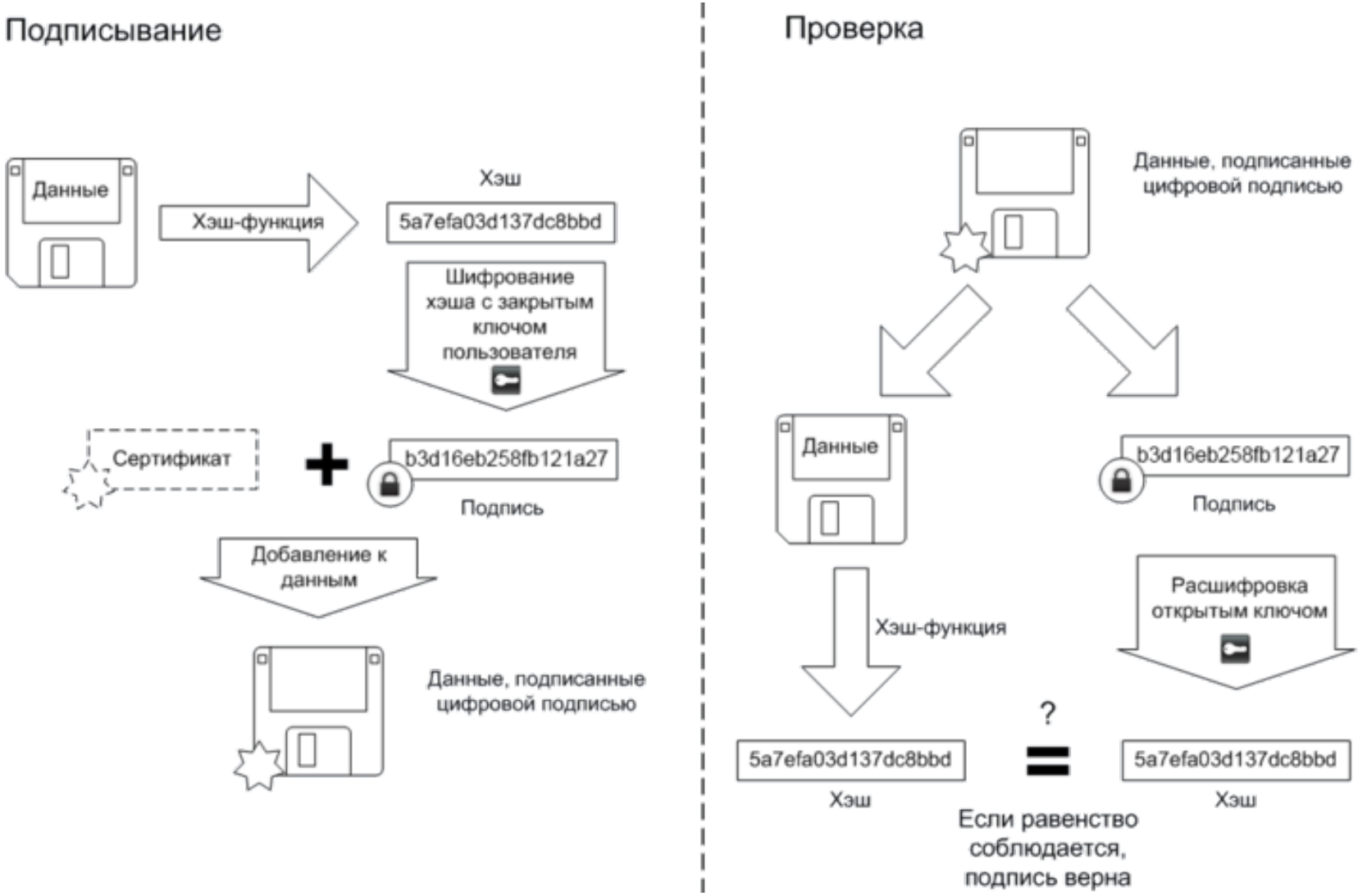
- **СКЗИ (средство криптографической защиты информации)** — это программа или устройство, которое шифрует документы и генерирует электронную подпись (ЭП).
- Все операции производятся с помощью ключа электронной подписи, который невозможно подобрать вручную, так как он представляет собой сложный набор символов. Тем самым обеспечивается надежная защита информации.

Принцип работы СКЗИ с ЭП

1. Отправитель создает документ
2. При помощи СКЗИ и закрытого ключа электронной подписи (ЭП) добавляет файл подписи, зашифровывает документ и объединяет все в файл, который отправляется получателю
3. Файл передается получателю
4. Получатель расшифровывает документ, используя СКЗИ и закрытый ключ своей электронной подписи
5. Получатель проверяет целостность ЭП, убеждаясь, что в документ не вносились изменения



Схема, поясняющая алгоритмы подписи и проверки

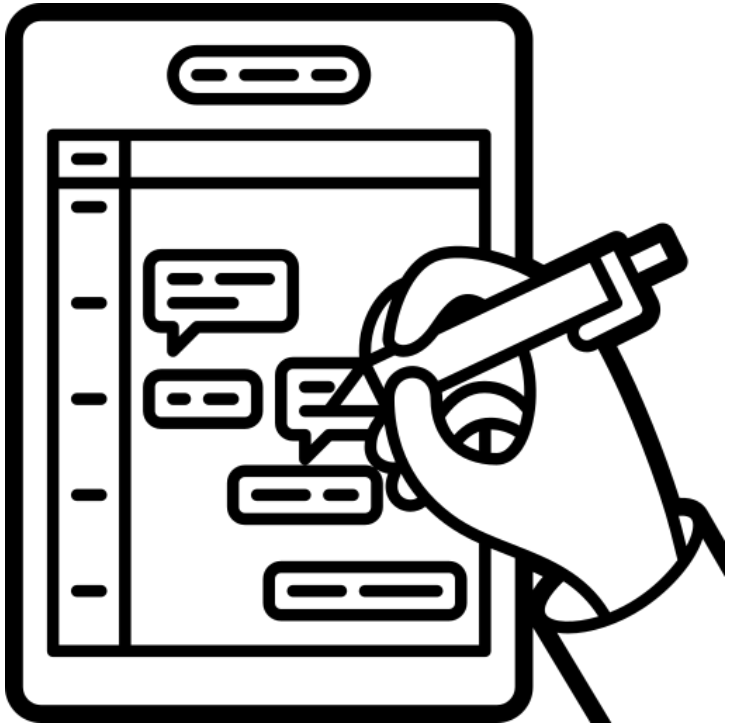


Перечень алгоритмов ЭП

- **Асимметричные схемы:**
  - FDH (Full Domain Hash), вероятностная схема RSA-PSS (Probabilistic Signature Scheme), схемы стандарта PKCS#1 и другие схемы, основанные на алгоритме RSA
  - Схема Эль-Гамаля
  - Американские стандарты электронной цифровой подписи: DSA, ECDSA (DSA на основе аппарата эллиптических кривых)
  - Российские стандарты электронной цифровой подписи: ГОСТ Р 34.10-94 (в настоящее время не действует), ГОСТ Р 34.10-2001 (не рекомендован к использованию после 31 декабря 2017 года), ГОСТ Р 34.10-2012 (основан на сложности вычисления дискретного логарифма в группе точек эллиптической кривой)
  - Евразийский союз: ГОСТ 34.310-2004 полностью идентичен российскому стандарту ГОСТ Р 34.10-2001
  - Украинский стандарт электронной цифровой подписи ДСТУ 4145-2002
  - Белорусский стандарт электронной цифровой подписи СТБ 1176.2-99 (в настоящее время не действует), СТБ 34.101.45-2013
  - Схема Шнорра
  - Pointcheval-Stern signature algorithm
  - Вероятностная схема подписи Рабина
  - Схема BLS (Boneh-Lynn-Shacham)
  - Схема DLR (Donna-Lynn-Rivest)
  - Схема GMR (Goldwasser-Micali-Rivest)

Перечень алгоритмов ЭП

- На основе асимметричных схем созданы модификации цифровой подписи, отвечающие различным требованиям:
  - Групповая цифровая подпись
  - Неоспоримая цифровая подпись
  - «Слепая» цифровая подпись и справедливая «слепая» подпись
  - Конфиденциальная цифровая подпись
  - Цифровая подпись с доказуемостью подделки
  - Доверенная цифровая подпись
  - Разовая цифровая подпись



Криптография на практике

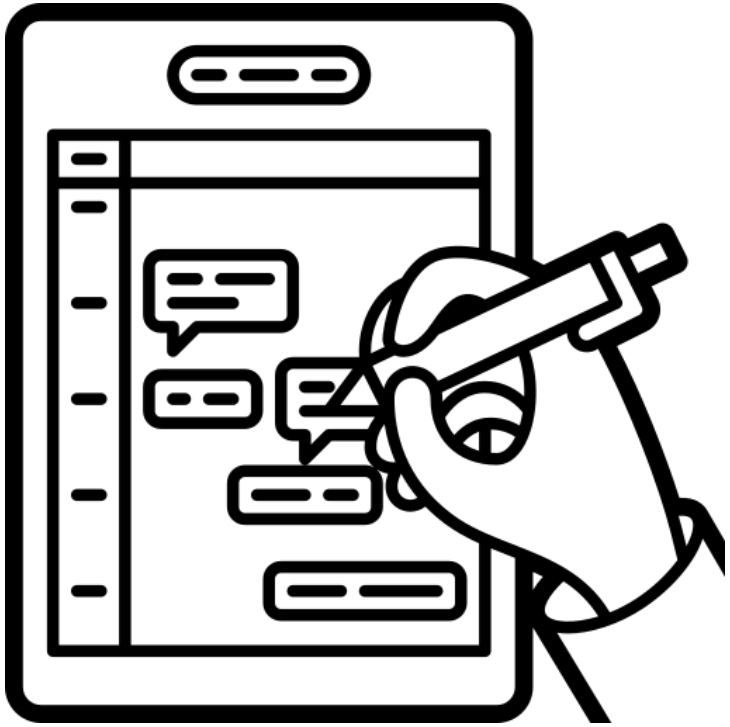
VeraCrypt

- **VeraCrypt** - Программа для шифрования данных на лету, используемая для систем и разделов. За ней периодически встречаются грешки, но постоянные патчи их оперативно исправляют. Её нельзя использовать как есть – необходимо уделить особое внимание настройкам и в параметрах обязательно установить время размонтировки. Также важно очищать кэш паролей при выходе, так как те остаются и, при большом желании, могут быть вытащены посредством танцев с бубном.

- **Аналогом VeraCrypt является устаревший TrueCrypt, обладающий абсолютно аналогичным функционалом, он ныне не имеющий поддержки.**

ZuluCrypt

- Еще одним хорошим инструментов шифрования является **ZuluCrypt** – простое консольное приложение созданное для управления зашифрованными виртуальными и физическими дисками, а также томами, размещенными в файлах изображений, lvm и mdraid.



Шифрование файлов в Windows

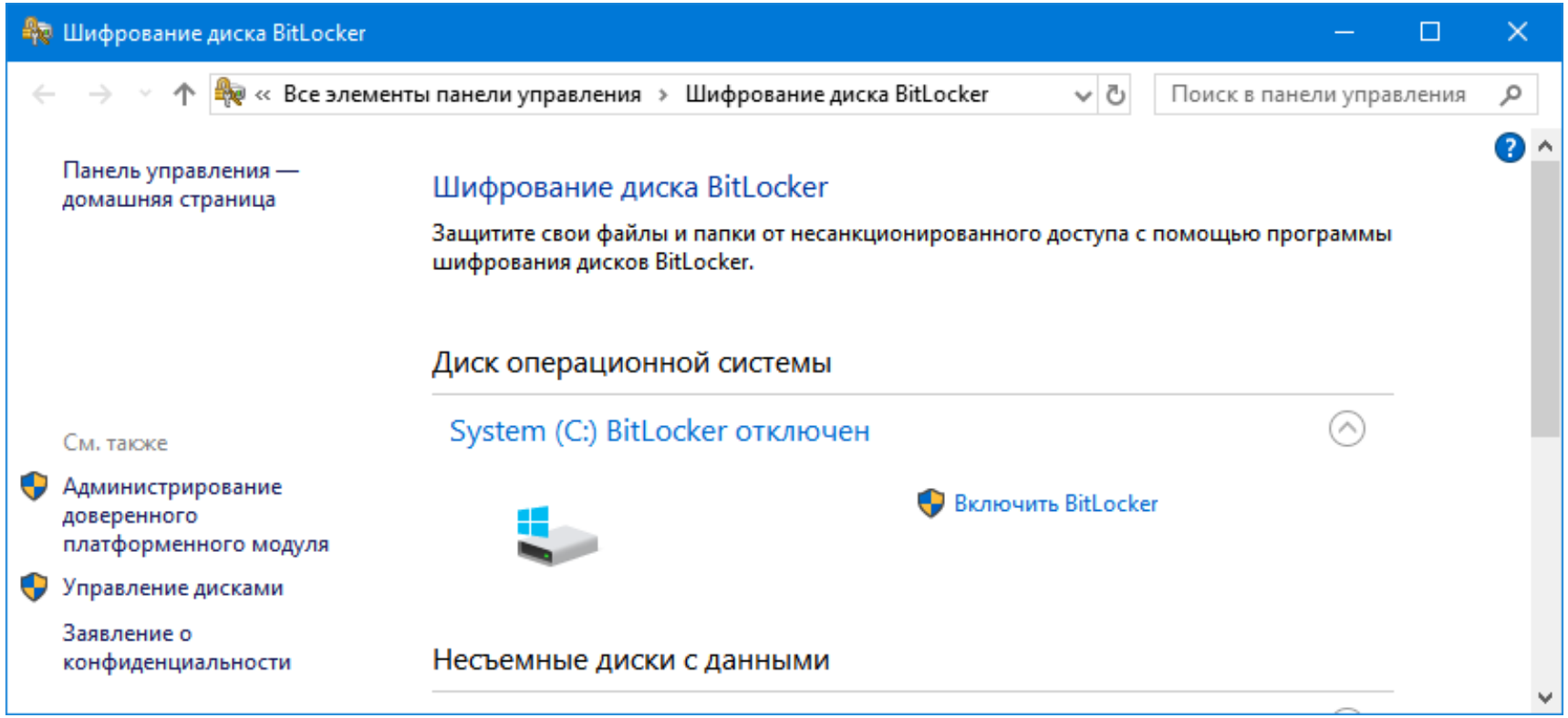
Шифрование файлов в Windows

- **Для шифрования файлов в Windows можно использовать:**
  - **Стандартные возможности Windows**
    - **BitLocker** (BitLocker Drive Encryption) — это технология шифрования содержимого дисков компьютера, разработанная компанией Microsoft.
    - файловая система **Encrypting File System** (EFS)
  - **Специализированное программное обеспечение**, например:
    - **VeraCrypt**
    - BestCrypt
    - Cybersafe
    - и многие другие, полный перечень ПО, для шифрования файлов можно посмотреть тут: https://en.wikipedia.org/wiki/Comparison_of_disk_encryption_software

Пароли

Шифрование файлов в Windows - BitLocker

- **BitLocker (BitLocker Drive Encryption)** — это технология шифрования содержимого дисков компьютера, разработанная компанией Microsoft. Она впервые появилась в Windows Vista.
- С помощью BitLocker можно было шифровать тома жестких дисков, но позже, уже в Windows 7 появилась похожая технология BitLocker To Go, которая предназначена для шифрования съемных дисков и флешек.
- **BitLocker является стандартным компонентом Windows** Professional и серверных версий Windows, а значит в большинстве случаев корпоративного использования он уже доступен. В противном случае вам понадобится обновить лицензию Windows до Professional.



Как работает BitLocker

- Эта **технология основывается на полном шифровании тома, выполняемом с использованием алгоритма AES (Advanced Encryption Standard)**. Ключи шифрования должны храниться безопасно и для этого в BitLocker есть несколько механизмов.
- **Самый простой, но одновременно и самый небезопасный метод — это пароль.** Ключ получается из пароля каждый раз одинаковым образом, и соответственно, если кто-то узнает ваш пароль, то и ключ шифрования станет известен.
- Чтобы не хранить ключ в открытом виде, его можно шифровать либо в TPM (Trusted Platform Module), либо на криптографическом токене или смарт-карте, поддерживающей алгоритм RSA 2048.
- TPM — микросхема, предназначенная для реализации основных функций, связанных с обеспечением безопасности, главным образом с использованием ключей шифрования. Модуль TPM, как правило, установлен на материнской плате компьютера, однако, приобрести в России и Беларуси компьютер со встроенным модулем TPM весьма затруднительно, так как ввоз устройств без нотификации Спецслужб в нашу страну запрещен.
- Использование смарт-карты или токена для снятия блокировки диска является одним из самых безопасных способов, позволяющих контролировать, кто выполнил данный процесс и когда. Для снятия блокировки в таком случае требуется как сама смарт-карта, так и PIN-код к ней.

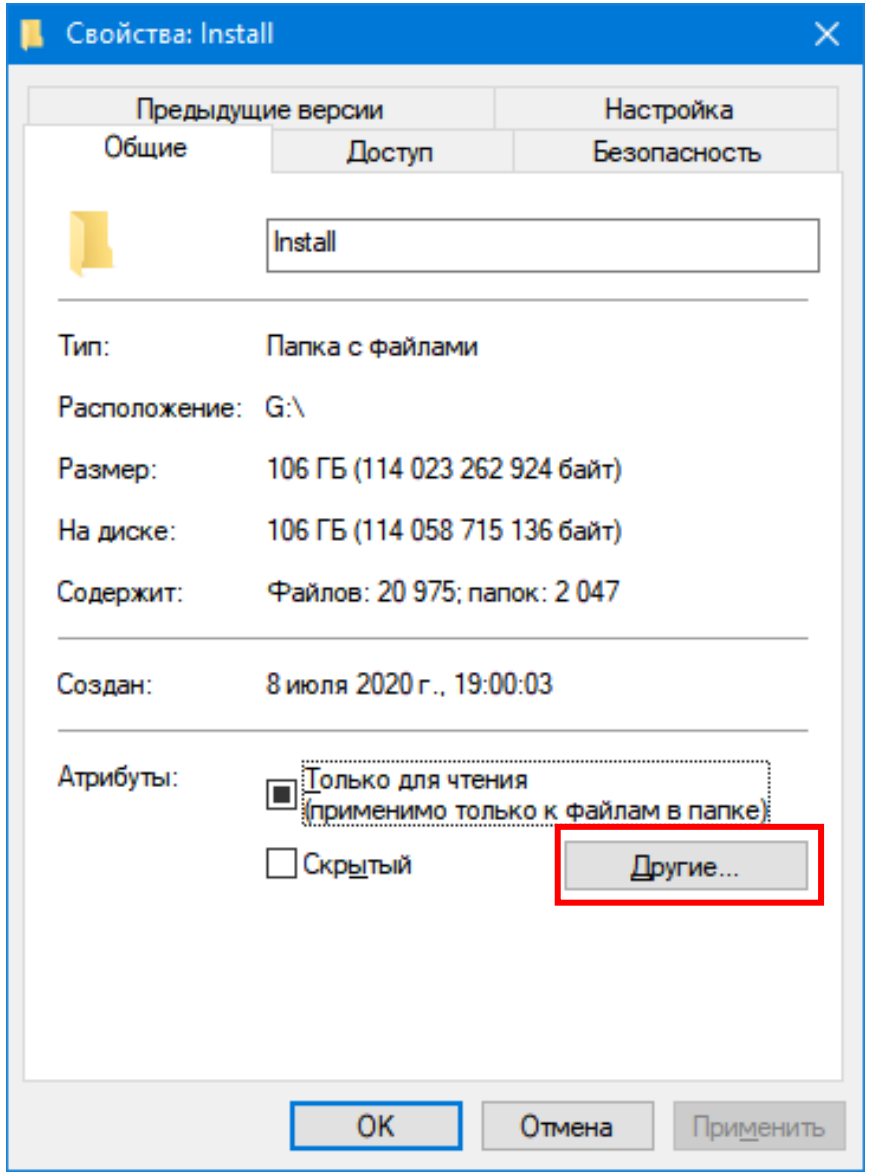
Encrypting File System

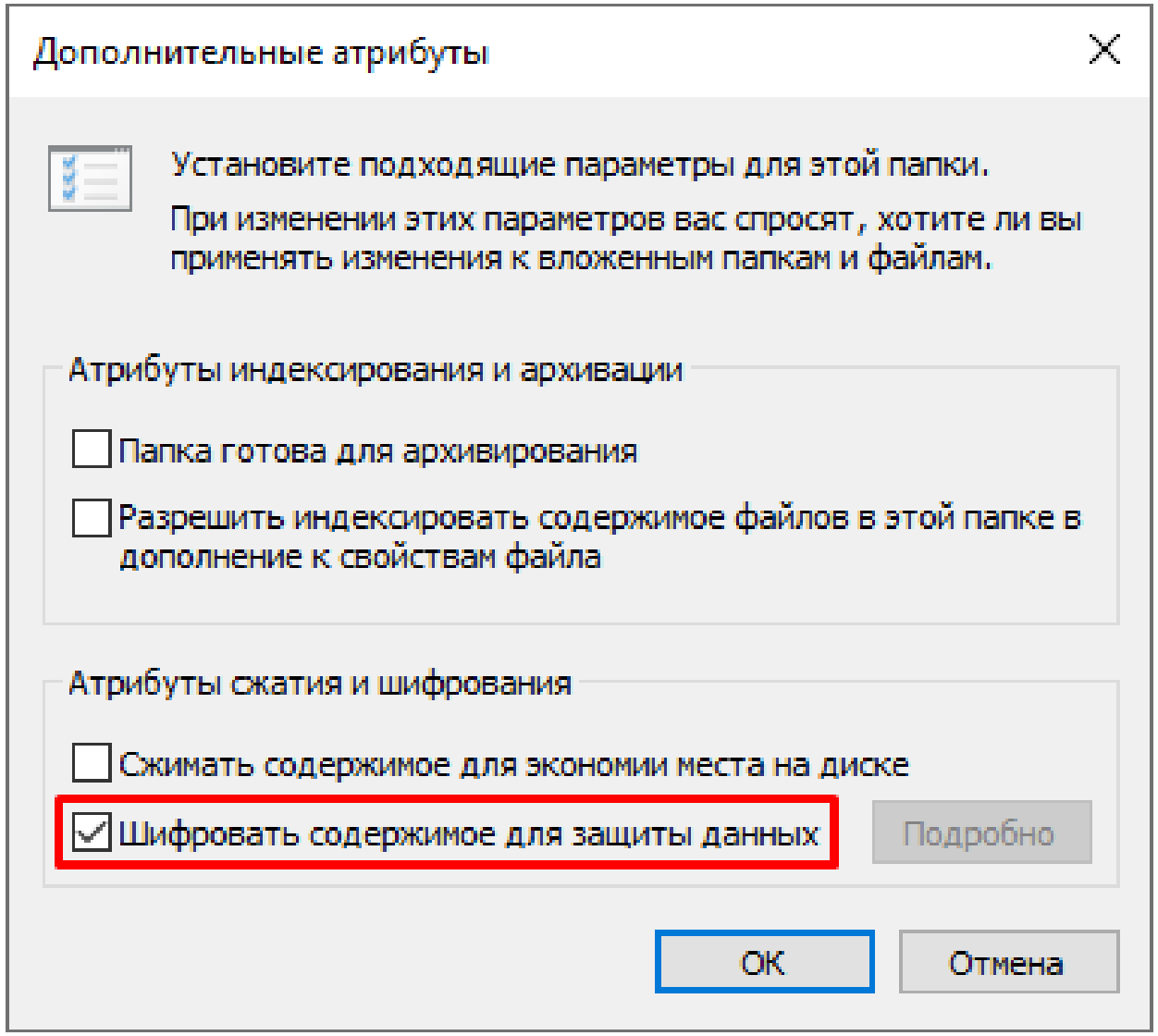
- **Encrypting File System (EFS) — система шифрования данных, реализующая шифрование на уровне файлов в операционных системах Microsoft Windows NT (начиная с Windows 2000 и выше),** за исключением «домашних» версий (Windows XP Home Edition, Windows Vista Basic, Windows Vista Home Premium, Windows 7 Starter (Home Basic и Premium), Windows 10 Pro, Enterprise, and Education editions, Windows Server 2016, Windows Server 2019.
- Данная система предоставляет возможность «прозрачного шифрования» данных, хранящихся на разделах с файловой системой NTFS, для защиты потенциально конфиденциальных данных от несанкционированного доступа при физическом доступе к компьютеру и дискам.
- Аутентификация пользователя и права доступа к ресурсам, имеющие место в NT, работают, когда операционная система загружена, но при физическом доступе к системе возможно загрузить другую ОС, чтобы обойти эти ограничения.
- **EFS использует симметричное шифрование для защиты файлов, а также шифрование**, основанное на паре открытый/закрытый ключ для защиты случайно сгенерированного ключа шифрования для каждого файла. По умолчанию закрытый ключ пользователя защищён с помощью шифрования пользовательским паролем, и защищённость данных зависит от стойкости пароля пользователя.

Encrypting File System

- EFS обладает **недостатками**, которые делают этот вариант неидеальным.
  - EFS работает только с дисками с форматированием NTFS
  - Если перенести зашифрованный EFS файл на диск с форматированием FAT32 или **exFAT**, он расшифровывается
  - Если перенести зашифрованный EFS файл через сеть или отправить по электронной почте, он расшифровывается
- **Процесс шифрования** файлов и папок при помощи EFS:
  - Запустите проводник и откройте место расположения нужного файла или папки.
  - Нажмите на них правой кнопкой мыши.
  - В контекстном меню нажмите на команду «Свойства».
  - На вкладке общие нажмите на кнопку «Другие».
  - Поставьте галочку «Шифровать содержимое для защиты данных»

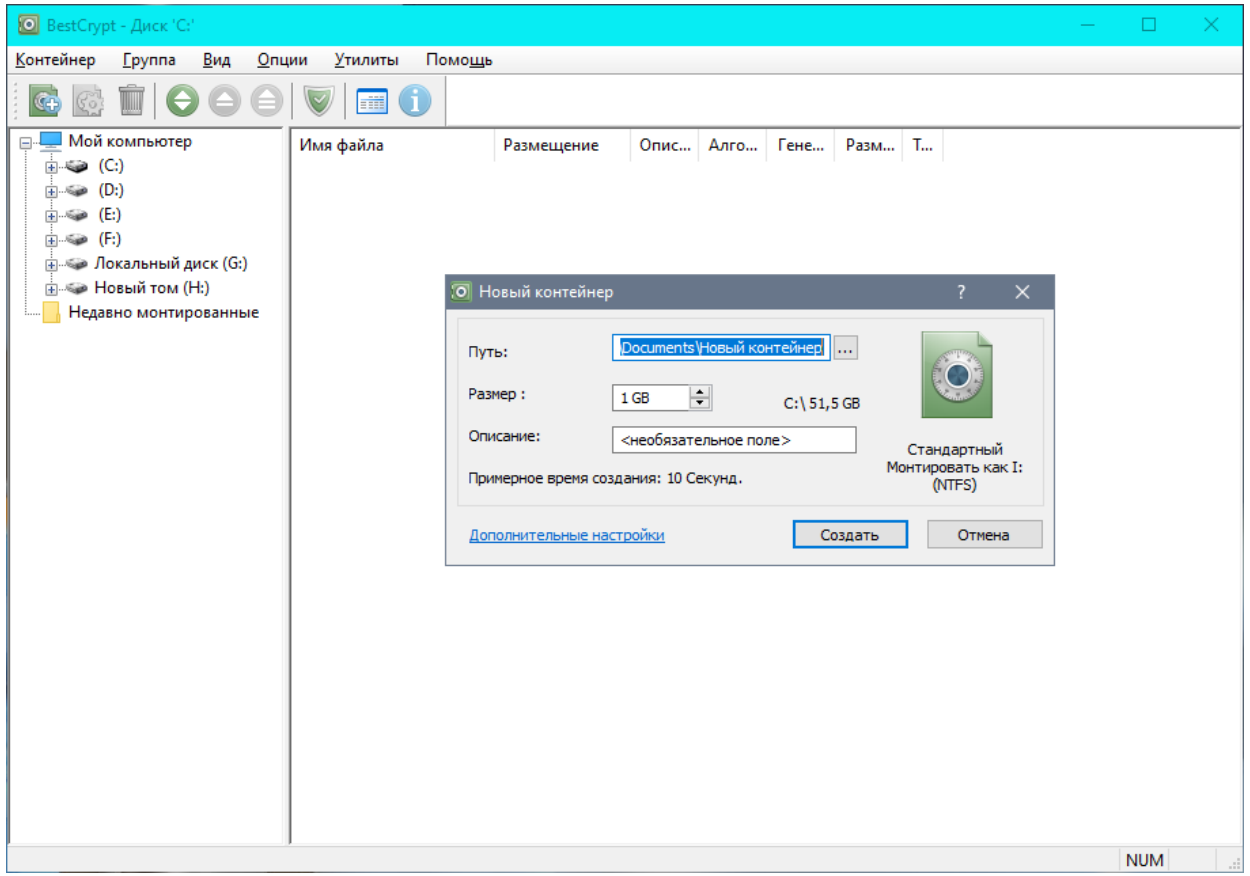
Encrypting File System





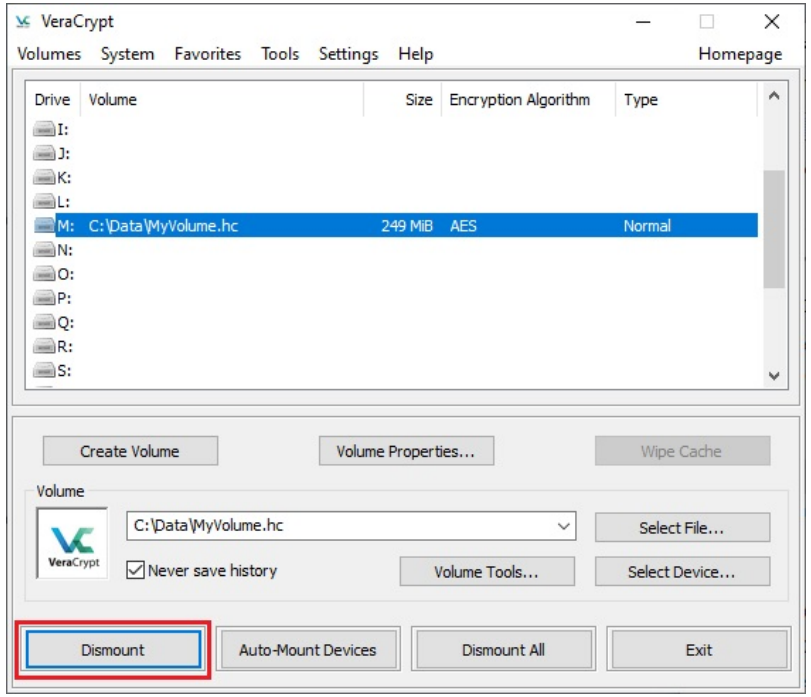
BestCrypt

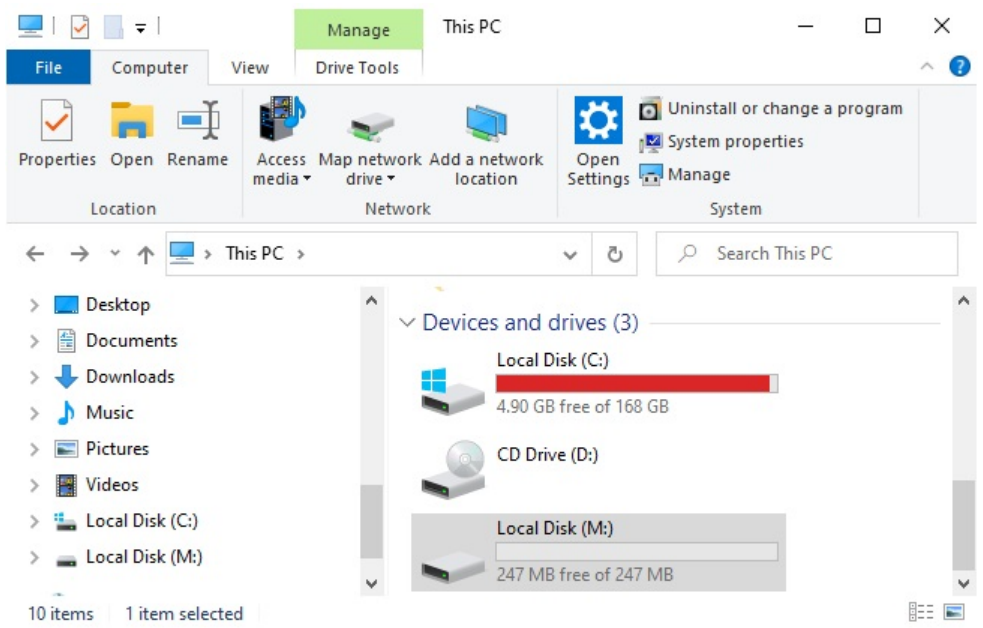
- **BestCrypt** — платный пакет проприетарных программ для создания на жёстком диске компьютера виртуального зашифрованного диска (контейнера) — одного или нескольких. Виртуальный диск работает, как обычный дисковый раздел.
- http://www.jetico.com/
- https://www.jetico.com/data-encryption/encrypt-files-bestcrypt-container-encryption



VeraCrypt - FREE

- **VeraCrypt – бесплатное ПО для шифрования файлов «на лету».**
- VeraCrypt может использовать следующие алгоритмы шифрования: AES, Serpent, Twofish, Camellia, Кузнечик, а также комбинации этих алгоритмов. Используемые криптографические хеш-функции: RIPEMD-160, SHA-256, SHA-512, Стрибог и Whirlpool.
- https://veracrypt.fr/code/VeraCrypt/
- https://veracrypt.fr/en/Downloads.html





Veracrypt download https://veracrypt.fr/en/Downloads.html

Home | Source Code | Downloads | Documentation | Donate | Forums

Note to publishers: If you intend to host our files on your server, please instead consider linking to this page. It will help us prevent spreading of obsolete versions, which we believe is critical when security software is concerned. Thank you.

Supported versions of operating systems

PGP Public Key: https://www.idrix.fr/VeraCrypt/VeraCrypt_PGP_public_key.asc (ID=0x680D16DE, Fingerprint=5069A233D55A0EEB174A5FC3821ACD02680D16DE)

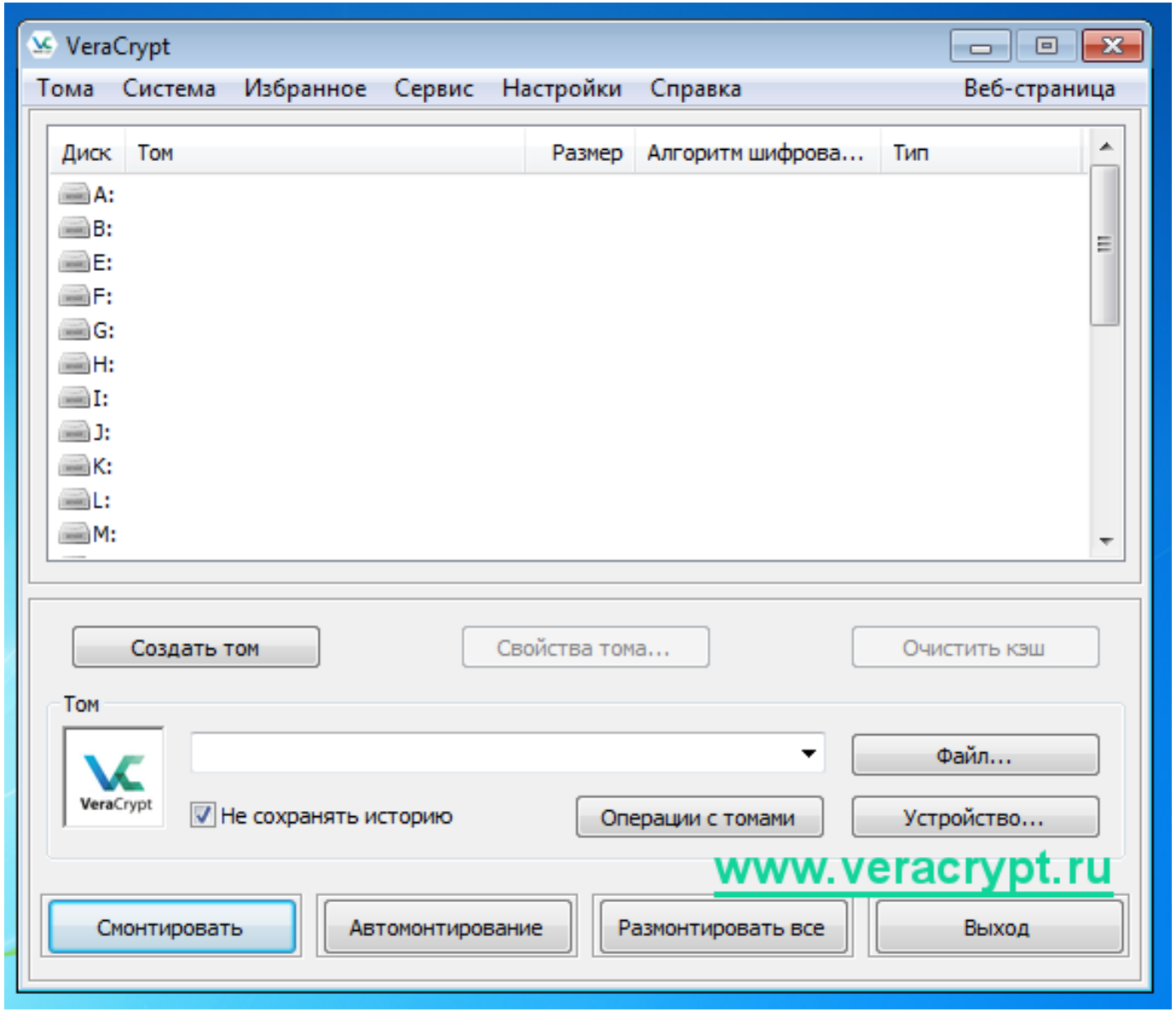
Latest Stable Release

For macOS 10.7 and later: 1.24-Update8 (Saturday November 28, 2020)
For the other operating systems: 1.24-Update7 (Friday August 7, 2020)

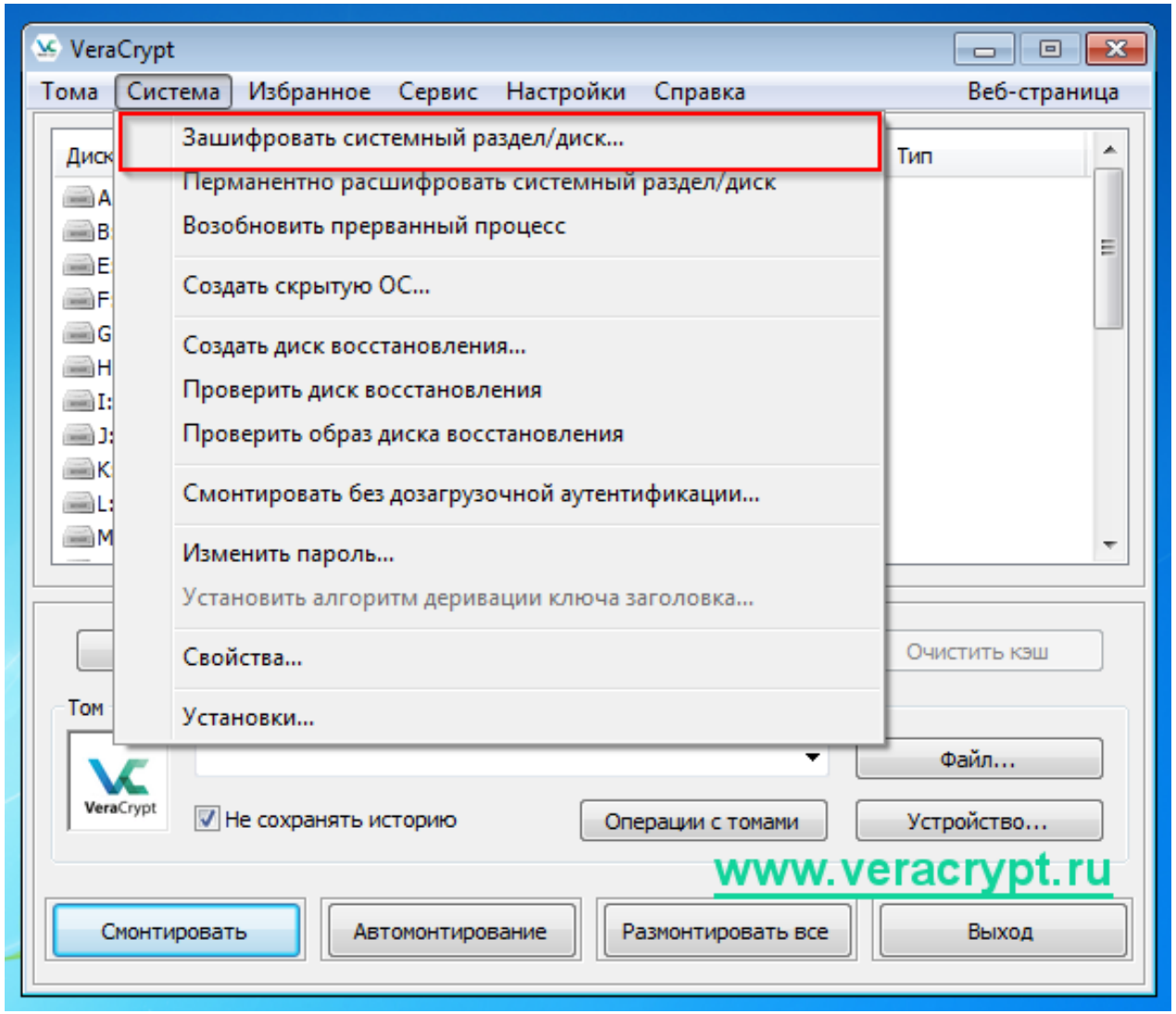
- ***Windows***:
  - Installer for Windows 8 and later: VeraCrypt Setup 1.24-Update7.exe (34.5 MB) (PGP Signature)
  - Portable version for Windows 8 and later: VeraCrypt Portable 1.24-Update7.exe (34.3 MB) (PGP Signature)
  - Installer for Windows XP, Vista and 7: VeraCrypt Legacy Setup 1.24-Update7.exe (34.5 MB) (PGP Signature)
  - Portable version for Windows XP, Vista and 7: VeraCrypt Legacy Portable 1.24-Update7.exe (34.3 MB) (PGP Signature)
  - Debugging Symbols: VeraCrypt_1.24-Update7_Windows_Symbols.zip (9.68 MB) (PGP Signature)
- ***macOS***:
  - macOS Mojave 10.14 and later: VeraCrypt_1.24-Update8.dmg (6.4 MB) (PGP Signature)
  - From macOS Lion 10.7 to macOS High Sierra 10.13: VeraCrypt_Legacy_1.24-Update8.dmg (9.9 MB) (PGP Signature)
  - **OSXFUSE** 3.10 or newer must be installed.
- ***Linux***:
  - Generic Installers: veracrypt-1.24-Update7-setup.tar.bz2 (14.3 MB) (PGP Signature)
  - Linux Legacy installer for 32-bit CPU with no SSE2: veracrypt-1.24-Update7-x86-legacy-setup.tar.bz2 (7.06 MB) (PGP Signature)
  - Debian/Ubuntu packages:
    - Debian 11:

Как зашифровать системный диск с Windows в VeraCrypt

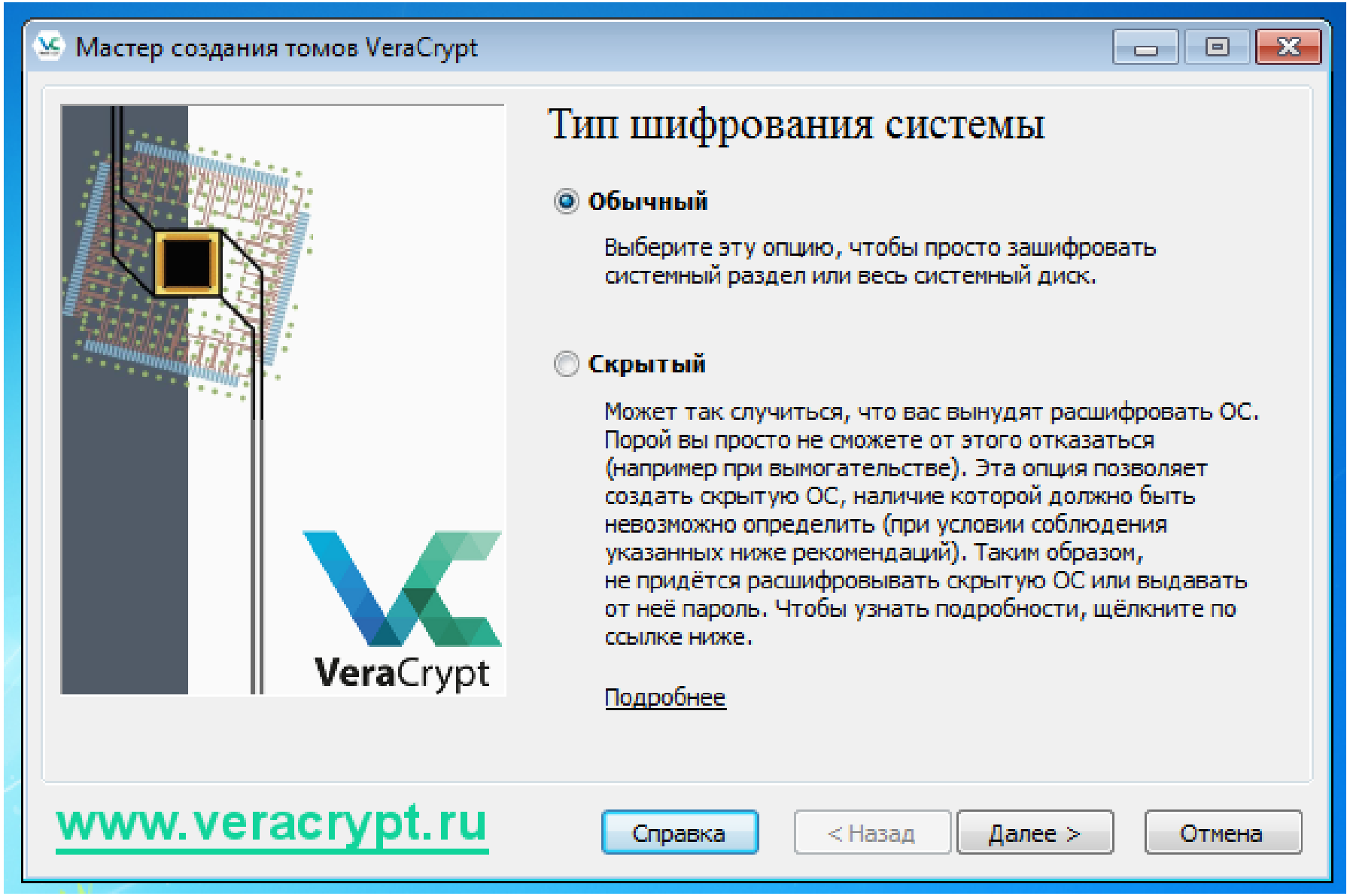
Главное окно программы VeraCrypt



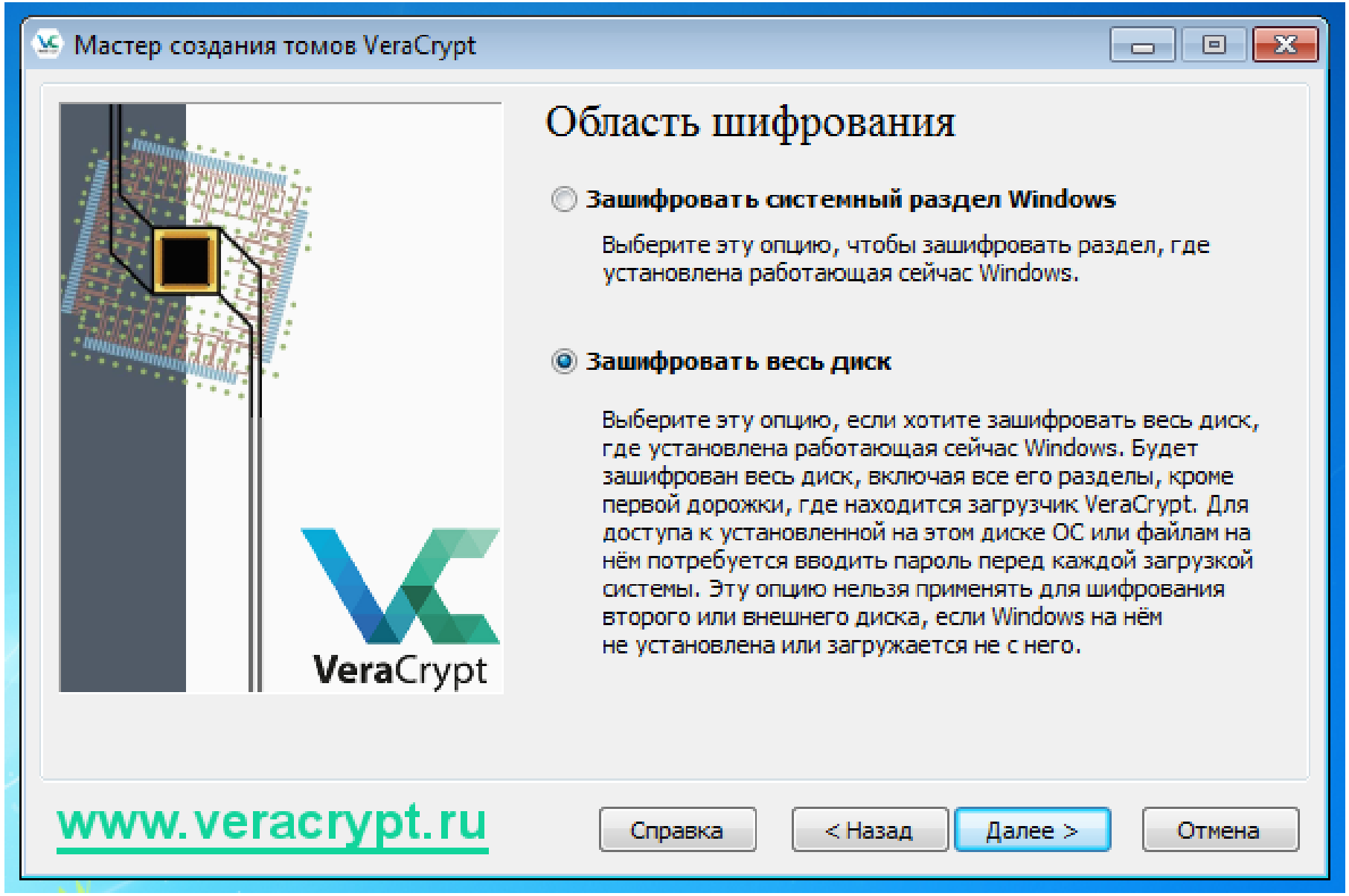
В меню «Система» выберите пункт «Зашифровать системный раздел/диск»



Укажите «Обычный» тип шифрования

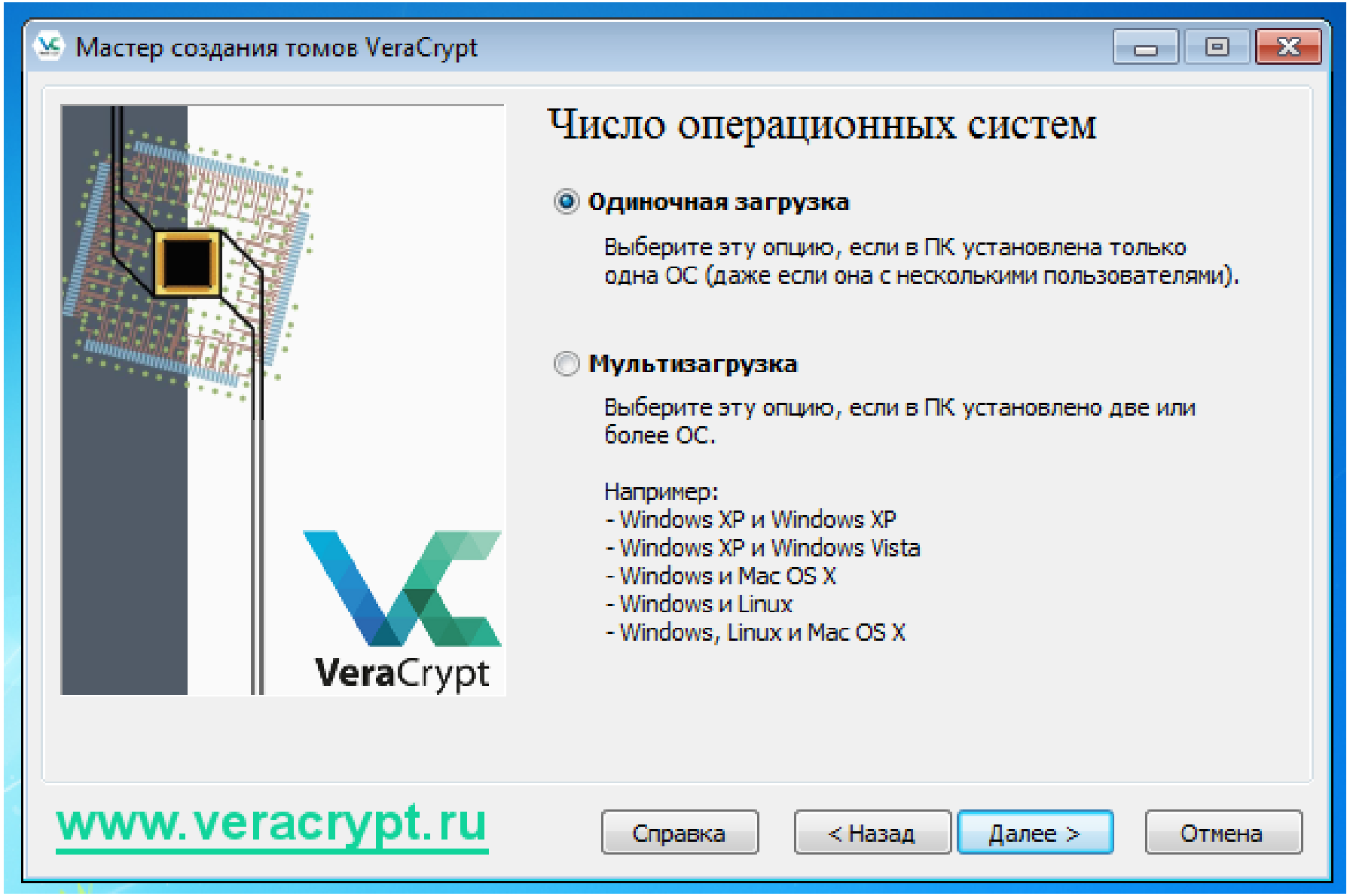


Укажите «Область шифрования»

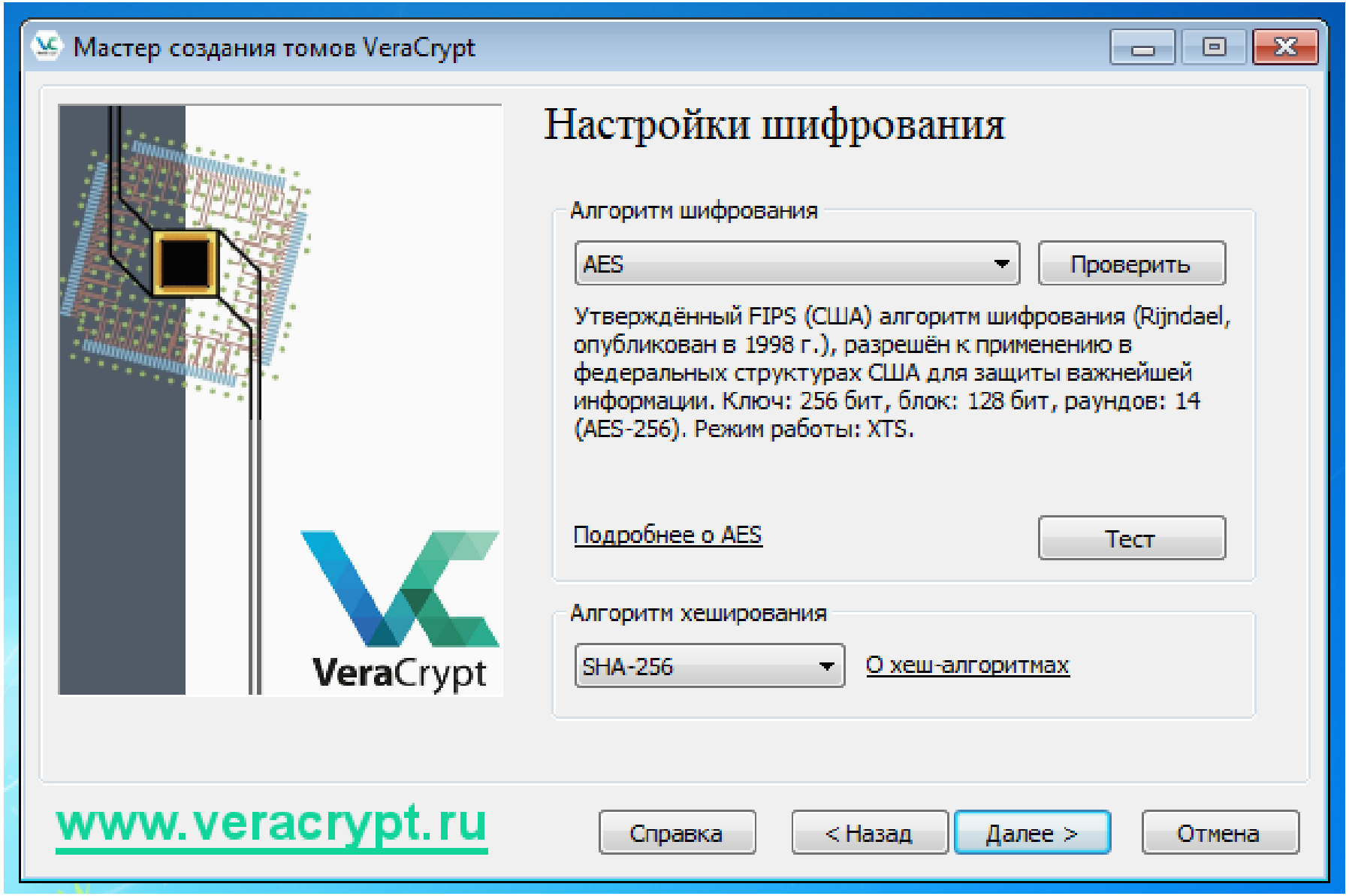


На вопрос о «Шифровании защищённой области» ответьте «Нет».

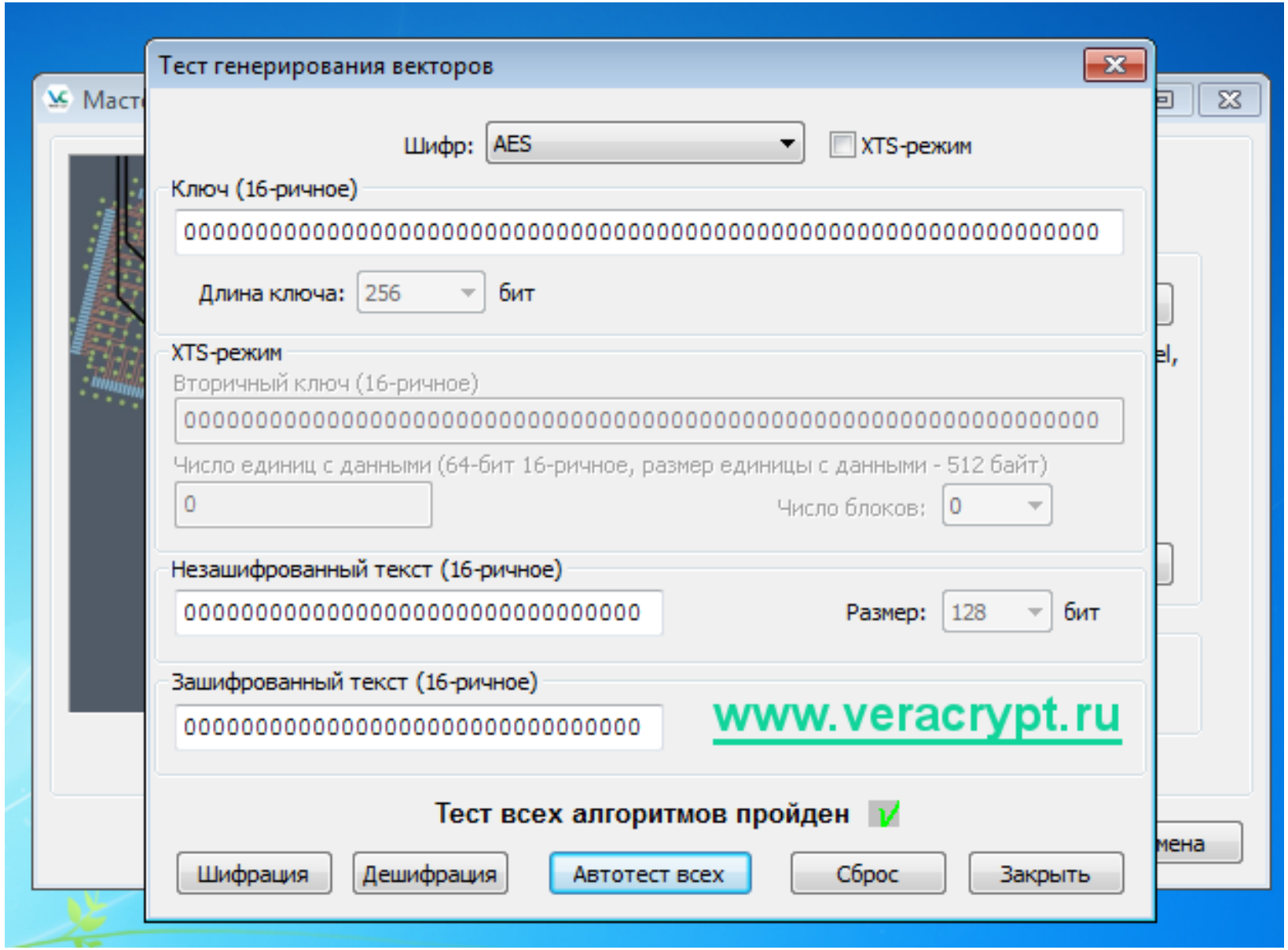
Укажите «Число операционных систем»



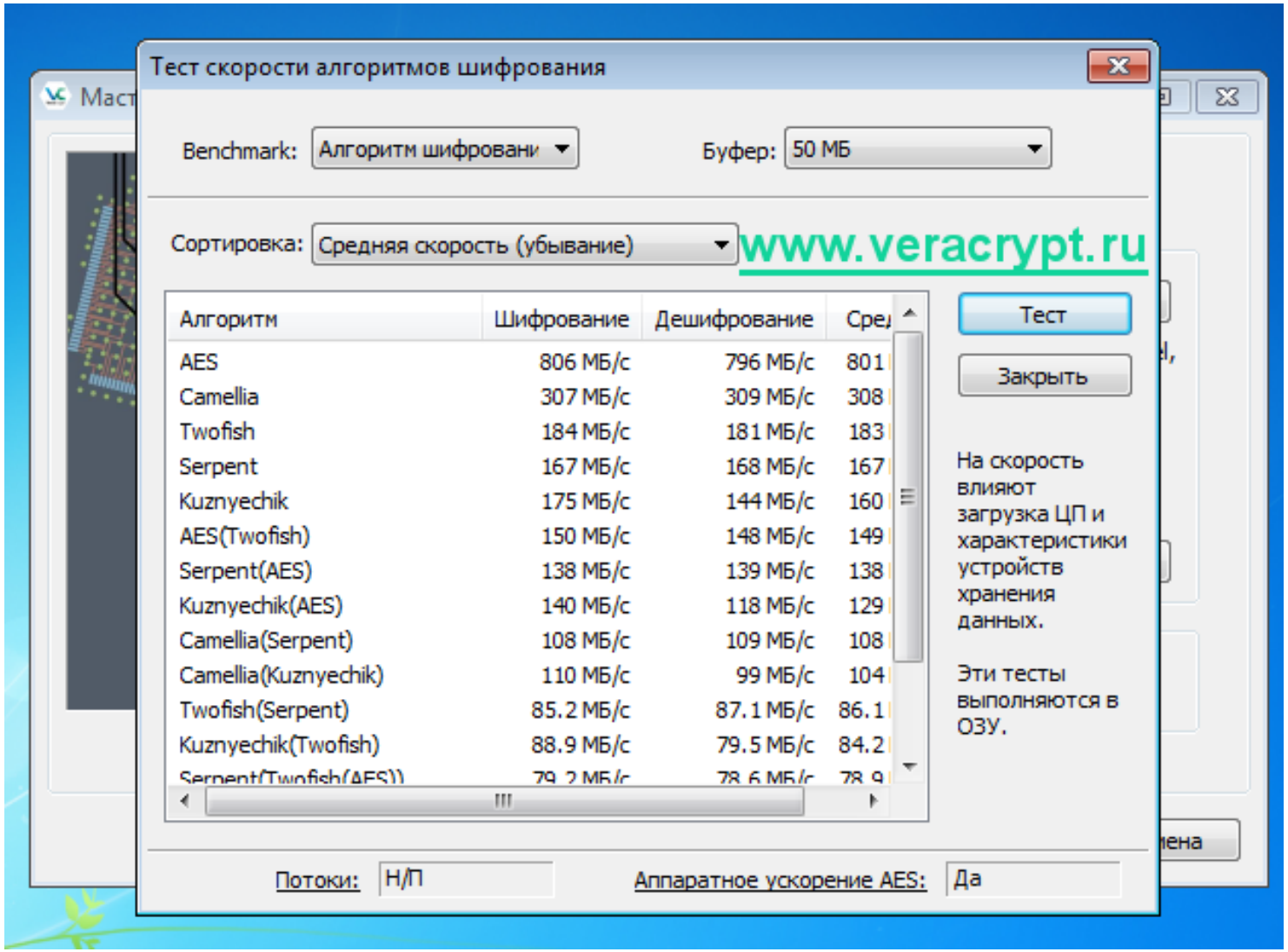
Выбор алгоритма шифрования и хеширования



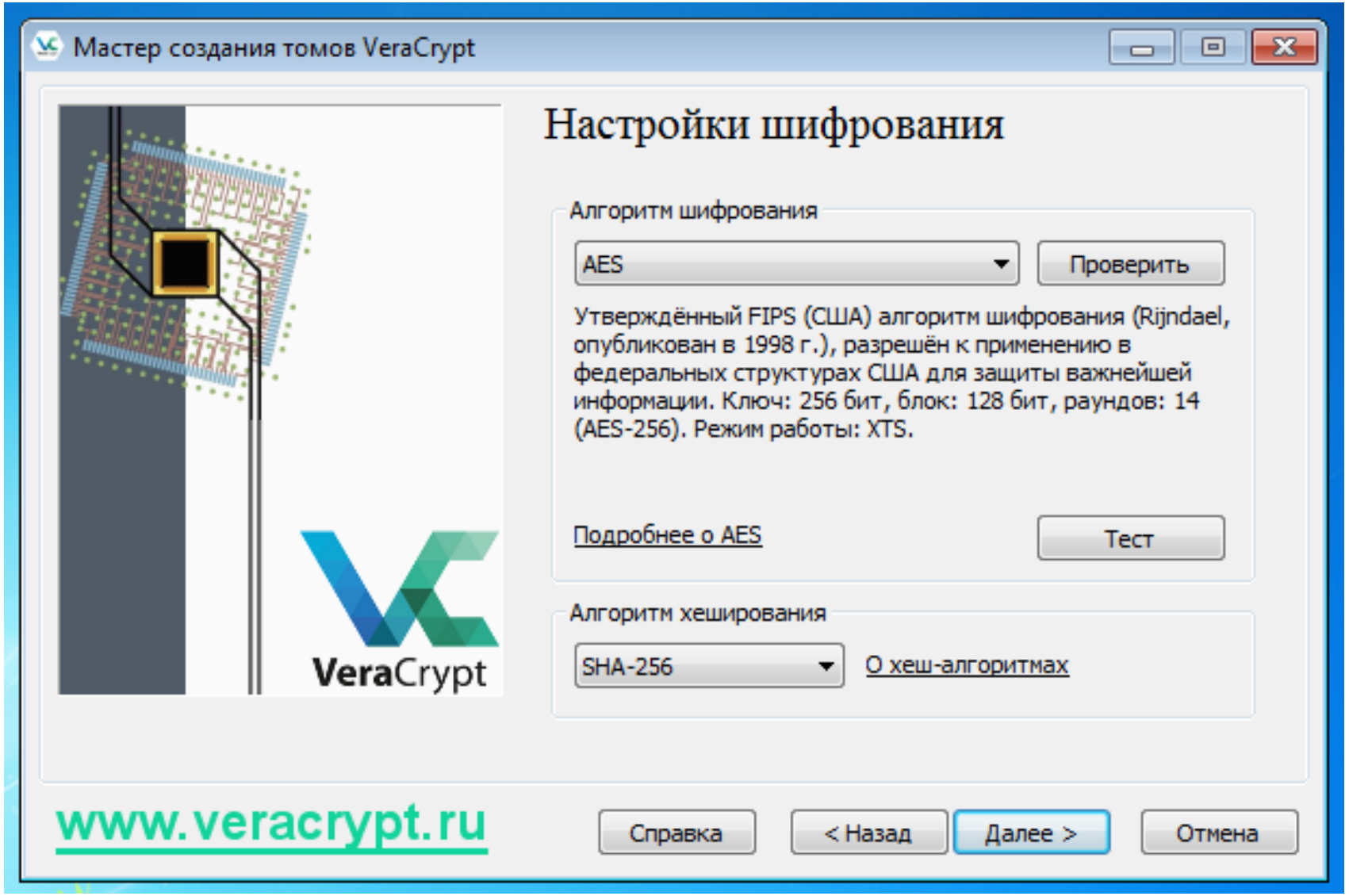
Сравнение производительности алгоритмов шифрования



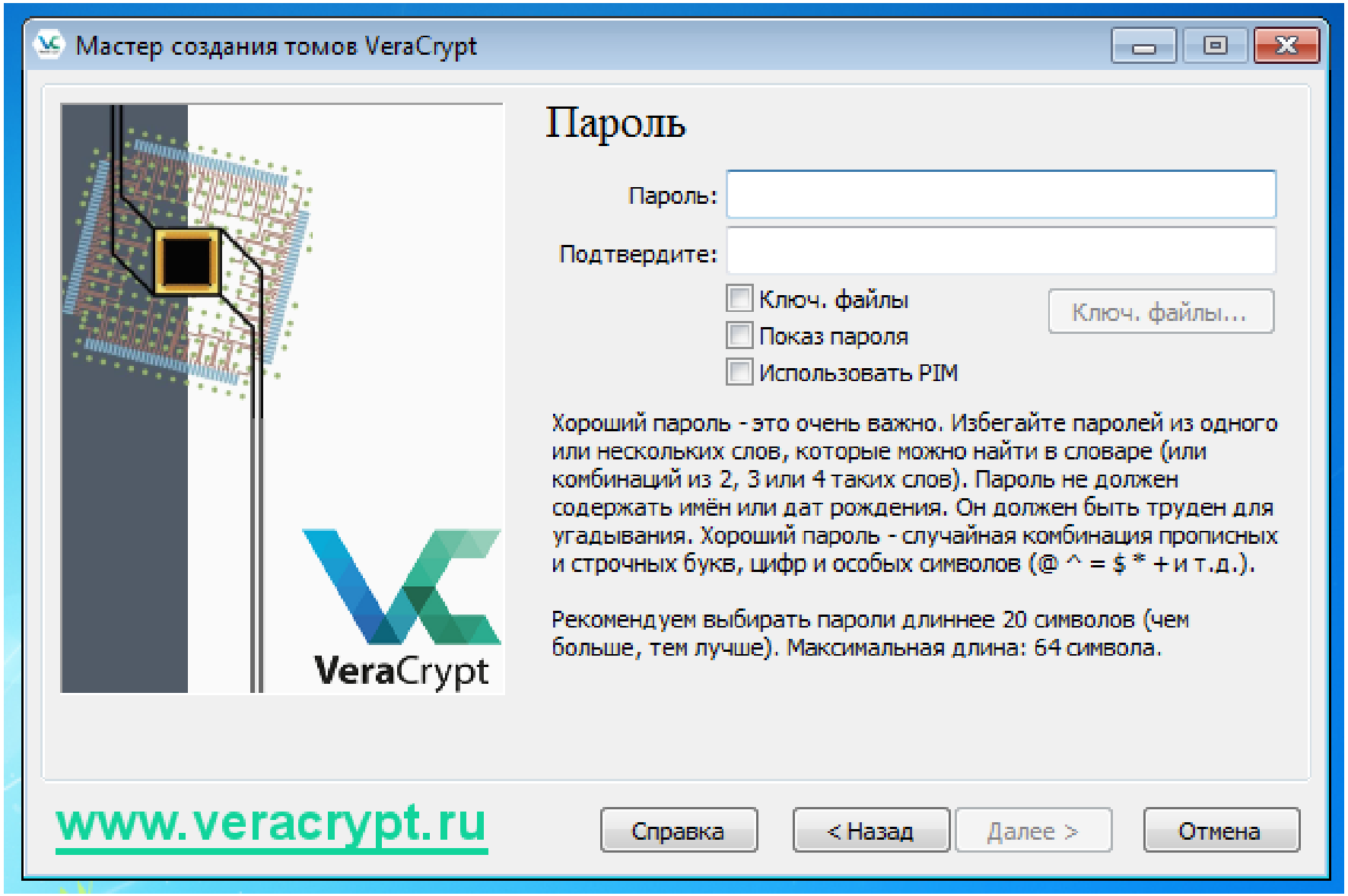
Тест производительности работы различных алгоритмов шифрования



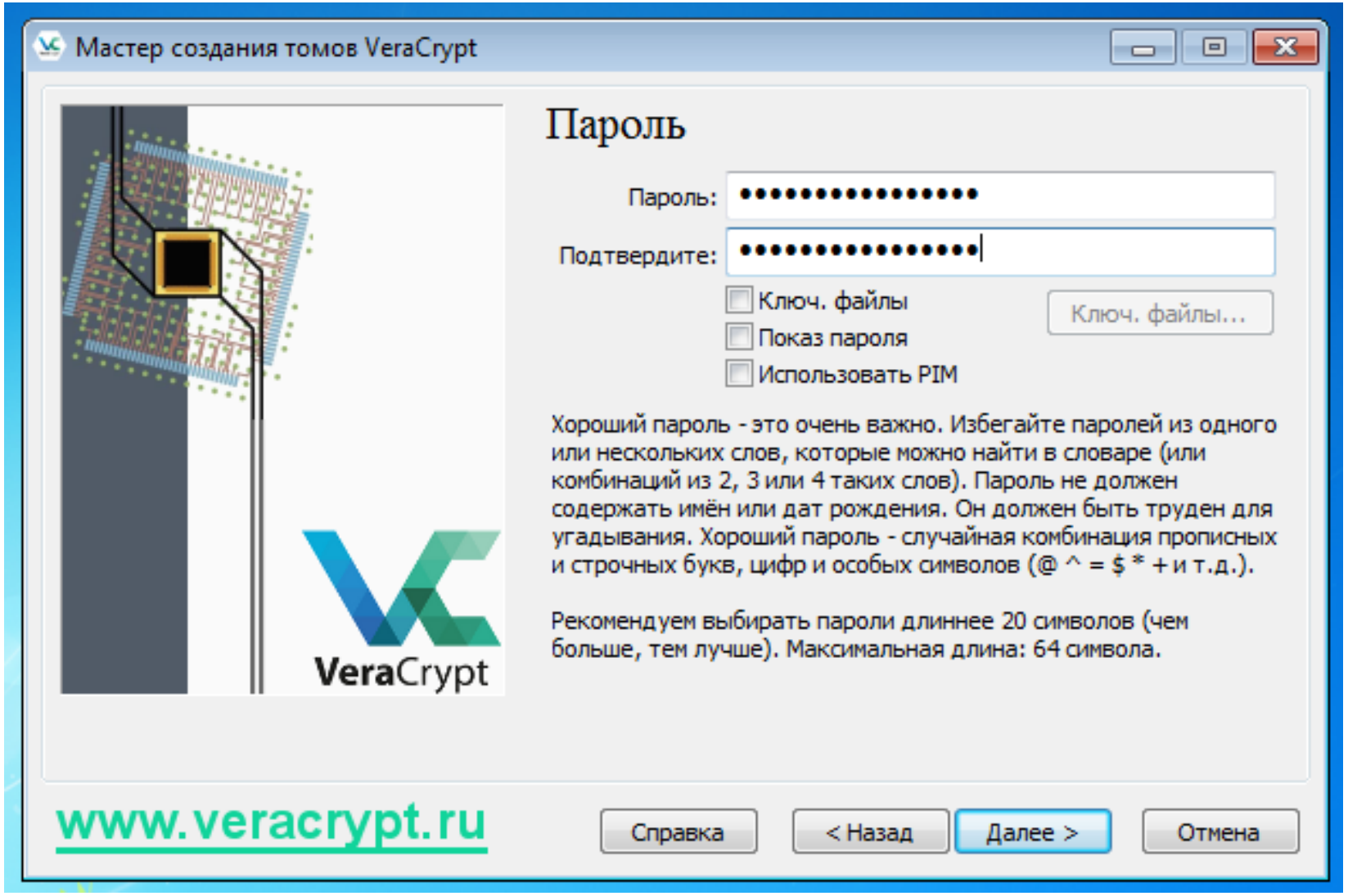
Определившись с алгоритмом шифрования и алгоритмом хеширования, нажмите «Далее»



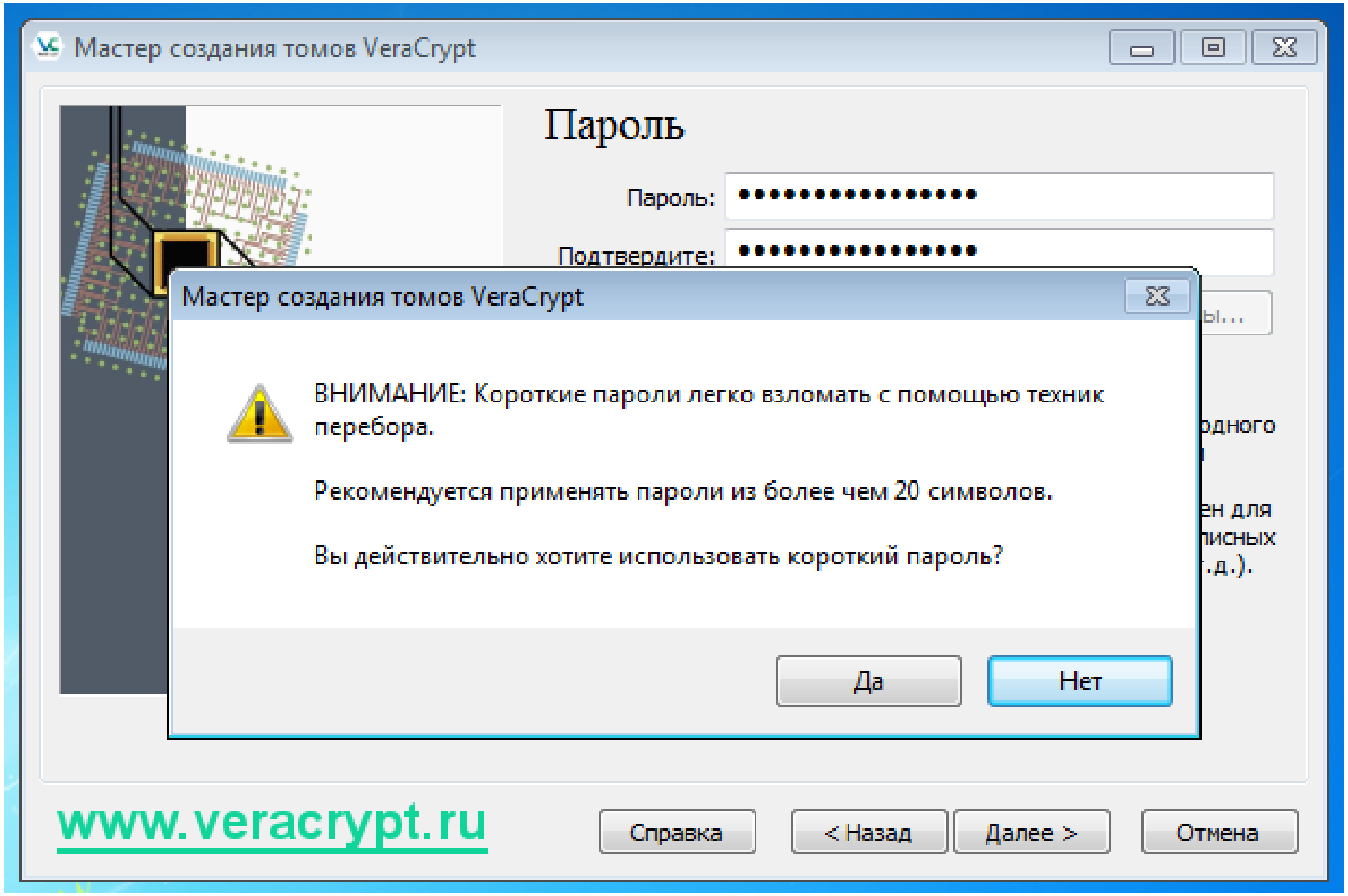
Установка пароля дешифрования



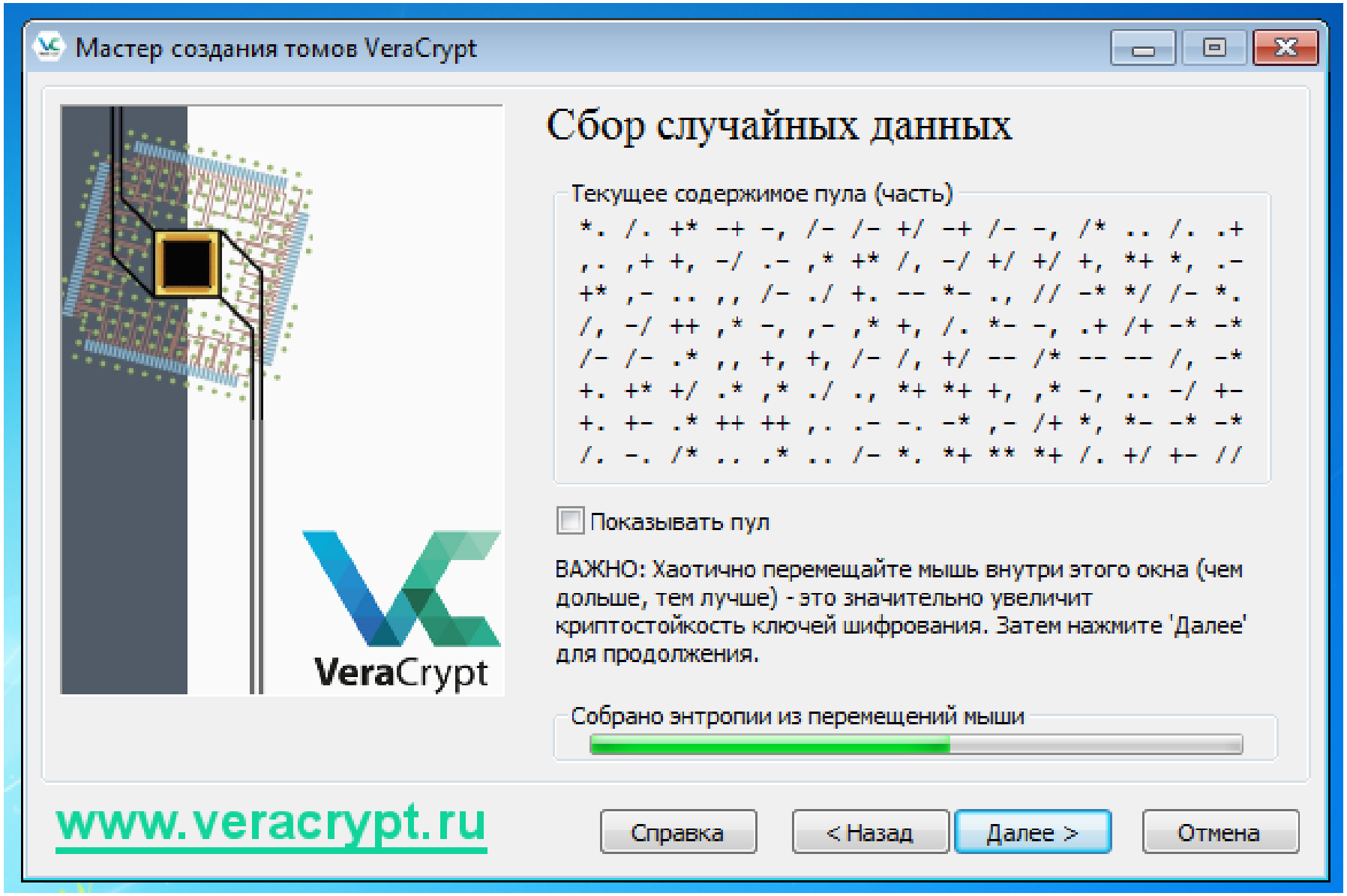
После того, как вы определились с паролем, нажмите кнопку «Далее»



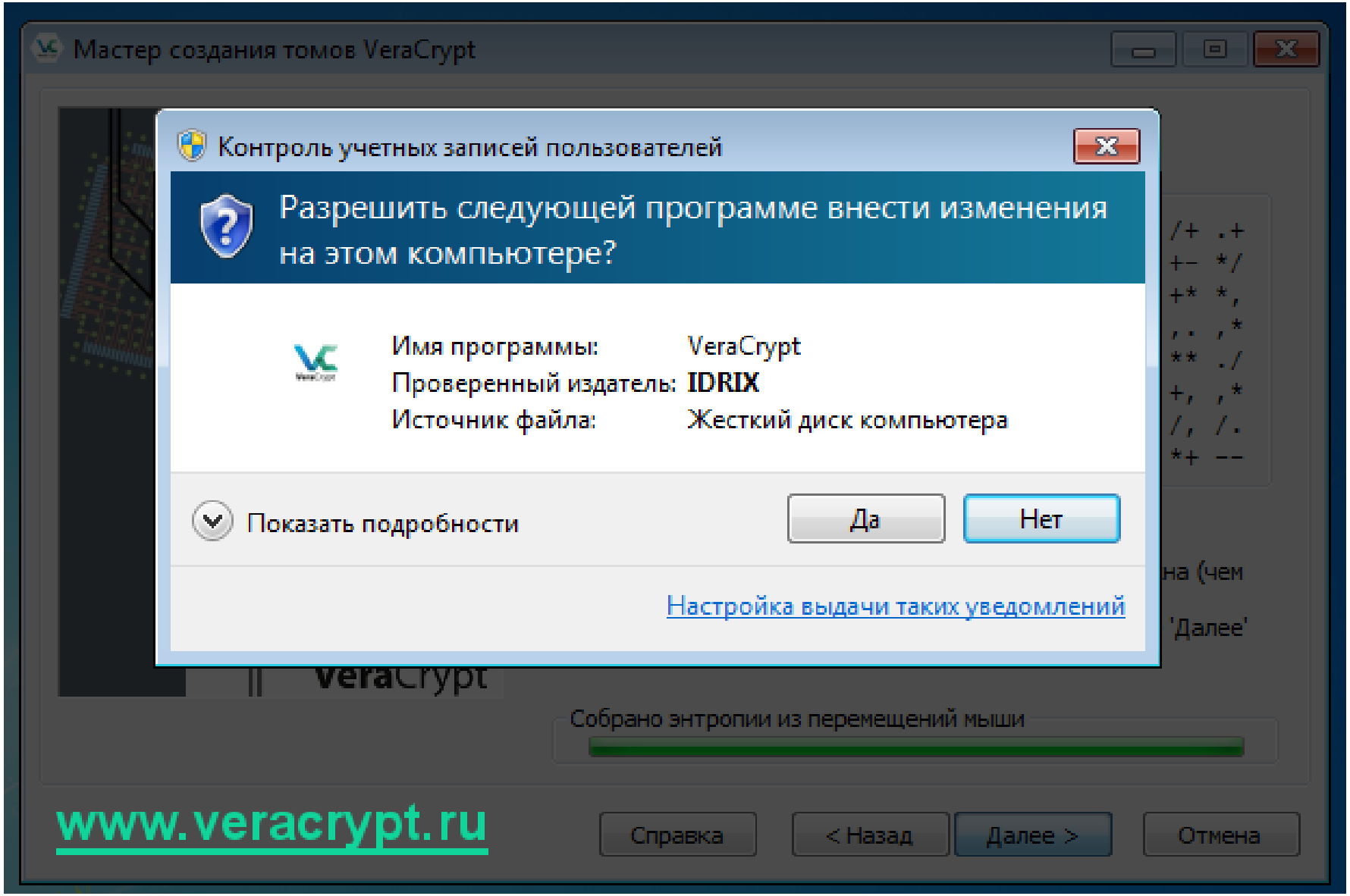
Короткие пароли легко взломать



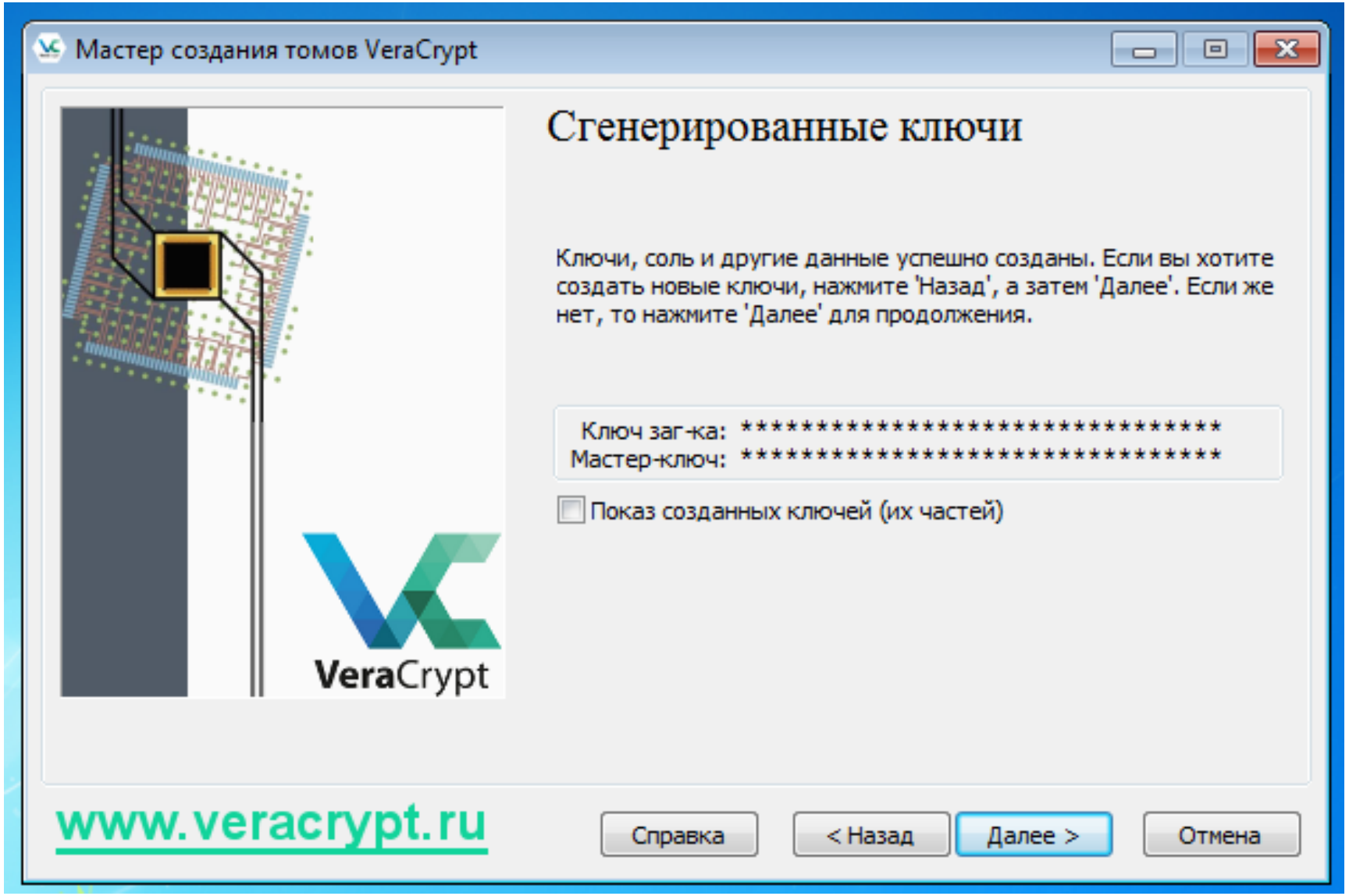
Генерация случайных данных



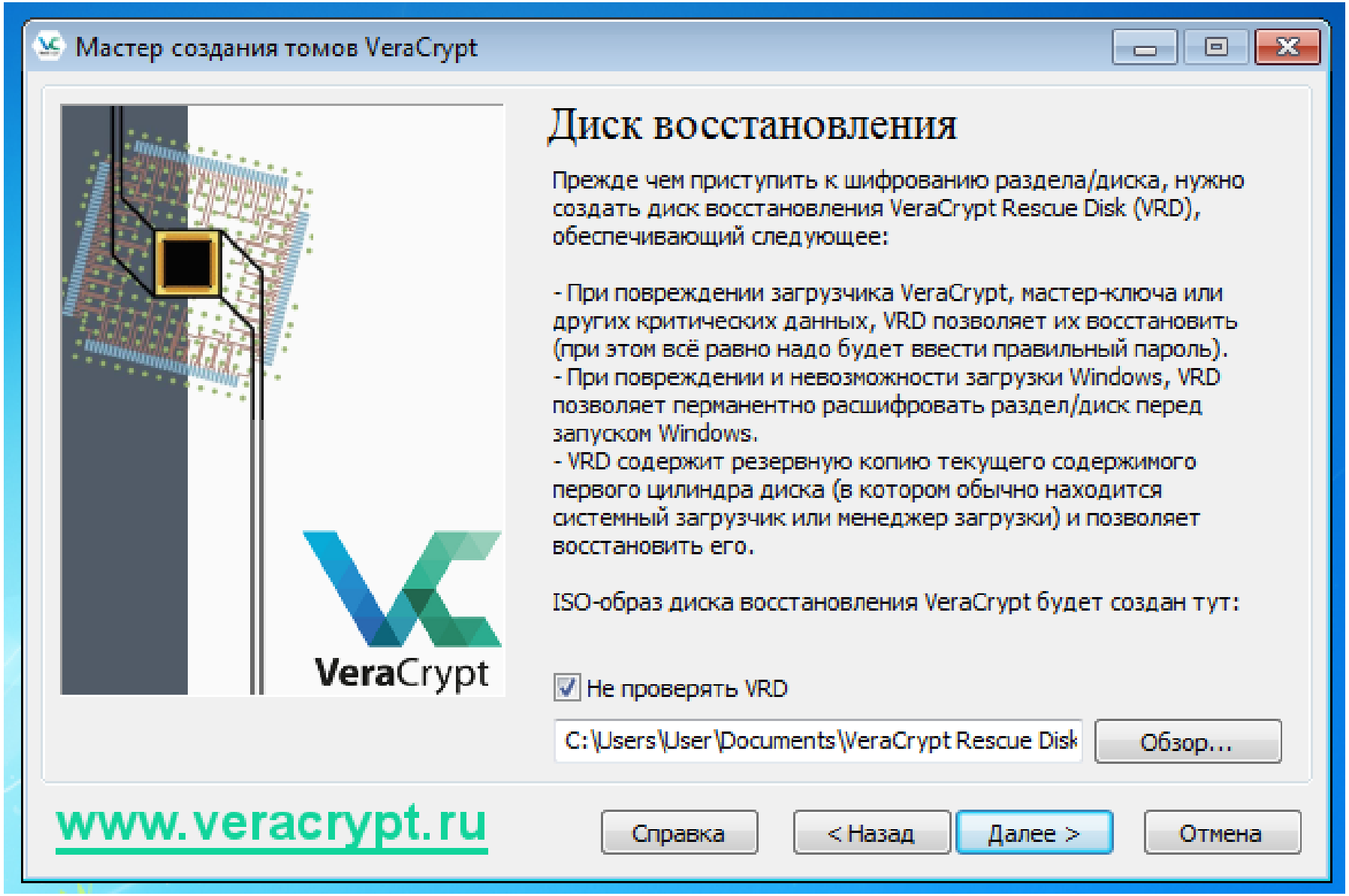
Далее VeraCrypt запишет свой загрузчик на системный диск Windows. Подтвердите данное действие.



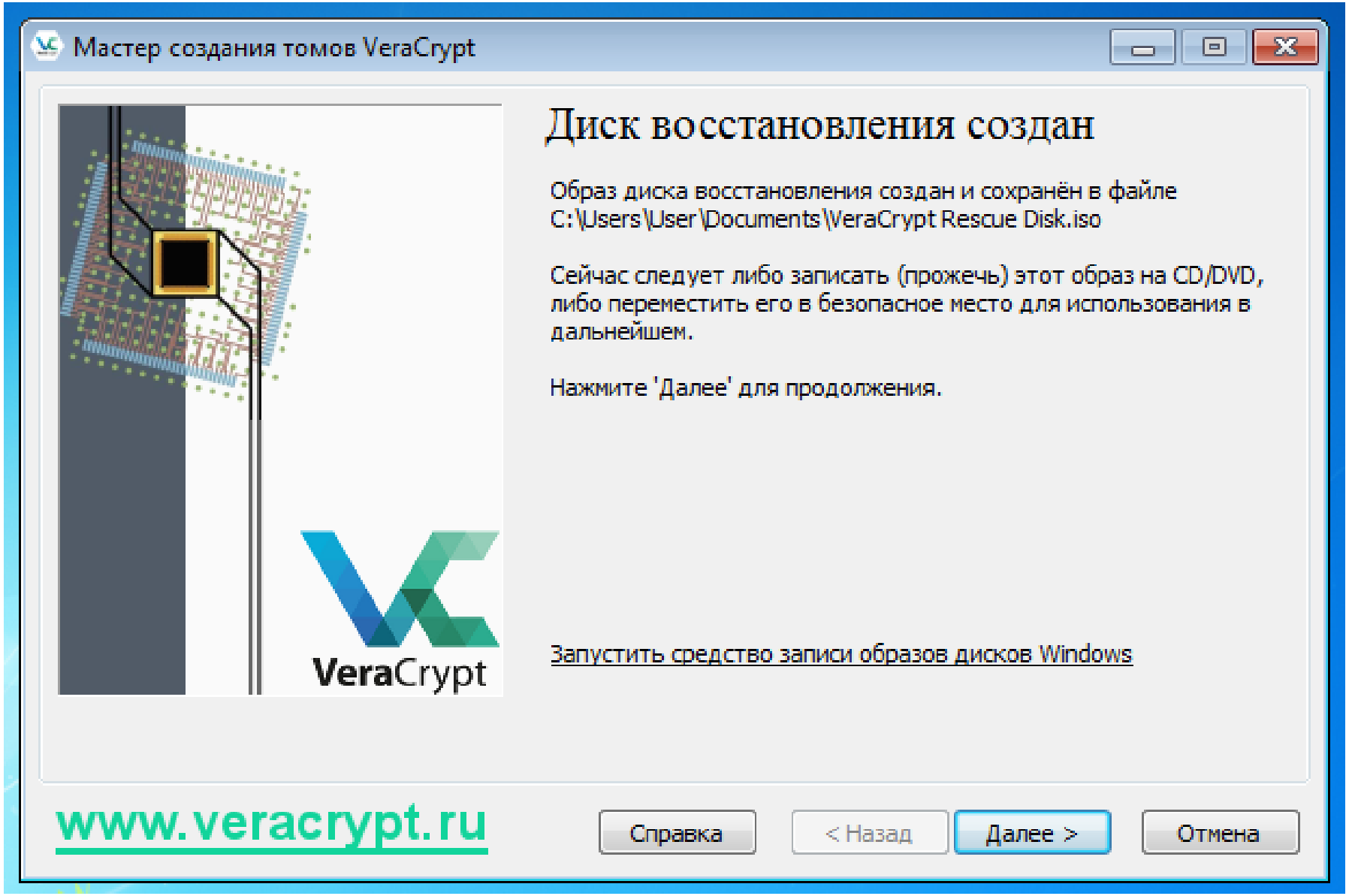
После этого VeraCrypt подтвердит, что успешно сгенерировались ключи. Нажмите «Далее».



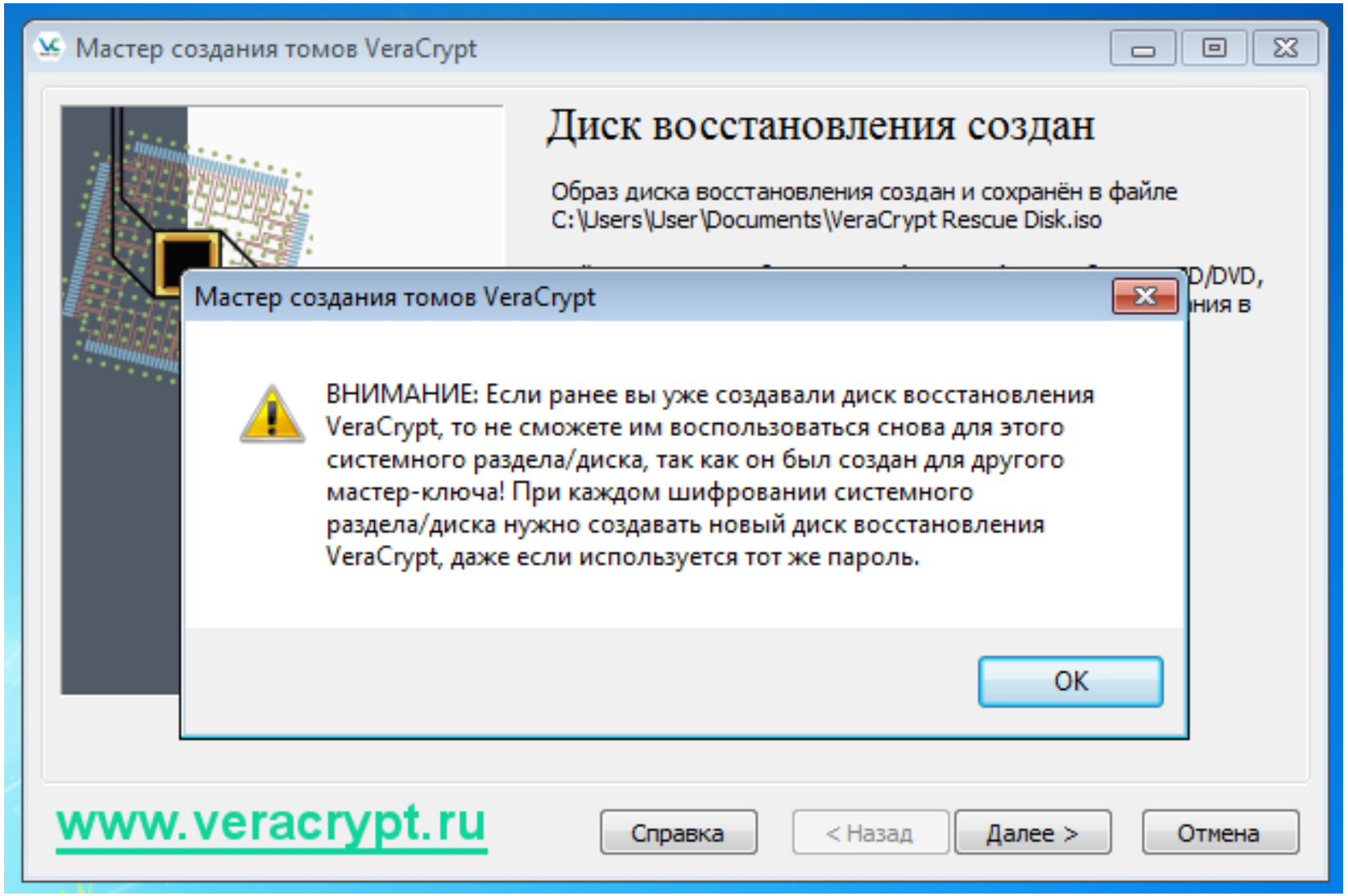
Диск восстановления VeraCrypt



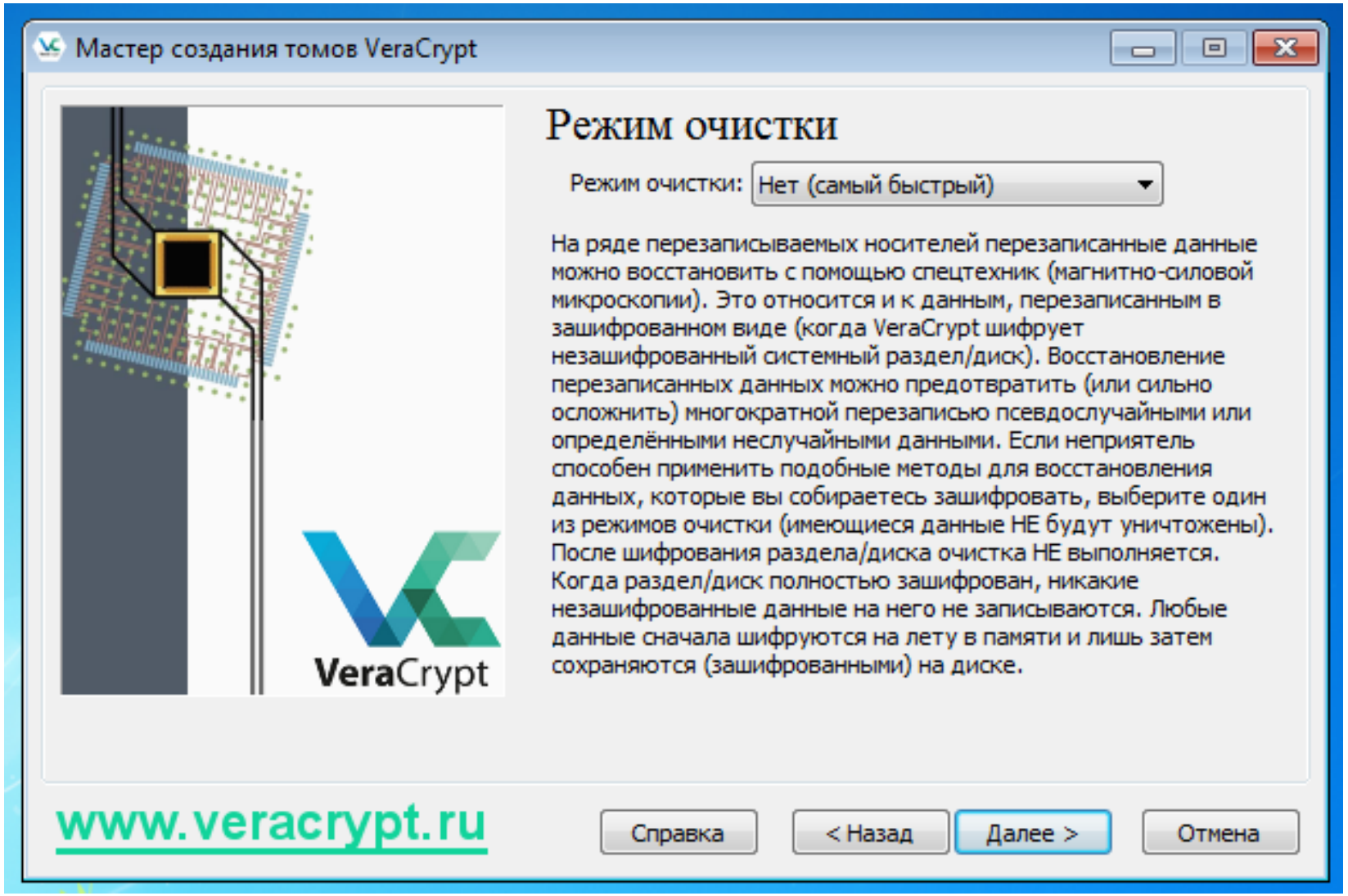
Диск восстановления VeraCrypt создан



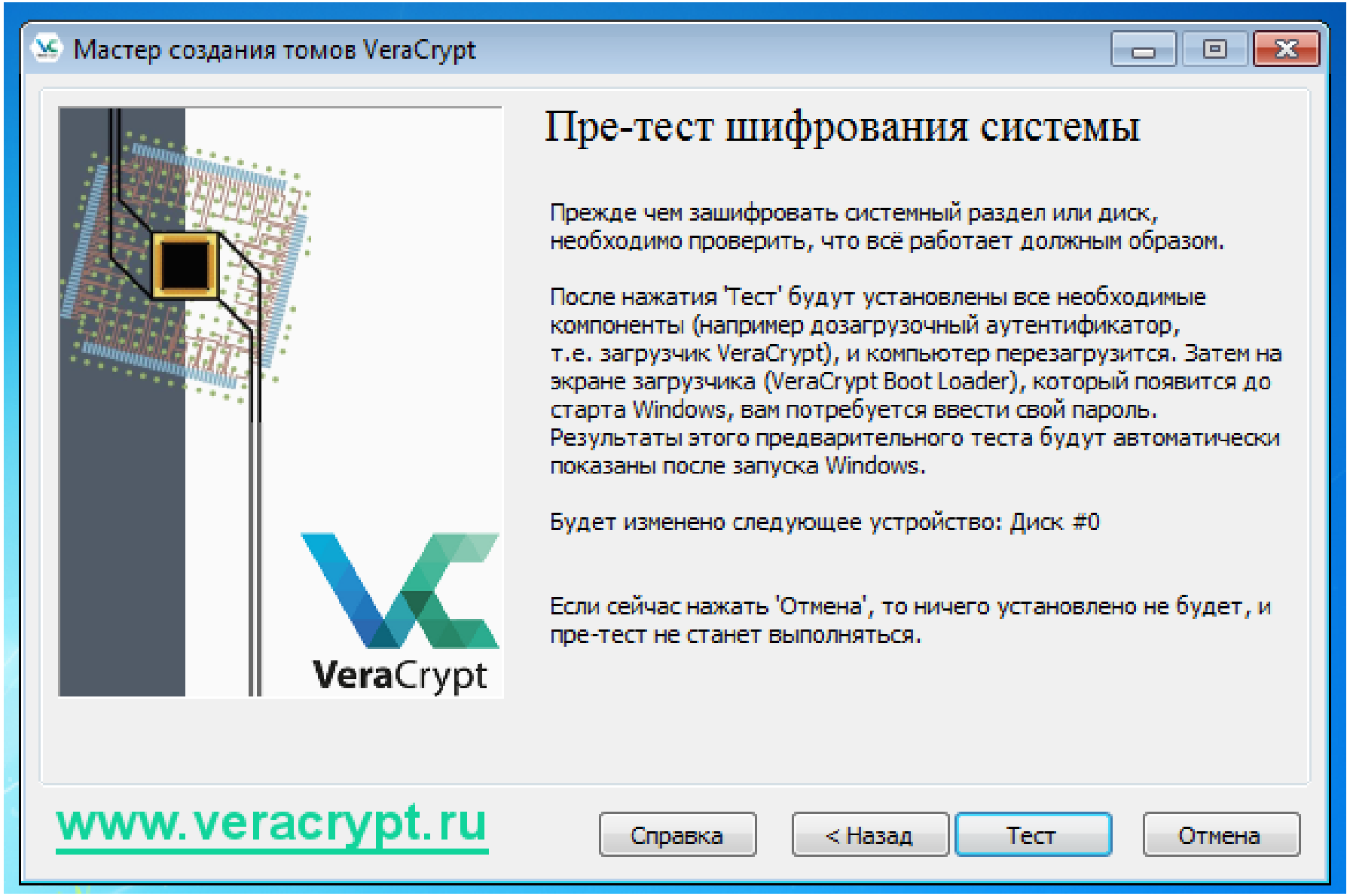
Теперь может использоваться только самый новый диск восстановления



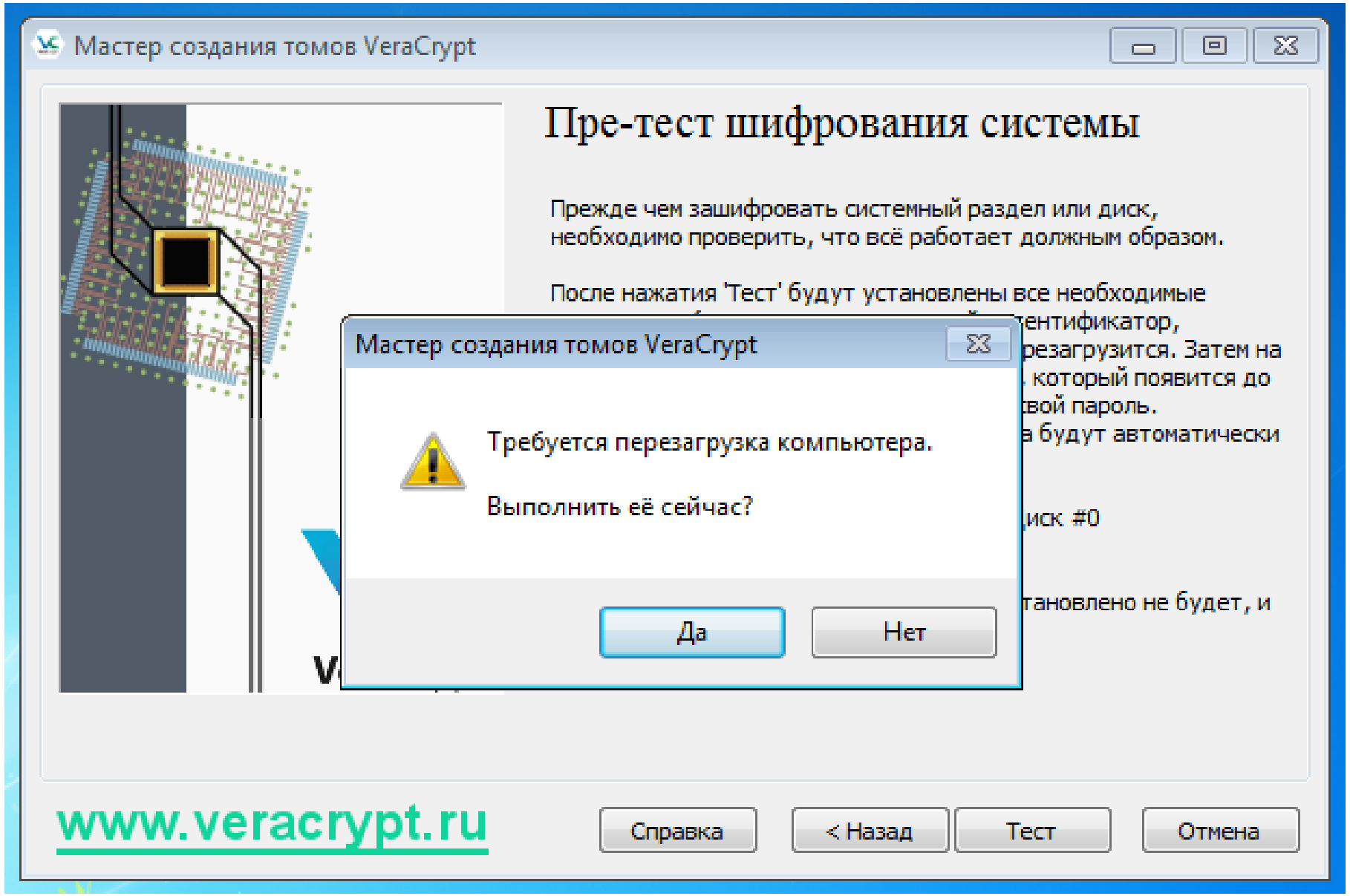
Режим очистки системного диска.
В большинстве же случаев вам не нужно указывать очистку и вы сможете сэкономить много времени.



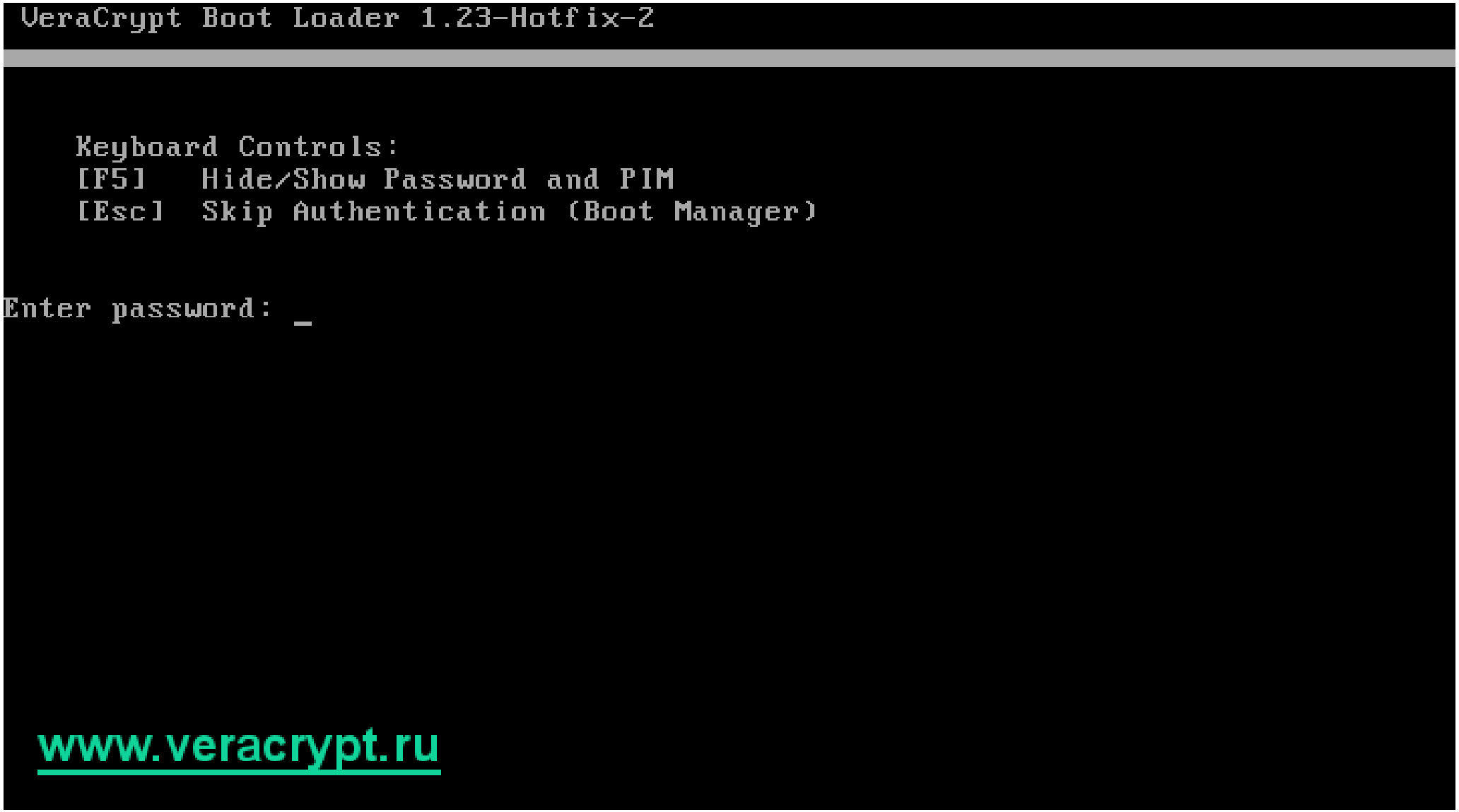
Пре-тест шифрования данных



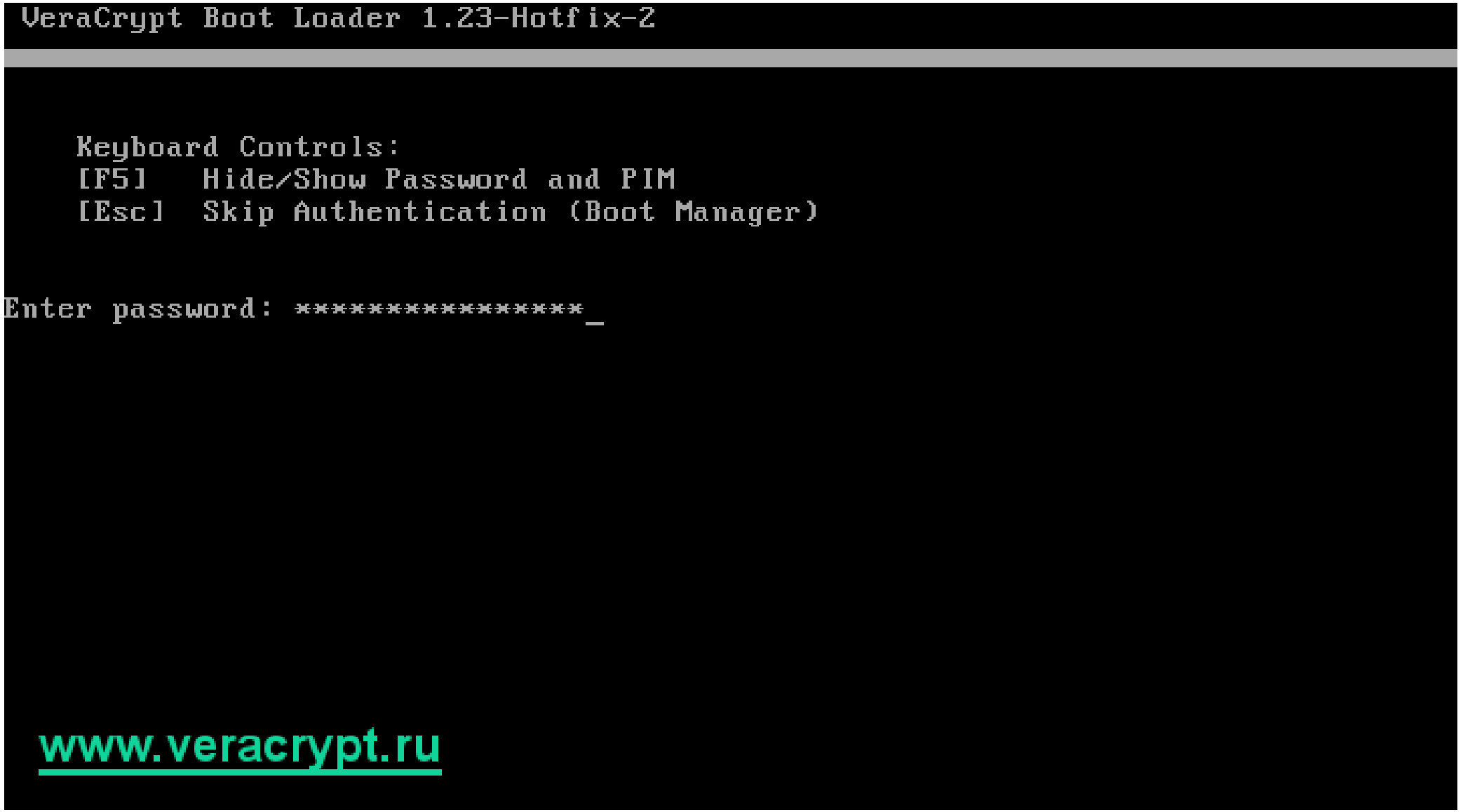
Последнее подтверждение перед перезагрузкой.



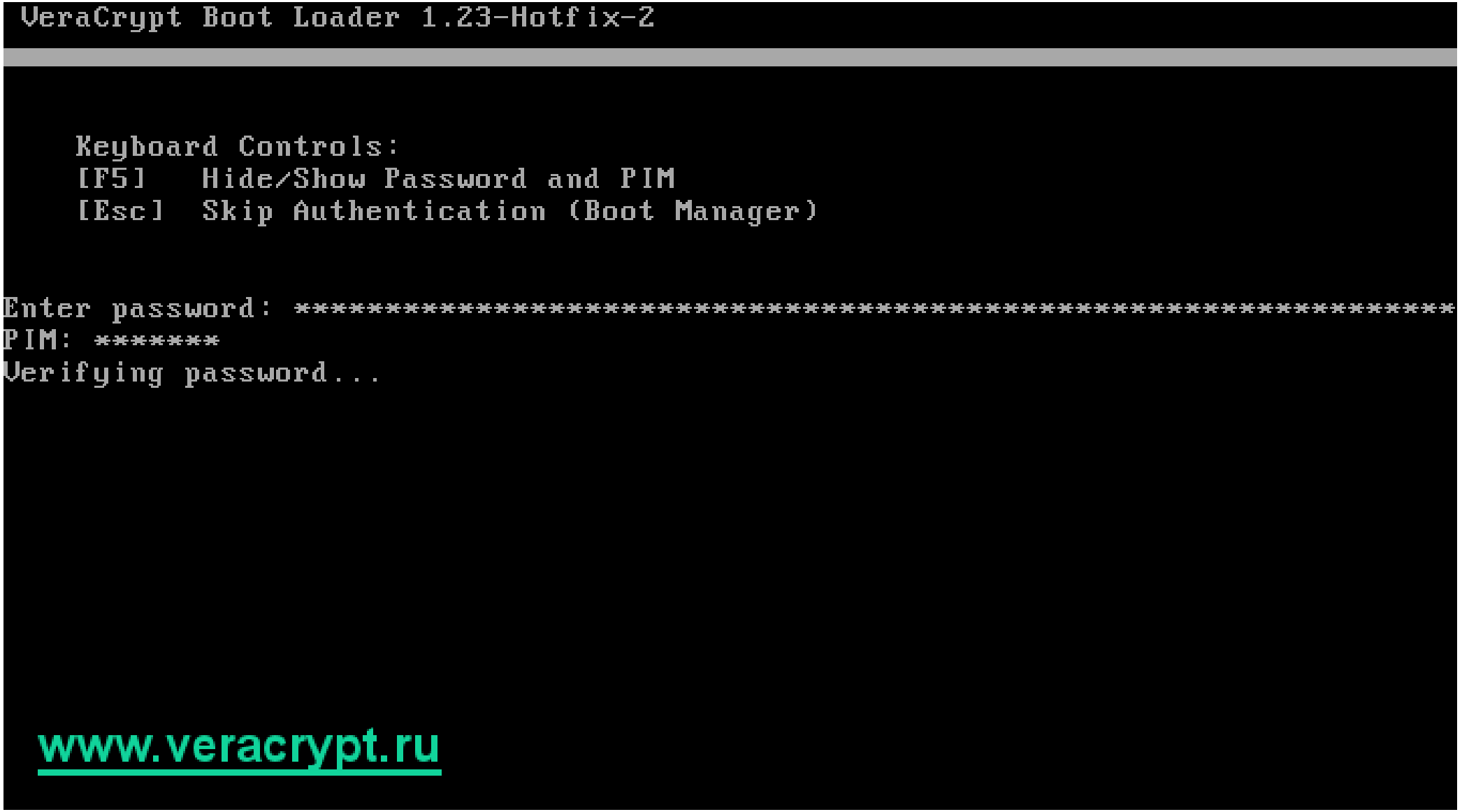
После того, как ваш компьютер перезагрузится, вы увидите интерфейс загрузчика VeraCrypt. Введите свой пароль для расшифровки



Укажите свой пароль для VeraCrypt

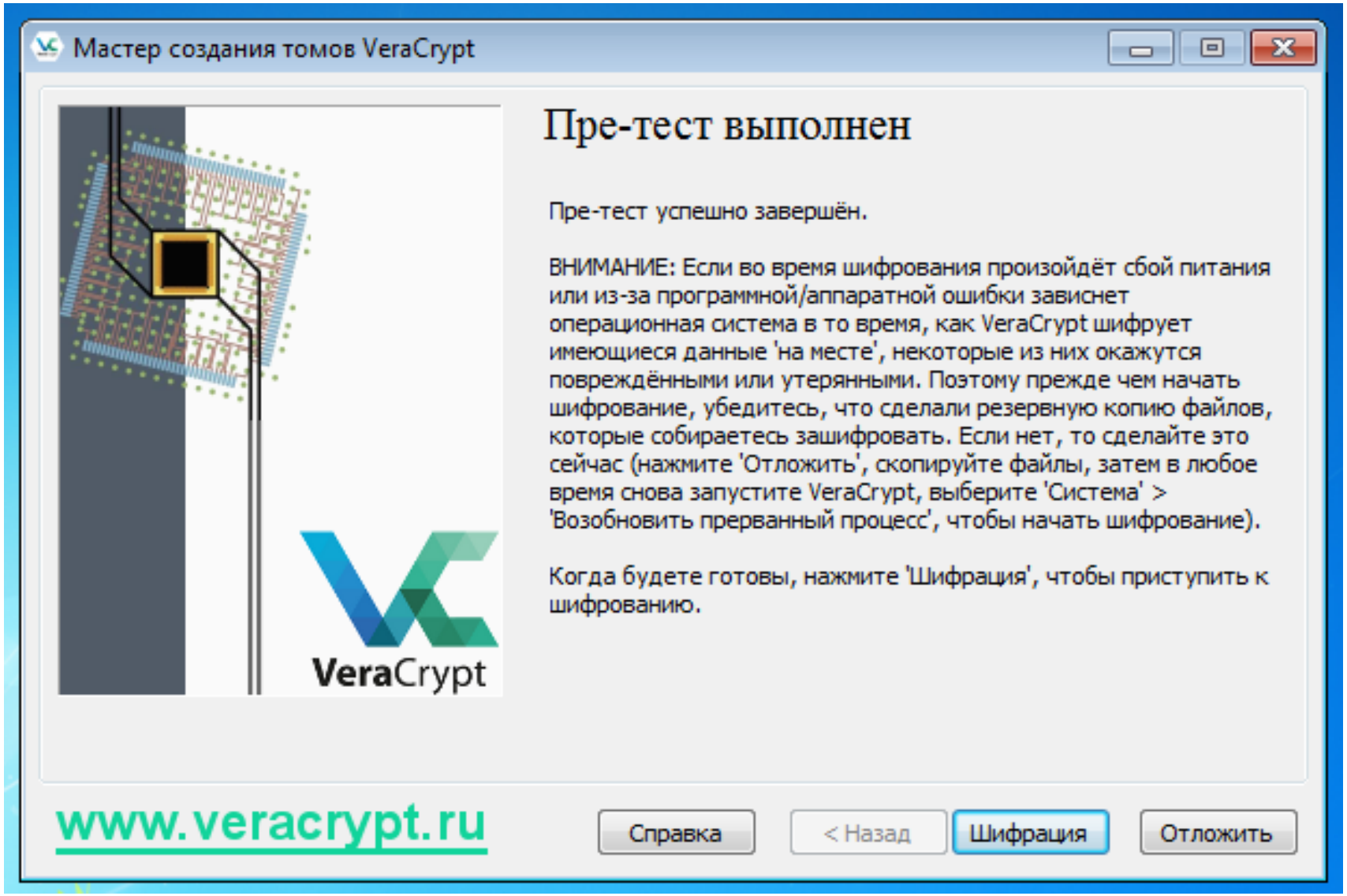


Проверка пароля

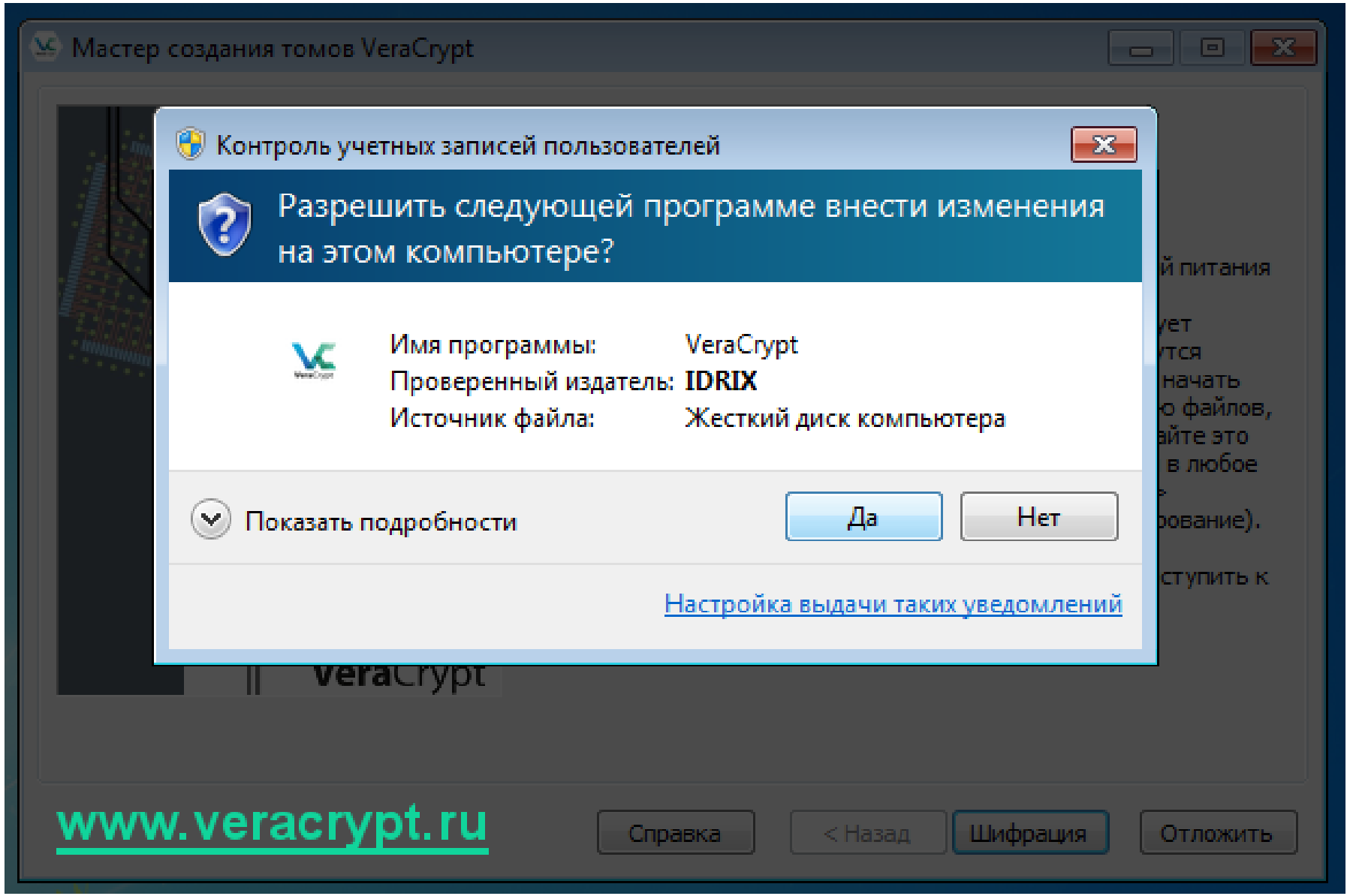


Пароль введён успешно, загрузка Windows началась

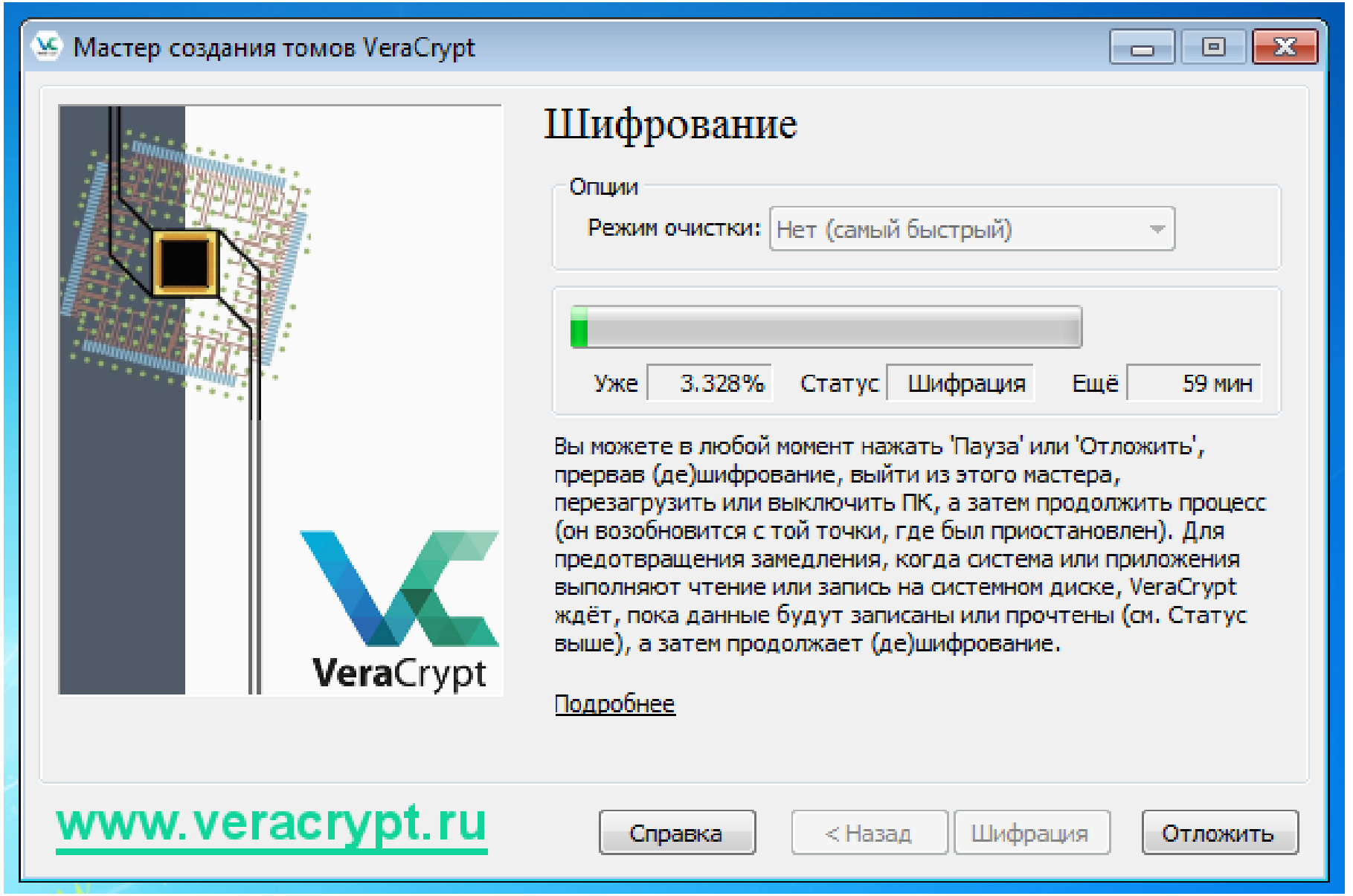
Нажмите кнопку «Шифрация» для старта шифрования всех данных на системном диске



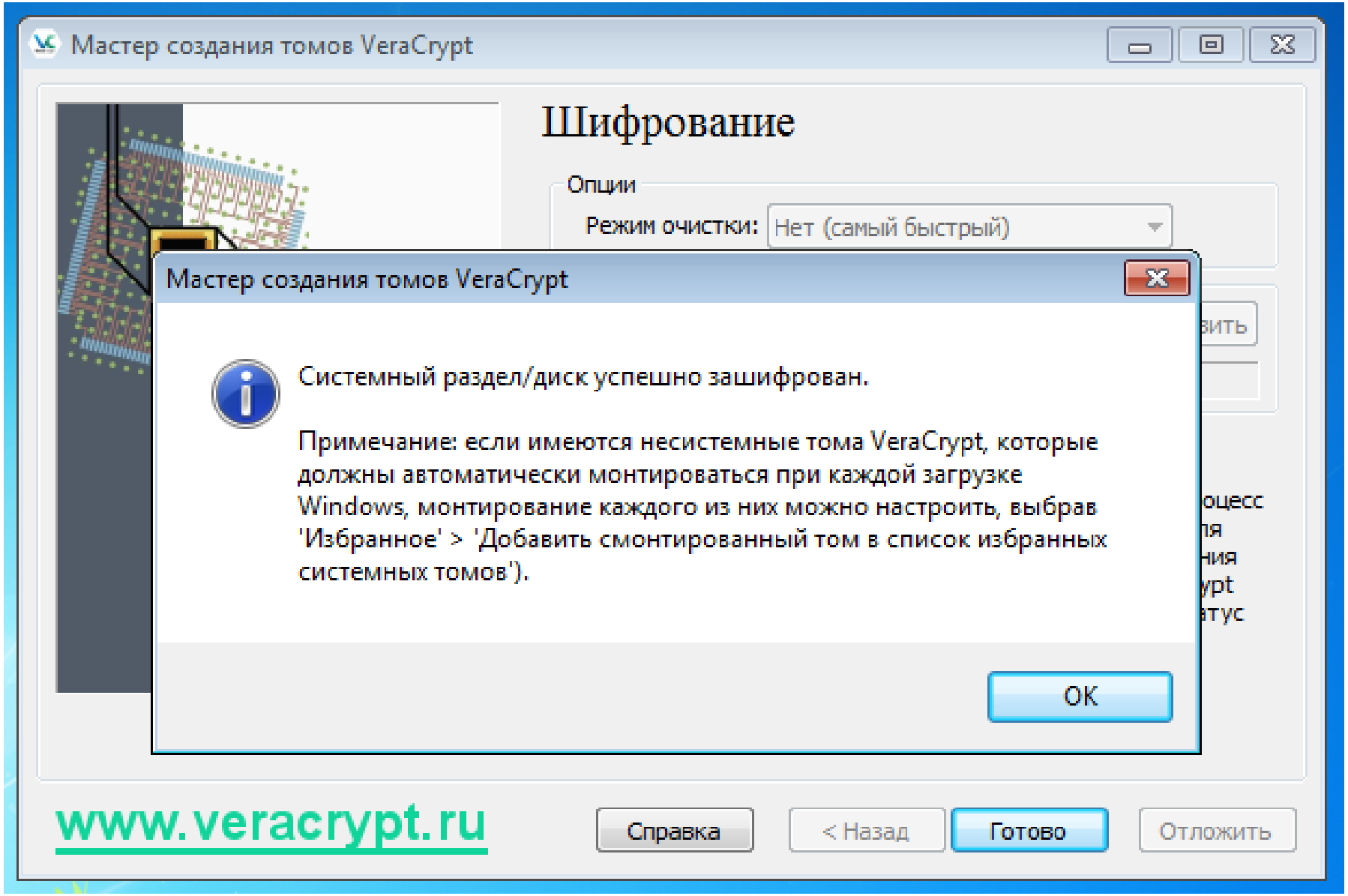
Начало шифрования данных на системном диске



Шифрование началось!



Системный диск успешно зашифрован!



Защита информации

Тема: Криптография. Применение криптографических средств защиты информации

Благодарю за внимание

КУТУЗОВ Виктор Владимирович

Белорусско-Российский университет, Кафедра «Программное обеспечение информационных технологий»
Республика Беларусь, Могилев, 2024

Список использованных источников

1. Рабочая программа дисциплины «Защита информации» / Кутузов В.В. – Могилев : Белорусско-Российский университет, 2019
2. Фотографии и картинки взяты с сайтов Яндекс.Картинки и Гугл.Картинки, иконки с flaticon.com
3. Защита информации : учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. — 3-е изд. — Москва : РИОР : ИНФРА-М, 2021. — 400 с. — (Высшее образование). — DOI: https://doi.org/10.12737/1759-3. - ISBN 978-5-369-01759-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/1210523
4. Криптография и защищённая связь: история первых шифров https://habr.com/ru/post/321338/
5. История криптографии https://ru.wikipedia.org/wiki/История_криптографии
6. 1 Лекция. Криптография с симметричными ключами https://moodle.kstu.ru/mod/page/view.php?id=10120
7. Основы криптографии https://crypto.rosatom.ru/upload/iblock/7c5/7c5e6c8f01fcf1401b800df7d6d09af9.pdf
8. Виды симметричных шифров https://ru.wikipedia.org/wiki/Симметричные_криптосистемы
9. Шифр Цезаря http://ru.wikipedia.org/wiki/Шифр_Цезаря
10. Шифр Виженера http://ru.wikipedia.org/wiki/Шифр_Виженера

Список использованных источников

11. Шифр Вернама (одноразовые блокноты)
    http://ru.wikipedia.org/wiki/Одноразовый_блокнот
12. Поточные шифры
    http://ru.wikipedia.org/wiki/Поточный_шифр
13. Алгоритм XOR
    https://ru.abcdef.wiki/wiki/XOR_cipher
14. Блочные шифры
    http://ru.wikipedia.org/wiki/Блочный_шифр
15. DES (Data Encryption Standard)
    http://ru.wikipedia.org/wiki/DES
16. Шифрование по ГОСТ 28147
    https://ru.wikipedia.org/wiki/ГОСТ_28147-89
17. AES / Rijndael
    https://ru.wikipedia.org/wiki/Advanced_Encryption_Standard
18. Криптография с асимметричными ключами
    https://ru.wikipedia.org/wiki/Криптосистема_с_открытым_ключом
19. Алгоритм RSA
    http://ru.wikipedia.org/wiki/RSA
20. Алгоритм Диффи — Хеллмана
    http://ru.wikipedia.org/wiki/Алгоритм_Диффи-Хеллмана

Список использованных источников

21. Аудит СКЗИ и криптоключей
https://habr.com/ru/post/280131/

22. ОАЦ РБ > Техническая и криптографическая защита информации > Средства защиты информации > Общие сведения
https://oac.gov.by/activity/information-security-tools/technical-and-cryptographic-information-protection/general-information

23. 2 Лекция. СКЗИ с симметричными ключами.
https://moodle.kstu.ru/mod/page/view.php?id=10121

24. Симметричное шифрование
https://encyclopedia.kaspersky.ru/glossary/symmetric-encryption/

25. Симметричное распределение ключей
http://ru.wikipedia.org/wiki/Симметричные_криптосистемы

26. 5 Лекция. СКЗИ с асимметричными ключами. ИОК (PKI). OSCP.
https://moodle.kstu.ru/mod/page/view.php?id=10124

27. Центр сертификации
https://ru.wikipedia.org/wiki/Центр_сертификации
https://ru.abcdef.wiki/wiki/Certificate_authority

28. X.509
http://ru.wikipedia.org/wiki/X.509

29. Электронная подпись
https://ru.wikipedia.org/wiki/Электронная_подпись

Список использованных источников

30. Что такое СКЗИ, и какие они бывают
https://tensor.ru/uc/ep/skzi

31. Comparison of disk encryption software
https://en.wikipedia.org/wiki/Comparison_of_disk_encryption_software

32. Скрытые возможности Windows. Как BitLocker поможет защитить данные?
https://habr.com/ru/company/aktiv-company/blog/335532/

33. Encrypting File System
https://ru.wikipedia.org/wiki/Encrypting_File_System

34. VeraCrypt – бесплатное ПО для шифрования файлов «на лету».
https://veracrypt.fr/code/VeraCrypt/
https://veracrypt.fr/en/Downloads.html

35. BestCrypt
http://www.jetico.com/
https://www.jetico.com/data-encryption/encrypt-files-bestcrypt-container-encryption

36. Пролубников, А. В. Криптографические средства защиты информации в сетях : учебно-методическое пособие / А. В. Пролубников. – 2-е изд., испр. – Омск : Изд-во Ом. гос. ун-та, 2015. – 190 с. ISBN 978-5-7779-1899-4
http://pozi.omsu.ru/docs/docs/security.pdf

37. VeraCrypt – Полное шифрование системного диска Windows 7
https://veracrypt.ru/veracrypt-polnoe-shifrovanie-sistemnogo-diska-windows-7/